Body of European Regulators for Electronic Communications

BEREC

BoR (16) 133

BEREC Response to the eprivacy Directive questionnaire

Part I. Questions on the evaluation on the current eprivacy Directive

This part comprises focuses on the evaluation criteria as defined in the Better Regulation Guidelines[1] aiming at collecting BEREC's views on a number of key issues for the purpose of evaluating the current framework.

(a) Effectiveness

1. Do you consider that the ePrivacy Directive has achieved its objectives of 1) ensuring full protection of privacy and confidentiality in the electronic communications sector; 2) free movement of data processed in connection with the provision of electronic communciations services and 3) ensuring the free movement of electronic communications terminal equipment?

   Please specify in your answer which provisions of the ePrivacy Directive have in your view failed to deliver on the above objectives.

   Please specify in your reply what are the causes for any failure and whether factors other than the ePrivacy Directive influenced the outcome.

2. Have you encountered any difficulties in applying the provisions of the ePrivacy Directive?

3. It is currently up to Member States to set up the national bodies entrusted with the enforcement of the e-Privacy Directive. Article 15a of the e-Privacy Directive refers indeed to the “competent national authority” and, where relevant, “other national bodies” as the entities entrusted with supervisory and enforcement powers in relation to the national provisions implementing the e-Privacy Directive.

   Based on your experience, do you consider that the fact that some Member States have allocated competence to different authorities has led to divergent interpretation of the rule in the EU or to fragmented enforcement?

   If you answered the previous question positively, please specify whether and how the above shortcomings have represented an obstacle for providers of services, for citizens or for the competent authorities.

[1] http://ec.europa.eu/smart-regulation/guidelines/docs/swd_br_guidelines_en.pdf

(b) Relevance

4. In your opinion, are specific rules in the electronic communications sector still needed to ensure the current objectives of the ePrivacy Directive of 1) ensuring full protection of privacy and confidentiality in the electronic communications sector; 2) free movement of data processed in connection with the provision of electronic communications services and 3) ensuring the free movement of electronic communications terminal equipment?

These objectives still need to be pursued and in certain areas, they may even have to be strengthened, as is the case of objective 1. At the same time, objectives 2) and 3) may not need to be ensured by specific ePrivacy rules as far as they are fully endorsed by the GDPR and the rest of the electronic communications regulatory framework.

5. Please specifiy your answer in relation to the provisions of the current ePrivacy and indicate which provisions are still needed today and which are not.

   In answering this question, please focus on the interplay between the current ePrivacy Directive and other legal instruments, such as in particular the new General Data Protection Regulation.

The ePrivacy Directive envisages a set of provisions on data protection, privacy and confidentiality that are particular to the electronic communications sector and are (still) needed, especially to ensure full protection of privacy and confidentiality in the electronic communications sector.

To this end the scope of the ePD should be adapted to primarily aim at the 'confidentiality of communication'[2] (as mentioned in Article 7 CFREU). This way, a clear dividing line between the scope of the GDPR (article 8 CFREU) and the scope of the ePD would be guaranteed. Consequently, the ePD provisions would be *lex specialis* with regard to all cases where the 'confidentiality of communication' would be concerned, making it clearer and easier to enforce than generic privacy rules, while also providing more legal certainty for market players and users.

Based on this, BEREC believes that following ePD rules are still relevant and may even be strengthened:

- Article 5 - "confidentiality". This rule should apply to all communication services provided over ECS/ECN, e.g. services/apps that provide communications between a finite number of persons (parties) by electronic means, irrespective of the underlying technology[3];
- Article 6, 9 and 10 - "traffic/location data": it should be made clear whether location and traffic data (including IP addresses) are always considered personal data. It should also be made clear that it applies to all communication services provided over ECS/ECN. There might be a special interest for protecting traffic and location data over and above the GDPR, because it is very sensitive data;
- Article 13 - "unsolicited marketing": the current e-PD is stricter than the GDPR (opt-in instead of opt-out), which is the preferred option to limit spam to a minimum; we note that provisions of the eCommerce directive (2000/31/ES – article 7 Unsolicitated commercial communication), should also be reviewed.

[2] In the context of electronic communication.
[3] Definition still needs to be improved.

- Article 7, 8 11 - "itemised billing, presentation/restriction of calling & automatic call forwarding": this should be extended to all services using numbering resources (e.g. E.164) and possibly to other kinds of public identifiers, such as SIP URIs;
- Article 12 - "directories": legal entities should be covered, which is not the case in the GDPR.

There are, however, two cases that deserve further analysis based on its adequacy to the to GDPR and FD:

The first one regards network and information security (art. 4(1, 1a), (2) and 5 ePD) (not related to personal data breaches).

The ePD should be in line with the electronic communications Regulatory Framework as a whole. For this reason, BEREC proposes that the rules regarding security of electronic communication services and networks (article 4 (1, 1a) ePD) and article 13a of the Framework Directive are merged into one article, while maintaining the same level of protection as currently.

