Council of the European Union

Brussels, 10 July 2018
(OR. en)

10975/18

Interinstitutional File:
2017/0003(COD)

TELECOM 221
COMPET 513
MI 522
DATAPROTECT 149
CONSOM 205
JAI 748
DIGIT 147
FREMP 123
CYBER 158
CODEC 1253

NOTE

From:	Presidency
To:	Delegations
No. Cion doc.:	5358/17 TELECOM 12 COMPET 32 MI 45 DATAPROTECT 4 CONSOM 19 JAI 40 DIGIT 10 FREMP 3 CYBER 10 IA 12 CODEC 52
Subject:	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text

I. INTRODUCTION

For the purpose of discussion in the WP TELE meeting of 17 July, delegations will find in Annex a revised text on articles 6, 8 and 10 (and the related recitals) of the ePrivacy proposal (ePR). In the Presidency's view and, also as confirmed at the TTE Council of 8 June, these rather complex provisions contain the core elements of the proposal and still require further discussion at the WP level. The Presidency is committed to advance this important dossier and has therefore proposed changes seeking to accommodate and address a number of delegations' concerns raised during the in-depth discussions in the WP TELE as well as in their written comments.

Modifications to the text are outlined in Section II below. For ease of reference, the latest changes to the text in Annex are underlined.

II. AMENDMENTS TO THE TEXT

1. Permitted processing (Article 6)

From the recent discussions both at the WP and at the Council level it is clear that there is the need for the regulation to be more future-proof. Bearing in mind all possible developments in the rapidly changing digital environment (such as AI, IoT) , the regulatory framework has to be flexible enough to enable the development of innovative services to the benefit of European citizens and the competitive capability of European companies. In order to achieve this effect, the Presidency has taken inspiration from art. 6(4) of the General Data Protection Regulation (GDPR) and has introduced a possibility for **further compatible processing of electronic communications metadata** in **new art. 6(2a)**.

At the same time, it is also clear that the regulation must ensure lawful and responsible treatment of citizens' data and be clear about the **procedures and safeguards** in place. For this purpose, the Presidency has introduced the same safeguards as those present in art. 6(4) of the GDPR and complemented them with extra safeguards specific to the ePrivacy context. Those have been included in the **1st and 2nd subparagraphs of art. 6(2a)**. In addition, the safeguards already present in art. 6(3a) (renumbered as 6(2aa)) have also been kept.

The Presidency recognises that this is an attempt to address those important issues and would like to invite delegations to share their views and, in particular, to indicate examples of the use of further compatible processing in practice so that the Presidency can provide solid explanations in recitals.

In connection with the above changes, the Presidency has also made a corresponding modification in **art. 6(2)(f)**. However, considering the introduction of further compatible processing, the Presidency would like delegations to indicate whether the provision of art. 6(2)(f) is needed at all.

The Presidency has introduced an amendment in **art. 6 (2)(b)** which is to clarify that the everyday business for operators, namely to process metadata for calculating and billing interconnection payments, which sometimes takes place without any relation to an end-user contract (when there are more interconnection providers involved), is allowed.

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

At this stage, the Presidency has not introduced any amendments to art. 8 as such but has, following a delegation's request, provided further details on conditional access to website content in **recital 20**. The Presidency would like to invite delegations to consider whether the new text can work together with art. 7(4) of the GDPR on freely given consent, in particular taking into account the guidance provided by the Working Party 29 in its guidelines on consent (WP29 rev.01).

3. Privacy settings (Article 10)

Throughout the discussions on the ePrivacy proposal, article 10 has raised a lot of concerns, including with regard to the burden for browsers and apps, the competition aspect, the link to fines for non-compliance but also the impact on end-users and the ability of this provision to address e.g. the issue of consent fatigue, thus raising doubts about its added value.Taking these elements into account, the Presidency would like to discuss with delegations the proposal to delete art. 10 and the respective recitals.

(15) Electronic communications data should be treated as confidential. This means that any **interference** ~~with the transmission~~ **processing** of electronic communications data, whether directly by human intervention or through the intermediation of automated processing by machines, without the consent of **all** the communicating parties should be prohibited. ~~**The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee**~~. Interception of electronic communications data may occur, for example, when someone other than the communicating parties, listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications. Interception also occurs when third parties monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned. As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the installation of equipment that gathers data from terminal equipment over targeted areas, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles. Other examples of interception include capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent.

