Council of the European Union

Brussels, 7 March 2018
(OR. en)

6726/18

Interinstitutional File:
2017/0003 (COD)

TELECOM 53
COMPET 125
MI 128
DATAPROTECT 24
CONSOM 51
JAI 184
DIGIT 22
FREMP 24
CYBER 40
CODEC 298

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 purposes of the **WP TELE meeting of 13 March**, delegations will find in Annex a revised text of the ePrivacy proposal (ePR), focusing on **Articles 1, 5, 6, 7, 12, 13 and 14 the related recitals**. The revisions are inspired by WP TELE discussions held on the basis of the Presidency discussion papers (doc. 5165/18 and 5569/18) and on the written comments provided by delegations in this context.

The Annex only includes provisions that the Presidency added or modified. For ease of reference, the latest changes to the text are underlined.

Delegations will find in section II an overview of the amendments introduced in the text. With regard to article 6 and processing of metadata, the Presidency would like to gather further views from the delegations before suggesting a new text. In section III, delegations will therefore find elements for their consideration in the context of article 6.

II. AMENDMENTS TO THE TEXT

a. Link to the General Data Protection Regulation (GDPR)

The Presidency has provided further clarifications on the link between the ePR and the GDPR in **recitals 2aa and 2a**, including on when the ePR particularises and when it complements the GDPR.

b. 'In transmission' and storage and erasure of data

Following calls for further clarification of the concept of data 'in transmission', the Presidency has included **new recital 15a** which provides examples of the moment of completion of the transmission.

The recital also provides the link to the obligation (under art. 7) to erase or anonymise data upon completion of the transmission and clarifies that, when the end-user has entrusted a third party to record, store or otherwise process data, this is done in accordance with the GDPR. Following this clarification, the last sentences of **art. 7(1) and 7(2)** have been deleted as redundant.

c. Ancillary services

In the Presidency's understanding most delegations seem to support that services, which enable interpersonal and interactive communication merely as an ancillary feature that is intrinsically linked to another service, should remain within the scope of the ePR. The Presidency is also of the view that certain questions about which services fall within this category could actually be addressed by recalling which services constitute interpersonal communication services. In other words, an ancillary feature is only covered if it qualifies as an interpersonal communication service. The modifications and examples introduced in **recital 11a** are meant to clarify this.

d. Machine-to-machine communications (M2M)

During the discussion on doc. 5165/18 most delegations seemed to support to keep the transmission services used for the provision of M2M services in the scope of the ePR. The Presidency is also of the view that the issue of distinction between the transmission and application layers is sufficiently addressed in the European Electronic Communications Code (EECC) at the level of definitions. While the transmission layer constitutes an electronic communications service, the application layer is out of the scope. Bearing in mind that the ePR specifically refers to the EECC definitions, there seems to be no need for the ePR to specifically address this issue in the operative part of the ePR. The Presidency has therefore proposed to delete **art. 5(2)**.

In addition, some delegations supported the idea of clarifying that the consent (including the consent in the context of M2M communications) may be obtained as a one-off consent at the moment of conclusion of the contract. Such clarification has been provided in **new recital 19b**.

e. Article 13

The **title of art. 13** has been amended to better reflect the text of the article.

A new exception has been added in **art. 13(1a)** that addresses situations where an anonymous call is made by an emergency organisation for emergency purposes to end-users who had chosen to reject anonymous calls. In such a case, the provider shall, where technically possible, override the end-user's choice.

Art. 13(3) has been amended to provide for more technology neutrality. This change comes together with a modification in **recital 28**.

f. Article 14

The Presidency has divided **art. 14** into two paragraphs to provide for better clarity.

Following the request by some delegations the word 'unwanted' has been reinserted in the text of **art. 14** and also in corresponding **recital 29**. This has been reflected also in **art. 13(2)**.

Recital 29 has been amended to provide examples of unwanted, malicious or nuisance calls addressed in art. 14.

g. Other changes

Following a request by some delegations, the Presidency has clarified in **recital 8** that processing of electronic communications data by end-users as recipients for different purposes, such as ensuring networks and information society, is not covered by ePR.

The deletion of the phrase 'electronic communications' in **art. 1(3) and in recital 2a** is meant as a clarification as the ePR does not deal only with personal data that are electronic communications data but also with other types of personal data.

