

# QUESTIONNAIRE FOR THE PUBLIC CONSULTATION ON THE EVALUATION AND REVIEW OF THE E-PRIVACY DIRECTIVE

Fields marked with \* are mandatory.

## QUESTIONNAIRE FOR THE PUBLIC CONSULTATION ON THE EVALUATION AND REVIEW OF THE E-PRIVACY DIRECTIVE

---

The e-Privacy Directive (Directive 2002/58/EC on privacy and electronic communications) concerns the protection of privacy and personal data in the electronic communication sector. The Communication on a Digital Single Market Strategy for Europe (COM(2015) 192 final) of 6 May 2015 (DSM Communication) sets out that once the new EU rules on data protection are adopted, the ensuing review of the e-Privacy Directive should focus on ensuring a high level of protection for data subjects and a level playing field for all market players.

Given that the e-Privacy Directive particularises and complements the Data Protection Directive 95/46/EC that will be replaced by the General Data Protection Regulation (**GDPR**), this questionnaire contains several questions related to the interplay between the e-Privacy Directive and the future GDPR.

In December 2015 the European Parliament and the Council of Ministers reached a political agreement on the final draft of the GDPR. All references to the GDPR in this questionnaire and background document are based on the text adopted in December[1]. After a legal and linguistic review, which may result in small changes to the text, the GDPR will be formally adopted by the European Parliament and Council and the official texts will be published in the Official Journal of the European Union in all official languages.

The purpose of this questionnaire is twofold: First, to gather input for the evaluation process of the ePD (see Section I of the questionnaire) and second, to seek views on the possible solutions for the revision of the Directive (see Section II). The Commission invites citizens, legal entities and public authorities to submit their answers by the 5th of July 2016.

The Commission will summarise the results of this consultation in a report, which will be made publicly available on the website of the Directorate General for Communications Networks, Content and Technology. The results will feed into a Staff Working Document describing the Commission findings on the overall REFIT evaluation of the e-Privacy Directive.

This questionnaire is available in **3** languages (French, English and German). You can skip questions that you do not wish to answer, except the ones marked with an asterisk. You can pause at any time and continue later. Once you have submitted your answers, you would be able to download a copy of your completed responses as well as upload additional material.

Please note that except for responses from visually impaired, in order to ensure a fair and transparent consultation process, only responses received through the online questionnaire will be taken into account and included in the summary.

[1]

[http://www.emeeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217\\_1/sitt-](http://www.emeeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-)

\*

## PRIVACY STATEMENT

Please indicate your preference for the publication of your response on the Commission's website (see specific privacy statement):

*Please note that regardless the option chosen, your contribution may be subject to a request for access to documents under Regulation 1049/2001 on public access to European Parliament, council and Commission documents. In this case the request will be assessed against the conditions set out in the Regulation and in accordance with applicable data protection rules.*

- Under the name given:** I consent to publication of all information in my contribution and I declare that none of it is subject to copyright restrictions that prevent publication.
- Anonymously:** I consent to publication of all information in my contribution and I declare that none of it is subject to copyright restrictions that prevent publication.
- Please keep my contribution confidential:** it will not be published, but will be used internally within the Commission.

Specific privacy statement e-Privacy

[Specific 20privacy 20statement ePrivacy.pdf](#)

**Before filling in the questionnaire, we suggest that you consult the background document at the right-hand side of the survey.**

Background document

[05 2004 20Background 20document.pdf](#)

## GENERAL INFORMATION

\*

Question I: If you answer on behalf of your organisation: Is your organisation registered in the Transparency Register of the European Commission and the European Parliament?

- Yes.
- No (if you would like to register now, please [click here](#)). If your entity responds without being registered, the Commission will consider its input as that of an individual.
- Not applicable (I am replying as an individual in my personal capacity).