The second one regards specific rules on personal data protection (art. 4(1a), (3), (4) and (5) of the ePD).

On the one hand, there may be some arguments for keeping these provisions and even extend their application to all communication services provided over ECS/ECN.

In the GDPR, the notification of a personal data breach to the supervisory authority has a different focus than the ePD: the parameters of the notification, such as the deadline (24 hours instead of 72), nature of personal data breach and the consequences of the breach as foreseen in article 33 GDPR.

Moreover, according to the ePD (article 4 (5)), the Commission may consult with the European Network and Information Security Agency (ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor to ensure consistency in implementation of the measures of the Directive, whereas according to the GDPR, this role is carried out only by the European Data Protection Board (article 63).

Furthermore, the scope of the reporting covers all incidents instead of only those that are '*likely to result in a risk for the rights and freedoms of individuals'.*

Finally, a new notification in case of breach of confidentiality (if no personal data involved) could be included in the e-PD.

On the other hand, there are also arguments for streamlining the process of notification of personal data breaches foreseen both in the ePD and the GDPR.

Having two different notification regimes will undoubtedly cause unnecessary administrative burdens and risk of non-compliance for the telecom industry as they are forced to make an individual assessment of which notification procedure to follow for each personal data breach event. This may be even more burdensome if the notification obligation is extended to all communication services provided over ECS/ECN.

For this reason, BEREC suggests to make both notification procedures as similar as possible.

Part II. Questions on the review of the current ePrivacy Directive

The purpose of this part is to seek BEREC's views on the regulatory challenges the reform of the ePrivacy Directive should address. Therefore, this part consists of deals with the key issues and provisions of the ePrivacy Directive.

A. General

1. Based on your experience and taking into account of the content of the future GDPR, what should be the priorities for a future ePrivacy legal instrument?

General principles

The general data protection EU legislative framework (hereinafter, GDPR) and the e-Privacy Directive (hereinafter, the ePD) have historically pursued distinct objectives; such a differentiation still remains in the current digital context, where ensuring confidentiality of communications and privacy is of the utmost importance in order to promote trust and security for users of electronic communications networks and services.The ePrivacy legislation, which shall deal with the electronic communications sector-specific issues, will continue to play a key role. Nevertheless the current provisions should be reviewed and, if needed, updated, with a view to streamline the relevant discipline while guaranteeing that the current standard of protection is not undermined and overlaps between the ePD and the GDPR should be avoided.

Finally, it should also be a priority to reassess the scope of the ePrivacy legal instrument to ensure an appropriate level of legal protection for users of communications services which are provided “over the top” (OTT), in particular taking into account various considerations such as the right to confidentiality of communications, recognised in Article 7 of the Charter of Fundamental Rights of the European Union (“hereinafter, the Charter”), and the need for a level playing field in the electronic communications sector.

Confidentiality of communications

The GDPR aims to protect natural persons in relation to the processing of personal data and to ensure the free flow of personal data between Member States. The protection of natural persons in relation to the processing of personal data is a fundamental right that stems from Article 8(1) of the Charter.

While the GDPR applies to all processing of personal data by automated means, it is not specifically designed to protect fundamental rights (e.g. privacy) in relation to unstructured data in transit, i.e. information being transmitted on an electronic communications network. Hence, the GDPR does not apply to information that cannot be directly or indirectly related to a natural person, such as information relating to legal persons or unidentifiable persons.

To a certain extent, the ePD particularises and complements the general personal data protection regime. However, while the GDPR applies to all processing of personal data by automated means, excluding legal persons, it is not designed to protect other fundamental rights (e.g. confidentiality) in relation to unstructured data in transit, i.e. information being transmitted on an electronic communications network. This is done by the current ePD.

This follows from Recitals 2 and 3 of the ePD and according to Article 1(1), the ePD aims to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to *both* privacy and confidentiality. This is further emphasised by Article 1(2), according to which the ePD also aims for protection of the legitimate interests of subscribers who are legal persons.

The principle of confidentiality of communications is closely linked to Article 7 of the Charter, according to which everyone has the right to respect for his or her private and family life, home and communications, as well as Article 8(1) of the European Convention on Human Rights (ECHR). Confidentiality of communications can be crucial to ensure other fundamental rights and freedoms, such as privacy, the right to freedom of expression and the right to private property.

It should be emphasised that while the GDPR comprehensively protects the right to protection of personal data, it cannot fully achieve the objective of ensuring confidentiality of communications which, as it is mentioned above, has a wider scope. Therefore, an important priority for a future ePrivacy legal instrument is that it should continue to implement the fundamental right of confidentiality of communications and, in particular, to maintain and strengthen the rights and the obligations on communications services providers (as defined under the new umbrella definition by the EC) that are necessary to ensure that right. The impact of emerging technologies like IoT and M2M also has to be considered.