Drafting improvements were introduced in **art. 5(1)**.

According to the amended **art. 12(4)** the providers should provide information not only about the options set out in art. 12(1) but also about the exceptions set out in art. 13(1), (1a) and (2). Also in art. 12(4), the phrase 'publicly available' has been deleted for consistency purposes.

III. PERMITTED PROCESSING OF METADATA DATA (ARTICLE 6(2))

During the discussions on doc. 5165/18 some delegations expressed interest in exploring the option to expand the permitted processing of electronic communications metadata to encompass more purposes than in doc. 15333/17 and the legality of such option. However, some delegations were satisfied with the text in doc. 15333/17 and a few others favoured the introduction of legitimate interest in line with the GDPR. Further to these discussions, the Presidency would request Member States to reflect on several elements, to share their views and, if they are supportive of expanding article 6(2), share their preferred way forward.

Such an option should be analysed against the full data protection and privacy legal framework, in particular, the Charter of Fundamental Rights and the interpretation thereof in the case law of the Court of Justice of the European Union (CJEU) and the GDPR.

In the context of the assessment of whether an interference with article 7 (respect for private life and communications) and article 8 (protection of personal data) of the Charter occurs, the CJEU refers in the Joined Cases C-293/12 and C-594/1 (*Digital Rights*), to the sensitive nature of electronic communications metadata. In Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige*), the CJEU rules regarding electronic communications metadata that it constitutes:

"information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."

The CJEU explains that:

> *"That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."*

Regarding the processing of personal data, the GDPR foresees two different regimes for the processing of personal data and for the processing of special categories of personal data. Electronic communications metadata may reveal special categories of personal data.

One possibility to expand the permitted use of electronic communications metadata would be to broaden the existing permissions. Article 6(2)(a) could be amended to allow for processing for quality of service requirements beyond those that are mandated by EECC or Regulation (EU) 2015/2120. This could be expanded to include for example also processing for network management and optimisation. Moreover, Member States could consider creating an additional permitted use for the offering of better tariffs, products and services to end-users.

Delegations are also asked to assess the possibility of creating a legal basis that goes beyond the above. When considering the validity of such an option and the construction of a possible permitted use, at least the following aspects are relevant:

a) whether the Regulation would set forth specific purposes for which the processing of electronic communications metadata would be permitted, or whether it would establish a non-specific purpose based permission to process electronic communications metadata.

A provision with specific purposes linked to a well-defined public interest and/or interest of the end-user concerned may justify such processing. This would be the case if, for example, the provision would permit the processing of electronic communications metadata if it is necessary to carry out statistics in the public interest.

However, it is highly doubtful whether a non-specific provision enabling the provider to justify an interference on the basis of merely the providers' economic interests would, given the sensitive nature of the data involved, be in line with the case-law of the CJEU. At any rate, such a path would seem hardly compatible with the purpose limitation principle, which is a basic tenet of the GDPR.

b) whether the permitted use would be limited to a sub-set of electronic communications metadata, such as location data, but would not encompass browsing history or calls and would be limited to a specific period of time. Processing could be subject to the condition that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous and that such data is erased or made data anonymous when it is no longer needed to fulfil the purpose, and at the latest 24 hours after its collection, and that only then it can be shared with a third party. No profiling of end-user's over time would be permitted.

Permitted use could also, where technically possible, be limited to electronic communications metadata that does not reveal special categories of personal data pursuant to article 9 of Regulation (EU) 2016/679. Where this would not be technically possible, the (sensitive) nature of such special categories of data would have to be taken into account (by way of analogy with the requirements laid down in article 6(4) of the GDPR).

c) whether end-users are given rights similar are to the ones that are linked to specific legal bases in the GDPR, namely that the end-user shall be informed of specific processing on the basis of such provision and be given the right to object to such processing.

d) which type of safeguards should be required as a tool to mitigate the interference and ensure the proportionality of the permitted processing. Examples that would appear appropriate are *inter alia*:

i) the supervisory authority is consulted. article 36(2) and (3) of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority;

ii) appropriate technical and organisational measures to ensure a level of security appropriate to the risk are applied, which may include encryption or pseudonymisation; and

iii) the provider has concluded that the interests or fundamental rights and freedoms of the end-user are not overridden.