\*

Question II: Please enter the name of your institution/organisation/business:

Information Commissioner's Office (UK)

Question III: Please enter your organisation's address:

Wycliffe House, Water Lane, Wilmslow, SK9 5AF, UK

Question IV: Please enter your organisation's website:

<http://www.ico.org.uk>

\*

Question V: Please enter the name of a contact person:

Lisa Atkinson

Question VI: Please enter the phone number of a contact person:

\*

Question VII: Please enter the e-mail address of a contact person:

[lisa.atkinson@ico.org.uk](mailto:lisa.atkinson@ico.org.uk)

\*

Question VIII: In which capacity are you participating in this consultation:

- Citizen
- Consumer association or user association
- Civil society association (e.g. NGO in the field of fundamental rights)
- Electronic communications network provider or provider of electronic communication services (e.g. a telecom operator)
- Association/umbrella organisation of electronic communications network providers or providers of electronic communication services
- Association/umbrella organisation/ trade association (other than associations of electronic communication service provider/network providers)
- Internet content provider (e.g. publishers, providers of digital platforms and service aggregators, broadcasters, advertisers, ad network providers)
- Other industry sector
- Government authority
- Competent Authority to enforce (part of) the e-Privacy Directive
- Other public bodies and institutions

\*

Question VIII H: Please specify which kind of competent authority:

- Data Protection Authority
- National Regulatory Authority (telecom)
- Consumer Protection Authority
- Other

\*

Question IX: Please indicate your country of residence? (In case of legal entities, please select the primary place of establishment of the entity you represent)

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Sweden
- Slovenia
- Slovak Republic
- Spain
- United Kingdom
- Other

## I. REFIT EVALUATION OF THE E-PRIVACY DIRECTIVE

Preliminary Question: How much do you know about the e-Privacy Directive?

	Very much	Much	Some	A little	Hardly anything	No opinion
<b>Its objectives</b>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Its provisions</b>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Its implementation</b>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Its relation to GDPR</b>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

### I.1. EFFECTIVENESS OF THE E-PRIVACY DIRECTIVE

The e-Privacy Directive aims to harmonise the national provisions required to ensure an equivalent level of privacy protection in connection with the processing of data in the electronic communications sector and to ensure the free movement of such data and electronic communication equipment. This section seeks to explore the extent to which the objectives of the e-Privacy Directive have been achieved. For more information please refer to the background document (see Section III).

**Question 1: Based on your experience, do you consider that the e-Privacy Directive objectives have been achieved? More particularly:**

	significantly	moderately	little	not at all	do not know
<b>Full protection of privacy and confidentiality of communications across the EU</b>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Free movement of personal data processed in connection with the provision of electronic communication services</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<b>Free movement of electronic communications equipment and services in the EU</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

**Question 1 A: Please specify your reply.** You may wish to focus on presenting the reasons why certain objectives were achieved/not achieved, please also consider whether factors other than the e-Privacy Directive influenced the outcome.

*Text of 1 to 1500 characters will be accepted*

The e-Privacy Directive has gone some way to protecting the privacy and confidentiality of communications across the EU by placing specific obligations on providers of public electronic communications networks. However it is difficult to guarantee full protection of privacy and confidentiality of communications against a changing technological landscape. For example, the increasing use of internet protocols for the transmission of EU communications which are routed internationally and therefore brought outside the scope of the e-Privacy Directive.

We have not provided an opinion on the effect on free movement of data, equipment and services as we feel this is better evaluated by industry and consumer representatives.

**Question 2: Have you encountered problems in applying/understanding the rules (in your role of provider or as individual)? More in particular in relation to:**

	Yes	No	No opinion
Notification of personal data breaches	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Confidentiality of electronic communications	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Specific rules on traffic and location data	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Unsolicited marketing communications sent and received though the Internet	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Itemised billing of invoices	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Presentation and restriction of calling and connected line	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Automatic call forwarding	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Directories of subscribers	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

**Question 2 A: If you answered “Yes”, please specify your reply.**

*Text of 1 to 1500 characters will be accepted*

As a competent authority we cannot provide an answer in a role as an individual or provider. However we would comment that there have been problems caused by a lack of clarity on definitions included within the Directive. For example, it's not clear whether some types of service (eg Wifi access offered by a cafe) fall within the definition of a publicly available electronic communications service. The definitions of 'location data' and 'traffic data' are vague, and it is not clear who they apply to. The current wording in relation to unsolicited marketing communications is proving restrictive when enforcing these provisions in the face of changing technology. The scope of the provisions in relation to directories of subscribers need to be revisited to ensure consistency in a digital world.

