Contribution ID: ea81ea67-2e99-439f-938b-11b6dc19f2dd
Date: 05/07/2016 10:17:36

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-1739884.

* **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.

2893800753-48

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

Verbraucherzentrale Bundesverband (vzbv)

Question III: Please enter your organisation's address:

```
Markgrafenstr. 66
10969 Berlin
Germany
```

Question IV: Please enter your organisation's website:

```
http://www.vzbv.de/
```

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

```
Lina Ehrig
```

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

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

```
Digitales@vzbv.de
```

* 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 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

While the ePrivacy Directive (ePD) is an important instrument to ensure protection of privacy and confidentiality of communications, it has in no way achieved full protection. While a few years ago, most communication was conducted via traditional telecommunication providers, consumers today communicate via information society services or the services of over-the-top providers ("OTTs") that provide communication services over the Internet (like Voice over IP or instant messages). For example in 2012, when the ePD was implemented in Germany, German consumers sent over 160 million SMS and 20 million WhatsApp messages per day [1]. In 2015, the numbers turned: Germans sent less than 40 million SMS per day but over 660 million WhatsApp messages. Those messages do not enjoy the same legal protections as SMS.

Also the objective of harmonising the rules on privacy and confidentiality in the electronic communication sector in the EU has only been achieved moderatel y. Some of the rules expressly allow divergent implementation. Other provisions, like rules on cookies and similar tracking techniques have been implemented differently by Member States [2]. This leaves consumers in an unclear situation, since it is harder for them to know and exercise their rights.

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

Consumers do not understand the scope of the directive: E.g. they dont understand why their communication via SMS is more protected than their communication via (instant) messages sent via OTTs.

The rules on cookies etc. are often misinterpreted. On the one hand users receive warning messages on almost every website, even when all the cookies etc. are necessary to provide the service. Also cookies and similar techniques are often placed on the equipment of the users, even before they have given their consent.

In Germany the provisions on cookies etc. led to lots of confusion. The German government has taken the position, that the provisions are implemented by the German Telemedia Act. But the German data protection authorities [3] and consumer organisations [4] disagree with this and are calling for action. E.g. the Telemedia Act only covers personal data and not information. Also for the purposes of advertising and market research, the service provider may establish profiles of usage based on pseudonyms (by cookies) as long as the recipient of the service does not object to this. This is an untenable situation for all concerned parties as it creates a high level of uncertainty.

Furthermore, it is not clear if unsolicited marketing communication transmitted via information society services such as webmail or social networks etc. fall within the scope of the directive.

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

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

The General Data Protection Regulation (GDPR) formulates only general rules. But due to specific risks in the electronic communications sector there is a need for specific rules for providers of electronic communication networks and services, information society services and OTTs which ensure a high level of protection. This is all the more important as two fundamental rights are concerned: the protection of personal data (Article 8 EU Charta of Fundamental Rights (CFR)) and the protection of the confidentiality of communication (Article 7 CFR) and with a view to the accession of the EU to the European Convention on Human Rights also Article 8 of the ECHR.

Since there is noticeably low trust in data protection by telecom and online companies (see Question 10 A) and repeated scandals of "lost", "hacked" or "stolen" data this sector needs specific and clear rules to provide companies with clear obligations and give the consumers trust that their data are protected and tools to protect their fundamental rights.

Notification of personal data breaches is already sufficiently covered by the GDPR.

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

All these legal instruments are coherent with the obligations of the ePrivacy directive. They complement each other and contain specific provisions regarding different elements and actors like network providers, service providers, terminal equipment, etc to ensure the protection of personal data and the protection of the confidentiality of communication on a high level.

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

Unsolicited telemarketing calls are often perceived as very intrusive. The harassment is not less compared to automated calls or electronic mail often it is rather higher since telephone calls are a direct way to communicate and interact with individuals in real time. In these situations consumers are often very vulnerable and under pressure which makes them susceptible to misleading practices or unwanted purchases (especially young or elderly persons).

