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.emeeting.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 I A: Please indicate your organisation's registration number in the Transparency Register.

52431421-12

*

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

Telefonica

Question III: Please enter your organisation's address:

Avenue des Arts, 20 - 1000 Brussels

Question IV: Please enter your organisation's website:

www.telefonica.com

*

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

Carlos Rodriguez Cocina

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

+32 2 230 95 55

*

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

carlos.rcocina@telefonica.com

*

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 C: Please specify if your company is an SME (<250 staff) or micro-enterprise (<10 staff):

See for the definition of SME and micro-enterprise EU recommendation 2003/361

- ○ SME
- ○ Micro-enterprise
- ◉ None of the above

*

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
Its objectives	◉	○	○	○	○	○
Its provisions	◉	○	○	○	○	○
Its implementation	◉	○	○	○	○	○
Its relation to GDPR	◉	○	○	○	○	○

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
Full protection of privacy and confidentiality of communications across the EU	○	○	◉	○	○
Free movement of personal data processed in connection with the provision of electronic communication services	○	○	◉	○	○
Free movement of electronic communications equipment and services in the EU	○	○	◉	○	○

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

Currently, European citizens cannot rely on European regulation to consistently protect their personal data and privacy, as different sets of rules are applied to functionally equivalent services, from the user point of view, depending only on the classification of the service provider (according to an old fashioned ECS definition). This weakens confidence in the European digital ecosystem and prevents consumers from fully benefitting from the potential of the single market. Telecommunication service providers are highly regulated as regards the privacy and security, while Over the Top (OTT) players are not regulated the same way for the provision of functionally equivalent services. The problem is not only for consumers but also for the competitivity of the European industry. The uneven application of privacy and data protection rules for equivalent services destroys the ability for these players to compete on equal footing in a single market. Therefore, the sectoral ePrivacy Directive, which contributes to a substantial value migration from European telecommunications operators to non EU based OTT players and device manufacturers, is now outdated and can no longer be justified in a world of converged and globally connected online services, particularly once the new GDPR has been approved. The coexistence of two different set of rules creates legal uncertainty and confusion for consumers, which does not play in favour of a coherent Consumer Policy online.

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	◉	○	○
Confidentiality of electronic communications	◉	○	○
Specific rules on traffic and location data	◉	○	○
Unsolicited marketing communications sent and received though the Internet	◉	○	○
Itemised billing of invoices	◉	○	○
Presentation and restriction of calling and connected line	◉	○	○
Automatic call forwarding	◉	○	○
Directories of subscribers	◉	○	○

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

Text of 1 to 1500 characters will be accepted

Europe needs to address the current patchwork of regulation, which compromises the effective and consistent protection of consumers across the digital value chain. Confusion for providers has been originated by the fact that together with general data protection rules (Directive 95/46/EC), there iss a sector specific regulation (ePrivacy Directive). Additionnally, in both cases, transposition of general data protection rules and transposition of ePrivacy Directive has been very different in Member States leading to a lack of harmonisation that has also been very negative for providers and for consumers.
Privacy is fundamental to building trust and confidence in the uptake and use of new digital services by Europe’s citizens. It is important that consumers are able to enjoy consistent privacy standards and experiences, irrespective of the technologies, infrastructure, business models, who provides a service or where a company may be located.
As long as the ePrivacy Directive coexists with the new GDPR, there will be no level playing field, consumers will not experience comparable digital privacy online and operators will continue to face this dual compliance regime and their competitive position will be compromised.
There are a wide range of references pointing to the conclusion that there is no need for sector specific regulation on ePrivacy.

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**
to divergent interpretation of rules in the EU?	○	◉	○	○	○
to non-effective enforcement?	○	◉	○	○	○

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
Providers of electronic communication services, information society services and data controllers in general	◉	○	○
Citizens	◉	○	○
Competent Authorities	○	○	◉

Question 4 A: Please specify your reply.

Text of 1 to 1500 characters will be accepted

Both Directive 95/46/EC and the GDPR foresee the Data Protection Authorities (DPAs) as the competent authorities for enforcement. However, the ePD left up to Member States to decide upon their respective enforcement bodies (DPAs, NRAs or Consumer Protection Authorities). This has led to a fragmented approach and a considerable level of confusion and uncertainty both for providers and citizens alike. For the sake of legal certainty, simplification should be the ultimate goal avoiding to have various competent Authorities responsible at the same time.

