Text of the compromise amendments

COMP 1 (Article 1)

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.

2. This Regulation ensures free movement of electronic communications data and electronic communications services within the Union, which shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural and legal persons and the protection of natural persons with regard to the processing of personal data.

3. The provisions of this Regulation particularise and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2.

Recitals

(1) Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") protects the fundamental right of everyone to the respect for his or her private and family life, home and communications. Respect for the privacy of one's communications is an essential dimension of this right. Confidentiality of electronic communications ensures that information exchanged between parties and the external elements of such communication, including when the information has been sent, from where, to whom, is not to be revealed to anyone other than to the **communicating parties** ~~***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 **inter**-personal messaging provided through social media. **It should also apply when the confidentiality of electronic communications and the privacy of the physical environment converge, i.e. where terminal devices for electronic communication can also listen into their physical environment or use other input channels such as Bluetooth signalling or movement sensors.**

(3) Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. Therefore, the provisions of this Regulation should apply to both natural and legal persons. Furthermore, this Regulation should

ensure that provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council[1], also apply to end-users who are legal persons. This includes the definition of consent under Regulation (EU) 2016/679. When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.

(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***~~ **are generally** personal data as defined in Regulation (EU) 2016/679.

(5) The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards electronic communications data that qualify as personal data. This Regulation therefore does not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. **On the contrary, it aims to provide additional, and complementary, safeguards taking into account the need for additional protection as regards the confidentiality of communications.** Processing of electronic communications data ~~***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.

(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.

---

[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).

[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).

COMP 2 (Article 2)

Article 2

Material Scope

1. This Regulation applies to**:**
~~***the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.***~~

(a) the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services, irrespective of whether a payment is required;

(b) the processing of information related to or processed by 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 provision of publicly available directories of subscribers of electronic communication;

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

2. This Regulation does not apply to:

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

(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;

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 26 , 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.

Recitals

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

(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.

COMP 3 (Article 3)

Article 3
Territorial scope and representative

1. This Regulation applies to:

(a) the ~~provision~~ ***offering*** of electronic communications services, ***software, publicly available directories, or direct marketing electronic communications*** to end-users in the Union, irrespective of whether a payment of the end-user is required;

(b) ~~***the use of such services; the activities referred to in Article 2 that are provided from the territory of the Union.***~~

(c) the ~~protection~~ ***processing*** of information related to ***or processed by*** the terminal equipment of end-users ~~located~~ ***that is*** in the Union.

2. Where the provider of an electronic communications service**, provider of software permitting electronic communications, a person processing information related to or processed by the terminal equipment of users or end-users, a provider of a publicly available directory, or a person using electronic communication services to transmit direct marketing communications** is not established in the Union, ~~**Article 27 of Regulation (EU) No 2016/679 shall apply.**~~ it shall designate in writing a representative in the Union.

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 in addition to or instead of the provider it represents, in particular, to supervisory authorities**, courts**, and end-users,

[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).

on all issues related to **the activities referred to in Article 2** ~~***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 **undertake the activities referred to in Article 2** ~~***processes electronic communications data in connection with the provision of electronic communications services***~~ from outside the Union~~***.to end-users in the Union.***~~

Recitals

(9) This Regulation should apply to electronic communications data processed in connection with the ~~***provision***~~ **offering** and use of electronic communications services in the Union, regardless of whether or not the processing takes place in the Union. Moreover, in order not to deprive end-users in the Union of effective protection, this Regulation should also apply to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to end-users in the Union. **This should be the case irrespective of whether the electronic communications are connected to a payment or not. For the purpose of this Regulation, where the provider of an electronic communications service is not established in the Union, it should designate, in writing, a representative in the Union.**

COMP 4 (Article 4)

Article 4
Definitions

1. For the purposes of this Regulation, following definitions shall apply:

(a) the definitions in Regulation (EU) 2016/679;

(b) the definition~~***s***~~ of **'call' in point (21)** ~~***'electronic communications network', 'electronic communications service', 'interpersonal communications service', 'number-based interpersonal communications service', 'number-independent interpersonal communications service', 'end-user' and 'call' in points (1), (4), (5), (6), (7), (14) and (21) respectively***~~ of Article 2 of [Directive establishing the European Electronic Communications Code];

(c) the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC 27 .

~~***2. For the purposes of point (b) of paragraph 1, the definition of 'interpersonal communications service' shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.***~~

3. In addition, for the purposes of this Regulation the following definitions shall apply:

(a a)(-a) 'electronic communications network' means a transmission system, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not

active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit -and packet- switched including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

(-aa) 'electronic communications service' means a service provided via electronic communications networks, whether for remuneration or not, which encompasses one or more of the following: an 'internet access service' as defined in Article 2(2) or Regulation (EU) 2015/2120;an interpersonal communications service; a service consisting wholly or mainly in the conveyance of the signals, such as a transmission service used for the provision of a machine-to-machine service and for broadcasting, but excludes information conveyed as part of a broadcasting service to the public over an electronic communications network or service except to the extent that the information can be related to the identifiable end-user receiving the information; ~~it includes services enabling interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service;~~ it also includes services which are not publicly available, but provide access to a publicly available electronic communications network;

(-ab) 'interpersonal communications service' means a service, whether provided for remuneration or not, that enables direct interpersonal and interactive exchange of information via electronic communications service between a finite number of persons whereby the persons initiating or participating in the communication determine the recipient(s);

(-ac) 'number-based interpersonal communications service' means an interpersonal communications service which connects to the public switched telephone network, either by means of assigned numbering resources, i.e. number or numbers in national or international telephone numbering plans, or by enabling communication with a number or numbers in national or international telephone numbering plans;

(-ad) 'number-independent interpersonal communications service' means an interpersonal communications service which does not connect with the public switched telephone network, either by means of assigned numbering resources, i.e. a number or numbers in national or international telephone numbering plans, or by enabling communication with a number or numbers in national or international telephone numbering plans;