As is elaborated further below, Articles 4, 5(1) and 6 of the ePD are of particular importance for the safeguarding of confidentiality of communications. In essence, the following should be the priorities for the future ePrivacy legal instrument:

- Articles 5(1) and 6 should be updated to match current technologies and current threats to confidentiality of communications.
- Articles 6 and 9 need to be adapted to the suggested new scope of the ePD.
- Information security, with appropriate technical and organisational security measures taken by the providers, remain key to ensure confidentiality of communications. Therefore the essence of Article 4 remains important to keep.

Article 5(1)

The basis for ensuring the right to confidentiality of communications is mentioned in Article 5(1) of the ePD. It emphasises that both the contents of communications and the related traffic data should be protected from all kinds of interception or surveillance. However, it does not explicitly govern all kinds of conveyance of communication[4] and/or storage of the contents of communications.

As technology has developed, so have the threats to confidentiality of communications. Nowadays, it is for instance possible to automatically analyse network traffic in real time (i.e. Deep Packet Inspection), even on a core network level. Such analysis could be used for anything from traffic management to profiling of the network users for marketing purposes. In order to ensure an effective protection of the confidentiality of communications, the wording of Article 5(1) should be amended to address recent

[4] With the exception of broadcasting.

developments in both technology and business models. It should be made clear that all kinds of conveyance of communication and storage of communications is within the scope of protection, and thus subject to the obligation to obtain consent.

Article 6

With the dramatically increased use of electronic communications in recent years, and the advance of technology to analyse and utilise large amounts of data, nowadays it is possible to extract very detailed and potentially sensitive information about subscribers and users merely from the traffic data generated when using electronic communication services. Maintaining explicit and restrictive rules on the processing of traffic data should therefore be a priority for a future ePrivacy legal instrument. While much traffic data is indeed personal data, ensuring confidentiality of communications requires protection of all traffic data, regardless of whether the subscriber or user is an identifiable natural person or not. Furthermore, bearing in mind the potential threat to confidentiality of communications presented by misuse of traffic data, it is essential to limit such data to what is necessary for the provision of the electronic communications service. Any further use should be subject to consent of the subscriber. For these reasons, it should be a priority to retain and update Article 6.[5]

See further below, in response to question 9.

Article 4

Finally, to ensure confidentiality of communications, it is vital that sufficient technological and organisational measures are put in place by both the network providers and the service providers. Article 4(1), (1a), (2) and (5) of the ePD requires electronic communications service providers, in conjunction with the providers of public communications networks, to safeguard security of its services. As is already the case in the current Directive, the obligations should not be limited to the processing of personal data but should also be applied to electronic communications services as such, and thus all information processed in conjunction with the provision of such services.

Security measures at the network level can be crucial to prevent unauthorised access to information in transit, which is why communications network providers should be obliged to take such measures even though they might not be considered processors of the communications data themselves.

In conclusion, it should be a priority to maintain the obligations on networks and services providers laid down in Article 4 (1), (1a), (2) and (5).

In the case that the REFIT overview would result in that the objectives in Article 4 should no longer be kept in the ePD BEREC notes that Article 13a of the Framework Directive also lays down obligations on providers of electronic communications services and networks, to undertake appropriate technical and organisational security measures. The objective of Article 13a has (according to ENISA) been interpreted by a majority of Member States as pertaining mainly to continuity of supply, whereas the objective of

[5] The question whether Article 9 ePD is obsolete depends on the extent of the modernisation of Article 6.

Article 4 (1), (1a), (2) and (5) of the ePD is to protect personal data processed in conjunction with the provision of communications services.

While there is currently little overlap between the respective objectives of Article 4 (1), (1a), (2) and (5) of the ePD and Article 13a of the Framework Directive, it could be considered to merge the two since they are both related to network and information security. This would require introducing amendments to Article 13a in order to ensure that the current objectives of Article 4 (1), (1a), (2) and (5) are properly incorporated.

Finally, since notification of security incidents provides an important tool for competent authorities to assess and properly address information security threats and vulnerabilities Article 4(3) should also be extended, so as to ensure that all incidents which could affect the confidentiality of communications – i.e. not only personal data breaches – are in scope. Examples of such incidents could be the unauthorised disclosure of the contents of a communication between two companies, or a message from an anonymous individual providing sensitive information to a media outlet. In the case of a merger between Article 4 and Article 13a it should also be considered if the notification mechanism in Article 4(3) could be merged with the similar mechanism in Article 13a(3) whilst streamlining the notification mechanisms with the GDPR.

2. In your opinion, could a directly applicable instruments (i.e. a Regulation) be needed or better suited to ensure the achievement of the objective of the current ePrivacy Directive?

Starting with the consideration that it is not up to BEREC to identify the most appropriate legal tool in this respect, the question has to be considered by the Commission of whether a Directive or a Regulation would be needed to better ensure the achievement of the objectives of ePrivacy-rules. Furthermore, the impact of picking a determined legal vehicle should be assessed, together with its consistency with the choice made in the field of general data protection, where a new framework will be entering into force in May 2018 by means of a Regulation, the abovementioned GDPR.

