Council of the European Union

Brussels, 11 January 2018
(OR. en)

5165/18

Interinstitutional File:
2017/0003 (COD)

TELECOM 4
COMPET 18
MI 14
DATAPROTECT 2
CONSOM 3
JAI 16
DIGIT 2
FREMP 2
CYBER 4
CODEC 14

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 discussion paper

INTRODUCTION

The Commission adopted the proposal for a Regulation on Privacy and Electronic Communications ('ePR' or 'e-privacy Regulation') on 10 January 2017 and, since then, the proposal was examined in numerous meetings of WP TELE under the MT and EE Presidencies. The current state of play is outlined in a comprehensive progress report put together by the EE Presidency for the December TTE Council[1]. The progress report clearly identifies a number of remaining issues requiring further discussion in the WP TELE. The latest version of the proposal can be found in document 15333/17 issued by the EE Presidency.

[1] Doc. 14374/17

While covering a complex subject matter, this proposal is one that the Presidency recognises as important for the completion of the Digital Single Market and is therefore committed to put considerable efforts towards seeking compromise solutions in order to strike the delicate balance between an adequate level of privacy protection and sufficient incentives for innovation.

The Presidency will hold a first WP TELE meeting on the e-PR on 17 January 2018 and, in order to steer further work on the file, it would like to organise a discussion on a number of selected topics, of both policy and technical nature. Those have been identified on the basis of the comments raised by delegations in previous WP TELE meetings, as well as delegations' written comments. The topics, together with proposed guiding principles or possible options are outlined below.

At the meeting of 17 January, the Presidency will invite delegations to express their views on these issues. If necessary, the discussion will continue in the next WP TELE meeting on e-PR on 30 January, otherwise planned for further outstanding aspects of the proposal, including presentation and restriction of the calling line identification; blocking incoming calls; publicly available directories and direct marketing communications. Restrictions to confidentiality of communications set out in Article 11 will be discussed later on.

DISCUSSION TOPICS

1. **Link to General Data Protection Regulation (GDPR) and clarification on where the e-PR complements and where particularizes it, with a focus on Articles 5, 6, 7, 8 and 10:**

In order to define the general relationship between the GDPR and the ePR, the Presidency tables for discussion the following guiding principles.

Some provisions of the ePR complement the GDPR, while others particularise it. When the ePR particularises the GDPR, it functions as *lex specialis*, meaning that whenever the ePR and GDPR norms deal with the same subject matter, the ePR applies.

This distinction is important because in the cases where the ePR complements the GDPR, the ePR creates rules that are not otherwise in GDPR or not within same scope (for instance as regards legal persons). This means no other rule to protect the privacy of electronic communications would apply, if such ePR article is absent. At the same time, it is important to realise that, in addition to the protection of personal data, the protection of electronic communications data reflects in secondary legislation the right to respect for communications laid down in Article 7 of the Charter of Fundamental Right of the European Union.

More specifically, based on the discussions so far, the relationship between Articles 5 to 8 and 10 ePR on the one hand, and the GDPR on the other hand, could be summarised as follows:

- Article 5 of the proposal complements the GDPR regarding the protection of electronic communications data that do not qualify as personal data. On top of that, the GDPR does not have a general prohibition to interfere with electronic communications. The ePR particularises the GDPR for electronic communications data that constitutes personal data in this respect.

- Article 6 of the ePR particularises the GDPR as far as it concerns the processing of electronic communications data that qualifies as personal data, and complements the GDPR as far as it concerns the processing of electronic communications data that do not qualify as personal data.

- Article 7 of the ePR on the storage and erasure of electronic communications data particularises the GDPR. It specifies the storage limitation principle of the GDPR by pointing out the moment in time when electronic communications data needs to be erased or anonymised.

- Article 8 of the ePR complements the GDPR regarding the protection of terminal equipment as such. The GDPR does not provide for a prohibition to use the processing and storage capabilities of the terminal equipment and to collect information from the end-user's terminal equipment, or to collect information emitted by terminal equipment to enable it to connect to another device and, or to network equipment, as the ePR does. In addition, Article 8 particularises the GDPR for the use of the processing and storage capabilities of the terminal equipment and the collection of information from the end-user's terminal equipment that qualifies as personal data or collection of information emitted by terminal equipment that qualifies as personal data.