(15aa) In order to ensure the confidentiality of electronic communications data, providers of electronic communications services should apply security measures in accordance with Article 40 of the [Directive establishing the European Electronic Communications Code] and Article 32 of Regulation (EU) 2016/679. Moreover, trade secrets are protected in accordance with Directive (EU) 2016/943.

(15a) The prohibition of interception of electronic communications ~~data~~ content under this Regulation should apply until receipt of the content of the electronic communication by the intended addressee, i.e. during the end-to-end exchange of electronic communications content between end-users. Receipt implies that the end-user gains control over, and has the possiblity to interact with, the individual electronic communications content, for example by recording, storing, printing or otherwise processing such data. The exact moment of the receipt of electronic communications content may depend on the type of electronic communications service that is provided. For instance, depending on the technology used, a voice call may be completed as soon as either of the end-users ends the call. For electronic mail or instant messaging, depending on the technology used, the moment of receipt ~~is~~ may be ~~completed~~ as soon as the addressee has collected the message, typically from the server of the electronic communications service provider. Upon receipt, electronic communications content and related metadata should be erased or made anonymous by the provider of the electronic communications service except when processing is permitted under this Regulation or when the end-users has entrusted the provider of the electronic communications service or another third party to record, store or otherwise process such data in accordance with Regulation (EU) 2016/679.

(16) The prohibition of **processing, including** storage of communications is not intended to prohibit any automatic, intermediate and transient **processing, including** storage of this information insofar as this takes place for the sole purpose of carrying out the transmission in the electronic communications network. It should not prohibit **~~either~~** the processing of electronic communications data **without consent of the end-user** to ensure the security **~~and continuity~~**, **including the availability, authenticity, integrity or confidentiality,** of the electronic communications services, **~~including~~ for example** checking security threats such as the presence of malware **or viruses, or the identification of phishing emails. Spam e-mails may also affect the availability of email services and could potentially impact the performance of networks and e-mail services, which justifies the processing of electronic communications data to mitigate this risk. Providers of electronic communications services are encouraged to offer end-users the possibility to check e-mails deemed as spam in order to ascertain whether they were indeed spam. ~~or~~ Neither should it prohibit** the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc**., nor the processing of metadata necessary for the purpose of management or optimisation of the network. Management or optimisation of the network refers to ~~improving the performance and~~ processing necessary to develop~~ment~~ and manage the scalability and capacity of the network. ~~nor t~~T**h**e processing of ~~meta~~data to make it anonymous ~~nor the processing of metadata to make it anonymous~~ **should not be prohibited either**.

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

(17aa) Metadata ~~that is~~ such as location data can provide valuable information, such as insights in human movement patterns and traffic patterns. Such information may, for example, be used for urban planning purposes. Further ~~P~~processing for such purposes ~~of statistical counting~~ other than for which the metadata where initially collected may take place without the consent of the end-users concerned, provided that such processing is compatible with the purpose for which the metadata are initially collected, certain additional conditions are met and safeguards are in place, including the consultation of the supervisory authority and the requirement to anonymise the result before sharing the analysis with third parties. As end-users attach great value to the confidentiality of their communications, including their physical movements, such data cannot be used to determine the nature or characteristics on an end-user or to build a profile of an end-user, in order to, for example, avoid that the data is used for segmentation purposes, to monitor the behaviour of a specific end-user or to draw conclusions concerning the private life of an end-user. For the same reason, the end-user must be provided with information about these processing activities taking place ~~for statistical counting~~ and given the right to object to such processing.

(17a) The processing of electronic communications metadata should also be regarded to be permitted where it is necessary in order to protect an interest which is essential for the life of the end-users who are natural persons or that of another natural person. Processing of electronic communications metadata of an end-user for the protection of the vital interest of an end-user who is a natural person should in principle take place only where the protection of such interests cannot be ensured without that processing.

(17b) Processing of electronic communication metadata for scientific research or statistical counting purposes should be considered to be permitted processing. This type of processing should be subject to ~~further~~ safeguards to ensure privacy of the end-users by employing appropriate security measures such as encryption and pseudonymisation. In addtion, end-users who are natural persons should be given the right to object.

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

(19) The **protection of the** content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications data in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content data to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After electronic communications content has been sent by the end-user and received by the intended end-user or end-users, it may be recorded or stored by the end-user, end-users or by a third party entrusted by them to record or store such data. Any processing of such data must comply with Regulation (EU) 2016/679.