While the differences between a Regulation and a Directive are therefore well understood in terms of trade-offs between potentially achieving either more harmonised or nationally more targeted solutions in implementing the e-privacy Directive, BEREC is of the view that a Regulation would more likely risk introducing minimum common denominator solutions compared to a Directive, while the latter might be able to allow Member States for a wider room of manoeuvre in protecting individuals' interests through country-specific solutions as to e-privacy protection.

B. Scope of the current ePrivacy Directive

3. The requirements set forth by the e-Privacy Directive to protect individual's privacy apply to publicly available electronic communication services (ECS). Such rules do not apply to so called Over-The-Top (OTT) services (e.g. unmanaged Voice over IP, instant messaging, web mail, messaging in social networks). This may result in both a void of protection for citizens and in an uneven playing field in this market. Although the rules to protect personal data of Directive 95/46/EC and the

future GDPR apply to OTT communications services, some specific rules of the e-Privacy Directive, such as the principle of confidentiality of communications, do not apply to these services.
Should the scope be broadened so as to cover OTT providers in order to ensure equivalent protection and a level playing field? If your answer is yes, which type of OTT services should be included? Which provisions of the current ePrivacy Directive should apply also to these OTT services?

BEREC has already been working with the Commission on identifying an appropriate scope for the obligations that shall apply to traditional and new online services respectively; also with a view to e-privacy, the reflection has recently evolved with the identification, by the Commission, of a possible new "umbrella definition" of "ECS" which would cover three categories and two subcategories of clearly defined service categories (1) Internet Access Service (IAS); 2) communication services a) using numbers (e.g. VoIP telephony, Instant Messaging using numbers) b) not using numbers (e.g. Email, Instant Messaging not using numbers), and 3) a third category covering the "pure" conveyance of signals for the purpose of communication (e.g. Transmission part of Broadcasting); this approach would allow a differentiated allocation among services of the relevant rules, in line with market dynamics.

It is currently agreed within BEREC that the present scope of e-privacy-related obligations should be widened to cover OTT-1-services[6] as well. Concerning OTT-2-services BEREC would bring the attention to the fact that some OTT-2-services contain ancillary functions, e.g. chat functions, that primarily serve the purpose of communication and could be substituted by OTT-1-services. In BEREC's opinion it should be carefully assessed, whether and in how far such functions should be treated as OTT-1-services, also taking into account different approaches (such as focusing on the key aspect of the respective OTT-1-services, treating them in their entirety according to where this key aspect lies). In any case, the principles of equality and proportionality have to be taken into account.

We note that BEREC response on the broadening of the scope is without prejudice to further examination of the question whether OTT-2 services, aside from their potential OTT-1 functions, should be subject to some of the rules of the e-Privacy Directive or whether the protection by the GDPR is sufficient.

With regard to the Comissions proposed categories the following table provides an idea of which provisions of the future ePD should apply to which category.

[6] As defined in the 'BEREC Report on OTT services' BoR (15) 142, p.3.

I. Rule by rule assessment:

Suggestions for the future scope of the ePD according to the classification proposed by the Commission.

	1 IAS	2a services using numbers	2b services not using numbers	3 pure conveyance of signals
Article 4 → security of processing	X	X	X	if applicable*
Article 5.1, 5.2 →confidentiality of communication	X	X	X	if applicable*
Article 5.3 → data in terminal equipment		X	X	
Article 6 & →traffic data	X	X	X	if applicable*
Article 7 →itemised billing		X	to some extent	
Article 8 → presentation of calling line identification		X		
Article 10 → Exceptions		X		
Article 11 → automatic call forwarding		X		
Article 12 → Directories		X		
Article 13 → unsolicited communication		X	to some extent**	

*category 3 contains different kinds of services. Therefore it is advisable to differentiate and to decide on a service by service basis if a provision is applicable.

**with regard to ancillary functions of OTT-2-services (e.g. chat-functions).

Article 4:

Article 4 ePD relates to data security and the notification of personal data breaches. Currently Article 4 applies to ECS-providers and ECN-providers.

Providers of category 1, 2a, 2b services have access to several kinds of communication data that they may store or process and may be equally at risk of accidental or unlawful data access, disclosure, destruction, loss, alteration or processing of data. Against this background it seems necessary and appropriate to ensure that all services adhere to the same set of rules.

The same line of thought could apply to some category 3 services. Because of the immanent diversity of this category an application of Article 4 has to be decided on a service by service basis.

Article 5:

The confidentiality of communication is one of the fundamental provisions of the ePD. Based on the wording of Article 5.1 it could be argued that Article 5 already applies to all services provided over an ECN (including all OTT services). In turn, Article 3 could be interpreted in the way that the ePD only applies to ECN/S. Surveys amongst BEREC-members have shown that a clarification would be helpful.

The argument – that the end user is likely to expect the same level of protection when using services that seem similar or interchangeable to him – applies in this case. This has to be seen against the background that category 1, 2a, 2b services accrue comparable amounts and types of data and that service providers can create revenue from these data. Again, the same line of thought could apply to some category 3 services. Because of the immanent diversity of this category an application of Article 4 has to be decided on a service by service basis.