(-ae) 'end-user' means a legal entity or a natural person using or requesting a publicly available electronic communications service;

(-af) 'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

(a) 'electronic communications data' means electronic communications content and electronic communications metadata;

(b) 'electronic communications content' means the content **transmitted, distributed or** exchanged by means of electronic communications services, such as text, voice, videos, images, and sound**. Where metadata of other electronic communications services or protocols are transmitted, distributed**

or exchanged by using the respective service, they shall be considered electronic communications content for the respective service;

(c) 'electronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the **terminal equipment processed** ***~~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-user of electronic communications services, whether in printed or electronic form, which is published or made available to the public or to a section of the public, including by means of a directory enquiry service;

(e) 'electronic mail' means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient;

(f) 'direct marketing communications' means any form of advertising, whether **in** written**, oral or video format, sent, served or presented** ***~~or oral, sent~~*** to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, **fax machines** etc.;

(g) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems***~~;~~*****, including calls made using automated calling and communication systems which connect the called person to an individual;**

(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.~~***

Recitals

(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. **Metadata can also be processed and analysed much easier than content, as it is already brought into a structured and standardised format. The protection of confidentiality of communications is an essential condition for the respect of other connected fundamental rights and freedoms, such as the protection of freedom of thought, conscience and religion, freedom of assembly, freedom of expression and information.**

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

(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, **also known as "over-the-top-services" (OTTs). This Regulation aims at ensuring** ~~*. In order to ensure*~~ an effective and equal protection of end-users when using functionally equivalent services, **so as to ensure the confidentiality of their communication, irrespective of the technological medium chosen.** ~~*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 It does** not only **cover** internet access services and services consisting wholly or partly in the conveyance of signals but also interpersonal communications services, which may or may not be number-based, such as for example, Voice over IP, messaging services and web-based e-mail services. ~~The protection of confidentiality of communications is crucial also as regards interpersonal communications services that~~ **include services which enable interpersonal and interactive communication merely as a minor** ~~*are*~~ ~~ancillary~~ **feature that is intrinsically linked** ~~to another service; therefore, such type of services also having a communication functionality should be covered by this Regulation.~~

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

[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)).

of end-users if the access to the service as a whole is provided to an undefined group of end-users.

(14) Electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning a~~n end~~ user of electronic communications services processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. **It should also include data necessary to identify users' terminal equipment and data emitted by terminal equipment when searching for access points or other equipment.** Whether such signals and the related data are conveyed by wire, radio, optical or electromagnetic means, including satellite networks, cable networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, the data related to such signals should be considered as electronic communications metadata and therefore be subject to the provisions of this Regulation. Electronic communications metadata may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content. **The exclusion of services providing "content transmitted using electronic communications networks" from the definition of "electronic communications service" in Article 4 of this Regulation does not mean that service providers who offer both electronic communications services and content services are outside the scope of the provisions of the Regulation which applies to the providers of electronic communications services.**

(14a) **Modern electronic communications services, including the Internet and the OTT services that run on top of it, function on the basis of a protocol stack. Each protocol defines content (also called payload), a header and sometimes a trailer. Any higher protocol in the stack would be encapsulated in the content part of a lower level protocol. For example, A TCP segment would be in the content part of an IP packet, whose header would include the source and destination IP addresses between which the IP packet should be routed. TCP segments could contain an SMTP message in their content part, i.e. an e-mail. At the SMTP protocol level, the header would notably contain the sender and receiver email addresses and the content part would contain the message itself. In practice, the header and the trailer of a protocol message correspond to metadata for the given protocol. This means that the metadata on one protocol layer will be content for the lower layers encapsulating the information. Where this Regulation lays down different rules for the processing of content and metadata, this should be understood specifically for the considered electronic communications service and the protocol layer it is operating on. For an Internet service provider, for example, the subject, the sender, the recipient and the body of an email will be altogether considered as content of the IP packets routed by it. However regarding an e-mail provider, only the subject and the body of the email will considered as content, whereas the recipient and the sender will be considered as metadata. This separation of protocol layers is crucial for maintaining the neutrality of the electronic communications services (net neutrality), which is protected under Regulation (EU) 2015/2120."**

COMP 5 (Article 5)

CHAPTER II

PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION ~~***STORED IN***~~ **PROCESSED BY AND RELATED TO** THEIR TERMINAL EQUIPMENT

Article 5
Confidentiality of electronic communications ~~**data**~~

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

1a. Confidentiality of electronic communications shall also apply to data related to or processed by terminal equipment.

Recitals

(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. **When the processing is allowed under any exception to the prohibitions under this Regulation, any other processing on the basis of Article 6 of Regulation (EU) 2016/679 should be considered as prohibited, including processing for another purpose on the basis of Article 6 paragraph 4 of that Regulation. This should not prevent requesting additional consent for new processing operations.** The prohibition of interception of communications ~~***data***~~ should apply **also** during their conveyance. **For non-real-time electronic communication such as email or messaging, the transmission starts with the submission of the content for delivery and finishes with the** receipt of the content of the electronic communication by the **service provider of the** intended **recipient**. ~~***i.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**, and analysis of users' traffic data,** including browsing habits without the ~~***end***~~ users' consent.

COMP 6 (Article 6)

Article 6
Lawful ~~Permitted~~ *processing of electronic communications data*

1. Providers of electronic communications networks and services ~~**or third parties acting on their behalf**~~ may process electronic communications data **only** if it is technically necessary to achieve the transmission of the communication, for the duration necessary for that purpose

(a) ~~it is **technically** necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or~~

1b. Providers of electronic communications networks and services **or other parties acting on behalf of the provider or the end-user** may process electronic communications data only if it is **technically** necessary to maintain or restore the **availability, integrity, confidentiality and security of the respective** ***~~security of~~*** electronic communications network**~~s~~** **or** ***~~and~~*** service***~~s~~***, or **to** detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpos**e.**

2. Providers of electronic communications services **and networks** may process electronic communications metadata **only** if:

(a) it is **strictly** necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120 28 for the duration **technically** necessary for that purpose; or

(b) it is **strictly** necessary for billing, ~~calculating~~ **determining** interconnection payments, 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 **without the processing of such metadata.*~~by processing information that is made anonymous.~~***

(2a) For the purposes of point (c) of paragraph 2, where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, Articles 35 and 36 of Regulation (EU) 2016/679 shall apply.