- Article 10 of the ePR on information and options for privacy settings to be provided complements the GDPR by setting forth requirements for specific types of software to have a specific setting available, but is at the same time inspired by the principle based provision on privacy by design and default of the GDPR.

The Presidency underlines that the overall aim should be not to lower the level of protection of fundamental rights as set by the GDPR as well as the existing Directive 2002/58/EC on privacy and electronic communications as amended by Directive 2009/136/EC, taking into account that the e-PR is proposed as *lex specialis* to the GDPR regarding the processing of personal data. With regard to data of legal persons, the GDPR does not apply, unless the e-PR specifically provides for it. This is the case concerning the definition of consent.

Doc. 15333/17 provides the following on the relationship between the ePR and GDPR:

Article 1(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.*"

Recital (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. This Regulation therefore does not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. Processing of electronic communications data by providers of electronic communications services should only be permitted in accordance with this Regulation. 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.***"

The Presidency seeks the views of delegations on:

- **First of all, whether they share the above analysis;**
- **Option 0:** Whether the clarification in Article 1(3) and recital (2a) of doc. 15333/17 on the relationship between the ePR and GDPR is sufficient for the purposes of clarifying the relation between the GDPR and the ePR.
- **Option 1:** If the clarification in doc. 15333/17 were not considered to be sufficient, where further clarification could be given in the text; in recitals and/or the articles?

2. Issues related to scope of the ePrivacy Regulation and the alignment with the proposal for a Directive establishing a European Electronic Communications Code (EECC):

Several delegations have requested alignment with the EECC. In this regard, the Presidency has identified the following outstanding issues based on previous comments and discussions on which it seeks guidance from delegations:

2.1 Ancillary services (Article 4.2):

Article 2(5) of the Council text from the Coreper mandate on the proposal for EECC provides that: "*'interpersonal communications service' means a service normally provided for remuneration that enables 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); it does not include services which enable interpersonal and interactive communication merely as a ancillary feature that is intrinsically linked to another service;*"

Recital 17 of the current compromise proposal for the EECC states that: *"**Under exceptional circumstances, a service should, not be considered as an interpersonal communications service if** Services that are not considered as an interpersonal communications service when the interpersonal and interactive communication facility is an ancillary feature to another service and for objective technical reasons cannot be used without that principal service, and its integration is not a means to circumvent the applicability of the rules governing electronic communications services. An example for such an exception could be, in principle, a communication channel in online games, depending on the features of the communication facility of the service".*

The ePR has taken a different approach than the EECC towards services which enable interpersonal and interactive communication merely as an ancillary feature that is intrinsically linked to another service.

Article 4(2) of the ePR (doc. 15333/17) provides that: "*For the purposes of point (b) of paragraph 1 **this Regulation**, the definition of 'interpersonal communications service' **referred to in point (b) of paragraph 1** shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.*"

While the EECC does not include such services within the scope of the electronic communications services definition for the reason that imposing the obligations of the EECC on such services may not be proportionate, the objective of the ePR of the protection of confidentiality of communications is different. From a perspective of the protection of fundamental rights, a broader scope might be justified.

The Presidency seeks the views from delegations on:

- **Option 0:** Maintaining the inclusion of services which enable interpersonal and interactive communication merely as an ancillary feature that is intrinsically linked to another service within the scope of the e-PR as in doc. 15333/17;
- **Option 1:** Excluding such services from the ePR scope;
- **Option 2**: Any other solution.

2.2 Machine-to-machine communications (Articles 2, 3 and 5):

Services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services (services involving an automated transfer of data and information between devices or software-based applications with limited or no human interaction) are included in the definition of 'electronic communications services' under Article 2(4) of the EECC.

Under the EECC compromise proposal the transmission services used for the provision of machine-to-machine services constitute an electronic communications service and as such should be covered by the ePR for the purposes of ensuring their confidentiality. However, the application layer of such machine-to-machine services, which does not normally constitute an electronic communications service, is not covered by the EECC/ePR. This follows the scope of the current ePrivacy Directive.