Concerning Article 5.3 even under the current regime no distinction was made with regard to the type of service that wanted to access the data stored on the terminal equipment. Therefore the essence of this provision should be kept. As category 3 only concerns the conveyance of singals it does not come into contact with data stored in terminal equipment. The same applies to IAS, as IAS does not include applications that may access data stored in terminal equipment.

Article 6:

Article 6 deals with the processing of traffic data. Under the current regime only ECN/S is subject to this provision.

BEREC would like to point out, that relevant data also accumulate during communication when using services other than ECS. These data need to be protected as they fall under the confidentiality of communication. Thus BEREC proposes that the definition of 'traffic data' should include IP-addresses and port-numbers, as well as data that are used by OTT service providers, that are similar to traffic data and used for identification purposes (also see below at question 9).[7]

Article 7:

Article 7 stipulates that subscribers shall have the right to receive non-itemised billing. Besides category 2a services some category 2b services might need to fall under this obligation as well, e.g. when they are billed. For example messenger services not using numbers containing video-chat-functions that are billed (e.g. message+ from DT). Then the subscriber's privacy could be at risk.

[7] The question whether Article 9 ePD is obsolete depends on the extent of the modernisation of Article 6.

Articles 8, 10, 11:
Article 8 says users can request to prevent presentation of calling and connected line identification. Article 10 provides exemptions from Article 8 in specific cases of nuisance and emergencies. Article 11 pertains to the right to stop automatic call forwarding. All these articles aim at protecting the users or subscribers privacy. With regard to the broadening of the scope of Article 8, only number-based services come to mind (category 2a), since they could provide a presentation of calling line identification. Consequently the same applies accordingly to the articles 10 and 11. BEREC therefore deems an expansion of the scope to all number-based services necessary.

Article 12:
Article 12 ensures privacy regarding the use of personal data in directories. This article only concerns number-based services as its counterpart in the regulatory framework, Article 5 USD, only applies to universal services. BEREC concludes that an expansion of the scope to all number-based services (category 2a) is required to ensure privacy.

Article 13:
Article 13 ensures protection from unsolicited communications. Category 2a and 2b services can also contain the risk of unsolicited communication. E.g. automatically generated marketing messages from messenger services or marketing messages created by your online-market-platforms integrated messaging system. On these grounds BEREC suggests to ensure that the same rules apply to these services, as they provide for the means to send unsolicited communication.

4. Should the scope of the ePrivacy Directive be broadened (eventually subjected to adaptations for different actors on proportionality grounds) so as to confirm that semi-private (or semi-closed networks), such as for instance non-commercial WIFI Internet access (e.g. ancillary to other activities) provided to customers/public in e.g. airports, hospital, mall, universities is covered by the scope of the ePrivacy Directive?
   Please specify how the scope should be defined in order to cover these entities, which are currently not subject to the ePrivacy Directive.

The EC seems to consider that semi-private networks, which are not currently defined under EU Law, are networks used to provide an access to online services that:

- would not be commercial in character and/or
- could be ancillary to another commercial activity or public service which is not dependent on the conveyance of signals on such networks (for example in airport, hospital, mall and universities).

Such networks would not be used to provide an access to online services in a purely private environment (such as a home) or to closed user groups (such as the employees of an office). Also, consistency should be ensured between the interpretation of the

notions of public and private networks and a possible new category of “semi private networks (if such category is necessary).

In order not to hinder the promotion of new services, and against this background, only certain provisions of the ePrivacy Directive seem to be relevant in the case of “semi-private networks” (SPN), i.e. articles 4 (security), 5 (confidentiality), 6 and 9 (traffic and location data). However BEREC would like to point out that the articles applicable to SPNs might need to be slightly adjusted to ensure that they do not act to the detriment of the further development of non-commercial WIFI-access.

In addition, in order to make proportionate the obligations set out in Articles 4, 5, 6 and 9, the European Commission shall be capable to exempt small entities (which still need to be defined) from applying the relevant ePrivacy provisions, and/or demand from ENISA that a security framework shall be designed for them.

In any case, it is rather fair that articles 7 (itemised billing), 8 (presentation of line identification), 11 (automatic call forwarding) and 12 (directories of subscribers) shall be considered as irrelevant when dealing with SPN.

C. Security and confidentiality

5. While an important number of laws imposing security requirements are in place, numerous publicly reported security breaches point to the need for additional policy measures. In your opinion, to what extent would the following measures improve this situation?
   - Development of minimum security standards for networks and services;

Security standards for networks and services shall not be further detailed in the ePrivacy Directive itself. The Directive shall instead refer to the specifications enacted by ENISA and other competent bodies[8].

- Extending security requirements so as to ensure coverage of software used in combination with the provision of electronic communications services;

- Extending security requirements to reinforce coverage of Internet of Things, such as those used in wearable computing, home automation, vehicle to vehicle communications etc.