3. Providers of the electronic communications services may process electronic communications content only:

(a) for the sole purpose of the provision of a specific service **requested by the user** ***~~to an end-user~~***, if the **user** ***~~end user or end user~~*** concerned has***~~ve~~*** given **his or her** ***~~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**~~;~~ by the provider;** 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 consulted the supervisory authority. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.

3a. The provider of the electronic communications service may process electronic communications data solely for the provision of an explicitly requested service, for purely individual usage, only for the duration necessary for that purpose and without the consent of all users only where such requested processing does not adversely affect the fundamental rights and interests of another user or users.

Recitals

(16) The prohibition of storage of communications is not intended to prohibit any automatic, intermediate and transient storage of this information insofar as this takes place for the sole purpose of carrying out the transmission. **It should not prohibit the processing of** ~~***in the***~~ electronic communications **data by public authorities, computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), providers** ~~***network. It should not prohibit either the processing***~~ of electronic communications **networks and services and by** ~~**certified**~~ **providers of security technologies and services, in compliance with Regulation 2016/679 and to the extent strictly necessary and proportionate for the sole purposes of ensuring network and information** security**, [i.e. preservation of availability, integrity], and confidentiality of information, and ensuring the security of the related** services **offered by, or accessible via, those networks and systems. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems,** ~~***data to ensure the***~~ security ~~***and continuity of the electronic communications***~~ services, ~~***including***~~ checking security threats such as the presence of malware, **spam or to check against DDoS attacks,** or the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc. **Such processing could** ~~**also**~~ **be carried out by another party which acts as a data processor in the meaning of Regulation (EU) 2016/679 for the provider of the service.**

(17a) Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure.

(19) The content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any ~~***interference with the***~~ **processing of** content **data** of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility 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 carry out an impact assesment as provided for in** ~~*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 **and if necessary under that Regulation, consult the supervisory authority prior to the** ~~*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, **which could be the electronic communications service provider.** Any processing of such **stored communications** data **where the data is stored on behalf of the user must comply with this Regulation. The user may further process the data and if it contains personal data,** must comply with Regulation (EU) 2016/679.

(19a) It should be possible to process electronic communications data for the purposes of providing services explicitly requested by a user for personal or personal work-related purposes such as search or keyword indexing functionality, virtual assistants, text-to-speech engines and translation services, including picture-to-voice or other automated content processing used as accessibility tools by persons with disabilities. This should be possible without the consent of all users but may ~~only~~ take place with the consent of the user requesting the service. Such specific consent also precludes the provider from processing those data for ~~different~~ other purposes.

(19b) Interference with the confidentiality of metadata or interference with the protection of information stored in and related to end-users' terminal equipment can only be regarded to be lawful where it is strictly necessary and proportionate to protect an interest which is essential for the life of the data subject or that of another natural person. Such interference based on the vital interest of another natural person should take place only in a specific case and where the processing cannot be manifestly based on another legal basis.

COMP 7 (Article 7)

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**, when it is no longer necessary for the provision of such service, as requested by the user.** ~~*or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients.*~~ Such data may be recorded or stored by the ~~*end*~~ users or by a third party entrusted by them to record, store or otherwise process such data**.** ~~,~~ **The user may process the data** in accordance with Regulation (EU) 2016/679.

2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer ~~needed~~ **necessary for the provision of such service, as requested by the user.** ~~***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 6(2), the **strictly necessary** ~~***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.

COMP 8 (Article 8)

Article 8

Protection of information **transmitted to,** stored in, related to, **processed by and collected from** ~~**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 **strictly** 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 **specific** consent; or

(c) it is **strictly technically** necessary for providing an information society service **specifically** requested by the ~~***end***~~user; or

(d) if it is **technically** necessary **for measuring the reach of an information society service requested by the user** ~~***for web audience measuring,***~~ provided that such measurement is carried out by the provider **or on behalf of the provider, or by a web analytics agency acting in the public interest including for scientific purpose; that the data is aggregated and the user is given a possibility to object; and further provided that no personal data is made accessible to any third party and that such measurement does not adversely affect the fundamental rights of the user;** ~~***of the information society service requested by the end-user.***~~ **Where audience measuring takes place on behalf of an information society service provider, the data collected shall be processed only for that provider and shall be kept separate from the data collected in the course of audience measuring on behalf of other providers; or**

(da) it is necessary to ensure security, confidentiality, integrity, availability and authenticity of the terminal equipment of the end-user, by means of updates, for the duration necessary for that purpose, provided that:

(i) this does not in any way change the functionality of the hardware or software or the privacy settings chosen by the user;

(ii) the user is informed in advance each time an update is being installed; and

(iii) the user has the possibility to postpone or turn off the automatic installation of any updates;

(d b) in the context of employment relationships, it is strictly technically necessary for the execution of an employee's task, where: (i) the employer provides and/or is the subscriber of the terminal equipment; (ii) the employee is the user of the terminal equipment; and (iii) it is not further used for monitoring the employee.

1a. No user shall be denied access to any information society service or functionality, regardless of whether this service is remunerated or not, on grounds that he or she has not given his or her consent under Article 8(1)(b) to the processing of personal information and/or the use of processing or storage capabilities of his or her terminal equipment that is not necessary for the provision of that service or functionality.