2.2.a Consequences of maintaining transmission services used for the provision of machine-to-machine services within the ePR scope, but adding additional provisions

Delegations have inquired about how should end-users who are legal persons give consent to enable the provider of transmission services used for the provision of machine-to-machine services to interfere in communications. Questions have been raised both in the event when such M2M communications may reveal personal information and otherwise.

It could be clarified that consent to the processing of electronic communications data, including M2M communications data, may be given at the time of subscription. This could be a one-off consent for processing of electronic communications data for the duration of the subscription.

In addition, doc. 15333/17 states the following on end-user who are legal persons and on how they can give consent:

Article 4a(**1a) "*Paragraph 1 is without prejudice to national legislation on determining the persons who are authorised to represent a legal person in any dealings with third parties or in legal proceedings.*"**

Recital (**3a) "*This Regulation should not affect national law regulating for instance the conclusion or the validity of a contract. Similarly, this Regulation should not affect national law in relation to determining who has the legal power to represent legal persons in any dealings with third parties or in legal proceedings.*"**

On the other hand, bearing in mind that the M2M communications are carried out with limited or without human intervention at all, it may be argued that communicating end-users should not have a right to the confidentiality of the information transferred in this way; hence, in case the electronic communications service provider wishes to interfere with electronic communications content or related metadata for other purposes than transmission, for example, to record the content or related metadata of M2M communications, communicating end-users using M2M communications should not have the right to control the processing by having to consent to this.

Therefore, adding a specific permitted processing for M2M communications data for cases of non-personal electronic communications content data and metadata is an option to be considered. It would be an option to include the legitimate interests of the provider of electronic communications services as a basis for permitted processing of such M2M communications data. This might be sufficient to overcome the risk of excessive burden on electronic communications service providers to obtain the consent of an end-user for processing.

It should be noted that it may not be clear when M2M communications would include personal data. For example, not only M2M communications related to end-users who are natural persons, but also M2M communications between end-users who are legal persons may include personal data (e.g., hospital – hospital). Furthermore, this would have the consequence that Article 7 of the Charter would not be implemented into secondary EU law with regard to M2M communications data related to businesses.

Note that the WP 29 suggests: "*a narrow category of pure machine-to-machine communications should be exempted if they have no impact on either privacy or the confidentiality of communications, such as for example the cases where such communication is performed in execution of a transmission protocol between network elements (e.g. servers, switches), to inform each other on their status of activity*' (WP 247, p. 28)."

2.2.b Consequences of excluding transmission services used for the provision of machine-to-machine services from the ePR scope

In the light of MS comments and discussions the Presidency considers that the differentiation between the application layer and the transmission layer in terms of protection of confidentiality of communications needs further discussions with delegations.

The overall exclusion of the transmission services used for the provision of machine-to-machine services from the ePrivacy Regulation would require carving out from the scope of application of the ePR (Article 2 and 3) this particular type of service. The ePR would apply only to the remaining electronic communications services set forth under Article 2(4) of the EECC.

In order to avoid dis-alignment with the draft Code, the exclusion of the transmission of machine-to-machine communications from the ePR Regulation does not seem appropriate. More importantly, given that the current ePR Directive also covers the transmission of M2M communications, if the ePR Regulation would exclude them, it could conceivably lower the current level of protection. Last but not least, it would jeopardise the confidentiality of M2M business communications.

2.2.c Practical implications

A problem for the options excluding transmission services used for the provision of machine-to-machine services or providing for specific permitted processing for M2M communications data for cases of non-personal electronic communications content data and metadata or for all M2M data concerns the difficulty for the service to determine in advance a) whether it is used for the provision of a machine-to-machine service (thus, whether it is transmitting M2M data) and; b) whether it is transmitting personal and / or non-personal data. It seems that processing is needed to make such a judgment, which may include processing of other types electronic communications data.

The Presidency seeks the views from delegations on:

- **Option 0:** whether the transmission services used for the provision of machine-to-machine services should remain within the scope of the ePR, as under the current ePrivacy Directive and doc. 15333/17.

