012985/EU XXVII. GP
Eingelangt am 21/02/20

Council of the European Union

Brussels, 21 February 2020
(OR. en)

5979/20

Interinstitutional File:
2017/0003(COD)

TELECOM 14
COMPET 35
MI 31
DATAPROTECT 18
CONSOM 21
JAI 115
DIGIT 8
FREMP 12
CYBER 17
CODEC 97

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	14068/19 + COR 1
No. Cion doc.:	5358/17
Subject:	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

I. INTRODUCTION

Delegations will find in Annex a revised part of the ePrivacy proposal, which introduces modifications in **articles 6 and 8 and the related recitals**.

The Presidency would like to provide sufficient time for delegations to analyse the new text and has therefore decided to devote **two WP TELE meetings** to the examination of these changes:

- on 5 March, the Presidency will present to the group the proposed modifications. In that meeting, delegations will also have an opportunity to ask for additional explanations or clarifications and to express their first reactions on the compromise proposal.

www.parlament.gv.at

- for the meeting on 12 March, the Presidency foresees an article-by-article examination of the amended provisions and would like to invite delegations to present their position on the changes, as well as, if needed, further drafting suggestions to the text. The Presidency would also like to signal to delegations that it is currently reflecting about possible modifications to other provisions, such as those related to the scope, and intends to issue, at the beginning of March, an additional document to be also discussed during the meeting on 12 March.

II. AMENDMENTS TO THE TEXT

During the recent discussions in the WP TELE, Coreper and in the December TTE Council, it became clear that majority of delegations could not support the text as it stands. A number of them expressed their wish for more substantial changes in the proposal. Based on those discussions and after a period of reflection on this topic, the Presidency is proposing to simplify the text of some of the core provisions and to further align them with the GDPR.

The provisions where the Presidency has introduced amendments are listed below. For ease of reference, the changes introduced by this document are underlined.

Permitted processing (Articles 6 to 6b) and related recitals

- in **art. 6(1)(a)**, the Presidency reverted to the previous text on transmission of electronic communications. This modification has to be read together with the changes introduced in art. 6b, in particular in paragraph (1)(ca).

- in **art. 6b(1)(ca)** the Presidency introduced a possibility to process metadata for the provision of electronic communications service for which the end-user has concluded a contract.

- in **art. 6b(1)(d)** the Presidency has introduced a possibility to process metadata for legitimate interests. This legal ground is accompanied, in line with the GDPR, by a number of conditions and safeguards provided in a **new art. 6b(2)**.

www.parlament.gv.at

- in connection with the two modifications listed above, the Presidency has deleted **art. 6b(a), (b) and (f)** as it is considered that those points are covered by the above new additions and the Presidency would like to avoid overlaps or duplications. These changes are also accompanied by changes in related **recitals 17, 17b and 17c** and deletion of **recital 18**. In the similar logic, the Presidency has deleted **art. 6c** on compatible processing.

N.B. The Presidency does not intend to discuss art. 6d on child imagery at this stage. The provision remains in square brackets.

Protection of end-users' terminal equipment information (Article 8) and related recitals

- in **art. 8(1)(g)** the Presidency has also introduced a new ground for processing for legitimate interests. Also in this case, the legal ground is accompanied by a number of conditions and safeguards provided in a **new art. 8(1a)**. In connection with this change, the Presidency has deleted **art. 8(1)(da) and (e)** as it is considered that they are covered by the new addition on legitimate interests. The changes are also reflected in the accompanying **recitals 20, 21, 21b and 21c**.

Related modifications

- in **art. 7**, the references have been adapted to the changes introduced in art. 6.