2. The ~~*collection*~~ **processing** of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:

(a) it is done exclusively in order to, for the time necessary for, and for the **sole** purpose of establishing a connection**, requested by the user**; or

(aa) the user has been informed and has given consent; or

(ab) the risks are mitigated.

~~*(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.*~~

~~*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.*~~

2a. For the purpose of points (d) of paragraph 1 and (ab) of paragraph 2, the following controls shall be implemented to mitigate the risks:

(a) the purpose of the data collection from the terminal equipment shall be restricted to mere statistical counting; and

(b) the processing shall be limited in time and space to the extent strictly necessary for this purpose; and

(c) the data shall be deleted or anonymised immediately after the purpose is fulfilled; and

(d) the users shall be given effective possibilities to object that do not affect the functionality of the terminal equipment.

2b. The information referred to in points (aa) and (ab) of paragraph 2 shall be conveyed in a clear and prominent notice setting out, at the least, details of how the information will be collected, the purpose of processing, the person responsible for it and other information required under Article 13 of Regulation (EU) 2016/679, where personal data are collected. The collection of such information shall be conditional on the application of appropriate technical and

organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679.

3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 27 determining the information to be presented by the standardized icon and the procedures for providing standardi**s**~~z~~ed icons.

Recitals

(20) Terminal equipment of ~~*end*~~ users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the ~~*end*~~ users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes **very sensitive data** ~~*information*~~ that may reveal details of the **behaviour, psychological features**, emotional **condition** and political **and** social **preferences of an individual**, ~~*an individual's complexities,*~~ including the content of communications, pictures, the location of individuals by accessing the ~~*device's*~~ GPS capabilities **of the device,** 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. **Furthermore, so-called spyware, web bugs, hidden identifiers and unwanted tracking tools can enter users' terminal equipment without their knowledge in order to gain access to information or to store hidden information, to process data and use input and output functionalities such as sensors, and to trace the activities.** 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. **Users should receive all relevant information about the intended processing in clear and easily understandable language. Such information should be provided separately from the terms and conditions of the service.**

(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 authori~~z~~**s**ing 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 **information (such as** cookies **and other identifiers)** for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages. ~~*Cookies*~~ **Such techniques, if implemented with appropriate privacy safeguards,** can also be a legitimate and useful tool, for example, in measuring web traffic to a website. **Such measuring implies that the result of processing is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.** Information society providers **could** ~~*that*~~ engage in configuration checking **in order** to provide the service in compliance with the ~~*end-*~~user's settings and the mere logging **revealing** ~~*of*~~ the fact that the ~~*end-*~~user's device is unable to receive content requested by the ~~*end-*~~user, should not constitute **illegitimate** access **to such a device, or use of the device processing capabilities for which consent is required.**

(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. **This Regulation should prevent the use of so-called "cookie walls" and "cookie banners" that do not help users to maintain control over their personal information and privacy or become informed about their rights.** The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent **by technical specifications, for instance** by using the appropriate settings of a browser or other application. **Those settings should include choices concerning the storage of information on the user's terminal equipment as well as a signal sent by the browser or other application indicating the user's preferences to other parties.** The choices made by ~~*end-*~~users when establishing ~~*its*~~ **the** general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties. Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the ~~*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, **or applications or operating systems** may be used as **the executor of a user's choices,** ~~*gatekeepers*~~, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored.

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

be used for more intrusive purposes, such as to send commercial messages to ~~*end-*~~users, for example when they enter stores, with personali~~*sz*~~ed offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should **either obtain the user's consent or anonymise the data immediately while limiting the purpose to mere statistical counting within a limited time and space and offering effective opt-out possibilities.** ~~*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.*~~

COMP 9 (Article 9)

Article 9

Consent

1. The definition of and conditions for consent provided for **in Regulation (EU) 2016/679/EU** ~~*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 **or withdrawn** by using ~~*the appropriate*~~ technical ~~*settings of a software application enabling access to the internet.*~~**specifications for electronic communications services or information society services which allow for specific consent for specific purposes and with regard to** specific service providers actively selected by the user in each case, pursuant to **paragraph 1. When such technical specifications are used by the user's terminal equipment or the software running on it, they may signal the user's choice based on previous active selections by him or her. These signals shall be binding on, and enforceable against, any other party.**

3. ~~**End-u**~~**U**sers who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3**), point (b) of Article 8(1) and point (aa) of Article 8(2)** shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 ~~*and be reminded of this possibility at periodic intervals*~~ as long as the processing continues.

3 a. Any processing based on consent must not adversely affect the rights and freedoms of individuals whose personal data are related to or transmitted by the communication**, in particular their rights to privacy and the protection of personal data.**

Recitals

(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~~**, **T~~t~~**his 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. 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.

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

COMP 10 (Article 10)

Article 10

Privacy settings and signals 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.~~**

(a) by default, have privacy protective settings activated to prevent other parties from transmitting to or storing information on the terminal equipment of a user and from processing information already stored on or collected from that equipment, except for the purposes laid down by Article 8 paragraph (1), points (a) and (c);

(b) upon installation, inform and offer the user the possibility to change or confirm the privacy settings options defined in point (a) by requiring the user's consent to a setting and offer the

option to prevent other parties from processing information transmitted to, already stored on or collected from the terminal equipment for the purposes laid down by Article 8, paragraph (1), points (a), (c), (d) and (da).

(c) offer the user the possibility to express specific consent through the settings after the installation of the software.

Before the first use of the software, the software shall inform the user about the privacy settings and the available granular setting options according to the information society service accessed. These settings shall be easily accessible during the use of the software and presented in a manner that gives the user the possibility for making an informed decision.

1a. For the purposes of:

(a) points (a) and (b) of paragraph 1,

(b) giving or withdrawing consent pursuant to Article 9(2) of this Regulation, and

(c) objecting to the processing of personal data pursuant to Article 21(5) of Regulation (EU) 2017/679,

the settings shall lead to a signal based on technical specifications which is sent to the other parties to inform them about the user's intentions with regard to consent or objection. This signal shall be legally valid and be binding on, and enforceable against, any other party.