**Question 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.

**On the basis of your experience, did the fact that some Member States have allocated enforcement competence to different authorities lead**

	significantly	moderately	little	not at all	do not know
<b>to divergent interpretation of rules in the EU?</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>to non-effective enforcement?</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Question 4:** If you answered 'significantly' or 'moderately' to the previous question, has this in your view represented a source of confusion for:

	Yes	No	Do not know
<b>Providers of electronic communication services, information society services and data controllers in general</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Citizens</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Competent Authorities</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Question 4 A: Please specify your reply.**

*Text of 1 to 1500 characters will be accepted*

Industry and consumer respondents are better placed to evaluate consistency and effectiveness of interpretation and enforcement across Europe. It is also difficult to form a conclusive view on whether any inconsistencies have been caused by the differences in the nature of competent authorities, or underlying differences in national approach and priorities in different member states. Either way, it is important that competent authorities ensure a consistent and effective approach regardless of the nature of the authority and their primary purpose (eg DPA/NRA).

## I.2. RELEVANCE OF THE E-PRIVACY DIRECTIVE

The Data Protection Directive 95/46/EC, which will be replaced by the General Data Protection Regulation (GDPR), is the central legislative instrument in the protection of personal data in the EU. More detailed rules were considered necessary for the protection of privacy and data protection in the electronic communications sector, which led to the adoption of the e-Privacy Directive. This section seeks to assess the relevance of the objectives of the e-Privacy Directive and each of its articles, taking into account technological, social and legal developments. For more information please refer to the background document.

**Question 5: In your opinion, are specific rules at EU level necessary to ensure the following objectives:**

	Yes	No	No opinion
<b>An equivalent level of protection (full protection) across the EU regarding the right to privacy and confidentiality with respect to the processing of personal data in the electronic communications sector</b>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>The free movement of personal data processed in connection with the provision of electronic communication services</b>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<b>Free movement of electronic communications equipment and services</b>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

**Question 6: Is there an added value to have specific rules for the electronic communications sector on...?:**

	Yes	No	No opinion
Notification of personal data breaches	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Confidentiality of electronic communications	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Specific rules on traffic and location data	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Unsolicited marketing communications sent and received through the Internet	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Itemised billing of invoices	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Presentation and restriction of calling and connected line	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Automatic call forwarding	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Directories of subscribers	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

**Question 6 A: Please specify your reply if needed.**

*Text of 1 to 1500 characters will be accepted*

We have answered "no" in relation to notification of personal data breaches and rules on traffic and location data in light of provisions within the GDPR which will address these areas. Our response also reflects the strong preference of the UK NRA for telecoms (Ofcom) to retain specific rules on itemised billing.

### **I.3. COHERENCE OF THE E-PRIVACY DIRECTIVE**

This section aims to assess whether the existing rules fit with each other and whether they are coherent with other legal instruments. See background document for more details (see Sections III.3 and III.6).

**Question 7: Are the security obligations of the e-Privacy Directive coherent with the following security requirements set forth in the different legal instruments:**

	significantly	moderately	little	not at all	do not know
--	---------------	------------	--------	------------	-------------

<p><b>The Framework Directive (Article 13a):</b> requiring providers of publicly available electronic communication services and networks to take appropriate measures to manage the risks posed to the security and integrity of the networks and services and guarantee the continuity of supply.</p>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<p><b>The future General Data Protection Regulation setting forth security obligations applying to all data controllers:</b> imposing on data controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, as appropriate, the pseudonymisation and encryption of personal data and the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.</p>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<p><b>The Radio Equipment Directive:</b> imposing privacy and data protection requirements upon all terminal equipment attached to public telecommunication networks.</p>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