- the Presidency has tried to group various recital parts relating to the same topic. This lead to moving parts of the text from one recital to another, however, mostly without changes in substance. This would concern in particular:

  - moving the last part of **recital 16** to **recital 17b**;

  - moving text parts of **recital 17** and the substance of the whole **recital 17aa** to **recital 17b**.

www.parlament.gv.at

(16) The prohibition of **processing, including** storage of communications is not intended to prohibit any automatic, intermediate and transient **processing, including** storage of this information insofar as this takes place for the sole purpose of carrying out the transmission in the electronic communications network**. Processing of electronic communications data by providers of electronic communications services and networks should only be permitted in accordance with this Regulation.** It should not prohibit ~~either~~ the processing of electronic communications data **without consent of the end-user** to ensure the security ~~and continuity~~, **including the availability, authenticity, integrity or confidentiality,** of the electronic communications services, ~~including~~ **for example** checking security threats such as the presence of malware **or viruses, or the identification of phishing. Security measures are essential to prevent personal data breaches in electronic communications. Spam electronic messages may also affect the availability of the respective services and could potentially impact the performance of networks and services, which justifies the processing of electronic communications data to mitigate this risk. Such security measures, including anti-spam measures, should be proportionate and should be performed in the least intrusive manner. Providers of electronic communications services are encouraged to offer end-users the possibility to check electronic messages deemed as spam in order to ascertain whether they were indeed spam.** ~~**Moreover, the prohibition of processing should neither prohibit** the processing of metadata to ensure the necessary quality of service requirements, such as latency, jitter etc~~**., nor the processing of metadata necessary for the purpose of management or optimisation of the network. Management or optimisation of the network refers to processing necessary to developand manage the scalability and capacity of the network. The processing of data to make it anonymous should not be prohibited either.**

www.parlament.gv.at

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

www.parlament.gv.at

~~(17aa) Metadata such as location data can provide valuable information, such as insights in human movement patterns and traffic patterns. Such information may, for example, be used for urban planning purposes. Further processing for such purposes other than for which the metadata 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, where appropriate, the consultation of the supervisory authority, an impact assessment by the provider of electronic communications networks and services and the requirement to genuinely anonymise the result before sharing the analysis with third parties. As end-users attach great value to the confidentiality of their communications, including their physical movements, such data cannot be used to determine the nature or characteristics on an end-user or to build a profile of an end-user, in order to, for example, avoid that the data is used for segmentation purposes, to monitor the behaviour of a specific end-user or to draw conclusions concerning the private life of an end-user. For the same reason, the end-user must be provided with information about these processing activities taking place and given the right to object to such processing.~~

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

www.parlament.gv.at

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

www.parlament.gv.at

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

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

www.parlament.gv.at

~~(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.~~

www.parlament.gv.at

(19) The **protection of the** content of electronic communications pertains to the essence of the fundamental right to respect for private and family life, home and communications protected under Article 7 of the Charter. Any interference with the content of electronic communications should be allowed only under very clear defined conditions, for specific purposes and be subject to adequate safeguards against abuse. This Regulation provides for the possibility of providers of electronic communications services to process electronic communications ~~data~~ **content** in transit, with the informed consent of all the end-users concerned. For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons. When processing such type of ~~data~~ **content**, the provider of the electronic communications service should ~~always~~ consult the supervisory authority ~~prior to the processing~~ **if necessary pursuant to Article 36 (1) of Regulation (EU) 2016/679**. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679. The presumption does not encompass the processing of content ~~data~~ to provide a service requested by the end-user where the end-user has consented to such processing and it is carried out for the purposes and duration strictly necessary and proportionate for such service. After electronic communications content has been ~~sent by the end-user and~~ received by the intended end-user or end-users, it may be recorded or stored by th**ose** ~~end-user,~~ end-users or by a third party entrusted by them to record or store such data **as this kind of processing is outside of the scope of this Regulation**. Any processing of such data must comply with Regulation (EU) 2016/679.

www.parlament.gv.at

A third party should refer to a legal or natural person that does not provide an electronic communications service to the end-user concerned. However, sometimes the same legal or natural person could also provide different kind of services to the same end-user, for example information society service such as cloud storage. With respect to the provision of this other service, the same legal person should be considered as a third party. If the other service is necessary for the provision of the electronic communication service, such as automatic storage of the messages in the cloud by web-based email, the provider of such a service should not be deemed to be a third party.

