# EDPS recommendations on specific aspects of the proposed ePrivacy Regulation

**5 October 2017**

The proposed ePrivacy Regulation, once adopted, will update the "rules of the road" for privacy and electronic communications. It will modernise existing principles, clarify the technological requirements and provide for effective enforcement. The EDPS issued his advice on the ePrivacy review in a Preliminary Opinion (5/2016) and on the European Commission's proposed Regulation in Opinion 06/2017. Given developments in deliberations on the proposal, and for the benefit of the co-legislator, we have decided to offer advice and clarifications on some specific issues, in line with our previous opinions.[1] These recommendations focus on the need to ensure legal certainty and a high level of protection of the fundamental rights to privacy and data protection.

## Key messages

- The ePrivacy Regulation should reflect the importance of **the principle of confidentiality of communications** which is closely linked to the right to private life and as such protected by the EU Charter of Fundamental Rights, the European Convention of Human Rights, and constitutional and legal orders of most of the Member States. The confidentiality of communications **encompasses both content and metadata and data related to the terminal equipment.** This should be adequately reflected in the permitted purposes of processing and the legal bases of processing. **These considerations apply to all provisions of the ePrivacy Regulation.**

- The ePrivacy Regulation should provide for a genuine protection in line with current and anticipated technological developments, in particular in the context of **machine-to-machine communications**. Therefore, we support amendments explicitly providing for the protection of the confidentiality of communications to "*data **related to or processed** by terminal equipment*". The confidentiality of communications should also be ensured when data **are stored in the cloud** rather than only in transmission.

- The approach according to which **the ePrivacy Regulation particularises and complements the GDPR** should be maintained to reflect the importance of the confidentiality of communications. **The ePrivacy Regulation should not lower the level of protection as foreseen in the GDPR**. **Instead, a higher level of protection than the one the GDPR offers should be provided.** At the same time, unnecessary repetitions of GDPR provisions should be avoided for the sake of clarity and legal certainty: selectively repeating some GDPR provisions risks failing to include important provisions.[2]

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

- Broad legal bases for processing of communications data by reference to the GDPR or by re-stating the GDPR would undermine the rationale for a specific legal instrument and would not adequately reflect the importance of the confidentiality of communications enshrined in both the Charter of Fundamental Rights and the CJEU and ECtHR case law. **In particular, there should be no possibility under the ePrivacy Regulation to process metadata under the legitimate interest ground**. Allowing processing on legitimate interest ground would significantly lower the standards applicable today under the ePrivacy Directive 2002/58/EC and put into question the added value of the draft Regulation. Similarly, **further processing of metadata would create a loophole** and allow circumventing the high level of protection. **Data related to the terminal equipment should be processed only upon consent or if technically necessary for a service requested by the user and only for the duration necessary for this purpose**. We, therefore, support amendments which remove the broad legal basis for tracking of individuals across time and space for any purpose.

- Appropriate definitions are crucial to implement the protection of the fundamental rights. Therefore, we support amendments that provide for **standalone definitions**, replacing the reference to the European Electronic Communications Code, ensuring that consent, when a legal entity subscribes to a service, is given by the natural person who is using the service and/or the technical equipment. We also support that services merely provided as ancillary features should be included in the definition of "interpersonal communications services". Finally, we strongly recommend that the definition of metadata shall not exclude data not required for the purpose of transmitting electronic communications content nor for the provision of the service. In this way, no loopholes are created for the processing of these data on the basis of the GDPR.

- **Consent under the ePrivacy Regulation must have the same meaning as in the GDPR, including that it must be freely given and specific.**
    - Therefore, we support amendments clarifying that all GDPR provisions, including Article 4(11) on the definition of consent, Article 7 and Article 8 GDPR, apply also for purposes of the ePrivacy Regulation.