<p><b>The future Network and Information Security (NIS) Directive:</b> obliging Member States to require that digital service providers and operators of certain essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in their operations.</p>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
--	-----------------------	-----------------------	-----------------------	-----------------------	----------------------------------

**Question 7 A: Please specify your reply if needed.**

*Text of 1 to 1500 characters will be accepted*

We have expressed a view in relation to GDPR where we have specific regulatory responsibility - where we would comment that the security obligations are coherent, but result in duplication. Our response on the Framework Directive (Article 13a) reflects the view of the UK NRA for telecoms (Ofcom) - which is again that although the security obligations are 'coherent' there is significant duplication. To the extent that we are aware, the other Directives listed are not inconsistent.

**Question 8:** The e-Privacy Directive prohibits the use of electronic mail, fax and automatic calling machines for direct marketing unless users have given prior consent (Article 13.1). However, it leaves to Member States the choice of requiring prior consent or a right to object to allow placing person-to-person telemarketing calls (Article 13.3).

**In your opinion, is the choice left to Member States to make telemarketing calls subject either to prior consent or to a right to object, coherent with the rules of Art 13.1 (which require opt in consent for electronic mail, fax and automatic calling machines), given the privacy implications and costs of each of the channels?**

- Yes
- No
- No opinion

**Question 8 A: Please specify your reply if needed.**

*Text of 1 to 1500 characters will be accepted*

There should be a harmonised opt-in approach with a clear set of rules which are easy for organisations to follow and for citizens to understand. These should be consistent with provisions in the GDPR. In our view, the privacy implications of receiving unwanted telemarketing calls are at least as great – and arguably greater, particularly for some vulnerable people – than other channels which already require an opt-in (eg electronic mail).

**Question 9: There is legal uncertainty as to whether messages sent through social media are covered by the opt-in provision applying to email (Art 13.1) or by opt-out provisions (Art 13.3). Please indicate whether you agree or not with the following statements.**

	Yes	No	No opinion
<b>I find it more reasonable to apply to marketing messages sent through social media the same rules as for email (opt in)</b>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<b>I find it more reasonable to apply to marketing messages sent through social media opt out rules (Art 13)</b>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

**I.4. EFFICIENCY OF THE E-PRIVACY DIRECTIVE**

In the following section we would like stakeholders to assess the costs and benefits of the e-Privacy Directive, including for citizens at large.

**Question 10: The protection of privacy and personal data in the electronic communications sector is also aimed to increase users' trust in these services. To what extent have the national provisions implementing the e-Privacy Directive contributed to raising users' trust in the protection of their data when using electronic communication services and networks?**

- Significantly
- Moderately
- Little
- Not at all
- Do not know

**Question 10 A: Please specify your reply if needed.**

*Text of 1 to 1500 characters will be accepted*

Consumer representatives are likely to be better placed to give a view on this issue. However, we would comment that while the reporting of personal data breaches is important and ensures organisations in the sector focus on their responsibilities; increased reporting, enforcement activity and related media coverage may act to undermine users' trust even as it raises awareness of security obligations.

**Question 11: To what extent did the e-Privacy Directive create additional costs for businesses?**

- Significantly
- Moderately
- Little
- Not at all
- Do not know

**Question 11 A: Please provide an estimation of the percentage of the total cost and/or any other information.**

*Text of 1 to 1500 characters will be accepted*

We consider industry representatives are better placed to respond on this issue.

**Question 12: In your opinion, are the costs of compliance with the e-Privacy Directive proportionate to the objectives pursued, in particular the confidentiality of communication as a measure to safeguard the fundamental right to privacy?**

- Yes
- No
- No opinion

**Question 12 A: Please specify your reply if needed.**

*Text of 1 to 1500 characters will be accepted*

### **I.5. EU ADDED VALUE OF THE ERIVACY DIRECTIVE**

This section seeks to assess the EU added value of the e-Privacy Directive especially in order to evaluate whether action at EU level is needed for this specific sector. See background document for more details (see Section III).