- **Option 1:** whether the transmission services used for the provision of machine-to-machine services should remain within the scope of the ePR and, in addition:

    - **Option 1.1:** additional provisions should be added, to further complement Article 4a(1a) and recital 3a of doc. 15333/17, setting forth how consent should be provided in those cases where M2M communications relate to end-users who are legal persons, both in cases when such M2M communications reveal personal data and otherwise, and / or;

    - **Option 1.2:** as a way to facilitate the provision of consent, adding an additional provision (or a recital) clarifying that consent should be subject to a one-off consent, e.g., upon subscription to the contract, provided that such processing does not adversely affect fundamental rights and interest of another end-user concerned, and / or;

    - **Option 1.3:** additional permitted processing should apply to M2M communications data that do not reveal personal data.

- **Option 2:** whether the transmission services used for the provision of machine-to-machine services altogether (i.e. independently of whether they transmit personal information or not) should be excluded of the scope of the ePR, i.e., the ePR would not be applicable to the transmission of M2M communications. Article 2 and 3 of the proposal setting for its material scope should be amended to reflect this.

The Presidency needs the views of the delegations on the suggested options for addressing the relations with the Code. Delegations are also invited to indicate whether they see other linkage with the Code that the Presidency should look into.

3. Article 6: Permitted processing of electronic communications data

The current ePrivacy Directive 2002/58/EC only allows electronic communications metadata (traffic and location data) to be processed for the purpose of the transmission of a communication; for billing purposes; or with consent of the end-user for the purpose of marketing electronic communications services or for the provision of value added services. In addition, electronic communications metadata (traffic and location data) that is made anonymous may be processed.

Article 6 of the e-PR sets forth the permitted processing of electronic communications data, meaning that the legal basis provided by the GDPR to process personal data cannot be relied upon to process electronic communications data. The ePR provides for specific purposes for permitted processing for which no consent is needed, while for processing for remaining purposes the consent of the end-user concerned is needed.

Some delegations have proposed including the GDPR legal basis 'legitimate interest', to allow for 'further processing' in Article 6(2) ePR regarding the permitted processing of electronic communications metadata or introduce a permitted processing for the purpose of web analytics and web measurement.

3.1 Considerations related to 'legitimate interests' legal ground

The GDPR allows the processing of personal data under Article 6(1)(f) if "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*"

Article 13(1)(d) of the GDPR requires that where the processing is based on point (f) of Article 6(1) of the GDPR, the controller shall, at the time when personal data are obtained, provide the data subject with information of the legitimate interests pursued by the controller, on top of other information required under Article 13 GDPR.

Article 21(1) of the GDPR gives data subject the right to object, on grounds relating to his or her particular situation at any time to processing of personal data concerning him or her which is based on point (f) of Article 6(1) GDPR. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Article 9 GDPR foresees a different regime for the processing of special categories of personal data ('sensitive data'). Article 9(1) provides that: "*processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*" This prohibition does not apply if one of the points (a)-(j) of Article 9(2) GDPR applies. This means that having a legitimate interest is not sufficient to process sensitive data under the GDPR.

3.2 Considerations related to 'further processing'

Article 6(4) of the GDPR allows under certain circumstances for "further processing" and to this end provides that *"Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject'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 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:*

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."

Further processing means that the same controller is processing the data for a purpose different than the one for which it initially collected the data. Moreover, further processing has to comply with the other data protection rules and principles, e.g. with the principle of fair processing and the obligation to inform the data subject about the (further) purposes of the processing.

It shall be noted that the electronic communications data may contain a special category of personal data under Article 9 GDPR. Without processing the electronic communications data, electronic communications services can technically not determine whether it concerns personal data, special categories of personal data, or non-personal data.