- Extending the security requirements to ensure coverage of all network components, including SIM cards, apparatus used for the switching or routing of the signals, etc.

Prima facie, BEREC considers all these components already fall within scope, to the extent these components are used by the service provider to produce the ECS. Therefore there would be no need for including such illustrations within the scope of Article 4. It

[8] See for instance, ENISA, Guideline on Security measures for Article 4 and Article 13a, 9 April 2015 and ENISA, Proposal for One Security Framework for Articles 4 and 13a, 20 December 2013

seems indeed that Article 4 already covers such security requirements, notably through the reference to “appropriate technical measures”.

6. In your opinion, should consumers continue to be asked their opt-in consent for the processing of personal data and other information stored in their terminal devices? Should there be any exemptions/exceptions?

In general, the review of the ePD should seek a more balanced approach, ensuring real protection of personal data and privacy without imposing unproportionate burdens burdens on the industry.

For example, BEREC would like to stress that in practice the opt-in consent has become a mechanical process on websites that might prove very little value and which consumers deem as a nuisance. Users’ consent are asked quite frequently. It might also be very burdensome to the industry as consent mechanisms have to be implemented on almost every website.

Therefore, BEREC finds that a continued stream of “tick-the box” on websites, following the requirements of an opt-in consent might eclipse the general goal of privacy protection as the consumers will be “fatigued” or unintentionally mislead by the information. Giving consent regarding the usage of personal data needs to be meaningful.

At this stage, BEREC cannot formulate a definite view on whether new exceptions should be added to the existing legislation. If specific legislation is still considered relevant, BEREC recommends that the provisions are focused on the purpose for which data is being collected rather than the technique used.

7. The practice of websites to deny access to users not agreeing with the the processing of personal data or with the placing of cookies has generated criticism that citizens do not have a real choice. In your view, should this practice be accepted, as a consequence of the principle of freedom of contract and freedom to engage in an economic activity or should it be reconsidered in light of the freedom to receive information and privacy rights? Please, specify your views on how these objectives may find an adequate balance.

7.1. Legal background

The basic rules regarding cookies are settled down in the ePrivacy Directive, in Article 5(3).

BEREC notes that although cookies are regulated in ePD those are not used normally by electronic communication service providers (hereafter: ECS), but are used usually by providers of information society services (hereafter: ISS), like webpages. In turn, the basic

rules regarding ISS are regulated in Directive 2000/31/EC[9] (Directive on electronic commerce, hereafter: eCD), but this directive does not deal with the topic of cookies.

7.2. Opinions and other EU related documents about cookies

The Article 29 Working Party issued several documents regarding cookies. The analytical report[10] regarding the usage of cookies was adopted on 3 February 2015. Working Document 02/2013[11] was adopted on 2 October 2013 and deals with the question of how to obtain consent for cookies. Opinion 04/2012[12] on Cookie Consent Exemption deals with cases when cookies can be used without users' consent.

These documents (especially the analytical report) also confirm the problems set in question 7. The report highlights: "The quality of information provided was variable with more than half (54%) of sites not requesting consent from the user, merely informing that cookies were in use."

7.3. Balance between data protection and the interests of ISS providers

The use of cookies can enhance user experience by storing and "remembering" the data of the users. Cookies also help ISS providers to improve their service and gain data about their users. However, the use of some cookies can raise data protection issues which can result in surveillance of the users. Most users do not know the purpose of cookies, especially the fact that by using cookies their personal data are processed and how they can control and delete cookies from their terminal equipment, usually by the fine-tuning of their browsers. Cookies can serve different purposes and either be merely technical or have commercial purposes. It has to be emphasised that the use of cookies is also a possibility for ISS providers to collect personal data about users in order to achieve the goals of the given homepage (e.g. data collected for statistics regarding the access to a specific site).

A balanced solution has to be found between these two conflicting interests. On the one hand users cannot be forced to accept cookies, and based on the current legislation they have the right to refuse them. On the other hand, ISS providers have legitimate interests to collect and process personal data in this way.

In the opinion of some NRAs, the practice mentioned in question 7, namely, denying access to users not agreeing use of cookies could be accepted. Other NRAs consider that access can only be denied if the user has been provided with the choice of acceding the version of the website clean of cookies in exchange of a fair, reasonable and adequate retribution and has refused this option.

The only reasonable exception BEREC proposes for consideration would be for governmental services (or for public initiative websites) or where the users have no other

[9] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031
[10] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp229_en.pdf
[11] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf
[12] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

choice but to use the service of the ISS in question as long as the cookie constitutes a risk to their personal data (e.g excluding anonymised data gathered for statistics).