    - We support amendments that clarify that **access to services and functionalities must not made conditional to consenting to the processing** of personal data and the processing of information related to or processed by the terminal equipment of end-users;

    - We also welcome amendments requiring that **the technical settings enabling user control under Article 9 should allow for sufficient granularity**. This requirement reflects the rule in the GDPR that consent to be specific shall be given for specified purposes and for specific data controllers (here providers). As mentioned above, there should be no unnecessary repetitions of the GDPR. Therefore, we recommend that the settings shall *'allow the user to actively select the purposes and the service providers'.*

- Without **appropriate technical, privacy settings** expressing and withdrawing consent in an on-line, highly sophisticated environment can be substantially hampered. We therefore support amendments strengthening Article 10 and **require privacy protective settings by default. Moreover,** privacy settings should genuinely support expressing and withdrawing consent in an **easy, binding and enforceable manner against all parties.** This includes that the last sentence of recital (24) of the Commission's proposal should become a substantive provision and a legal requirement. Accordingly, end-users shall be given the possibility "*to change their privacy settings at any time during use*

*and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed"*.

- **Any restrictions on rights under Article 11 should properly reflect the importance of the confidentiality of communications, in line with the CJEU settled case-law**. For this reason, the restrictions should be more limited in scope than in the GDPR, and specific obligations should be provided towards enhancing transparency of access requests. When restricting the scope to serious crimes, this notion should be further defined. The minimum requirements for a legislative measure from Article 23(2) should apply in all cases.

- **The Data Protection Authorities should be entrusted with the supervision of the ePrivacy Regulation.** As the supervisory authorities in charge of ensuring compliance with the GDPR, they are best placed to ensure legal certainty and consistent application between the two, strongly interrelated, legal instruments. Moreover, the DPAs will be uniquely placed to deliver consistent application of the ePrivacy Regulation throughout the Union thanks to the European Data Protection Board.

- **Protection against unsolicited communications should be effective.** We therefore welcome amendments that provide that semi-automated calling systems are permitted only upon consent and call on the EU legislator to ensure that such systems are clearly included in the definition for "automated calling and communication system". We also welcome amendments that provide for effective technical measures, in particular the combined application of presenting the calling line and using a prefix to identify unsolicited calls, and support broadening the scope of protection to all forms of unsolicited communications rather than only "direct marketing communications".

The following pages provide our specific recommendations on the key points highlighted above.

# 1. Any processing of communications data must be based on a legal ground under the ePrivacy Regulation (Article 6, recital 5)

One of the main potential benefits of the draft ePrivacy Regulation is that - as the ePrivacy Directive today - it would provide additional protection for electronic communications by limiting and specifying the legal grounds on which basis these data can be processed.

We welcome the proposed amendments to Article 6, which clarify that **'notwithstanding Article 6 of the [GDPR]'**, electronic communications data may **'only'** be processed [on the legal grounds specified in the ePrivacy Regulation]. This Article, as amended, helps ensure clarity and legal certainty regarding the fact that other legal grounds such as the legitimate interest ground, are not applicable for processing under the Proposed Regulation.

We also welcome LIBE 4, which also clarifies, by amending recital 5, that processing should only be permitted *'on a legal ground specifically provided for under the [ePrivacy] Regulation'.* As an additional improvement we would recommend to rephrase this sentence in order to make this provision applicable to any parties, not just providers of electronic communications services.

We would further welcome, as advocated in our Opinion, amendments, which would specify, in a substantive provision, that *'**neither providers of electronic communications services, nor any third parties, shall process personal data collected on the basis of consent or any other legal ground under the ePrivacy Regulation, on any other legal basis not specifically provided for in the ePrivacy Regulation***.'

# 2. Legal grounds under the ePrivacy Regulation must not include legitimate interest

Some **amendments propose an additional exemption to the confidentiality of communications based on legitimate interest** of service providers and other parties to process electronic communications data.

Neither the current ePrivacy Directive nor the Proposed Regulation contain such exemption and the Draft Report also did not propose any such exemptions, neither for metadata nor for content. The data protection authorities and independent experts support this position and all agree in their assessment that **an additional exemption on legitimate interest grounds, either for metadata or for content, would risk creating a loophole and would take away much of the protection provided by the ePrivacy Regulation for the confidentiality of communications**.[3]

The legislator should keep in mind that the information about the circumstances of communications and who participated in it are explicitly protected by the fundamental right to communications secrecy, and as such it is protected by the constitutions and legal order of many Member States. Allowing the processing of communications related data without consent or a limited purpose which is specifically and with sufficient precision laid down in the legislation could affect the very essence of this fundamental right and end the tradition of trustworthy messengers.