1b. In accordance with Article 9 paragraph 2, such software shall ensure that a specific information society service may allow the user to express specific consent. A specific consent given by a user under Article 8 paragraph 1 point (b) shall prevail over the existing privacy settings for that particular information society service. Without prejudice to paragraph 1, where a specified technology has been authorised by the data protection board for the purposes of point (b) of Article 8(1), consent may be expressed or withdrawn at any time both from within the terminal equipment and by using procedures provided by the specific information society service.

~~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.~~

2. In the case of software which has already been installed on **[xx.xx.xxxx]** ~~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 **six months after [the date of entry into force of this Regulation].**

Recitals

(23) The principles of data protection by design and by default are ~~***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 **permitting** ~~***enabling***~~ **electronic communications (such as browsers, operating systems and communication apps), irrespective of whether the software is obtained separately or bundled with hardware, shall configure the software so that privacy is protected, the cross- domain tracking and the storing of information on the terminal equipment by third parties is prohibited .** ~~***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'***~~ **In addition, providers of such software are required to offer sufficiently granular options to consent to each distinct category of purposes. These distinct categories include, at least, the following categories: (i) tracking for commercial purposes or for direct marketing for non-commercial purposes (behavioural advertising); (ii) tracking for personalised content; (iii) tracking for analytical purposes; (iv) tracking of location data; (v) providing personal data to third parties (including providing unique identifiers to match with personal data held by third parties) No consent is required for** information **that is collected from end-users'** terminal equipment **when it is strictly necessary for providing an information society service requested by the end-user, for example in order to adapt the screen size to the device, or to remember items in a shopping basket. Web browsers, operating systems and communication apps should allow the end-user to consent to** cookies **or other information that is stored on, or read from terminal equipment (including the browser on that equipment) by a specific website or originator even when the general** settings **prevent the interference and vice versa. With regard to a specific party, web browsers and communication apps should also allow users to separately consent to internet-wide tracking. Privacy settings should also include options to allow the user to decide for example, whether multimedia players, interactive programming language viewers, or similar software can be executed, if a website can collect geo-location data from the user, or if it can access specific hardware such as a webcam or microphone**. ~~***or 'only accept first party cookies').***~~ Such privacy settings should be presented in a an easily visible and intelligible manner**, and at the moment of installation or first use, users should be informed about the possibility to change the default privacy settings among the various options. Information provided should not dissuade users from selecting higher privacy settings and should include relevant information about the risks associated to allowing cross-domain trackers, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising or sharing with more third parties. Software manufacturers should be required to provide easy ways for users to change the privacy settings at any time during use and to allow the user to make exceptions for or to specify for such services websites trackers and cookies are always or never allowed.**

(24) ~~***For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such***~~

~~*cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send 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.*~~

COMP 11 (Article 11)

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) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests.~~

~~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.~~

Article 11a

Restrictions on the rights of the user

1. Union or Member State law to which the provider is subject may restrict by way of a legislative measure the scope of the obligations and principles relating to processing of electronic communications data provided for in Articles 6, 7 and 8 of this Regulation in so far as its provisions correspond to the rights and obligations provided for in ~~Articles 12 to 22 of~~ Regulation (EU) 2016/679, when such a restriction fully respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (d) of Regulation (EU) 2016/679.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, pursuant to Article 23(2) of Regulation (EU) 2016/679.

Article 11b

Restrictions on confidentiality of communications

1. Union or Member State law may restrict by way of a legislative measure the scope of the rights provided for in Article 5 where such a restriction fully respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the following general public interests:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of serious criminal offences, unauthorised use of electronic communication systems or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, pursuant to Article 23(2) of Regulation (EU) 2016/679.

Article 11 c

Documentation and reporting of restrictions

1. Providers of electronic communications services shall keep documentation about requests made by competent authorities to access communications content or metadata pursuant to Article 11b(2).This documentation shall include for each request:

(a) the in-house staff member who handled the request;

(b) the identity of the body making the request;

(c) the purpose for which the information was sought;

(d) the date and time of the request;

(e) the legal basis and authority for the request, including the identity and status or function of the official submitting the request;

(f) the judicial authorisation of the request;

(g) the number of subscribers to whose data the request related;

(h) the data provided to the requesting authority;and

(i) the period covered by the data.

The documentation shall be made available to the competent supervisory authority upon request.

2. Providers of electronic communications services shall publish once per year a report with statistical information about data access requests by law enforcement authorities pursuant to Articles 11a and 11b.The report shall include, at least

(a) the number of requests;

(b) the categories of purposes for the request;

(b) the categories of data requested;

(c) the legal basis and authority for the request;

(d) the number of subscribers to whose data the request related;

(e) the period covered by the data;

(f) the number of negative and positive responses to those requests.

3. Member States' competent authorities shall publish once per year a report with statistical information per month about data access requests pursuant to Articles 11a and 11b, including requests that were not authorised by a judge, including, but not limited to, the following points:

(a) the number of requests;

(b) the categories of purposes for the request;

(c) the categories of data requested;

(d) the legal basis and authority for the request;

(e) the number of subscribers to whose data the request related;

(f) the period covered by the data;

(g) the number of negative and positive responses to those requests.

The reports shall also contain statistical information per month about any other restrictions pursuant to Articles 11a and 11b.

Recitals

(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).*~~

(26a) In order to safeguard the security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design. Member States should not impose any obligation on encryption providers, on providers of electronic communications services or on any other organisations (at any level of the supply chain) that would result in the weakening of the security of their networks and services, such as the creation or facilitation of "backdoors".

COMP 12 (Article 12)

CHAPTER III
NATURAL AND LEGAL PERSONS' 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] of the [Directive 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 the calling end-user.

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.

Recitals

(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.

COMP 13 (Article 13)

Article 13
Exceptions to presentation and restriction of calling and connected line identification

1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of an ~~***end-***~~user for the processing of metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.

