Council of the European Union

Brussels, 20 September 2018
(OR. en)

12336/18

Interinstitutional File:
2017/0003(COD)

TELECOM 297
COMPET 612
MI 646
DATAPROTECT 184
CONSOM 259
JAI 899
DIGIT 177
FREMP 149
CYBER 200
CODEC 1502

NOTE

From:	Presidency
To:	Delegations
No. Cion doc.:	5358/17 TELECOM 12 COMPET 32 MI 45 DATAPROTECT 4 CONSOM 19 JAI 40 DIGIT 10 FREMP 3 CYBER 10 IA 12 CODEC 52
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) - Examination of the Presidency text

For the purpose of discussion in the WP TELE meeting of 27 September, delegations will find in Annex a revised text of the ePrivacy proposal (ePR). For ease of reference, the latest changes to the text in Annex are underlined.

With a view to advance this dossier, the Presidency had introduced, in the latest Presidency compromise text (10975/18), significant changes to articles 6 and 10 and raised certain policy/legal issues for article 8. The discussions in the WP TELE on 17 July and the written comments provided by MSs demonstrated quite diverging views among delegations on those core issues.

Moreover, delegations raised many other fundamental questions in relation to this file, such as:

- Precise scope of the regulation and delineation to the GDPR
- Problematic mixture of the fundamental rights of confidentiality on the one hand and data protection on the other hand
- Level playing field - Treatment of GPS location data
- How does the tight frame of the e-privacy fit together with the European goals for pushing developments in fields like AI, IoT and automated driving?

The Presidency has therefore decided to stick, for the time being, to the principle approach outlined in doc. 10975/18 and would like to ask delegations for further guidance, including concrete drafting suggestions, for the most crucial issues. At the same time, the Presidency has already tried to accommodate some of the concerns raised by delegations, as outlined below.

1. Permitted processing (article 6)

a. Further processing

The latest compromise text introduced more flexibility in the proposal by including a possibility for further compatible processing of electronic communications metadata. Although there was significant support for this direction of the text, some MSs strongly argued for an even more flexible approach - bearing in mind the likely development of the text during the inter-institutional negotiations - while other MSs clearly rejected the concept as being too broad.

The Presidency would like to invite delegations to indicate which of the following options they could support, if possible also including concrete drafting suggestions:

Option 1: elaborating the Presidency approach on further processing of electronic metadata with the aim of tightening the concept of further processing by including additional safeguards, or

Option 2: elaborating the Presidency approach with the aim of including further flexibility in the concept of further processing, e.g. by aligning the text closer to the GDPR.

b. Modifications to article 6

Following the discussion in the WP TELE and based on the delegations' written comments, the Presidency has introduced the following modifications in article 6:

- art. 6(2)(a): the word 'mandatory' has been replaced with 'technical' in order to allow traffic management permissible under the TSM Regulation (which does not have any mandatory quality of service requirements);

- changes in **art. 6(2)(b)** are meant to take into account that the activities in question can take place without being necessarily linked to the performance of the contract;

- **art. 6(2)(f)**: the word 'counting' has been replaced with 'purposes' to ensure better alignment with the GDPR wording;

- in **art. 6(2a)(c)** the reference to art. 10 of GDPR was included, again, to ensure coherence with the GDPR;

- **rec. 16**: the Presidency has introduced a clarification that permitted security measures should be performed in a least intrusive manner;

- minor linguistic modifications were made in **art. 6(2aa)(d)** and **6(3)(aa)**.

2. Protection of end-users' terminal equipment information (article 8)

a. Conditional access to website content

The Presidency would like to continue the discussion on conditional access to website content that is currently addressed in recital 20. During the discussion on 17 July, a number of MSs had a positive view on the text in the recital and some of them would even wish to address this issue in articles. Others were not convinced, though, about the compatibility with the GDPR and the concept of 'freely given consent'.

At the WP TELE of 27 September, the Presidency would like to discuss possible solutions of this issue, including drafting suggestions tabled by some delegations.

b. Modifications to article 8

Following the discussion in the WP TELE and based on the delegations' written comments, the Presidency has introduced the following modification in article 8:

- **art. 8(1)(e)**: changes were included to cover situations where updates are not of purely security nature and therefore software providers would not be obliged to split security updates from other updates.