IV. CONCLUSION

At the meetings of 13 March, the Presidency intends to invite delegations to express their **views on the proposed changes as well as on the elements concerning processing of metadata as set out in Section III of this note.**

The Presidency would also like to ask delegations to provide **written comments and drafting suggestions on the issues covered in this note, on articles 18 to 29, as well as on any additional comments on the remaining articles by the end of March**.

…

(2aa) Regulation (EU) 2016/679 regulates the protection of personal data. This Regulation protects in addition the respect for private life and communications, which applies both to end-users who are natural persons and who are legal persons.

(2a) The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679 as regards ~~electronic communications~~ data that qualify as personal data. The provisions particularise Regulation (EU) 2016/679 by translating its principles into specific rules. They complement Regulation (EU) 2016/679 by setting forth rules regarding subject matters that are not within the scope of Regulation (EU) 2016/679. This Regulation therefore does not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. Processing of electronic communications data by providers of electronic communications services and networks should only be permitted in accordance with this Regulation. If no specific rules are established in this Regulation, Regulation (EU) 2016/679 should apply to any processing of ~~electronic communications~~ data that qualify as personal data. Insofar as end-users who are legal persons are concerned, provisions of Regulation (EU) 2016/679 should apply only to the extent specifically required by this Regulation.

…

(8) This Regulation should apply to providers of electronic communications services, to providers of publicly available directories, and to ~~software~~ providers **of software** permitting electronic communications, including the retrieval and presentation of information on the internet. This Regulation should also apply to natural and legal persons who use electronic communications services to send **or present** direct marketing commercial communications or **make use of processing and storage capabilities of terminal equipment or** collect information ~~related to~~ **processed by or emitted by** or stored in end-users' terminal equipment. **Furthermore, this Regulation should apply regardless of whether the processing of electronic communications data or personal data of end-users who are in the Union takes place in the Union or not, or of whether the service provider or person processing such data is established or located in the Union or not.**

Some end-users process as recipients their electronic communications data for different purposes, such as ensuring network and information security. Such processing is not covered by this Regulation.

…

(11a) The protection of confidentiality of communications is crucial also as regards interpersonal communications services that are ancillary to another service; therefore, **the processing of electronic communications data in the context of the provision of** such type of **ancillary** services ~~**also having a communication functionality**~~ should be covered by this Regulation. ~~**In such cases, this Regulation applies only to the ancillary feature itself and the electronic communications functionality it provides. To determine whether an electronic communications functionality constitutes an ancillary feature, the end-users expectations have to be taken into account.**~~ ~~**For example such communications functionality is considered to be ancillary feature in**~~

In all the circumstances where electronic communication is taking place between a finite, that is to say not potentially unlimited, number of end-users which is determined by the sender of the communications, e.g. any messaging application allowing two or more people to connect and communicate, such services constitute interpersonal communications services. Conversely, a communications channel does not constitute an interpersonal communications service when it does not enable direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s). This is for example the case when the entity providing the communications channel is at the same time a communicating party, such as a company that operates a communications channel for customer care that allows customers solely to communicate with the company in question. ~~However~~ Also, where access to ~~an~~ electronic communications ~~functionality~~ is available for anyone, e.g. communications in an electronic communications channel in online games which is open to all persons playing the game, such channel does not constitute an ~~ancillary~~ interpersonal communications feature. This reflects the end-users' expectations regarding the confidentiality of a service.

…

(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.

(15a) 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. The exact moment of the completion of the transmission of electronic communications content may depend on the type of electronic communications service that is provided. For instance for a voice call the transmission will be completed as soon as either of the end-users terminates the connection. For electronic mail or instant messaging the transmission is completed as soon as the addressee has collected the message, typically from the server of the electronic communications service provider. Upon completion of the transmission, 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.

…

(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.