(19a) Services that facilitate end-users everyday life such as index functionality, personal assistant, translation services and services that enable more inclusion for persons with disabilities such as text-to-speech services are emerging. Therefore, processing electronic communications content for services explicitly requested by the end-user for their own individual use, consent should only be requested from the end-user requesting the service taking into account that the processing must be limited to that purpose, limited to the duration necessary for providing the requested services and shall not adversely affect fundamental rights and interest of another end-user concerned.

(19b) Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal entity having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service. In such case, consent needs to be obtained from the individual concerned.

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

Not all cookies are needed in relation to the purpose of the provision of the website service. Some are used to provide for additional benefits for the website operator. **Making access to the website content provided without direct monetary payment conditional to the consent of the end-user to the storage and reading of cookies for additional purposes would normally not be considered disproportionate in particular if the end-user is able to choose between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes on the other hand. Conversely, ~~I~~i**n some cases, making access to website content conditional to consent to the use of such cookies may be considered to be disproportionate. This **~~is for example~~ would normally be** the case for websites providing certain services, such as those provided by public authorities, where the user could be seen as having few or no other options but to use the service, and thus having no real choice as to the usage of cookies.

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

(21a) Cookies can also be a legitimate and useful tool, for example, in **assessing the effectiveness of a delivered information society service, for example of website design and advertising or by helping to** measure~~ing web traffic to~~ **the numbers of end-users visiting** a website**, certain pages of a website or the number of end-users of an application. This is not the case, however, regarding cookies and similar identifiers used to determine the nature of who is using the site**. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities. **Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerablities and other security bugs, provided that such updates do not in any way change the functionality of the hardware or software or the privacy settings chosen by the end-user and the end-user has the possibility to postpone or turn off the automatic installation of such updates. Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not fall under this exception. Consent should not be necessary either if the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment is necessary for the provision of information society services, such as those used by IoT devices (for instance connected devices, such as connected thermostats), requested by the end-user.**

~~(22) The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result, end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the possibility to express consent by using the appropriate settings of a browser or other application. The choices made by end-users when establishing its general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties.~~

~~(22a) Web browsers are a type of software application that permits the retrieval and presentation of information on the internet. Other types of applications, such as the ones that permit calling and messaging or provide route guidance, have also the same capabilities. Web browsers mediate much of what occurs between the end-user and the website. From this perspective, they are in a privileged the position to play an active role to help the end-user to control the flow of information to and from the terminal equipment. More particularly web browsers may be used as gatekeepers, thus helping end-users to prevent information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored. The responsibility for obtaining consent with the storage of a cookie and for any penalties for breach of duty lies on the information society service provider.~~

(23) The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as 'reject third party cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept allow cookies') to lower (for example, 'always accept allow cookies') and intermediate (for example, 'reject third party cookies' or 'only accept allow first party cookies'). Such privacy settings should be presented offered in a an easily visible and intelligible manner. General privacy settings that do not provide the end-user with information about the purpose for which information can be stored on the terminal equipment, or information already stored on that equipment can be processed, as a consequence of the configured privacy settings, cannot signify the end-user's consent to the storing of information on the terminal equipment or the processing of information already stored on that equipment.

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

(25) Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI**, the WiFi signal** etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer **physical movements'** tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, **such as** providing data on the number of people waiting in line, ascertaining the number of people in a specific area, ~~etc~~ **referred to as statistical counting for which the consent of end-users is not needed, provided that such counting is limited in time and space to the extent necessary for this purpose. Providers should also apply appropriate technical and organisations measures to ensure the level if security appropriate to the risks, including pseudonymisation of the data and making it anonymous or erase it as soon it is not longer needed for this purpose**. **Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.** This information may be used for more intrusive purposes, **which should not be considered statistical counting,** such as to send commercial messages to end-users, for example when they enter stores, with personalized offers locations**, subject to the conditions laid down in this Regulation,** ~~.~~ ~~While some of these functionalities do not entail high privacy risks, others do, for example, those involving~~ **as well as** the tracking of individuals over time, including repeated visits to specified locations. ~~Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679.~~

Article 6

Permitted processing of electronic communications data

1. Providers of electronic communications networks and services ~~may~~ **shall be permitted to** process electronic communications data **only** if:

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

(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors **and/or security risks and/or attacks** in the transmission of electronic communications, for the duration necessary for that purpose.