Hence, a possible solution to the questions could be some slight amendments of the ePD. These amendments should:

- Specify the exceptions when it is forbidden to deny access for users who refuse the use of cookies including the identification of the cookies that may constitute a high risk to personal data.
- Offer users the possibilities in a straightforward way to use or not use cookies and to call their attention to the consequences of this choice either to not have access to the website or to provide a fair, reasonable and adequate retribution to have access to it without commercial cookies being installed on their terminal equipment.
- Ensure that users are informed that they can “fine tune” the use of cookies by changing the setting of their browsers.
- Guarantee that manufacturers of terminal equipment including operating systems and browsers should be required to offer their products with privacy by default settings (e.g. third party cookies off by default).
- It might be worthwhile to establish different stipulations for governmental websites (or for public initiative websites) or where the users have no other choice but to use the service of the ISS in question as long as the cookie constitutes a risk to their personal data (e.g excluding anonymised data gathered for statistics).

8. It has been argued that requesting users' consent to the storage/access of information in their devices, in particular tracking cookies, may disrupt Internet experience. To facilitate this process and users' ability to consent, a new e-Privacy instrument should (several options possible):
   - Require manufacturers of terminal equipment including operating systems and browsers to place on the market products with privacy by default settings (e.g. third party cookies off by default)
   - Adopt legislation, delegated acts for example, defining mechanisms for expressing user preferences regarding whether they want to be tracked
   - Mandate European Standards Organisations to produce standards (e.g. Do Not Track; Do not Store/Collect)
   - Introducing provisions prohibiting specific abusive behaviours, irrespective of user's consent (e.g. unsolicited recording or filming by smart home devices)
   - Support self-co regulation
   - Other

BEREC believes that e-Privacy Directive should be amended in line with the suggestions discussed in question 7. In general we do not support the adoption of delegated acts because of risk of over-regulation.

Self and co-regulation and standards in theory could be a useful tool. However, it must be noted that this kind of regulation already exists[13], and on the basis of our experience self-regulation alone did not solve the above mentioned problems.

9. Do you consider that the exemptions to consent for processing traffic and location data should be amended? Do you consider that the exemptions to consent for processing traffic and location data should be amended?

In particular, should the exceptions be broadened to include the use of such data for statistical purposes, with appropriate safeguards. Should they be broadened to include the use of such data for public purposes (e.g. research, traffic control, etc.), with appropriate safeguards? Should their processing be allowed for other purposes, provided that the data is fully anonymised?

As stated above, in response to question 1, maintaining explicit and restrictive rules on the processing of traffic data should be a priority for a future ePrivacy legal instrument.

The definition of traffic data

Before considering amending the exemptions to consent for processing of traffic data, a deficiency of the current ePrivacy Directive should be addressed. According to Article 2(b), "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. As new services are created and the service providers' business models (including billing principles) evolve, the data processed for different purposes will vary. And, since the definition of traffic data refers to the purposes for which the data is being used, the data being considered as traffic data will vary accordingly.

Following technology developments and consolidation of services, most electronic communications services are currently provided using the Internet Protocol (IP). However, it is particularly unclear what data should be considered as traffic data for IP communications. There is a need to amend the definition of traffic data in order to minimise such uncertainty. One interpretation of traffic data, which seems appropriate, has been put forward by the EDPS. According to an EDPS opinion on traffic management, the IP packet header should be considered traffic data, while the IP packet payload should be considered contents of the communication, regardless of the purposes for which such data is being used.[14] BEREC has concluded in recital 66 of the BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, that NRAs should ensure that no specific content (e.g. transport layer protocol payload) is monitored. BEREC also proposes that the definition of 'traffic data' should include IP-addresses and port-numbers, as well as data that are used by OTT service providers, that are similar to traffic data and used for identification purposes.[15]

[13] http://www.iab.com/insights/the-future-of-the-cookie/

[14] See Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data (7 October 2011), paragraph 48.

[15] The question whether Article 9 ePD is obsolete depends on the extent of the modernisation of Article 6.

It is important to keep the definition of traffic data technology neutral, but it must be amendedto ensure a clear delimitation of the data in scope, independently of the intentions of or decisions made by individual service providers.

The need for new exemptions

Processing of traffic data which can be directly or indirectly linked to an individual subscriber or user should only be allowed to the extent necessary for the provision of the electronic communications service. However, processing for other purposes should be allowed, provided that the data is fully anonymised or when there is consent. For most relevant purposes, such as research, anonymised data should be sufficient. Should the service provider wish to use non-anonymised data, e.g. for more specific statistical or marketing purposes, it is reasonable to require that consent is obtained. In case the service provider wishes to use non-anonymised data an additional provision might be needed (it has to be ensured that the request for usage of non-anonymised data does not become the norm and it should not be detrimental to the user (e.g. deterioration of QoS) if its consent is not provided.

D. Enforcement

10. Should the consistency mechanism put in place by the future GDPR be extended to the future ePrivacy instrument?

The E-Privacy Directive foresees the possibility that the relevant competent national regulatory authorities adopt measures to ensure effective cross-border cooperation for the enforcement of measures adopted within the scope of the Directive and to create harmonised conditions for the provision of services involving cross-border data flows. However, such measures to ensure effective cross-border cooperation for the enforcement of the Directive have not been adopted so far. There might be several reasons for this:

First, the national institutional set-up, allowing for the identification by Member States of different national authorities competent for e-privacy, might hinder the adoption and design of any general coordination measures as, for instance, fragmentation may make it difficult to identify the relevant authority or burdensome to reach agreements for each different provision of the Directive with different authorities.