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
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	○	◉	○
The free movement of personal data processed in connection with the provision of electronic communication services	○	◉	○
Free movement of electronic communications equipment and services	○	◉	○

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	○	◉	○
Confidentiality of electronic communications	○	◉	○
Specific rules on traffic and location data	○	◉	○
Unsolicited marketing communications sent and received though the Internet	○	◉	○
Itemised billing of invoices	○	◉	○
Presentation and restriction of calling and connected line	○	◉	○
Automatic call forwarding	○	◉	○
Directories of subscribers	○	◉	○

Question 6 A: Please specify your reply if needed.

Text of 1 to 1500 characters will be accepted

Further to the approval of the GDPR, some provisions of the ePrivacy Directive become redundant and should thus be eliminated. Otherwise, maintaining specific regulation would implicitly acknowledge that the new GDPR has failed, does not provide the necessary level of protection and it is not the future proof and technologically neutral legal instrument that the EC imagined when it put forward its proposal. Maintaining two different set of rules in parallel exacerbates existing market distortions and weaknesses in consumer privacy protection. Duplicity of rules is against legal certainty for providers and consumers.
Additionally, it would be necessary to re-organise the current sector-specific consumer protection rules included in the Universal Service Directive and in the ePrivacy Directive. It concerns provisions currently included in the ePrivacy Directive, such ascalling line identification, automatic call forwarding or directories. We believe that there should be a thorough assessment on whether these provisions are still relevant and, to the extent in which it is concluded that there is still a need to keep any of these provisions, they should be transferred to another legislation different from the ePrivacy.

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
The Framework Directive (Article 13a): 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.	○	◉	○	○	○

The future General Data Protection Regulation setting forth security obligations applying to all data controllers: 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.	○	○	○	◉	○
The Radio Equipment Directive: imposing privacy and data protection requirements upon all terminal equipment attached to public telecommunication networks.	○	◉	○	○	○
The future Network and Information Security (NIS) Directive: 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.	○	◉	○	○	○

Question 7 A: Please specify your reply if needed.

Text of 1 to 1500 characters will be accepted

In 2009, ePrivacy Directive introduced for the first time some obligations on security. The GDPR has extended the scope of the new rules on security to all sectors with the primary aim to have a comprehensive, technologically neutral set of rules on security of processing and data breach notifications.
As both Art. 4 of the ePrivacy as well as Art. 32 of the GDPR focus on the security of personal data that is processed, there undeniably is an overlap between both instruments that cannot be justified and is no longer required. As data processing security obligations included in the GDPR offer the same or even a higher level of protection as the ones included in the ePrivacy Directive, it makes more sense to retain that more advance and horizontal regime.
Therefore, it does not make sense to maintain dissimilar security requirements under the ePrivacy Directive, the GDPR and the Framework Direcitve, as this creates an undesired and overly complex situation for telecom providers, stakeholders, authorities and consumers. Maintaining specific rules embedded in a sectoralspecific ePrivacy legal instrument together with the new GDPR provisions on security of processing is not sustainable. Therefore, only the new regime set up by the GDPR should be retained and the ePrivacy provisions should be repealed.

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

As this question refers the ePrivacy, the answer is positive as the Directive left room for Member States to choice between various regimes. However, today this issue is already covered by GDPR without room for monoeuvre for Member States.

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
I find it more reasonable to apply to marketing messages sent through social media the same rules as for email (opt in)	○	○	○
I find it more reasonable to apply to marketing messages sent through social media opt out rules (Art 13)	◉	○	○

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

The GDPR will contribute as it has already done even before its adoption to raising users' trust and awareness. A specific sector regulation will only increase confusion for users as they do not know by which rule they are protected. Here it is important to recall the Digital Single Market Strategy, which explicitly mentions that GDPR will increase trust in digital services, as it should protect individuals with respect to the processing of personal data by all companies that offers their services on the European market.
The ongoing ePrivacy review is an opportunity and a must for a move towards a more horizontal approach in EU legislation as sector specific rules are inadequate for dynamic environments. As an example, the new GDPR will imply a more consistent and horizontal approach leading to a level playing field and thus contributing to users trust and awareness.

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

The implementation of the ePrivacy Directive has implied additional direct costs for the regulated businesses, but the most important costs are no doubt the opportunity costs, as traditional telecommunications operators have been prevented from offering new services that have been launched by other actors not subject to the ePrivacy (eg.: geo-location based services). These services are very demanded and widely adopted by consumers, but telecom operators have not been able to respond to this demand due to regulatory burdens. This imposes a significant loss of competitiveness on the concerned organizations and a relevant impact on the innovation and on the time to market for new services. Besides, investments that would have been made in the absence of regulation are delayed of finally discarded.