**For these reasons,** we strongly oppose any amendments that would introduce the ground of legitimate interests as a basis for processing under the ePrivacy Regulation**. Any possibility for further processing must not create a back-door to the high level of protection of confidentiality of communications.**

We would welcome amendments introducing a a provision to clarify that *'**when the processing is allowed under any exception to the prohibitions under the ePrivacy Regulation, any other processing on the basis of Article 6 of the GDPR should be considered as prohibited, including processing for another purpose on the basis of Article 6(4) of the GDPR. This should not prevent controllers from asking for additional consent for new processing operations'**.*

We take note of amendments introduced to Article 7, suggesting that *'the user may further process the data in accordance with [the GDPR], if applicable.* This clarification may also be acceptable, in addition to the amendments suggested above.

**At the same time, we strongly oppose any amendments that would allow further processing more broadly**, as this would seriously undermine the protection of confidentiality of communications and create a dangerous loophole allowing circumvention of the Regulation, as explained in our Opinion.

# 3. Confidentiality of communications data shall be ensured 'at rest' and for machine-to-machine communications (Article 5)

In the Opinion, we argued that the ePrivacy Regulation must not only clearly provide for the confidentiality and security of communications while **in transit** but must also protect the confidentiality and security of end user equipment and communications data stored **in the 'cloud'**. **We recommended that Article 5 and Recital 15 of the Proposal should be revised to clearly cover both situations.**

To this end, we would further suggest extending this provision to also cover communication data not only in transit but also when stored by the provider or any other party (a typical case may be content of emails stored in the 'cloud'). Amendments to Article 5 specifying that the prohibition set forth in paragraph 1 shall also apply to ***'electronic communications data that is stored after the transmission has been completed'*** (see LIBE 399 and 400) are a good example of the type of language that may be used to this effect. The language used in LIBE 401, *'regardless of whether this data is in transit or stored'* may also be helpful.

As explained in our Opinion, **the protection of communications privacy should not be dependent on whether humans themselves speak or listen, type or read the content of a communication, or whether they simply rely on the increasingly smart features of their terminal devices to communicate content on their behalf**.

To this end, we support amendments (based on LIBE 59, 409, 410) providing that '*confidentiality of electronic communications shall also apply to data **related to or processed** by terminal equipment'*. Another way of formulating the same provision could be: *'the prohibition set forth in paragraph 1 shall also apply to data related to or processed by terminal equipment.'*

# 4. The protection of data related to the terminal equipment deserve equally high protection

The protection of data related to terminal equipment should be implemented in line with the technological developments, and consistently with the principle of confidentiality of communications and with the rule that the ePrivacy Regulation should not lower the level of protection provided by the current ePrivacy Directive and the GDPR.

**We therefore welcome the amendments that require the consent of the user** and remove the overbroad exception in Article 8(2)(b) of the Commission Proposal. We also welcome that the information provided to users is turned to an additional requirement in line with the principle of transparency and does not become a legal basis for tracking of individuals across time and space for any purpose. We support amendments that clarify that when the processing is permitted for the sole purpose of establishing a connection, this is limited to the time necessary.

At the same time, we do not encourage detailed additional legal grounds to be added to the ePrivacy Regulation to provide further, specific exceptions (with a possible, very narrowly tailored exception for 'people-counting').

Nevertheless, if such detailed exceptions were to be proposed as part of a compromise at any stage of the legislative process, it must be ensured, at a minimum, that they are drafted in such a way to avoid creation of inadvertent loopholes. This applies, in addition to 'people counting', to the proposed legal grounds relating to establishing a connection, security updates, employment relationships, and web audience measuring.