The Presidency seeks the views from delegations on:

- **Option 0:** the grounds for processing electronic communications metadata shall remain as proposed in doc. 15333/17;

- **Option 1:** a further extension of the list of exceptions permitting the processing of electronic communications metadata without consent for a lawful business practice, provided that there are no significant risks for the privacy of individuals. In particular, the data collection is performed solely by the entity concerned on behalf of the ECS for web analytics and web audience, in light of the EC Impact Assessment from January 2017 laying out the proposals for legitimate exceptions for processing, including for "*a lawful business practice provided that there are no significant risks for the privacy of individuals. In particular, the data collection is performed solely by the entity concerned on behalf of the ECS for the purpose of web analytics and web measurement*".[2]. Delegations are asked to take into account the reasons on which this option was discarded, as stated above;

- **Option 2:** inclusion of a legitimate interest ground for the processing of electronic communications metadata. A legitimate interest legal ground could take several forms. The use of legitimate interest could be conditioned upon *inter alia*:

    1. A purpose limitation, such as for public interest purposes;

    2. A requirement that the data is erased or anonymised after a certain pre-determined period of time;

    3. Certain safeguards, such a DPA consultation, Data Protection Impact Assessment and security measures such as pseudonymisation;

    4. The pre-condition that electronic communications services could not rely on the legitimate interest legal ground if the purpose could be fulfilled with anonymous data;

    5. The possibility for end-users to object to such processing.

---

[2] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT *Accompanying the document* 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). p. 25.

Delegations are invited to express their views on whether including a form of legitimate interest legal ground to process metadata would not lower the level of protection offered by the GDPR, and on whether it would not lower the protection of the current ePrivacy Directive?

- **Option 4:** inclusion of permitted processing of electronic communications metadata based on the compatibility with the purpose for which the data were initially collected. Further processing could be conditioned upon *inter alia*:

    1. A purpose limitation, such as for public interest purposes;

    2. A requirement that the data is erased or anonymised after a certain pre-determined period of time;

    3. Certain safeguards, such a DPA consultation, Data Protection Impact Assessment and security measures such as pseudonymisation;

    4. The pre-condition that electronic communications services could not rely on the legitimate interest legal ground if the purpose could be fulfilled with anonymous data;

    5. The possibility for end-users to object to such processing.

- **Option 5:** whether for the processing of electronic communications metadata, the protection provided by the GDPR regarding the protection of personal data would be sufficient and thus delete Article 6(2) of the ePR, making the GDPR legal bases applicable for the processing of electronic communications data qualifying as personal data. Delegations supporting this options are asked what in their view the legal bases should be for processing of electronic communications data that qualifies as non-personal data, bearing in mind that Article 5 ePR requires confidentiality of electronic communications and prohibits processing, irrespective whether the data is personal data or not;

4. Article 7: Storage and erasure of electronic communications data

Article 7 concerns the storage and erasure of electronic communications data. It includes a specific rule establishing when the data should be anonymised or deleted. which is linked to the prohibition to interfere with communications data, both content and metadata. Article 7 of the proposal aims at ensuring legal certainty.

In addition, rules on storage and erasure of electronic communications content are helpful to clarify that after the delivery of the content, recipients may dispose of such data as they wish under GDPR; because the confidentiality of communications *per se* is terminated. This is further clarified in recital 15, stating that: "*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.*"

Article 7 ePR builds upon Article 6 of the ePrivacy Directive, which provides that traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of the a communications, without prejudice to data kept for billing purposes and with consent of the user for the provision of value added services.

The Presidency seeks the views from delegations on:

- **Option 0:** retain the text as proposed in doc. 15333/17.
- **Option 1:** delete the last sentence of Article 7(1), "*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*", while retaining the text of Article 7(1) on when the electronic communications content must be erased or anonymised.
- **Option 2:** any other solution.

5. Article 8: Protection of information stored in terminal equipment of end-users and related to or processed or emitted by such equipment

More discussion is needed on the issue of the protection of the end-users' terminal equipment, including the use of cookies and other tracking techniques as well as on device tracking.

Doc. 15333/17 allows the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment without the consent of the end-user if:

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

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

(d) it is necessary for 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

(e) it is necessary for a security update'

Exceptions (a) and (c) already exist under Article 5(3) the ePrivacy Directive. The Article 29 Working Party has issued Opinion 04/2012 on Cookie Consent Exemption (WP 194), interpreting these exceptions and giving as examples of cookies that would normally be exempted from consent under certain conditions if they are not used for additional purposes:

1) User input cookies (session-id), for the duration of a session or persistent cookies limited to a few hours in some cases.