(19a) Services that facilitate end-users everyday life such as index functionality, personal assistant, translation services and services that enable more inclusion for persons with disabilities such as text-to-speech services are emerging. Processing of electronic communication content might be necessary also for some functionalities used normally in services for individual use, such as searching and organising the messages in email or messaging applications. Therefore, as regards the processing of electronic communications content for services requested by the end-user for their own individual use, consent should only be ~~requested~~ required from the end-user requesting the service taking into account that the processing should not adversely affect fundamental rights and interest of another end-user concerned. Processing of electronic communications data should be allowed with the prior consent of the end-user concerned and to the extent necessary for the provision of the requested functionalities.

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

www.parlament.gv.at

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

www.parlament.gv.at

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

The responsibility for obtaining consent for the storage of a cookie or similar identifier lies on the entity that makes use of processing and storage capabilities of terminal equipment or collects information from end-users' terminal equipment, such as an information society service provider or ad network provider. Such entities may request another party to obtain consent on their behalf. The end-user's consent to storage of a cookie or similar identifier may also entail consent for the subsequent readings of the cookie in the context of a revisit to the same website domain initially visited by the end-user.

~~**Making access to website content provided without direct monetary payment dependent on the consent of the end-user to the storage and reading of cookies for additional purposes would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer [by the same provider] that does not involve consenting to data use for additional purposes, on the other hand. Conversely, in some cases, making access to website content dependent on consent to the use of such cookies may be considered, in the presence of a clear imbalance between the end-user and the service provider as depriving the end-user of a genuine choice. This would normally be the case for websites providing certain services, such as those provided by public authorities. Similarly, such imbalance could exist where the end-user has only few or no alternatives to the service, and thus has no real choice as to the usage of cookies for instance in case of service providers in a dominant position.**~~

www.parlament.gv.at

(20a) End-users are often requested to provide consent to the storage and access to stored data in their terminal equipment, due to the ubiquitous use of tracking cookies and similar tracking technologies. As a result, end-users may be overloaded with requests to provide consent. This can lead to a situation where consent request information is no longer read and the protection offered by consent is undermined. Implementation of technical means in electronic communications software to provide specific and informed consent through transparent and user-friendly settings, can be useful to address this issue. Where available and technically feasible, an end user may therefore grant, through software settings, consent to a specific provider for the use of processing and storage capabilities of his or her terminal equipment for one or multiple specific purposes across one or more specific services of that provider. For example, an end-user can give consent to the use of certain types of cookies by whitelisting one or several providers for their specified purposes. Providers of software are encouraged to include settings in their software which allows end-users, in a user friendly and transparent manner, to manage consent to the storage and access to stored data in their terminal equipment by easily setting up and amending whitelists and withdrawing consent at any moment.

www.parlament.gv.at

(21) ~~Exceptions to the obligation to obtain consent to make u~~**U**se of the processing and storage capabilities of terminal equipment or ~~to~~ access **to** information stored in terminal equipment **without the consent of the end-user** should be limited to situations that involve ~~no, or~~ only very limited, intrusion of privacy. For instance, consent should not be requested for authorizing the technical storage or access which is ~~strictly~~ necessary and proportionate for the ~~legitimate~~ purpose of ~~enabling the use of~~ **providing** a specific service ~~explicitly~~ requested by the end-user. This may include the storing of cookies for the duration of a single established session on a website to keep track of the end-user's input when filling in online forms over several pages**, authentication session cookies used to verify the identity of end-users engaged in online transactions or cookies used to remember items selected by the end-user and placed in shopping basket**. **In the area of IoT services which rely on~~/deploy~~ connected devices (such as connected thermostats, connected medical devices, smart meters or automated and connected vehicles), the use of the processing and storage capacities of those devices and access to information stored therein should not require consent to the extent that such use or access is necessary for the provision of the service requested by the end-user. For example, storing of information in or accessing information from a smart meter might be considered as necessary for the provision of a requested energy supply service to the extent the information stored and accessed is necessary for the stability and security of the energy network or for the billing of the end-users' energy consumption**

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

www.parlament.gv.at

~~**To the extent that use is made of processing and storage capabilities of terminal equipment and information from end-users' terminal equipment is collected for other purposes than for what is necessary for the purpose of carrying out the transmission of an electronic communication over an electronic communications network or for the provision of the service requested, consent should be required. In such a scenario, consent should normally be given by the end-user who requests the service from the provider of the service**~~.