- With regard to **'people counting',** we recommend, at the minimum, adding requirements to ensure that 'the purpose of processing is limited to mere statistical counting of individuals or objects'; 'data are anonymised as soon as possible after collection'; and processing is 'strictly limited to a distinct and limited geographical area'; and that 'users are given effective opt-out possibilities'.

- With regard to **'establishing a connection'**, we endorse amendments that specify that this must be done for the 'sole purpose of' establishing a connection 'requested by the user'.

- With regard to '**web audience measuring'**, we reiterate our concern that this ground must be narrowly tailored and interpreted and should not be unduly broadened during the legislative process. Amendments adding the requirement that 'such measurement does not adversely affect the fundamental rights of the user' are welcome.

- With regard to **'security updates',** we recommend, at a minimum, that security updates must be 'strictly necessary', 'not lowering the level of confidentiality provided by user settings', and that the user is 'informed before each update' and 'has the possibility to turn off the automatic installation of these updates'.

- With regard to proposed **exceptions in the employment context**, any exception must be 'strictly limited for what is necessary for the execution of an employee's task', 'limited to cases where the employer provides and/or is the subscriber of the terminal equipment', and the 'employer does not use this legal ground for monitoring its employees'.

# 5. Appropriate definitions are crucial to implement the protection of the fundamental rights (Article 4)

### *5.1 Replacement of reference to the definitions of the European Electronic Communications Code (Code) by self-standing definitions (Article 4)*

For certain key definitions[4] the Proposal refers the reader to the European Electronic Communications Code (Code).

**We welcome, as advocated in our Opinion, the amendments that replace the reference to the Code, still undergoing the legislative process, by standalone definitions** (see LIBE 46 onwards). It is important to ensure that the definitions used in the ePrivacy Regulation are independent from the proposal for the Code and that central terms are defined in the ePrivacy Regulation.

Standalone definitions are particularly important in all cases when the definition of a term differs, in one or more significant aspects, from the definition used in the Code, such as the case with the definition of 'interpersonal communications service', which is also to include 'services enabling interpersonal and interactive communication merely as an ancillary feature'. We welcome amendments aiming at such clarifications.

Standalone definitions are also important in all other cases, even when at present the Code definitions appear suitable, considering that the definitions in the Code may be subject to changes in a separate ongoing legislative procedure. For this reason, we recommend that a standalone definition be included for 'call' as well, instead of referring to Article 2(21) of the Code as in the Draft Report.

### *5.2 Definition of 'user' and/or 'end-user'*

We **welcome amendments aiming to re-introduce the definition of 'user',** based on the currently existing definition in the ePrivacy Directive, which reads as follows: '*any natural person using a publicly available electronic communications services, for private or business purposes, without necessarily having subscribed to this service'.*

If these amendments are made, however, **it is equally crucial that the term 'user' be then consistently used throughout the Regulation instead of the term 'end-user',** which is defined in the draft Code, and was used in the Commission Proposal.

As a general rule, the term 'user' should be used throughout the Regulation in all cases where this was also already the case in the current ePrivacy Directive in equivalent provisions. As explained in our Opinion, **it must be clear that it is the individuals concerned and affected, rather than, for example, their employers or landlords who should be in a position to provide valid consent to the processing of their communications**.

Special attention should be paid, however, that in some cases, in particular, where a provision specifically aims at protecting the rights of legal persons who are requesting, subscribing to, or using a service, another, more appropriate term and definition be used instead or in addition to the term 'user' to ensure that legal entities also remain protected. Under the current Directive, the term 'subscriber' is usually used for this purpose.

### *5.3 Definition of Metadata*

**The proposed amendments show that MEPs are aware of the privacy and data protection risks of processing metadata**. **Notwithstanding this awareness, the amendments continue to** follow the approach of the Proposal and **limit the notion of metadata** to data '*processed for the purpose of transmitting, distributing or exchanging electronic communications content'* and/or limit it to data that is '*processed for the provision of the service'*.

While these definitions encompass a large part of metadata, this definition is not exhaustive as it neglects any metadata that is neither required *for the purpose of transmitting, distributing or exchanging electronic communications content* nor *processed for the provision of the service.* An example for this is location data in an instant messaging application.