2. **Without prejudice to paragraph 1, ~~P~~p**roviders of electronic communications **networks and** services ~~may~~ **shall be permitted to** process electronic communications metadata **only** if:

(a) it is necessary **for the purposes of network management or network optimisation, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous and for the duration necessary for that purpose,** or to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120[1] for the duration necessary for that purpose; or

(b) it is necessary for **calculating and billing interconnection payments or for the performance of the contract to which the end-user is party, ~~including to the extent more~~ in particular if necessary for** billing, ~~calculating interconnection payments,~~ detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or

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

(c) the end-user concerned has given ~~his or her~~ consent to the processing of ~~his or her~~ communications metadata for one or more specified purposes, including for the provision of ~~specific~~ services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous**; or**

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

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

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

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

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

(f) it is necessary for statistical counting, ~~other than based on electronic communications metadata that constitute location data,~~ or for scientific research purposes, provided it is based on Union or Member State law which shall be proportionate to the aim pursued and provide for specific measures, including encryption and pseudonymisation, to safeguard fundamental rights and the interest of the end-users. Processing of electronic communications metadata under this point shall be done in accordance with paragraph 6 of Article 21 and paragraphs 1, 2 and 4 of Article 89 of Regulation (EU) 2016/679.

2a. Where the processing for a purpose other than that for which the electronic communications metadata have been collected is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11 , the provider shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the electronic communications metadata have been collected and the purposes of the intended further processing;

(b) the context in which the electronic communications metadata have been collected, in particular regarding the relationship between end-users concerned and the provider;

(c) the nature of the electronic communications metadata, in particular where such data could reveal categories of data, pursuant to Article 9 of Regulation (EU) 2016/679;

(d) the possible consequences of the intended further processing for end-users;

(e) the existence of appropriate safeguards.

Such processing, if considered compatible, may only take place, provided that:

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

- the processing is limited to electronic communications metadata that is pseudonymised,

- the electronic communications metadata is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.

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

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

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

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

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

3. **Without prejudice to paragraph 1, ~~P~~p**roviders of the electronic communications **networks and** services ~~may~~ **shall be permitted to** process electronic communications content only:

~~(a) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or~~

(aa) for the purpose of the provision of an explicitly requested services by an end-user for purely individual use if the requesting end-user has given consent and where such requested processing does not adversely affect fundamental rights and interest of another person concerned and does not exceed the duration necessary for the provision of the requested services and is limited to that purpose only; or

(b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has **prior to the processing carried out an assessment of the impact of the envisaged processing operations on the protection of electronic communications data and** consulted the supervisory authority. ~~Points (2) and (3) of~~ Article 36**(2) and (3)** of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.

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

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

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

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

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

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

…

Article 8

Protection of ***end-users' terminal equipment*** *information* ~~***stored in terminal equipment of end-users and related to or processed by or emitted by end-users' terminal such equipment***~~

1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or

(b) the end-user has given his or her consent; or

(c) it is necessary for providing an information society service requested by the end-user; or

(d) ~~if~~ it is necessary for ~~web~~ audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user **or by a third party on behalf of the provider of the information society service provided that conditions laid down in Article 28 of Regulation (EU) 2016/679 are met~~.~~; or**

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

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

(i) security updates are necessary and do not in any way change the privacy settings chosen by the end-user are not changed ~~in any way~~,

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

(iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates; or

~~(f) it is necessary to locate, at the time of the incident, a caller of an emergency call from the terminal by organisations dealing with emergency communications.~~

2. The collection of information emitted by terminal equipment **of the end-user** to enable it to connect to another device and, or to network equipment shall be prohibited, except ~~if~~ **on the following grounds**:

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

(b) the end-user has given his or her consent; or

(c) it is necessary for the purpose of statistical counting that is limited in time and space to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose.

~~(b)~~**2a. For the purpose of paragraph 2 points (b) and (c),** a clear and prominent notice ~~is~~ **shall be** displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.

2b. For the purpose of paragraph 2 points (b) and (c), ~~T~~**t**he collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.

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

4. **[**The Commission shall be empowered to adopt delegated acts in accordance with Article 2~~5~~**7** determining the information to be presented by the standardized icon and the procedures for providing standardized icons.**]**

…

Article 10

Information and options for privacy settings to be provided

1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third any other parties than the end-user from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.

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

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

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

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