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

The objectives of ensuring confidentiality of communications might be very relevant, but the point is that the costs of compliance have only be put on a certain number of actors (e-communications service providers) while other actors not covered by EPD should also ensure the confidentiality of communications and the fundamental right to privacy. This has put European telecommunications service providers at a competitive disadvantage vis-à-vis other players offering the same services.

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 valueto achieve the following objectives:

	Strongly agree	Agree	Disagree	Strongly disagree	Do not know
Increasing confidentiality of electronic communications in Europe	○	○	◉	○	○
Harmonising confidentiality of electronic communications in Europe	○	○	◉	○	○
Ensuring free flow of personal data and equipment	○	○	◉	○	○

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 GDPR makes specific sector specific regulation redundant and counterproductive. The recent CERRE study on Consumer Privacy in Network Industries states that a future proof regulation requires a common approach to all industries and that sector-specific privacy regulations are inadequate in a dynamic environment and should be withdrawn. This was also the conclusion published by the EC in June 2015 on the ePrivacy Directive, which concluded that maintaining a distinct regulatory regime for ecommunications services, information society services or audiovisual services will most probably become less relevant in the future. The long term priority of the ePrivacy review should enable European businesses to compete at the global level in Big Data, Cloud, IoT. Therefore, once GDPR adopted, the review should focus in removing overlapping provisions with GDPR, transferring consumer protection rules (not strictly related to privacy) into more appropriate tools and clarifying the scope of the remaining provisions, if any, in order to achieve a true level playing field between traditional telcos and Internet based service providers in the interest of businesses and end users (as stated in the DSM Strategy). Only after this throughout exercise, if still some pro
visions are considered necessary, a new Privacy instrument should take the form of a Regulation to align with GDPR and achieve full harmonisation at the EU level, one of the major shortcomings of the current ePrivacy.

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	(●)	( )	( )	( )	( )
Confidentiality of communications (prior consent to intercept electronic communications)	( )	(●)	( )	( )	( )
Traffic and location data (prior consent to process)	( )	(●)	( )	( )	( )
Unsolicited marketing communications (i.e. should Article 13 apply to messages sent via OTT services?)	( )	(●)	( )	( )	( )

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	◉	○	○
Confidentiality of communications	◉	○	○
Obligations on traffic and location data	◉	○	○

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

There is no need to define further security measures and obligations in order to ensure the right of individuals to secure their communications. Confidentiality of communications is already safeguarded by the legislation, although it needs to be applied equally to all communications services, whether considered to be ECS or OTT. Consequently there is no need for complementing the right of confidentiality of communications with additional legal provisions on encryption regarding the communication between individuals, especially as they cannot keep pace of technology developments. Applications that offer encryption for voice, text and video messages have been around for years. Such apps are increasingly being used to provide appropriate and user-friendly solutions. It is in the interest of industry to offer consumer-friendly solutions as a central differentiating factor between companies (race to the top). The current challenge is the spreading of encrypted data flows that impacts on several obligations that apply to network operators. When traffic is encrypted and routed through browser proxies by internet players, operators cannot develop security measures like malware detection and anti-virus protections, or cooperate with national law enforcement authorities to ensure interception of communications, fight against child pornography and content filtering (parental control). Thus, legislation should focus on providing a coherent solution to tackle all these challenges.

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	○	○	○	◉	○
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	○	○	○	◉	○
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.	○	○	○	◉	○
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.	○	○	○	◉	○

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	○	○	○	◉	○
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)	○	○	○	◉	○

Question 22 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

If there is an exchange of value, the offering must have the right to ask the customer to accept his/her respective part in the transaction (advertising and cookies placement). This is the data as a currency model where the user accept to participate with different extension and terms in the advertising ecosystem in exchange of a free service. This model must be based upon the assumption of informed consent where the transaction is under the reasonable expectations of the consumer. If that is the case, the regulation must not prevent enterprises to freely decide its business model, always based on the respect to fundamental rights and freedoms of individuals.