Such telemarketing may impose costs on the recipient, e.g. when he is abroad and has to pay for incoming calls.

Also see answers to question 28 A.

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

As the latest Eurobarometer 431 on Data Protection shows, in Germany the number of users that trust in telephone and internet providers increased between 2010 and 2015 from 20% to 32%. On the other hand in 2015 only 19% of the Germans trust online businesses (3% increase since 2010). Still 70% of Germans are concerned about their information being used for a different purpose from the one it was collected for (e.g. direct marketing, targeted online advertising, profiling).

Trust is also low because of personal data collection by government and law enforcement agencies. 48% of people in Germany say these collections have had a negative impact on their level of trust.

Hence, the consumers trust in the digital economy overall is quite low. To reinforce trust, the ePD should ensure the protection of personal data, the confidentiality of all electronic communication of the users and the confidentiality of their online activities.

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

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

Even without knowing the exact costs of compliance with the ePD for businesses, we can assume, that they are proportionate to the objectives pursued. The protection of personal data and the protection of the confidentiality of communication are fundamental rights. It should be also recognised, that the provisions of the ePD are not only good for consumers but for the industry too. They lead to EU-wide harmonisation and build consumers trust in the internet economy. Clear rules also favour companies that are already compliant to the principles of data protection and confidentiality of communication.

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:

- [x] Widening the scope of its provisions to over-the-top service providers (OTTs)
- [ ] Amending the provisions on security
- [x] Amending the provisions on confidentiality of communications and of the terminal equipment
- [x] Amending the provisions on unsolicited communications
- [x] Amending the provisions on governance (competent national authorities, cooperation, fines, etc.)
- [x] 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 provisions of the future ePD should not only be widened to cover OTTs, but also information society services in general to ensure data protection and confidentiality of communications on a high level in the whole online environment. This would also future-proof the legislation with regard to expected technological developments in the information society service sector.

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

Users should always have the right to secure their networks, equipment and communication with the best available techniques. They should also have the right, to secure their network, equipment and communication against malvertising [5] and mobile cramming with the use of ad-blockers and similar means.

On the other hand, providers of electronic communication services should be obliged to secure all communication by using the best available techniques to ensure confidentiality. The inclusion of backdoors in soft- and hardware should be prohibited since strong encryption is not only essential for the security of the citizens and consumers trust but also for the European economy [6]. With regard to critical infrastructure and the extension of such infrastructure by way of technological progress (e.g. automated cars, smart-homes, intelligent energy system, machine-to-machine communication) obliging providers to use the best available techniques – including regular updates – to secure their systems is essential.

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

Information society services should be required to make available an alternative to payment with users' personal information used to enable behavioural advertising. However, it might be problematic to require a paying service since this could lead to the situation that only people who can afford it can protect their fundamental right to privacy and data protection. Requiring a paying service could also hamper the development of new business models. But there are other alternatives to behavioural advertising, e.g. context-based advertising or advertising based on information about interests actively provided by the user.

The ePD should not fall behind the GDPR: Accordingly consumers should always have the right to object to direct marketing and profiling without a negative impact. Also consent should be presumed not to be freely given if the provision of a service is dependent on consent despite such consent not being necessary for such performance.

The use of "anti-anti-tracking-tools" or "adblocker-blockers" should be prohibited without prior explicit consent of the user, since these techniques often require information stored on the devices of the users. In Germany 57% of the people that use adblockers do this to protect themselves from being tracked on the internet [7].

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):

- [x] 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
- [x] 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

Since a majority of Europeans (53%) is uncomfortable with the fact that internet companies use information about their online activity to tailor advertisements to their interests [8], their prior consent should always be necessary in particular when their personal data or information from their terminals is used for advertising purposes by third parties but also by the first parties themselves. A European data protection seal might be an alternative to consent for the first parties, when they use pseudonymised identifiers for frequency capping.