**Question 13: Do you think that national measures would have been/be needed if there were no EU legislation on e-Privacy for the electronic communication sector?**

- Yes
- No
- No opinion

**Question 14: In your experience, to what extent has the e-Privacy Directive proven to have a clear EU added value to achieve the following objectives:**

	Strongly agree	Agree	Disagree	Strongly disagree	Do not know
<b>Increasing confidentiality of electronic communications in Europe</b>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Harmonising confidentiality of electronic communications in Europe</b>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Ensuring free flow of personal data and equipment</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

## II. REVISING THE E-PRIVACY DIRECTIVE: LOOKING AHEAD

This section covers forward looking questions to assess the possible solutions available to revise the e-Privacy Directive, in case its evaluation demonstrates the need for review.

**Question 15: Based on your experience with the e-Privacy Directive and taking due account of the content of the GDPR, what should be the priorities for any future legal instrument covering privacy and data protection issues in the electronic communications sector? Multiple answers possible:**

- Widening the scope of its provisions to over-the-top service providers (OTTs)
- Amending the provisions on security
- Amending the provisions on confidentiality of communications and of the terminal equipment
- Amending the provisions on unsolicited communications
- Amending the provisions on governance (competent national authorities, cooperation, fines, etc.)
- Others
- None of the provisions are needed any longer

**Questions 16: In your opinion, could a directly applicable instrument, one that does not need to be implemented by Member States (i.e. a Regulation), be better to ensure an equivalent level of privacy protection in connection with the processing of data in the electronic communications sector and to ensure the free movement of such data?**

- Yes
- No
- Other

**Question 16 A: If you answered 'Other', please specify.**

*Text of 1 to 1500 characters will be accepted*

The new instrument should aim to create a more consistent legal regime across Europe to ensure equal protection for individuals and a level playing field for all relevant actors across EU Member States. However, we consider that, as long as the text of the revised instrument is clear and unambiguous in its definitions and requirements, this aim could be met via either a Directive or a Regulation.

## **II.1. REVIEW OF THE SCOPE**

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. See background document for more details (see Section III.2).

**Question 17: Should the scope be broadened so that over-the-top service providers (so called "OTTs") offer the same level of protection when they provide communications services such as Voice over IP, instant messaging, emailing over social networks).**

- Yes
- In part
- Do not know
- Not at all

**Question 18: If you answered "yes" or "in part" to the previous question, please specify which e-Privacy principles & obligations should apply to so called OTTs (multiple replies possible):**

	Strongly agree	Agree	Disagree	Strongly disagree	Do not know
Security obligations	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Confidentiality of communications (prior consent to intercept electronic communications)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Traffic and location data (prior consent to process)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Unsolicited marketing communications (i.e. should Article 13 apply to messages sent via OTT services?)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Question 19: In your opinion, which obligations should apply to the following types of networks (eventually subject to adaptations for different actors on proportionality grounds)?**

	All networks, whether public, private or closed	Non-commercial WIFI Internet access (e.g. ancillary to other activities) provided to customers/public in, e.g. airport, hospital, mall, universities etc.	Only publicly available networks (as currently)
Security obligations	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Confidentiality of communications	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Obligations on traffic and location data	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

## II.2. ENSURING SECURITY AND CONFIDENTIALITY OF COMMUNICATIONS

The e-Privacy Directive requires Member States to ensure confidentiality of communications in public communication networks and for related traffic data. Listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users without the consent of the citizen concerned, except when legally authorised, is prohibited. The requirement for prior consent is extended to cover the information stored in users' terminal, given that users have very sensitive information in their computers, smartphones and similar devices. See background document for more details (see Sections III.3 and III.4).

**Question 20:** User empowerment and the possibility for users to protect their communications, including, for example, by securing their home WiFi connections and/or by using technical protection measures, is increasingly relevant given the number of security risks.

**Do you think that legislation should ensure the right of individuals to secure their communications (e.g. set forth appropriate passwords for home wireless networks, use encryption apps), without prejudice of law enforcement needs to safeguard important public interests in accordance with the procedures, conditions and safeguards set forth by law?**

- Yes
- No
- Do not know

**Question 20 A: Please explain, if needed.**

*Text of 1 to 1500 characters will be accepted*

We have responded 'do not know' as the wording of this question is not clear. However, we support the right of individuals to secure their communications in line with current law, subject to exemptions where necessary and proportionate for national security or law enforcement purposes.