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 and 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
- [x] 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

Telefónica cannot answer to this question "as a consumer" as we are answering to this questionnaire as a corporation.
Currently, most of the cookies used can be classified as first party cookies. Art. 29 WG has already recommended that first party analytics cookies should not require prior consent of website visitors as they are not likely to create a privacy risk (ART 29 WG Opinion 4/2012). Similarly, identifiers placed to detect fraud, for frequency capping or those immediately anonymised so that it is impossible to identify the users' device should not require prior consent. These identifiers do not imply any potential negative impact in the privacy of the individuals and are counterproductive as they cause users' fatigue without providing any enhanced level of protection to the right of confidentiality of the individual.
We understand that from a privacy protection perspective, cookies are already regulated under the GDPR. Such cookies which do not represent a risk to privacy given that no personal data processing is involved (tech cookies, for instance) no regulatory action is needed. For the rest of the cookies, the GDPR provides enough regulatory basis. Such cookies which provide first party analytics, a legitimate interest legal basis could be valid, for other third party advertising cookies or tracking cookies which pose a risk to the privacy of the data subjects an informed consent based on GDPR provisions is already required.

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
- [x] Others

Question 24 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

Telefónica believes that there is no need for a new ePrivcay instrument. Self-regulation and European standards on Do Not Track solutions should be developed as they will help to increase the level of privacy protection without disrupting consumers' Internet experience. Already the GDPR recognises the importance of self-regulation and encourages the drafting of Codes of Conduct by industry. Therefore, another sector specific ePrivacy incorporating these points would be redundant. Europe should fully take stock of the GDPR, which creates a level playing field for all companies offering services in the EU.

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:

- [x] should be broadened to include the use of such data for statistical purposes, with appropriate safeguards
- [x] 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
- [x] 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

Compared with Directive 95/46/EC, the GDPR provides for a higher level of protection for the processing of personal data, therefore there is no longer a rationale to treat the processing of traffic data and location data by telecom providers on the one hand and all other players (including OTTs) on the other hand differently, especially in a convergent landscape. The current provisions on traffic and location data of the ePrivacy Directive should be repealed for the sake of simplification and the need to avoid overlapping provisions
In case the Legislator would still consider necessary sectoral specific rules on traffic and location data, the same legal grounds for processing put forward by GDPR should apply, including the possibility to use such data for statistical purposes or public purposes (research, traffic control) with appropriate safeguards, as required by 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:

	This provision continues being relevant and should be kept	This provision should be amended	This provision should be deleted	Other
Non-itemised bills	○	○	◉	○
Presentation and restriction of calling and connected line identification	○	○	◉	○
Automatic call forwarding	○	○	◉	○
Subscriber directories	○	○	◉	○

Question 26 A: Please specify, if needed.

Text of 1 to 1500 characters will be accepted

There should be a thorough assessment on whether these consumer-focused provisions are still relevant. Rules on CLI or directories are redundant because they are outdated or already addressed by industry in practice. For instance, regarding directories, the development of powerful search engines and online services have changed the ability to search for professional services. Additional obligations on traditional telecommunications providers are no longer relevant or necessary, which is reflected by the fact that 18 Member States have already taken directory enquiries out of the scope of the Universal Service Obligation. Only in case, consumer related provisions of the ePrivacy would still be considered necessary, they should be mover to the new framework covering communications.

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
Direct marketing telephone calls (with human interaction) directed toward individual citizens	○	◉	○
Direct marketing communications to legal persons, (automatic calling machines, fax, e-mail and telephone calls with human interactions)	○	◉	○

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
Regime for direct marketing communications by telephone calls with human interaction	○	◉	○
Regime of protection of legal persons	○	◉	○

Question 28 A: Please explain, if needed.

Text of 1 to 1500 characters will be accepted

An overall standard at EU level is necessary to ensure that consumers in Europe are not protected in a different way depending on their location. In this sense, the European legislator has already decided on an opt-out standard within the GDPR. Therefore, there is no need for any additional specific regulation.

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

The co-existence between various national competent Authorities is due to the fact that the exists duplicity of rules covering the sector. Therefore, the most important thing is to avoid this duplicity and allow the GDPR to create the necessary level playing field between all players irrespective of sector or geographic location. For that, no sector specific legislation seems justified anymore.

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

```
EC COM STUDY (June 2015)
https://ec.europa.eu/digital-agenda/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data
o        CERRE studies
November 2014: CERRE Study on Market Definition, Market Power and Regulatory Interaction in Electronic Communications Markets
http://www.cerre.eu/sites/default/files/141029_CERRE_MktDefMktPwrRegInt_ECMs_Final_0.pdf:
January 2016: CERRE Study on Consumer Privacy in Network Industries
http://www.cerre.eu/publications/consumer-privacy-network-industries
o        DLA Piper Studies (2015 & 2016)
May 2015: DLA Piper Study on repealing ePrivacy Directive

http://www.iisp.gatech.edu/working-paper-online-privacy-and-isps
```

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

Background Documents

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

Contact

Regine.MENZIES@ec.europa.eu