When a fist party places identifiers for website analytics etc. opt-out of the user should be sufficient. Also consent shouldnt be needed when only anonymised data is used. Anonymising personal data is a very difficult task in times of big data though if even possible at all.

In any case strict purpose limitation must be ensured, e.g. identifiers used for fraud-detection or for first party website analytics etc. must not be used for other purposes.

Tracking and profiling should be seen as monitoring of the behaviour of the data subject" and should therefore fall under the strict provisions of the GDPR on such monitoring (e.g. mandatory data protection assessment).

Users should be asked always for their prior explicit consent when other information like address books, location data, installed apps, advertising IDs / UDIDs etc. is collected from their devices by automated means.

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):**

- [x] 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)
- [x] Adopt legislation, delegated acts for example, defining mechanisms for expressing user preferences regarding whether they want to be tracked
- [x] Mandate European Standards Organisations to produce standards (e.g. Do Not Track; Do not Store/Collect)
- [x] 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

Privacy-by-design and -by-default are important instruments to ensure that consumers are protected, in particular those which have only little knowledge about internet-technologies. These principles are part of the GDPR and should be implemented in detail in sector specific legislation like the ePD.

The past has shown that clear rules defining mechanisms for expressing user preferences are needed, e.g. the current rules are interpreted very differently in the member states (but this question cannot be considered without having in mind the question how users are informed in an appropriate and meaningful manner).

Under certain requirements standards like DNT could be an option, but they have to be set to no tracking by default and all websites and advertisers have to honour the requests without disadvantages for the users.

There should be limitations to some forms of exceptionally intrusive tracking, even if users have given their consent. This is an approach that is followed in other consumer protection legislation. E.g. tracking by telecom companies via Unique Identifier Headers (UIDH) - so called super cookies that are used in several EU countries [9] or cookies that are automatically recreated after deletion and therefore circumvent users choice - so-called zom bie cookies - should be prohibited.

While co-regulation (in accordance with Art. 40 GDPR) could be part of a solution, self-regulation regarding cookies etc has proven ineffective in the past [10]

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

GPS location data or Wi-Fi networks location data etc should be included in the provisions, since in practice consumers are confronted primarily with these localisation techniques that are even more accurate than traffic and location data collected by telecommunication providers.

The principles of data minimisation and purpose limitation are key parts of the GDPR and should be implemented in detail in sector specific legislation like the ePrivacy Directive. Therefore traffic and location data should be reduced to the least-granular that is needed for the purpose for which they were collected. When the data should be used for another legitimate purpose, it should be reduced to the least-granular that is needed for this other purpose.

It is extremely difficult to anonymise location data and combined location data might still lead to identification, like the Article 29 Group pointed out in its Opinion on Geolocation services on smart mobile devices [11]. In 2013, researchers at MIT and Harvard University showed, how easy it is to single out specific individuals on basis of their mobile phone location data [12]. In another study a researcher at Columbia University and Google Research has demonstrated in 2016 that geotagged posts on just two social media apps are enough to link accounts held by the same person [13].

In no case it should be allowed to process traffic and location data for direct marketing purposes on the basis of Art. 6.1(f) of 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:

	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

These provisions are still necessary and relevant to ensure the protection of personal data of the consumers in the telecommunications sector. Itemised bills are metadata and therefore very revealing. Also consumers should have the possibility to protect their anonymity when calling and to block automatic call forwarding to their equipment. Consumers should also have the control whether their personal data is made available to the public.

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

Despite the opt-in requirements for telemarketing, unsolicited telemarketing calls are still a big issue for German consumers. Between 01.07.2013 and 30.06.2015 the German NRA Bundesnetzagentur has received over 60,000 written consumer inquiries and complaints about unsolicited telemarketing and over 40,000 inquiries and complaints via telephone about unsolicited telemarketing and telephone number misuse [14]. Since 2014 the number of complaints decreases (since July 2013 the Bundesnetzagentur can be impose fines up to 300,000 Euros for unsolicited telemarketing).