2. ~~***Member States***~~**The Commission** shall **be empowered to adopt implementing measures in accordance with Article 26(1)** ~~***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.

Recitals

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

COMP 14 (Article 14)

Article 14
Incoming call blocking

Providers of publicly available number-based interpersonal communications services shall ~~***deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also***~~ provide the called end-user with the following possibilities, free of charge:

(a) to block incoming calls from specific numbers**, or numbers having a specific code or prefix identifying the fact that the call is a marketing call referred to in Article 16(3)(b),** or from anonymous sources;

(b) to stop automatic call forwarding by a third party to the ~~***end-***~~user's terminal equipment.

Recitals

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

COMP 15 (Article 15)

Article 15
Publicly available directories

1. **Without prejudice to Articles 12 to 22 of Regulation (EU) 2016/679,** the ~~**providers of publicly available directories**~~ **electronic communication services providers** shall obtain the consent of ~~***end-users who are natural persons***~~ **users** to include their personal data in the **publicly available** directory and, consequently, shall obtain consent from these ~~***end-***~~users for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the directory**.** ~~***as determined by the provider of the directory. Providers shall give end-users who are natural persons the means to verify, correct and delete such data.***~~ **Electronic communication service providers shall give users the means to verify, correct, update,** ~~***complete***~~ **supplement and delete such data. When electronic communication service providers obtain consent of users, they shall make users' data available for public directory providers in an immediate, non-discriminatory and fair manner.**

2. The providers of a publicly available directory shall inform ~~***end-***~~users ~~***who are natural persons***~~ whose personal data are in the directory of the available search functions of the directory and **provide the users the option to disable** ~~***obtain end-users' consent before enabling***~~ such search functions related to their own data.

3. The ~~*providers of publicly available directories*~~ **electronic communication service providers** shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. **Electronic communication service P**~~p~~roviders shall give such end-users that are legal persons the means to verify, correct and delete such data. **For the purposes of this Article, natural persons acting in a professional capacity, such as independent professionals, operators of small businesses or freelancers, shall be equated with legal persons, as regards their data related to their professional capacity.**

4. **Without prejudice to Article 12(5) of Regulation (EU) 2016/679, the information to the users and the possibility** ~~*The possibility for end-users*~~ not to be included in a publicly available directory, or to verify, correct**, update, supplement** and delete any data related to them shall be provided free of charge **and in an easily accessible manner by the electronic communication services providers.**

4a. Where the personal data of the users of number- based interpersonal communications services have been included in a publicly available directory before this Regulation enters into force, the personal data of such users may remain included in a publicly available directory, including versions with search functions, unless the users have expressed their objection against their data being included in the directory or against available search functions related to their data.

Recitals

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

(31) If **end-**users ~~*that are natural persons*~~ give their consent to their data being included in such directories, they should be able to determine on a consent basis which categories of personal data are included in the directory (for example name, email address, home address, user name, phone number). In addition, ~~**providers of publicly available directories or**~~ **electronic communications service providers** should inform the ~~*end-*~~users of the purposes of the directory and of the search functions of the directory before including them in that directory. ~~*End-*~~Users should be able to determine by consent on the basis of which categories of personal data their contact details can be searched. The categories of personal data included in the directory and the categories of personal data on the basis of which the ~~*end-*~~user's contact details can be searched should not necessarily be the same. **The providers or publicly available directories shall provide information about the search functions, as well as if new options and functions of the directories are available in the publicly available directories and provide the users the option to disable such functions.**

COMP 16 (Article 16)

Article 16
Unsolicited communications

1. **The use by n**~~N~~atural or legal persons **of electronic communications services, including automated calling, communications systems, semi-automated systems that connect the call person to an individual, faxes, e-mail or other use of** ~~***may use***~~ electronic communications services for the purposes of **presenting or** sending ~~***unsolicited or***~~ direct marketing communications to ~~***end-***~~users ~~***who are natural persons***~~**, shall be allowed only in respect of users who** ~~***that***~~ have given their **prior** consent.

2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own ~~***similar***~~ products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The **customer shall be informed about the** right to object **and** shall be given **an easy way to exercise it** at the time of collection and each time a message is sent.

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 line on which they can be contacted; or

(b) present a specific code/or prefix identifying the fact that the call is a marketing call.

3a. The masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited communications for direct marketing purposes is prohibited.

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. **Member States shall provide that users can object to receiving the direct marketing voice-to-voice calls via a Do Not Call Register, thereby also ensuring that the user needs to opt- out only once.**

5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to unsolicited communications sent by means set forth under paragraph 1 are sufficiently protected.

6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner **and free of charge**, to receiving further marketing communications.

7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(**1*~~2~~***) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.

Recitals

(32) In this Regulation, direct marketing refers to any form of advertising by which a natural or legal person sends direct marketing communications directly to one or more identified or identifiable end-users using electronic communications services, **regardless of the form it takes**. In addition to the offering of products and services for commercial purposes, this should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties. The same should apply to messages sent by other non-profit organisations to support the purposes of the organisation.

(33) Safeguards should be provided to protect end-users against unsolicited communications ***~~for~~*** **or** direct marketing ***purposes***, which intrude into the private life of end-users. The degree of privacy intrusion and nuisance is considered relatively similar independently of the wide range of technologies and channels used to conduct these electronic communications, whether using automated calling and communication**s** systems, **semi-automated systems,** instant messaging applications, **faxes**, e-mails, SMS, MMS, Bluetooth, etc. It is therefore justified to require that consent of the end-user is obtained before commercial electronic communications for direct marketing purposes are sent to end-users in order to effectively protect individuals against the intrusion into their private life as well as the legitimate interest of legal persons. Legal certainty and the need to ensure that the rules protecting against unsolicited electronic communications remain future-proof **and** justify the need to define a single set of rules that do not vary according to the technology used to convey these unsolicited communications, while at the same time guaranteeing an equivalent **high** level of protection for all ***~~citizens~~*** **end-users** throughout the Union. However, it is reasonable to allow the use of e-mail contact details within the context of an existing customer relationship for the offering of **other** ***~~similar~~*** products or services. Such possibility should only apply to the same company that has obtained the electronic contact details in accordance with Regulation (EU) 2016/679.