Also, the current European institutional set-up for e-privacy does not foresee a European forum for the coordinated enforcement of this Directive which could facilitate reaching this kind of agreements, and the procedure to adopt coordination measures may be long and burdensome, considering the various institutions involved.

Notwithstanding, BEREC notes that, in case that the scope of the E-Privacy Directive is broadened to cover all communication services (i.e. including OTTs that provide voice and instant messaging), a further harmonised approach to the decisions to be taken under the E-Privacy Directive will be needed and stronger cross-border cooperation means should be introduced, with a view to a consistent implementation of the Directive.

A consistency mechanism has been established in the GDPR in order to contribute to its harmonised application when a supervisory authority intends to adopt certain decisions.

Depending on the particular measures that trigger this mechanism, the procedure may end with an opinion or a binding decision issued by the European Data Protection Board.

However, both the possibility to extend the EDPB mechanism to the enforcement of the E-Privacy Directive and the application of the E-Privacy Directive mechanism as it is, are at odds with the current institutional set-up at national and EU level:

At national level, the national bodies entrusted with the enforcement of the E-Privacy Directive are diverse throughout the EU: some Member States have allocated these competences to the data protection supervisory authorities, others to the electronic communication national regulatory authorities, others to another type of bodies, such as consumer authorities and others have distributed different sets of competences envisaged by the mentioned Directive to different national Bodies[16].

Moreover, the enforcement of EU general data protection rules can also be fragmented amongst different national bodies, as foreseen in article 51.1 of the GDPR. In this sense, entrusting the national data protection supervisory authorities with the enforcement of the E-Privacy Directive would not ensure, under the current formulation of the GDPR, a clearer landscape of the national authorities competent for e-privacy, hence further legal certainty for operators as well as a solution to the problem of regulatory fragmentation.

Furthermore, when reasoning around how sorting out such legal certainty issues and identifying accordingly the best placed authority to perform the tasks as in the forthcoming E-Privacy Directive, it may be worthwhile to assess the advantages stemming from granting the competences to the electronic communications NRAs, considering the specific technical expertise needed for the application of the E-Privacy provisions and the relevant efficiency gains.

At EU level, the institutional coordination in the field of general data protection envisages that only one supervisory authority of each Member State is represented at the newly established European Data Protection Board. In case there is more than one supervisory authority responsible for monitoring the application of the Regulation in a Member State, the Member State shall designate the supervisory authority which is to represent all other competent authorities in the Board. Considering the varied national institutional set-ups described above in relation to the implementation of the E-Privacy Directive, jointly with the configuration of the Board established under the GDPR, should the consistency mechanism established in the GDPR be extended to the E-Privacy Directive, the risk would be that a significant part of the members of the Board that have to adopt the opinion or the binding decision foreseen in the procedure are not familiar with the concrete provisions of the Directive. This situation may create even greater inconsistencies than the ones intended to overcome through the cooperation mechanism.

[16] The EC background document to the public consultation on the evaluation and review of the e-Privacy Directive underlines fragmentation of the enforcement tasks foreseen in this Directive and the GDPR among different national bodies as a potential issue for the consistent implementation of these both at national level and across the EU.
http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=15039

In light of this, cross-border cooperation should be enhanced in the e-privacy segment in order to be able to cope with the challenges posed by the development of the communication services within the Digital Single Market.

BEREC considers that the most efficient and suitable way to enhance cooperation would be the establishment of a forum specialised in E-Privacy. This forum would allow competent authorities to exchange experiences and discuss enforcement issues related to the E- Privacy.

In particular and in view of the analysis above, BEREC recommends:

1. Enhancing cross-border cooperation amongst the different authorities entrusted with the implementation of the E-Privacy Directive, since the communication services of tomorrow will be digital and cross border;
2. Because the procedure foreseen in the GDPR is not the most suitable one to ensure further the consistency in the implementation of the E-Privacy Directive, BEREC recommends to review the cooperation mechanisms foreseen under article 15 (a) of the E-Privacy Directive in order to develop a simple, flexible and workable mechanism. In BEREC's view, this would be best achieved by the establishment of a forum specialised in E-Privacy;
3. Furthermore, it may be worth to reason around granting the e-privacy competences to the electronic communications NRAs, considering the specific technical expertise needed for the application of the relevant provisions;
4. A cooperation mechanism between data protection authorities and NRAs could be created. As a reminder, Article 5 and recital 35 FD impose on NRAs and National competition authorities to exchange information. The same could be done for the application of the future ePrivacy legislation . Cross-opinions mechanism could also be established.

E. Other

11. Should any of the provisions of the current ePrivacy Directive be deleted, as no longer needed or fit for purpose?