Telemarketing calls often lead to contracts, which consumers dont want. Between July 2014 and November 2015 German Consumer Organisations received more than 19,500 complaints about unsolicited telemarketing calls and contracts that have been foisted on to them over the phone [15].

Also see answers to question 8 A.

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

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

The goal of the ePD to not only protect the privacy of the users (Article 8 CFR) but also to protect the confidentiality of their communication and information stored on their devices should be further emphasized (Article 7 CFR). Therefore the ePD should introduce a Right to Confidentiality and Integrity of Information Technology Systems, like it was created by the German Federal Constitutional Court in 2008. Member States should enforce this right.

The ePD should include not only telecommunications services and OTTs that provide communications services, but also information society services in general.

The ePD should specify the basic principles of the GDPR, in particular data minimisation, purpose limitation, privacy by design and privacy by default for these services to ensure a high level of data protection and privacy in the online environment. To strengthen the abstract principle of data minimisation, the ePD should make clear, that in general, individuals must be able to use and/or pay public communication services pseudonymously or even anonymously where it is proportionate in relation to processing activities.

ePD should clarify, that it covers (new and future) tracking techniques, even if these techniques dont store information or gain access to information stored in the terminal equipment of a user (like browser / canvas / device

fingerprinting [16], cross-device-tracking, tracking devices via mac addresses, etc), since these techniques are often much more intrusive than regular cookies.

ePD should make clear, that the confidentiality of electronic communication should also be protected against intrusions by automated means (e.g. deep packet inspection) and not only intrusions by persons other than the users.

If the successor of the ePD will be a regulation, it should be made clear, that it has the same territorial scope than the GDPR.

[1] http://de.statista.com/statistik/daten/studie/3624/umfrage/entwicklung-der-anzahl-gesendeter-sms--mms-nachrichten-seit-1999
[2] DLA Piper: EU Law on Cookies, 2014
[3] https://www.datenschutz.hessen.de/ub20150205.htm
[4] http://www.vzbv.de/meldung/cookies-nur-mit-einwilligung
[5] https://www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising
[6] ITIF: Unlocking Encryption, 2016
[7] Hans-Bredow-Institut: Reuters Institute Digital News Survey 2016, p. 68
[8] Special Eurobarometer 431, 2015, p. 40
[9] Access Now: The Rise of Mobile Tracking Headers, 2015
[10] BEUC: EASA - IAB Best Practice Recommendations, 2011
[11] Article 29 Working Party, WP 185, 2011
[12] Scientific Reports; Unique in the Crowd: The privacy bounds of human mobility, 2013
[13] Columbia University: Linking Users Across Domains with Location Data, 2016
[14] Bundesnetzagentur: Ttigkeitsbericht Telekommunikation 2014/2015, p. 207
[15] https://www.verbraucherzentrale.de/unerlaubte-telefonwerbung-nervt-weiterhin
[16] Article 29 Working Party, WP 244, 2014

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

1ad94907-80cc-4e11-809a-4701cb61bc90/_10__2011-09975-01-e.pdf
c8678988-6265-4141-9637-4286e3b9600c/_11__wp185_en.pdf
7c67ff97-1188-453d-9a6f-c2fd947f0bc8/_12__srep01376.pdf
af7c2969-0b64-49b5-b60d-b1f5fccebe1f/_13__RiedererWWW2016.pdf
09f48749-7f4b-4589-889d-7f9515dcc61f/_16__wp224_en.pdf
bb39ea94-d535-4dfe-9e88-3c88cce10e55/_2__EU_Cookies_Update_September_2014.pdf
41b0e9ff-5fff-45e0-87d5-dc129ec68350/_6__2016-unlocking-encryption.pdf
6a5b4be4-0801-472e-8b19-4c2b74342872/_7__38RDNS16_Germany.pdf

Background Documents

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

Contact

Regine.MENZIES@ec.europa.eu