Thus, the EDPS proposes to change the definition to cover all metadata, as follows:

*c) 'electronic communications metadata' means data processed in an electronic communications network* ***that is not 'electronic communications content', as well as*** *data broadcast or emitted by the terminal equipment that* **provides additional information about the communication or** *is used to identify end-users' terminal equipment in the network* ***or*** *to enable it to connect to such network or to other terminal equipment.*

***It includes, but is not limited to,*** *data used to trace and identify the source and destination of a communication, data on the location of the device and the date, time, duration and type of communication.*

# 6. Consent must have the same meaning as in the GDPR, including be freely given and specific (Article 6, 8 and 9). Technical and privacy settings should genuinely and in an easy manner support giving and withdrawing consent (Article 9 and 10)

With regard to Article 9(1), we would welcome amendments **clarifying that all GDPR provisions relating to consent** (including Article 8 of the GDPR on children's consent) **apply also for purposes of the ePrivacy Regulation**. In particular, we would welcome the following text: '*The definitions of and conditions for consent provided for in Regulation (EU) 2016/679/EU, including, inter alia, in its Article 4(11), 7 and 8 shall apply'.* When this is ensured, unnecessary repetitions of constitutive elements of consent, such as "specific" consent, may be omitted.

The elements of consent, notably a freely given consent, imply that the processing does not have adverse effects on the rights and freedoms of individuals. We therefore welcome amendments requiring that *'**any processing based on consent must not adversely affect the rights and freedoms of individuals whose personal data are related to or transmitted by the communications**, in particular their rights to privacy and the protection of personal data.'*

We strongly support amendments which re-enforce the principle that consent must be freely given, and prohibit take it or leave it approaches. In particular, we support the proposed amendments to Article 6, which clarify that consent to the processing must not be ***'a condition to access or use a service'.*** This should apply to processing of both content and metadata.

Similar proposed amendments to Article 8, clarifying that consent must not be a **'condition to access or use a service or use a terminal equipment'** are also welcome. We also welcome the proposed amendments requiring that ***'no user shall be denied access to any information society***

***service or functionality, regardless of whether this service is remunerated or not, on ground that he or she has not given his or her consent under Article 8(1)(b) to the processing of personal data and/or use of the storage capabilities of his or her terminal equipment that is not necessary for the provision of that service or functionality.***'

With regard to Article 9(2), **we welcome amendments requiring that the technical settings referred to in this paragraph should allow for sufficient granularity in terms of purposes and providers,** while avoiding unnecessarily repeating provisions of the GDPR. As an alternative to further improve current amendments, the provision may provide instead that the settings shall *'allow the user to actively select the purposes and the service providers'.*

These amendments should further specify that the **technical settings signalling the user's preferences *'shall be binding on, and enforceable against, any other party'.***

We would also support additional clarifications that if a user provides consent, this shall update the pre-existing privacy settings. This update, however, should be limited for the processing requested by the user for this particular service. (For example, a user may agree to be tracked on a particular news website by a specific ad network. However, this should not permit the same ad network to track the user on a different website, unless the user has also specifically consented to be tracked when visiting that other website.)

We would strongly welcome amendments that would strengthen Article 10 and would **require privacy protective settings by default.** Accordingly, we recommend that **software placed on the market** permitting electronic communications **shall '*by default, offer privacy protective settings to prevent anyone other than the user from storing information on the terminal equipment of the user and from processing information already stored on that equipment.'***

We would also welcome amendments (see LIBE 639, 640) **for the requirements of data protection by default to apply not only to software but also to hardware providers**. This would provide a stronger and more direct incentive for providers of Internet of Things (IoT) devices to consider data protection by default and by design.

Finally, **we consider it crucial that users should have an easy way to give or withdraw their consent at a granular level, for specific purposes and with regard to specific service providers at any time during or after installation of the software.** This should include easy ways to update their privacy settings (e.g. add or remove one or several specific organisations to their individual, customised white-lists and/or black-lists saved in their privacy settings), without having to go through a range of settings and options each time they navigate to a different website.