3. Clarification of scope in article 2 and recital 8

At the WP TELE of 17 July and/or in their written comments, a number of delegations requested further modifications in relation to **information security measures**, which should not be prohibited by the ePrivacy Regulation, and this not only for providers of electronic communications networks and services (art. 6(1)(b)) but also for end-users or third parties taking such measures on their behalf. In the Presidency's view, the latter category is not at all covered by the ePrivacy Regulation, which was already, to a certain extent, addressed in recital 8. However, the Presidency feels that further clarifications in this respect are necessary and considers that article 2 on the scope is the most appropriate place for doing so. A new **art. 2(2)(f)** has been therefore introduced in the proposal. In addition, explanations in **recital 8** have also been further developed.

Art. 2(2)(e) has been slightly amended to make it clearer which data are covered by this exemption.

At the WP TELE of 27 September, the Presidency would like delegations to indicate whether the introduced modifications adequately address their concerns.

_____

ANNEX

(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 include~~s~~ 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 as regards 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. The provisions particularise Regulation (EU) 2016/679 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. They 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. Insofar as end-users who are legal persons are concerned, provisions of Regulation (EU) 2016/679 should apply only 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 Council[1], 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.

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

~~(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 Council[2] 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.

(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 regarding activities concerning national security and defence.

[2] 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).

(8) This Regulation should apply to providers of electronic communications services, to providers of publicly available directories, and to ~~software~~ providers **of software** 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 ~~**or present**~~ 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.**

Some end-users, for example providers of payment services ~~providers and~~ or payment systems, process as recipients their electronic communications data for different purposes or ~~permit other~~ request a third parties to process their electronic communications data on their behalf. It is also important that end-users, including legal entities, have the possibility to take the necessary measures to secure their services, networks, employees and customers from security threats or incidents. Information security services may play an important role in ensuring the security of end-users' digital environment. ~~Such processing may include the processing by~~ For example, an end-user as an information society service provider~~, or another~~ may process its electronic communications data, or may request a third party, such as a provider of security technologies and services, to process that end-user's electronic communications data on its behalf, for purposes such as ensuring network and information security, including the prevention, monitoring and termination of fraud, unauthorised access and Distributed Denial of Service attacks, or facilitating efficient delivery of website content. Such processing of their electronic communications data by the end-users concerned, or by a third party requested by the end-users concerned to process their electronic communications data on their behalf, ~~is~~ should not be covered by this Regulation.

(8a) This Regulation does not apply to the electronic communications data of deceased persons. Member States may provide for rules regarding the processing of electronic communications data of deceased persons.

~~(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 Council[3]. 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.

[3] 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 of the European Parliament and of the Council establishing the European Electronic Communications Code[4]]. 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. **~~Services such as linear broadcasting, video on demand, websites, social networks, blogs, or exchange of information between machines, should not be considered as interpersonal communications services.~~**

[4] 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)).

(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 **ancillary** services ~~**also having a communication functionality**~~ should be covered by this Regulation. ~~**In such cases, this Regulation applies only to the ancillary feature itself and the electronic communications functionality it provides. To determine whether an electronic communications functionality constitutes an ancillary feature, the end-users expectations have to be taken into account. For example such communications functionality is considered to be ancillary feature in**~~

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 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. While the services provided at the application-layer of such services do normally not qualify as an electronic communications service as defined in the [Directive establishing the European Electronic Communications Code],** ~~T~~**t**he transmission **services used for the provision** of machine-to-machine ~~communications~~ **services regularly** involves the conveyance of signals ~~over~~ **via** a**n electronic communications** network and, hence, ~~usually~~ ~~**normally**~~ constitutes an electronic communications service. In order to ensure full protection of the rights to privacy and confidentiality of communications, and to promote a trusted and secure Internet of Things in the digital single market, it is necessary to clarify that this Regulation**, 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 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 electronic communications services and public communications networks. In contrast, this Regulation should not apply to closed groups of end-users such as corporate networks, access to which is limited **pre-defined group of end-users, e.g.** to members of the corporation**, courts, court administrations, financial, social and employment administrations**. **Therefore, only networks proving access to a group of end-users which is not pre-defined and where end-users get access to the network under the same conditions, e.g. wifi network of a department store open to all customers, are regulated by this Regulation.**

(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~~ **processing** 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 the [Directive establishing the European Electronic Communications Code] 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 ~~data~~ 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 possiblity to interact with, the individual electronic communications content, for example by recording, storing, printing or otherwise processing such data. 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 ~~is~~ may be ~~completed~~ 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 by the provider of the electronic communications service except when processing is permitted under this Regulation or when the end-users has entrusted the provider of the electronic communications service or another third party to record, store or otherwise process such data in accordance with Regulation (EU) 2016/679.