(34) When end-users have provided their consent to receiving unsolicited communications for direct marketing purposes, they should still be able to withdraw their consent at any time in an easy manner. To facilitate effective enforcement of Union rules on unsolicited messages for direct marketing, it is necessary to prohibit the masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited commercial communications for direct marketing purposes. Unsolicited marketing communications should therefore be clearly recognizable as such and should indicate the identity of the legal or the natural person transmitting the communication or on behalf of whom the communication is transmitted and provide the necessary information for recipients to exercise their right to oppose to receiving further written and/or oral marketing messages.

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

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

COMP 17 (Article 17)

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 p***~~**P**roviders of ~~***an***~~ electronic communications service**s** shall **comply with the security obligations as prescribed Regulation (EU) 2016/679 and [European Electronic Communications Code].** ~~***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***~~**. As regards the security of networks and services and related security obligations, the obligations of Article 40 of the [European Electronic Communications Code] shall apply mutatis mutandis to all services in the scope of this Regulation. This Article shall be without prejudice to the obligations provided for in Articles 32 to 34 of Regulation (EU) 2016/679 and the obligations provided for in Directive (EU) 2016/1148.**

1a. Providers of electronic communications services shall ensure that there is sufficient protection in place against unauthorised access or alterations to the electronic communications data, and that the confidentiality and integrity of the communication in transmission or stored are also guaranteed by technical measures according to the state of the art, such as cryptographic methods including end-to-end encryption of the electronic communications data. When encryption of electronic communications data is used, decryption by anybody else than the user shall be prohibited. Notwithstanding Article 11 of this Regulation, member States shall not impose any obligations on electronic communications service providers or software manufacturers that would result in the weakening of the confidentiality and integrity of their networks and services or the terminal equipment, including the encryption methods used.

1b. Providers of electronic communications services, providers of information society services, and manufacturers of software permitting the retrieval and presentation of information on the internet shall not use any means, no matter if technical, operational, or by terms of use or by contracts, that could prevent users and subscribers from applying the best available techniques against intrusions and interceptions and to secure their networks, terminal equipment and electronic communications. Notwithstanding Article 11 of this Regulation, breaking, decrypting, restricting or circumventing such measure taken by users or subscribers shall be prohibited.

1c. In the case of a particular risk that may compromise the security of networks, electronic communications services, information society services or software, the relevant provider or manufacturer shall inform all subscribers of such a risk and, where the risk lies outside the

scope of the measures to be taken by the service provider, inform subscribers of any possible remedies. It shall also inform the relevant manufacturer and service provider.

Recitals

(37) Service providers who offer electronic communications services should **process electronic communications data in such a way as to prevent unauthorised processing, including access, or alteration. They should ensure that such unauthorised access or alteration can be detected, and also ensure that electronic communications data are protected by using state-of the art software and cryptographic methods including encryption technologies. Service providers should also** inform ~~***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. **The obligations of Article 40 of the [European Electronic Communications Code] should apply to all services within the scope of this Regulation as regards the security of networks and services and related security obligations thereto.**

COMP 18 (Article 18)

CHAPTER IV
INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT

Article 18
Independent supervisory authorities

1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. **Where Regulation (EU) 2016/679 refers to data subjects, t**~~***T***~~he tasks and powers of the supervisory authorities shall be exercised with regard to end-users **under this Regulation. Where Regulation (EU) 2016/679 refers to data controllers, the tasks and powers of the supervisory authorities shall be exercised with regard to providers of electronic communications services and information society services, and manufacturers of software under this Regulation.**

2. The supervisory authority or authorities referred to in paragraph 1 shall cooperate whenever appropriate with national regulatory authorities established pursuant to the [Directive Establishing the European Electronic Communications Code].

Recitals

(38) To ensure full consistency with Regulation (EU) 2016/679, The enforcement of the provisions of this Regulation should be entrusted to the same authorities responsible for the enforcement of the provisions Regulation (EU) 2016/679 and this Regulation relies on the consistency mechanism of Regulation (EU) 2016/679. Member States should be able to have more than one supervisory authority, to reflect their constitutional, organisational and administrative structure. The supervisory authorities should also be responsible for monitoring the application of this Regulation regarding electronic communications data for legal entities. **Where more than one supervisory authority is established in a Member State, such authorities should cooperate with each other. They should also cooperate with the authorities appointed to enforce the European Electronic Communications Code and other relevant enforcement authorities, such as the authorities tasked with consumer protection.** 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, **including adopting binding decisions,** 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, **including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers,** without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.

COMP 19 (Article 19)

Article 19
European Data Protection Board

1. The European Data Protection Board, established under Article 68 of Regulation (EU) 2016/679, shall have competence to ensure the consistent application of this Regulation. To that end, the European Data Protection Board shall exercise the tasks laid down in Article 70 of Regulation (EU) 2016/679. The Board shall also have the following tasks:

(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 and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation.

(ba) draw up guidelines for supervisory authorities concerning the application of Article 9 paragraph (1) and the particularities of expression of consent by legal entities;

(bb) issue guidelines to determine which technical specifications and signalling methods fulfil the conditions and objectives pursuant to point 1a (new) of Article 10;

(bc) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph for the purpose of further specifying the criteria and requirements for types of services that may be requested for purely individual or work-related usage as referred to in Article 6 point (3anew);

(bd) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph for the purpose of further specifying the criteria and requirements for:

(i) measuring the reach of an information society service referred to in Article 8 paragraph (1) point (d),

(ii) security updates referred to in Article 8 paragraph (1) point (da);

(iii) the interference in the context of employment relationships referred to in Article 8 paragraph (1) point (db);

(iv) the processing of information emitted by the terminal equipment referred to in Article 8 paragraph (2) point (c);

(v) technical specifications and signalling methods that fulfil the conditions for consent and objection pursuant to Article 8 (2a);

(vi) software settings referred to in Article 10 paragraph (1) and (2); and

(vii) technical measures to ensure confidentiality and integrity of the communication pursuant to Article 17 paragraph (1).