(21a) Cookies can also be a legitimate and useful tool, for example, in **assessing the effectiveness of a delivered information society service, for example of website design and advertising or by helping to** measure~~ing web traffic to~~ **the numbers of end-users visiting** a website**, certain pages of a website or the number of end-users of an application. This is not the case, however, regarding cookies and similar identifiers used to determine the nature of who is using the site, which always require the consent of the end-user**. Information society providers that engage in configuration checking to provide the service in compliance with the end-user's settings and the mere logging of the fact that the end-user's device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.

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

www.parlament.gv.at

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

Similarly, 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 be considered as a legitimate interest.

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

[1] **As amended by Directive (EU) 2018/1808**

www.parlament.gv.at

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

~~**Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security 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.**~~

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

www.parlament.gv.at

Article 6

Permitted processing of electronic communications data

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

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

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

(c) it is necessary to detect or prevent security risks or attacks on end-users' terminal equipment;

(d) it is necessary for compliance with a legal obligation to which the provider is subject laid down by Union or Member State law ~~in accordance with Article 11~~, which respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security.

www.parlament.gv.at

2. Electronic communications data shall only be permitted to be processed for the duration necessary for the specified purpose or purposes according to Articles 6 to 6be and if the specified purpose or purposes cannot be fulfilled by processing information that is made anonymous.

3. A third party acting on behalf of a provider of electronic communications network or services may be permitted to process electronic communications data in accordance with Articles 6 to 6be provided that the conditions laid down in Article 28 of Regulation (EU) 2016/679 are met.

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

Permitted processing of electronic communications content

~~3~~**1**. **Without prejudice to Article ~~(~~6~~)~~(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~~

(a) for the purpose of the provision of an service requested by an end-user for purely individual use if the requesting end-user has given consent and where such requested processing does not adversely affect fundamental rights and interests of another person concerned; or

www.parlament.gv.at

(b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes ~~that cannot be fulfilled by processing information that is made anonymous, and~~

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

Article 6b [previous art 6(2)]

Permitted processing of electronic communications metadata

~~2.~~**1.** **Without prejudice to Article ~~(~~6~~)~~(1), ~~P~~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, or** to meet mandatory **technical** quality of service requirements pursuant to [Directive **(EU) 2018/1972** establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120[2] for the duration necessary for that purpose; or~~

~~[2] 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).~~

www.parlament.gv.at

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

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

(ca) it is necessary for the provision of an electronic communications service for which the end-user has concluded a contract; or

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

(e) it is necessary for the purpose of the legitimate interests pursued by the electronic communications service or network provider, except when such interest is overridden by the interests or fundamental rights and freedoms of the end-user, in particular where the end-user is a child.

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

www.parlament.gv.at

~~(f) it is necessary for statistical purposes, or for scientific research purposes, provided it is in accordance with Union or Member State law and subject to appropriate safeguards, including encryption and pseudonymisation, to protect fundamental rights and the interest of the end-users. Processing of electronic communications metadata under this point shall be done in accordance with paragraph 6 of Article 21 and paragraphs 1, 2 and 4 of Article 89 of Regulation (EU) 2016/679.~~

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

(a) carry out an assessment of the impact of envisaged processing on the confidentiality of communications and the privacy of end-users in accordance with Article 35 of Regulation (EU) 2016/679, which may result in the prior consultation of the supervisory authority in accordance with Article 36(1) to (3) of Regulation (EU) 2016/679;

(b) inform the end-user of the envisaged processing operations based on paragraph 1(e) and of the end-user's right to object to such processing, at any time, free of charge and in an easy and effective manner; and