2) Authentication cookies, used for authenticated services, for the duration of a session.

3) User centric security cookies, used to detect authentication abuses, for a limited persistent duration.

4) Multimedia content player session cookies, such as flash player cookies, for the duration of a session.

5) Load balancing session cookies, for the duration of session.

6) UI customization persistent cookies, for the duration of a session (or slightly more).

7) Third party social plug-in content sharing cookies, for logged in members of a social network.

Opinion 04/2012 states that the following cookies would not be exempted under Article 5(3) of the ePrivacy Directive:

- Social plug-in tracking cookies;
- Third party cookies used for behavioural advertising;
- First party analytics.

Some delegations have questioned as well what the consequences under the ePR and other relevant legislation should be if an end-user refuses to give consent for his or her data to be processed. The questions is whether the provider shall be obliged to provide the service nevertheless, which would *de facto* entail a prohibition of the use of so called "cookie walls"or whether the provider should be permitted to refuse the access to the service or whether the provider should propose such end-user another option for access (for instance subscription or payment).

Recital 25 of Directive 2002/58/EC refers to the formulation of Article 5.3 before it was amended in 2009 (when the legal ground was changed from right to object to prior consent) and states regarding access to a service and consent to the processing of data:

"(However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. ***Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose."***

The Presidency seeks the views from delegations on:

- **Option 0:** retaining the text as proposed in doc. 15333/17.
- **Option 1:** whether it is needed to extend the current list of exceptions to consent, based on their function/goal, by inclusion of more non-privacy intrusive purposes. Delegations supporting this option are asked to provide examples of such purposes, taking into account the already exempted purposes.
- **Option 2:** a new harm based approach in this provision e.g., by differentiating cookies and similar techniques by the level of their harm. Delegations supporting this option are requested to give specific examples of the envisaged levels to be differentiated on.

- **Option 3:** whether recognizing the legitimate interests for cookies / similar techniques whose function is to deliver targeted advertisement coupled with the right of object would be a more appropriate standard than consent to legitimize processing of the use of the processing capability of terminal equipment for the purposes of advertisement. Recital 25 of Directive 2002/58/EC refers to the formulation of Article 5.3 before it was amended in 2009 (when the legal ground was changed from right to object to prior consent).

Option 4: whether it is needed to explicitly address in the text access to a service in the absence of consent to process information. Inspiration could be taken from recital 25 of Directive 2002/58/EC, stating that: "*Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose*."

Option 5: any other solution.

6. Article 10: software privacy settings

Article 10 requires software permitting electronic communications to offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment. In addition, it requires that upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, that the software requires the end-user to consent to a setting.

In the course of the discussions, delegations raised a number of relevant questions that need to be addressed such as the impact on the role of browsers in the Internet ecosystem, the added value from the user perspective and the question whether, given the existing market solutions, regulation is needed at all in this respect.

The Presidency seeks the views from delegations on:

- **Option 0:** retain the text as proposed in doc. 15333/17.
- **Option 1:** Require software to offer the end-user privacy settings to authorize or prevent third parties from *storing* information on the terminal equipment or *processing* information already stored on that equipment and offer information to the end-user about the possibility to choose a setting without prompting the end-user to agree with the settings upon installation.
- **Option 2:** retain the text as proposed in doc. 15333/17 while including an additional requirement on software to provide settings that would allow the end-user to accept cookies or similar techniques for a specific website. Such approach may first have the advantage for end-user of having easier ways to accept cookies rather than having to go back to the general settings to change them for the specific website, and second it may have the advantage for websites of having easier means to approach end-users with the question to effectively whitelist them.
- **Option 3**: Any other solution.

The Presidency would welcome reactions from delegations which of the outlined guiding principle and/or options could be supported for the purposes of future compromise drafting.

The Presidency remains open to any other solutions on the provisions above if Member States are of the view that there could be also other options.

_____