In practice, this could mean that individuals visiting a website and encountering a new request for consent could update their privacy settings directly by clicking one of the options offered on the website and their choice will then be stored in their privacy settings. If the individual wishes to withdraw his or her consent, this should also be done in a similar, easy manner.

The last sentence of recital 24 of the Proposal already hints at such a possibility, providing that *'web browsers are encouraged to provide easy ways for end-users to change their privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed'.* **We recommend that this recital and 'encouragement' be turned into a substantive provision and a legal requirement.** Further, this legal requirement should be applicable not only to web-browsers, but also to any providers coming under the scope of

Article 10. Accordingly, **we recommend that Article 10 include a requirement that *'hardware and software placed on the market permitting electronic communications shall provide easy ways for users to change their privacy settings at any time during use'.***

# 7. Restrictions on the rights should be limited in scope (Article 11)

The EDPS supported in his Opinion the approach of the Proposal pursuant to which only selected grounds listed in Article 23(1) of the GDPR can be accepted as grounds for restricting the scope of certain rights and obligations set out in the ePrivacy Regulation. Respect of confidentiality of communications as enshrined in Article 7 of the Charter is essential for the exercise of other fundamental rights and it has thus a distinct role to play. This role is recognised in the constitutional traditions of many Member States which provide for a separate right protecting the confidentiality of communications. Some of these constitutional traditions limit the possibility to restrict this right for the purpose of combatting serious crimes only. We therefore support amendments towards a less intrusive degree of interference which limit the categories of public interest to those specified in Article 23(1)(a) to (d) of the GDPR.

It follows from the CJEU case law that an interference with the rights enshrined in Article 7 and 8 shall be strictly necessary. The condition of *strict necessity* is a horizontal one, irrespective of the sector at issue, such as commercial or law enforcement[5]. We support amendments that refer to the *'strict necessity'* of a measure limiting the rights provided for in Article 5 of the ePrivacy Regulation.

We also support, in accordance with the Opinion, amendments which require that Union or Member State laws which restrict the rights should at least contain a set of provisions that help ensure legal certainty and a minimum set of safeguards. In fact, this requirement implements settled case law on the conditions for a lawful limitation of fundamental rights[6]. For instance, a law that does not provide for the purpose of processing or for the categories of data will not resist judicial scrutiny, as it lacks foreseeability, undermines legal certainty and the necessity of the legislative measure cannot be demonstrated, either. Consequently, reference to Article 23(2) GDPR is all the more required where the law provides for a restriction of the right to confidentiality as provided for in Article 5 of the ePrivacy Regulation.

Given the need to provide for clear and precise rules capable of passing the necessity test, amendments which refer to 'serious crime' should further define the degree of seriousness, as such definition cannot be left entirely to the Member States.[7]

Finally, we support the greatest possible transparency of access requests. To this end, and in accordance with the Opinion, we support amendments introducing periodic reporting obligations of the providers *vis-à-vis* the supervisory authorities (in addition to the obligation, already foreseen in the Proposal, to provide information upon request by the supervisory authorities). We also support amendments imposing an obligation on the providers to publish information on access requests.

# 8. Weakening of confidentiality and integrity of communications should be prohibited (Article 17)

Restrictions on the rights under Article 11 may include technical measures to gain access to communications data. The EDPS supported in his Opinion the right of the users to use encryption and the prohibition of any measures reversing encryption. We therefore support amendments prohibiting the overall weakening of confidentiality and integrity of electronic

communications both at the level of the service itself and the user's terminal equipment (for instance, by mandating to build-in backdoors).

Based on the foregoing, we would welcome amendments based on LIBE 776-780.

## 9. Supervision powers should be granted to the Data Protection Authorities (Article 18)

In his Opinion, the EDPS supported the Proposal, which entrusted data protection authorities ('DPAs') with the supervision of the ePrivacy Regulation. We continue to support this approach, as it ensures legal certainty and consistent application of the data protection framework, for example, with regard to interpreting key concepts such as 'consent'. It also avoids possible duplication of roles amongst DPAs and other authorities, including overlapping of competence, for example if an authority other than the DPA would be competent for confidentiality of communications which entails the processing of personal data. We also oppose amendments that provide for the representation of all national competent authorities (not only DPAs) at the European Data Protection ('EDPB'). These amendments would significantly change the institutional setup as set forth in the GDPR and would bring additional - and possibly unmanageable - complexity. The current rules provide that members of the EDPB are only DPAs and in case of more than one DPAs the Member States have to designate a joint representative.