(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. 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 emails. Spam e-mails may also affect the availability of email services and could potentially impact the performance of networks and e-mail 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 e-mails deemed as spam in order to ascertain whether they were indeed spam. ~~or~~ Moreover, the prohibition of processing ~~Neither~~ should neither~~it~~ 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 ~~improving the performance and~~ processing necessary to develop~~ment~~ and manage the scalability and capacity of the network. ~~nor t~~**T**he processing of ~~meta~~data to make it anonymous ~~nor the processing of metadata to make it anonymous~~ **should not be prohibited either**.

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

(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 Pprocessing for such purposes other than for which the metadata where initially collected may take place without the consent of the end-users concerned, provided that such processing is compatible with the purpose for which the metadata are initially collected, certain additional conditions are met and safeguards are in place, including the consultation of the supervisory authority and the requirement to anonymise the result before sharing the analysis with third parties. As end-users attach great value to the confidentiality of their communications, including their physical movements, such data cannot be used to determine the nature or characteristics on an end-user or to build a profile of an end-user, in order to, for example, avoid that the data is used for segmentation purposes, to monitor the behaviour of a specific end-user or to draw conclusions concerning the private life of an end-user. For the same reason, the end-user must be provided with information about these processing activities taking place and given the right to object to such processing.

(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) Processing of electronic communication metadata for scientific research or statistical counting purposes should be considered to be permitted processing. This type of processing should be subject to safeguards to ensure privacy of the end-users by employing appropriate security measures such as encryption and pseudonymisation. In addtion, end-users who are natural persons should be given the right to object.

(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 in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After electronic communications content has been sent by the end-user and received by the intended end-user or end-users, it may be recorded or stored by the end-user, end-users or by a third party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679.

(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. Therefore, processing electronic communications content for services explicitly requested by the end-user for their own individual use, consent should only be requested from the end-user requesting the service taking into account that the processing must be limited to that purpose, limited to the duration necessary for providing the requested services and shall not adversely affect fundamental rights and interest of another end-user concerned.

(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 entity having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service. In such case, consent needs to be obtained from the individual concerned.

(20) Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is ~~stored in~~ **processed by** or emitted by or **stored in** such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere**, including the privacy of one's communications,** of the end-users requiring protection under the Charter of Fundamental Rights of the European Union ~~and the European Convention for the Protection of Human Rights and Fundamental Freedoms~~. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and for specific and transparent purposes. **The 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. Access to specific website content may still be made conditional on the consent to the storage of a cookie or similar identifier.**

Not all cookies are needed in relation to the purpose of the provision of the website service. Some are used to provide for additional benefits for the website operator. Making access to the website content provided without direct monetary payment conditional to the consent of the end-user to the storage and reading of cookies for additional purposes would normally not be considered disproportionate in particular if the end-user is able to choose 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 conditional to consent to the use of such cookies may be considered to be disproportionate. This would normally be the case for websites providing certain services, such as those provided by public authorities, where the user could be seen as having few or no other options but to use the service, and thus having no real choice as to the usage of cookies.

(21) Exceptions to the obligation to obtain consent to make use of the processing and storage capabilities of terminal equipment or to access information stored in terminal equipment should be limited to situations that involve no, or only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is ~~strictly~~ necessary and proportionate for the legitimate purpose of enabling the use of a specific service ~~explicitly~~ requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages**, 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**. ~~**Access to specific website content may still be made conditional on the well-informed acceptance of the storage of a cookie or similar identifier, if it is used for a legitimate purpose. This will for example not be the case of a cookie which is recreated after the deletion by the end-user.**~~

(21a) Cookies can also be a legitimate and useful tool, for example, in **assessing the effectiveness of a delivered information society service, for example of website design and advertising or by helping to** measure~~ing 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. **Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerablities 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. Consent should not be necessary either if the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment is necessary for the provision of ~~the~~ information society services, such as those used by IoT devices (for instance connected devices, such as connected thermostats), requested by the end-user.**

(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.

(22a) 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 the 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. The responsibility for obtaining consent with the storage of a cookie and for any penalties for breach of duty lies on the information society service provider.

(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 allow cookies') to lower (for example, 'always accept allow cookies') and intermediate (for example, 'reject third party cookies' or 'only accept allow first party cookies'). Such privacy settings should be presented offered in a an easily visible and intelligible manner. General privacy settings that do not provide the end-user with information about the purpose for which information can be stored on the terminal equipment, or information already stored on that equipment can be processed, as a consequence of the configured privacy settings, cannot signify the end-user's consent to the storing of information on the terminal equipment or the processing of information already stored on that equipment.