**Question 21:** 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?**

	significantly	moderately	little	not at all	do not know
Development of minimum security or privacy standards for networks and services	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Extending security requirements to reinforce coverage of software used in combination with the provision of a communication service, such as the operating systems embedded in terminal equipment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Extending security requirements to reinforce coverage of Internet of Things devices, such as those used in wearable computing, home automation, vehicle to vehicle communication, etc.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Extending the security requirements to reinforce coverage of all network components, including SIM cards, apparatus used for the switching or routing of the signals, etc.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

**Question 22:** The practice of websites to deny access to those users who refuse to accept cookies (or other technologies) have generated critics that citizens do not have a real choice. **To what extent do you agree to put forward the following measures to improve this situation?**

	strongly agree	agree	disagree	strongly disagree	do not know
Information society services should be required to make available a paying service (without behavioural advertising), as an alternative to the services paid by users' personal information	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Information service providers should not have the right to prevent access to their non-subscription based services in case users refuse the storing of identifiers in their terminal equipment (i.e., identifiers not necessary for the functioning of the service)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Question 22 A: Please explain, if needed.**

*Text of 1 to 1500 characters will be accepted*

These issues are addressed by GDPR. We also consider that any specific rules in this area should ensure users are informed and can exercise choice in how their information is used, but in line with GDPR should seek to balance users' privacy against the legitimate interests of online businesses. Revised e-Privacy rules should avoid dictating business models, especially where there is minimal privacy impact for the individual.

**Question 23: As a consumer, do you want to be asked for your consent for the processing of your personal data and other information stored on your smart devices as regards the following? Select the option for which you want to be asked for your consent (several options possible):**

- Identifiers placed/collected by a third party information society service (not the one that you are visiting) for online behavioural advertising purposes
- Identifiers placed/collected by an information society service you are visiting – when their purpose is website analytics, measuring number of website visitors, where visitors go within the website, etc. ( e.g. "first party" cookies or equivalent technologies)
- Identifiers placed/collected by an information society service you are visiting whose purpose is to support user experience, such as language preference cookies[1]
- Identifiers collected/placed by an information society service to detect fraud
- Identifiers collected/placed by an information society service for frequency capping (number of times a user sees a given ad)
- Identifiers collected and immediately anonymised in a way that it is impossible to identify the users' device
- Other

[1] See Article 29 Working Party Opinion 04/2012 on Cookie Consent Exemption of 7.06.2012

**Question 23 A: Please explain, if needed.**

*Text of 1 to 1500 characters will be accepted*

As a competent authority we cannot answer as a consumer. However, we would comment that requiring consent for the processing of personal data has not delivered the expected protection for individuals because some personal data must be processed in order for the consent mechanism to operate. In our view the rules should also seek to achieve a proportionate balance between the legitimate interests of information society services and the privacy rights of individuals. There is a case for an exemption or an alternative basis for processing other than consent, particularly in cases where the privacy impact on the individual is minimal.

**Question 24:** 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
- Others

**Question 24 A: Please explain, if needed.**

*Text of 1 to 1500 characters will be accepted*

Placing obligations on the manufacturers of terminal equipment is a powerful option which could have far reaching consequences if not considered carefully. The definition of terminal equipment would need to be carefully defined as it could include connected cars, IoT devices and legacy equipment. Consideration also needs to be given as to whether all of these devices are capable of delivering privacy choices. The impact on small start-up companies would need to be carefully considered to avoid a disproportionate detrimental impact on innovation. Again, in our view any rules in this area should seek to achieve a proportionate balance between the legitimate interests of businesses and the privacy rights of individuals, and not impose onerous and disruptive requirements in cases where privacy impact is minimal. Provisions relating to Data Protection Impact Assessments and accountability within the GDPR should already provide protection in this area.