…

(28) There is justification for overriding the elimination of calling line identification presentation in specific cases. End-users' rights to privacy with regard to calling line identification should be restricted where this is necessary to trace **malicious or** nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services, such as eCall, to carry out their tasks as effectively as possible. **Location information established by the terminal equipment, using its built-in Global Navigation Satellite Systems (GNSS) capabilities or other types of terminal equipment based location data, such as location data derived from the WiFi functionality, may supplement the location data supplied by providers of number-based interpersonal communications services when a call is made to emergency services. The temporary denial or absence of consent of an end-user to access location data provided by the terminal equipment GNSS, for example, because location settings are turned off, shall not prevent the transfer of such information to emergency services for the purposes of facilitating access to such services.**

(29) Technology exists that enables providers of electronic communications services to limit the reception of **unwanted, malicious or nuisance** calls by end-users in different ways, including blocking silent calls and other ~~fraudulent~~ **unwanted, malicious** and nuisance calls**, such as calls originating from invalid numbers, i.e. numbers that do not exist in the numbering plan, valid numbers that are not allocated to a provider of a number-based interpersonal communications service, and valid numbers that are allocated but not assigned to an end-user**. Providers of ~~publicly available~~ number-based interpersonal communications services should deploy this technology and protect end-users against ~~nuisance~~ **such** calls ~~and~~ free of charge. Providers should ensure that end-users are aware of the existence of such functionalities, for instance, by publicising the fact on their webpage.

…

Article 1

Subject matter

1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural ~~and legal~~ persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data.

1a. This Regulation lays down rules regarding the protection of the fundamental rights and freedoms of legal persons in the provision and use of the electronic communications services, and in particular their rights to respect of communications.

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

3. The provisions of this Regulation particularise and complement Regulation (EU) 2016/679 **with regard to the processing of ~~electronic communications~~ data that qualify as personal data** by laying down specific rules for the purposes mentioned in paragraphs 1 ~~and~~ **to** 2.

…

Article 5

Confidentiality of electronic communications data

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

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

…

Article 7

Storage and erasure of electronic communications data

~~[~~1. Without prejudice to point (b) of Article 6(1) and points (a), and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. **~~Such data may be recorded or stored 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 (b) of Article 6(1) and points (a), **(c)** and (~~c~~**e**) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication. **~~Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679~~**.

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

…

Article 12

Presentation and restriction of calling and connected line identification

1. Where presentation of the calling and connected line identification is offered in accordance with Article [107] of the [Directive establishing the European Electronic Communication Code], the providers of ~~publicly available~~ number-based interpersonal communications services shall provide the following:

(a) the calling end-user with the possibility of preventing the presentation of the calling line identification on a per call, per connection or permanent basis;

(b) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls;

(c) the called end-user with the possibility of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling end-user;

(d) the called end-user with the possibility of preventing the presentation of the connected line identification to **which** the calling end-user **is connected**.

2. The possibilities referred to in ~~points (a), (b), (c) and (d) of~~ paragraph 1 shall be provided to end-users by simple means and free of charge.

3. Point (a) of paragraph 1 shall also apply with regard to calls to third countries originating in the Union. Points (b), (c) and (d) of paragraph 1 shall also apply to incoming calls originating in third countries.

4. Where presentation of calling or connected line identification is offered, providers of ~~**publicly available**~~ number-based interpersonal communications services shall provide information to the public regarding the options set out in ~~points (a), (b), (c) and (d) of~~ paragraph 1 **and the exceptions set forth in Article 13(1), (1a) and (2)**.

Article 13

*Exceptions to **presentation and restriction of calling and connected line identification, to rejection of incoming calls and to provide access to emeregency services***

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

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

2. Member States shall establish more specific provisions with regard to the establishment of **transparent** procedures and the circumstances where providers of ~~publicly available~~ number-based interpersonal communication services shall override the elimination of the presentation of the calling line identification on a temporary basis, where end-users request the tracing of **unwanted,** malicious or nuisance calls.

3. Regardless of whether the end-user has prevented access to the terminal equipment's Global Navigation Satellite Systems (GNSS) capabilities capabilities or other types of terminal equipment based location data through the terminal equipment settings, when a call is made to emergency services, such settings may not prevent access to ~~GNSS~~ such location data to determine and provide the ~~caller~~ calling end-user's location to emergency services for the purpose of responding to such calls.

Article 14

Incoming call blocking

1. Providers of ~~publicly available~~ number-based interpersonal communications services shall deploy state of the art measures to limit the reception of **unwanted**, **malicious or nuisance** calls by end-users**. ~~and~~**

2. Providers of number-based interpersonal communications services shall also provide the called end-user with the following possibilities, free of charge:

(a) to block incoming calls from specific numbers or from anonymous sources **or from numbers using a specific code or prefix referred to in Article 16(3a)**; **and**

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