~~(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 It is necessary to require providers of software enabling access to internet that, at the moment of installation or first use and at the moment of every update that change the privacy settings, end-users are informed about the possibility to choose the available 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 default setting and about the risks associated with the different privacy settings, including those related 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. Updates of software enabling access to internet should not alter the privacy settings selected by the end-user. 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. This Regulation does should not prevent website providers from requesting the consent of the end-user for the use of cookies irrespective of the privacy setting selected by the end-user.~~

(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 if 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 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.~~

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

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 **with regard to the processing of ~~electronic communications~~ data that qualify as personal data** 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~~ **~~in transmission~~ 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~~ **~~processed by or emitted by or stored in the terminal equipment of end-users~~**.

(c) **the placing on the market of software permitting electronic communications, including the retrieval and presentation of information on the internet;**

(d) **the offering of a publicly available directory of end-users of electonic communications services;**

(e) **the sending ~~or presenting~~ of direct marketing communications to end-users.**

2. This Regulation does not apply to:

(a) activities **which fall outside the scope of Union law;**

(aa) **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 content processed by the end-users <u>concerned</u> after receipt, or by a third party entrusted by them to record, store or otherwise process <u>~~such data~~ their electronic communications content;</u>**

(f) electronic communications metadata processed by the end-users concerned or by a third party entrusted by them to record, store or otherwise process their electronic communications metadata on their behalf.

3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies is governed by Regulation (EU) 00/0000 [new Regulation replacing Regulation 45/2001].

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC[5], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

5. This Regulation shall be without prejudice to the provisions of Directive 2014/53/EU.

Article 3

Territorial scope and representative

1. This Regulation applies to:

(a) the provision of electronic communications services to end-users **who are** in the Union~~, irrespective of whether a payment of the end-user is required;~~

(aa) the processing of electronic communications content ~~in transmission~~ 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~~ **~~processed by or emitted by or stored in the terminal equipment~~** of end-users ~~located~~ **who are** in the Union.

(ca) the placing on the Union market of software permitting electronic communications, including the retrieval and presentation of information on the internet;

---

5 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).

(cb) **the offering of publicly available directories of end-users of electronic communications services who are in the Union;**

(cc) **the sending ~~or presenting~~ 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 the provider of software enabling electronic communications or a person using electronic communications services to send ~~or present~~ direct marketing communications or makes use of processing and storage capabilities or collects 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) respectively of Article 2 of [Directive establishing the European Electronic Communications Code];

(c) the definition of 'terminal equipment' in ~~point (1) of~~ Article 1**(1)** of Commission Directive 2008/63/EC[6]~~.~~ **;**

(d) the defintion of ‘information society service’ in point (b) of Article 1 (1) of Directive (EU) 2015/1535[7].

[6] 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).

[7] 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).

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.

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;

(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 ~~to identify~~ 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 **~~or presented~~** to one or more identified or identifiable 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.

*Article ~~9~~**4a***

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(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~~ **the** possibility **to withdraw their consent** at periodic intervals of **[no longer than ~~6~~12** 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

~~**1.**~~ Electronic communications data shall be confidential. Any **interference with** ~~**processing of**~~ electronic communications data, ~~such as by~~ **including** listening, tapping, storing, monitoring, scanning or other kinds of interception, ~~**or**~~ 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.

~~2. **[Confidentiality of electronic communications data shall apply to the transmission of machine-to-machine electronic communications where carried out via an electronic communications service.]**~~

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 achieve the transmission of the 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.

2. **Without prejudice to paragraph 1, ~~P~~p**roviders 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, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous and for the duration necessary for that purpose,** or to meet ~~**mandatory**~~ **technical** quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120[8] for the duration necessary for that purpose; or

[8] 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 the contract to which the end-user is party, ~~including to the extent more~~ 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**

(d) it is necessary to protect the vital interest of a natural person, in the case of emergency, upon request of a competent authority, in accordance with Union or Member State law; or

~~**(e) it is necessary for the purpose of statistical counting, provided that:**~~

~~**- the processing is limited to electronic communications meta-data that constitutes geolocation data that is pseudonymised,**~~

~~**- the processing could not be carried out by processing information that is made anonymous, and the location data is erased or made anonymous when it is no longer needed to fulfil the purpose, and**~~

~~**- the location data is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.**~~

(f) **it is necessary for statistical ~~counting~~purposes, ~~other than based on electronic communications metadata that constitute location data,~~ or for scientific research purposes, provided it is based on Union or Member State law which shall be proportionate to the aim pursued and provide for specific measures, including encryption and pseudonymisation, to safeguard 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**.