On the other hand, we support amendments re-enforcing cooperation of National Regulatory Authorities with the DPAs. These amendments calling for a reciprocal cooperation obligation complement the Commission Proposal, which already included a unilateral obligation for DPAs to cooperate with National Regulatory Authorities.

Finally, effective supervision can only be delivered when adequate resources are effectively provided. According to the GDPR, the EDPS is responsible to provide the Secretariat to the EDPB, including staff. We would therefore suggest including a provision requiring the Member States and the EU budgetary authority to ensure adequate resources for national DPAs and the EDPS, respectively.

## 10. Protection against unsolicited communications should be comprehensive (Article 16)

We welcome amendments replacing the word *'or'* between paragraphs 16(3)(a) and (b) by *'and'*. In effect, these amendments will make sure that the presentation of the identity of a line on which the natural or legal person placing the call can be contacted (Article 16(3)(a)) and the use a specific code/prefix to identify it as a marketing call (Article 16(3)(b)) will not remain alternatives, as provided in the Proposal, rather, they will be both mandatory.

We also welcome amendments adding the word 'sending' in addition to 'presenting', which updates the current wording in line with technological changes.

We welcome amendments providing that semi-automated telephone calls (i.e. those using automated systems to eventually connect an individual to the called person) be treated the same way as fully automated systems, and thus, would require prior (opt-in) consent. In this case, national or European do not call registries could be considered for (purely) voice-to-voice calls (not including semi-automated calls).

We also support amendments providing that *'the masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited communications is prohibited'.* This prohibition should apply whatever the purpose of unsolicited communication (e.g. a phishing attempt may be just as or even more unlawful than unsolicited marketing communications).

Finally, as explained in the Opinion, we would also welcome amendments broadening and clarifying the definition and scope of '*direct marketing communications'*, as well as providing protection against all forms of *'unsolicited communications'.*

Brussels, 5 October 2017

[1] These comments take into account: (i) the draft report ('*Draft Report'*) prepared by MEP Marju Lauristin for the LIBE Committee; (ii) the (draft) opinions of the three other EP Committees involved (IMCO, IURI and ITRE); and (iii) the additional amendments 136 to 827 submitted by Members of the LIBE Committee to the Draft Report. All relevant EP documents available at the European Parliament's Legislative Observatory at
http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en
The EDPS also takes note of developments at the Council. See, e.g. Council 11995/17, 8 September 2017.

[2] For instance, some amendments to Article 19 suggest a specific list of topics on which guidelines should be issued by the European Data Protection Board ('*EDPB*'). A general reference to the possibility to issue such guidelines, as already provided for in the Commission Proposal should be sufficient instead. Similarly, the remedies in Article 21 could merely refer to the respective articles of the GDPR and be complemented by the categories of persons entitled to remedies, such as end-users.

[3] See EDPS Opinion 06/2017, WP29 Opinion 1/2017 and reports of independent academics such as the study commissioned for the LIBE Committee, prepared in 2017 by Borgesius and others, available at
http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf

[4] Such as for the definition of 'electronic communications network', 'electronic communications service', 'interpersonal communications service', 'number-based interpersonal communications service', 'number-independent interpersonal communications service', 'end-user', and 'call'.

[5] EDPS, *'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit',* II.4, and the recent Opinion of the CJEU 1/15, para. 140 which re-states the strict necessity requirement.

[6] See also the recent CJEU Opinion 1/15, para. 141, which states that a measure limiting the rights must lay down clear and precise rules governing the scope and application of the measure and imposing minimum safeguards in terms of circumstances and conditions under which a measure limiting a right may be adopted.

[7] CJEU Opinion 1/15, para. 141 in conjunction with 177.