**Question 25:** The e-Privacy Directive contains specific privacy protections for the processing of traffic and location data in order to ensure confidentiality of the related communications. In particular, they must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication or consent to users should be asked in order to use them for added value services (e.g. route guidance, traffic information, weather forecasts and tourist information). Under the existing exemptions, the processing of traffic data is still permitted for a limited time if necessary e.g. for billing purposes. See background document for more details.

**Do you consider that the exemptions to consent for processing traffic and location data should be amended? You can choose more than one option. In particular, the exceptions:**

- should be broadened to include the use of such data for statistical purposes, with appropriate safeguards
- should be broadened to include the use of such data for public purposes (e.g. research, traffic control, etc.), with appropriate safeguards
- should allow the data to be used for other purposes only if the data is fully anonymised
- should not be broadened
- the provision on traffic and location data should be deleted

**Question 25 A: Please explain, if needed.**

*Text of 1 to 1500 characters will be accepted*

We consider these issues are covered by the GDPR.

### **II. 3. NON-ITEMISED BILLS, CONTROL OVER CALL LINE IDENTIFICATION, AUTOMATIC CALL FORWARDING AND SUBSCRIBERS DIRECTORY**

The e-Privacy Directive provides for the right of subscribers to receive non-itemised bills. The e-Privacy Directive also gives callers the right to prevent the presentation of the calling-line identification if they wish so to guarantee their anonymity. Furthermore, subscribers have the possibility to stop automatic call forwarding by a third party to their terminals. Finally, subscribers must be given the opportunity to determine whether their personal data is included in a public directory (printed, electronic or obtainable through directory inquiry services). See background document for more details (see Section III.5).

**Question 26: Give us your views on the following aspects:**

	<b>This provision continues being relevant and should be kept</b>	<b>This provision should be amended</b>	<b>This provision should be deleted</b>	<b>Other</b>
<b>Non-itemised bills</b>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Presentation and restriction of calling and connected line identification</b>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Automatic call forwarding</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<b>Subscriber directories</b>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Question 26 A: Please specify, if needed.**

*Text of 1 to 1500 characters will be accepted*

CLI - this should be amended to prohibit the withholding of CLI on calls made for sales and marketing purposes and to ensure any CLI displayed enables the call recipient to directly contact the caller (to avoid "spoofing")

Subscriber directories - this needs modernisation to reflect the prevalence of contact through social networking and messaging services, and for the reverse lookup rules to apply to other identifiers such as email address or user name.

**II.4. UNSOLICITED COMMERCIAL COMMUNICATIONS**

The e-Privacy Directive requires prior consent to send commercial communications through electronic mail (which includes SMS), fax and automatic calling machines without human interaction). However, companies which have acquired an end-user's email in the context of a sale of products or services can send direct marketing by email to advertise their own similar products or services, provided that the end-user is given the possibility to object (often referred to as 'opt-out'). Member States can decide whether to require opt in or opt out for marketing calls (with human interaction). Furthermore, the protection against all types of commercial communications also benefits to legal persons but the e-Privacy Directive leaves it to Member States to decide whether they are protected by an opt-in or opt-out regime. See background document (see Section III.6) for more details.

**Question 27: Do you think that the Member States should retain the possibility to choose between a prior consent (opt-in) and a right to object (opt-out) regime for:**

	Yes	No	Do not know
<b>Direct marketing telephone calls (with human interaction) directed toward individual citizens</b>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<b>Direct marketing communications to legal persons, (automatic calling machines, fax, e-mail and telephone calls with human interactions)</b>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

**Question 28: If you answered "no" to one or more of the options in the previous question, please tell us which system should apply in your view?**

	consent (opt-in)	right to object (opt-out)	do not know
<b>Regime for direct marketing communications by telephone calls with human interaction</b>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<b>Regime of protection of legal persons</b>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Question 28 A: Please explain, if needed.**

*Text of 1 to 1500 characters will be accepted*

We have elected for opt-in consent on the basis that one consistent rule in all circumstances is simpler to understand and to enforce, and to reflect our experience of the level of consumer concern over unwanted marketing calls. However we can foresee challenges in ensuring that valid consent is obtained from legal persons where they consist of multiple individuals.