Recitals

(7) The **European Data Protection Board** ~~***Member States***~~ should, **where necessary, issue guidance and opinions** ~~***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***~~ **Cooperation and consistency between Member States, in particular between national Data Protection Authorities, is essential to** maintain a balance between the protection of private life and personal data and the free movement of electronic communications data.

(38a) The enforcement of the provisions of this Regulation often requires cooperation between the national supervisory authorities of two or more Member States, for example in combating interferences with the confidentiality of the terminal equipment. In order to ensure a smooth and rapid cooperation in such cases, the procedures of the cooperation and consistency mechanism established under Regulation 2016/679/EU should apply to Chapter II of this Regulation. Therefore, the European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, in particular by issuing opinions in the context of the consistency mechanisms or by adopting binding decisions in the context of dispute resolution as provided in Article 65 of Regulation 2016/679/EU, as regards Chapter II of this Regulation.

COMP 20 (Article 20)

Article 20
Cooperation and consistency procedures

Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For this purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII of Regulation (EU) 2016/679 regarding the matters covered by this Regulation.

COMP 21 (Article 21)

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 **and, where applicable, every body, organisation or association,** shall have the same remedies provided for in Articles 77, 78, ~~***and***~~ 79 **and 80** of Regulation (EU) 2016/679.

1a. Without prejudice to any other administrative or non-judicial remedy, every end-user of electronic communications services shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning him or her. End-users shall also have such a right where the supervisory authority does not handle a complaint or does not inform the end- user within three months on the progress or outcome of the complaint lodged. Proceedings against a supervisory authority shall be brought before the court of the Member State where the supervisory authority is established.

1b. Every end-user of the communications services shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed. Those proceedings against a provider of electronic communication service, the provider of a publicly available directory, software provider enabling electronic communication or persons sending direct marketing commercial communications or collecting information related to or stored in the end-users terminal equipment shall be brought before the courts of the Member State where they have an establishment. Alternatively, such proceedings shall be brought before the court of the Member State of the habitual residence of the end-user.

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.

COMP 22 (Article 22)

Article 22
Right to compensation and liability

Any end-user of electronic communications services who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the infringer for the damage suffered, unless the infringer proves that it is not in any way responsible for the event giving rise to the damage in accordance with Article 82 of Regulation (EU) 2016/679.

COMP 23 (Article 23)

Article 23
General conditions for imposing administrative fines

1. For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this Regulation, **mutatis mutandis.**

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;*~~

(aa) the obligations of the providers of electronic communications services pursuant to Article 11c;

~~*(b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;*~~

(ba) the obligations of the providers of publicly available number-based interpersonal communication services pursuant to Article 12, 13 and 14.

(c) the obligations of the providers of publicly available directories pursuant to Article 15;

(d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16.

3. Infringements of the **following provisions of this Regulation** ~~*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**:**

(a) the principle of confidentiality of communications pursuant to Article 5;

(b) the permitted processing of electronic communications data, pursuant to Article 6,

(c) the time limits for erasure and the confidentiality obligations pursuant to Article 7;

(d) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8;

(e) the requirements for consent pursuant to Article 9;

(f) the obligations of the provider of software enabling electronic communications, pursuant to Article 10;

(g) ***the obligations of the providers of electronic communications services, of the providers of information society services, or of the manufacturers of*** **software permitting the retrieval and presentation of information on the internet pursuant to Article 17.**

~~***4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13, 14, and 17.***~~

4. In the event that the same act or omission by the same person results in non-compliance with both Regulation (EU) 2016/679 and this Regulation, then the maximum administrative fine shall be no more than the maximum administrative fine applicable under this Regulation for that type of infringement.

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.

Recitals

(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.

COMP 24 (Article 24)

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.

COMP 25 (Article 25)

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 data 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.

Recitals

(41) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons **in the provision and use of electronic communication services** and in particular their right to ~~***the protection***~~ **respect of their private life and communications with regard to the processing** of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to supplement this Regulation. In particular, delegated acts should be adopted in respect of the information to be presented, including by means of standardised icons in order to give an easily visible and intelligible overview of the collection of information emitted by terminal equipment, its purpose, the person responsible for it and of any measure the ~~***end***~~ user of the terminal equipment can take to minimise the collection. Delegated acts are also necessary to specify a code to identify direct marketing calls including those made through automated calling and communication systems. It is of particular importance that the Commission carries out appropriate consultations and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016[5]. 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.

[5] 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).

COMP 26 (Article 26)

Article 26
Committee

1. **For the purpose of Article 13 (2),** the Commission shall be assisted by the Communications Committee established under Article 110 of the [Directive establishing the European Electronic Communications Code. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011 29 .

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

COMP 27 (Article 27)

CHAPTER VII

FINAL PROVISIONS

Article 27
Repeal

1. Directive 2002/58/EC **and Commission Regulation 611/2013 are** ~~***is***~~ repealed with effect from ~~**25** ***May*** **2018**~~**.[XXX]**

2. References to the repealed Directive shall be construed as references to this Regulation.

COMP 28 (Article 28)

Article 28
Monitoring and evaluation clause

By ~~***1 January 2018***~~ **[the date of entry into force of this Regulation]** at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation.

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.

COMP 29 (Article 29)

Article 29
Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

2. It shall apply ~~***from* 25 *May* 2018~~ **one year from [the date of entry into force of this Regulation]**

Recitals

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