2a. Where the processing for a purpose other than that for which the electronic communications metadata have been collected 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 shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia:

(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, in particular where such data 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 processing, if considered compatible, may only take place, provided that:

- **the processing could not be carried out by processing information that is made anonymous, and electronic communications metadata is erased or made anonymous as soon as it is no longer needed to fulfil the purpose, and**
- **the processing is limited to electronic communications metadata that is pseudonymised,**
- **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.**

~~3a~~**2aa. For the purposes of ~~point (e) of~~ paragraph 2a, the providers of electronic communications networks and services shall:**

~~**(a) exclude electronic communications metadata that constitue location data that reveal special categories of personal data pursuant to Article 9 of Regulation (EU) 2016/679 from processing;**~~

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

(c) prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protection of electronic communications data and consult the supervisory authority. Points (2) and (3) of Article 36(2) and (3) of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority; and

(d) inform the end-user of specific processing on the basis of ~~point (e) of~~ paragraph 2a and ~~give of~~ the right to object to such processing free of charge, at any time, and in an easy and effective manner.

3. **Without prejudice to paragraph 1, ~~P~~p**roviders 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~~

(aa) for the purpose of the provision of an explicitly requested service<u>s</u> 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 interest<u>s</u> of another person concerned and does not exceed the duration necessary for the provision of the requested services and is limited to that purpose only; 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 the provider has **prior to the processing carried out an assessment of the impact of the envisaged processing operations on the protection of electronic communications data and** consulted the supervisory authority. ~~Points (2) and (3) of~~ Article 36**(2) and (3)** of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.

~~**3a. For the purposes of point (e) of paragraph 2, the providers of the electronic communications networks and services shall:**~~

~~**(a) exclude electronic communications metadata that constitue geolocation data that reveal special categories of personal data pursuant to Article 9 of Regulation (EU) 2016/679 from processing;**~~

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

~~**(c) prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protection of electronic communications data and consult the supervisory authority. Points (2) and (3) of Article 36(2) and (3) of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority; and**~~

~~**(d) inform the end-user of specific processing on the basis of point (e) of paragraph 2 and give the right to object to such processing.**~~

4. A third party on behalf of a provider of electronic communications network or services shall be permitted to process electronic communications data in accordance with paragraphs 1 to 3 provided that conditions laid down in Article 28 of Regulation (EU) 2016/679 are met.

Article 7

Storage and erasure of electronic communications data

1. Without prejudice to point (b) of Article 6(1) and **~~points (a), and (b)~~** of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients**. Such data may be recorded, ~~or~~ stored or otherwise processeed by the end-users after receipt, or by a third party entrusted by them to record, store or otherwise process such data. Such processing shall take place in accordance with Regulation (EU) 2016/679.**

2. Without prejudice to point (b) of Article 6(1) and points (a), **(~~c~~d) ~~and~~ to** (~~c~~**ef**) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication. **~~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~~**.

3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.

Article 8

Protection of ***end-users' terminal equipment*** *information* ~~***stored in terminal equipment of end-users and related to or processed by or emitted by end-users' terminal such 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 on behalf of the provider of the information society service provided that conditions laid down in Article 28 of Regulation (EU) 2016/679 are met.; or**

(da) it is necessary to maintain or restore the security of information society services, prevent fraud or detect technical faults for the duration necessary for that purpose; or

(e) it is necessary for a ~~security~~ software update provided that:

(i) ~~security~~ such update~~s~~ ~~are~~ is necessary for security reasons and do~~es~~ 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, at the time of the incident, a caller of an emergency call from the terminal by organisations dealing with emergency communications.**~~

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.

~~(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~~**t**he 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 2**a** 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 2~~5~~**7** 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 any other parties than the end-user from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.**~~

~~**2. Upon At the time of installation or first usage and every updates that change the privacy settings options, the software referred to in paragraph 1 shall inform the end-user about the privacy settings options and/or navigate the way the end-user through may use them. The software shall offer the end-user the choice to be reminded about the privacy settings options., to continue with the installation or usage, require the end-user to consent to a setting shall remind the end-users of the availability of privacy settings with periodic intervals.**~~

~~**2a. The software referred to in paragraph 1 shall provide in a clear manner easy ways for end-users to change the privacy setting consented to under paragraph 2 at any time during the use.**~~

~~**3. In the case of software which has already been installed on [25 May 2018 the date of entry into application], the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than [25 August 2018 3 months after the date of entry into application].**~~

~~**4. This provision shall not apply to software that is no longer supported at the time of entry into application of this Regulation.**~~

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.