#### **II.4. FRAGMENTED IMPLEMENTATION AND INCONSISTENT ENFORCEMENT**

Some provisions of the e-Privacy Directive may be formulated in too broad and general terms. As a consequence, key provisions and concepts may have been implemented and transposed differently by Member States. Moreover, while the Data Protection Directive entrusts the enforcement of its provisions to data protection supervisory authorities, the e-Privacy Directive leaves it up to Member States to designate a competent authority, or where relevant other national bodies. This has led to a fragmented situation in the Union. Some Member States have allocated competence to data protection supervisory authorities (DPAs), whereas others to the telecom national regulatory authorities (NRAs) and others to yet another type of bodies, such as consumer authorities. See section III. 7 of background document for more details.

**Question 29: Do you consider that there is a need to allocate the enforcement to a single authority?**

- Yes
- No
- Do not know

**Question 30: If yes, which authority would be the most appropriate one?**

- National data protection authority
- National (telecom) regulatory authority
- National Consumer protection authority
- Other

**Question 30 A: If 'Other', please specify.**

*Text of 1 to 1500 characters will be accepted*

We express no view on the appropriate distribution of enforcement responsibilities. In the UK, we as the national data protection authority have primary responsibility for enforcing the e-Privacy rules, with expert support and advice from the national telecoms regulatory authority (Ofcom) as required. It is unlikely that any one authority could operate entirely in isolation given overlap with other regulatory frameworks, for example in the telecoms sphere. However, it is important that all relevant regulators should be taken into account when considering cooperation and consistency mechanisms, and access to EDPB.

**Question 31: Should the future consistency mechanism created by the GDPR apply in cross-border matters covered by the future e-Privacy instrument?**

- Yes
- No
- Do not know

**Question 32: Do you think that a new e-Privacy instrument should include specific fines and remedies for breaches of the relevant provisions of the new e-Privacy legal instrument, e.g. breaches of confidentiality of communications?**

- Yes
- No
- Do not know

**Question 33: These questions aim to provide a comprehensive consultation on the functioning and review of the e-Privacy Directive. Please indicate if there are other issues that should be considered. Also please share any quantitative data reports or studies to support your views.**

*Text of 1 to 3000 characters will be accepted*

Preliminary question - we have detailed knowledge of implementation within the UK. We have more limited knowledge of implementation in other jurisdictions.

Question 9 - we have responded 'no opinion' as the relevant considerations are likely to be different depending on the way the messages are communicated, whether via direct message or displayed on a newsfeed. We do however consider that direct messages sent through social media should be opt-in.

Question 17 - we have answered this as 'in part' on the basis that there needs to be a clear and suitably restricted definition of an OTT.

Question 19 - We have selected "only publically available networks" for this question because it is unclear whether all articles would be considered within the extended scope. We can see value in requiring some types of non-commercial networks to be required to provide a minimum standard of security and confidentiality but it may not be appropriate to apply these to a broad group of poorly defined network operators.

Question 21 - our answer here incorporates the views of the UK NRA for telecoms (Ofcom). Security standards already exist elsewhere in telecoms framework, including for software, IOT devices and network components. However, there may be some merit in reinforcing minimum privacy standards, where this goes beyond security measures. Careful thought would also need to be given to extending the scope of obligations beyond service providers within the EU to device manufacturers, and how this could work in a global market.

Question 31 - on the basis that the consistency mechanism adopts a proportionate, common-sense based approach.

Question 32 - any fine or remedy regime should be consistent with, but not necessarily identical to, the provisions within GDPR (on the basis that e-Privacy does not necessarily always relate to personal data).

Please upload any quantitative data reports or studies to support your views.

## **Background Documents**

[document de rfrence \(/eusurvey/files/c6df1ba2-dd8d-4833-829d-5d777561d8c6\)](/eusurvey/files/c6df1ba2-dd8d-4833-829d-5d777561d8c6)

---

## **Contact**

Regine.MENZIES@ec.europa.eu

---