(c) implement appropriate technical and organisational measures, such as pseudonymisation and encryption.

www.parlament.gv.at

~~Article 6c~~

~~Compatible processing of electronic communications metadata~~

~~1. Where the processing for a purpose other than that for which the electronic communications metadata have been collected under Articles 6 and 6b is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11 , the provider of electronic communications networks and services shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications metadata are initially collected, take into account, inter alia:~~

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

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

~~(c) the nature of the electronic communications metadata as well as the modalities of the intended further processing, in particular where such data or the intended further processing could reveal categories of data, pursuant to Article 9 or 10 of Regulation (EU) 2016/679;~~

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

~~(e) the existence of appropriate safeguards, such as pseudonymisation and encryption.~~

www.parlament.gv.at

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

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

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

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

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

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

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

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

www.parlament.gv.at

[**Article 6d**

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

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

(i) it creates a unique, non-reconvertible digital signature ("hash") of material attached to electronic communications for the sole purpose of comparing that hash with a database containing hashes of material previously reliably identified as constituting material defined in Article 2(c) of Directive 2011/93/EU;

(ii) electronic communications data and hashes of material attached to electronic communications are erased immediately after comparison with the database, except in the cases where material constituting material defined in Article 2(c) of Directive 2011/93/EU has been detected by virtue of a hash.

www.parlament.gv.at

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

3. The provider of number-independent interpersonal communications services shall inform the users about the processing taking place in accordance with this article and provide suitable complaint procedure.]

www.parlament.gv.at

Article 7

Storage and erasure of electronic communications data

1. ~~Without prejudice to points (b) of Article 6(1) and points (a), and (b) of Article 6(3)a, t~~**T**he provider of the electronic communications service shall erase electronic communications content or make that data anonymous **when it is no longer necessary for the purpose of processing in accordance to article 6(1) and 6a(1)** ~~after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded, or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data in accordance with Regulation (EU) 2016/679.~~

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

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

4. Union or Member state law may provide ~~in accordance with Article 11~~ that the electronic communications metadata is retained, ~~in order~~ to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security, for a limited period that is longer than the period set out in this Article .

www.parlament.gv.at

Article 8

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

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

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

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

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

(d) ~~if~~ it is necessary for ~~web~~ audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user **or by a third party, or by third parties jointly, on behalf of ~~the~~ one or more providers of the information society service provided that conditions laid down in Article 28, or where applicable Article 26, of Regulation (EU) 2016/679 are met; or**

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

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

~~(i) such update is necessary for security reasons and does not in any way change the privacy settings chosen by the end-user are not changed in any way,~~

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

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

www.parlament.gv.at

(f) it is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number '112' or a national emergency number, in accordance with Article 13(3).

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

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

1a. Service providers using processing and storage capabilities of the end-user's terminal equipment or collecting information from the end-user's terminal equipment pursuant to paragraph 1(g) shall not share the information with any third party other than its processors, acting in accordance with Article 28 of Regulation (EU) 2016/679 *mutatis mutandis*, unless it has been made anonymous. Prior to any use of processing or storage facilities in, or collection of information from the end-user's terminal equipment, the service provider shall:

(a) carry out an assessment of the impact of the use of the processing and storage capabilities or the collection of information from the end-users' terminal equipment and of the envisaged processing on the confidentiality of communications and the privacy of end-users in accordance with Article 35 of Regulation (EU) 2016/679, which may result in the prior consultation of the supervisory authority in accordance with Article 36(1) to (3) of Regulation (EU) 2016/679;

(b) inform the end-user of the envisaged processing operations based on paragraph 1(g) and of the end-user's right to object to such processing, free of charge, at any time, and in an easy and effective manner; and

www.parlament.gv.at

c) implement appropriate technical and organsational measures, such as pseudonymisation and encryption.

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

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

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

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

(d) it is necessary for providing a service requested by the end-user.

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

2b. For the purpose of paragraph 2 points (b) and (c), ~~T~~**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.

www.parlament.gv.at

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.

www.parlament.gv.at