

# ANNEX 1

## Text proposals for the ePrivacy Regulation

*Changes are relative to the latest Council text.<sup>1</sup>*

- i. Who is the end-user? – Clarifying that when end-users are legal persons, ePrivacy should apply only to such legal persons as opposed to the natural persons who may be using the related services or terminal equipment, to whom the General Data Protection Regulation (GDPR) should instead in any event apply.

### *Recital 3*

Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value and the protection of which allows legal persons to conduct their business, supporting among other innovation. Therefore, the provisions of this Regulation should in principle apply to both natural and legal persons. Furthermore, this Regulation should ensure that, where necessary, provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council, also apply *mutatis mutandis* to end-users who are legal persons. This includes the provisions on consent under Regulation (EU) 2016/679.

***Consent for the processing of electronic communications data given by the legal person concerned shall be sufficient for the purposes of this Regulation. To the extent that personal data of end-users who are natural persons is concerned, the provisions of Regulation (EU) 2016/679 shall apply.***

### *Recital 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~~ ***the provisions of Regulation (EU) 2016/679 shall apply to the individuals concerned.***

### *Recital 21aa*

***Consent for the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment given by the legal person concerned shall be sufficient for the purposes of this Regulation. To the extent that personal data of end-users who are natural persons is concerned, the provisions of Regulation (EU) 2016/679 shall apply.***

***Where end-users who are legal persons enable the use of the terminal equipment by end-users who are natural persons, such as employees, the provisions of Regulation (EU) 2016/679 shall apply to the individuals concerned.***

---

<sup>1</sup> Doc. 6771/19

- ii. Relationship with the GDPR – Clarifying that the ePrivacy Regulation only applies to the moment of collection of terminal equipment information, while the GDPR should apply to processing activities after the collection point.

*Recital 21b*

*This Regulation should not affect the applicability of Regulation (EU) 2016/679 to the processing of terminal equipment information that qualifies as personal data, provided such information has been collected in compliance with this Regulation.*

- iii. Adding two legal bases (for anonymisation and for collection with by-design limited impact) for the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment as recommended by the Article 29 Working Party in its Opinion 03/2016.

*Article 8*

*Protection of end-users' terminal equipment information*

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 service **or terminal equipment functionality** 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
- (da) it is necessary to maintain or restore the security of ~~information society the services~~ **or terminal equipment**, 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,
  - (ii) the end-user is informed in advance each time an update is being installed, and
  - (iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates; or
- (f) it is necessary to locate 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); **or**
- (g) the data is anonymous or made anonymous before any further processing; or**
- (h) the data collection serves a legitimate purpose and is limited by design to have little or no impact on the end-user's right to privacy and confidentiality of communications.**

*Recital 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 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. Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to **provide software updates, including to** fix security vulnerabilities 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.~~

#### *Recital 21b*

*Consent for the collection of end-users' terminal equipment information should not be necessary if the data are anonymous or immediately and irreversibly anonymised during collection on the device or on the endpoints of the network or sensors. Consent should also not be necessary when the data collection serves a legitimate purpose and is limited by design to have limited impact on the end-user's right to privacy and confidentiality of communications. This can in particular be the case, depending on the circumstances, by using samples instead of the full dataset, keeping the categories and volume of collected data to the minimum necessary for this specific purpose, and/or by applying comprehensive pseudonymisation and anonymisation mechanisms to the collected data after a limited period of time.*