

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

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

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

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

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

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

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

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

[1]

[http://www.emeeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217\\_1/sitt-1739884](http://www.emeeeting.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  
[File](#)

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

Background document  
[File](#)

**NB: Please select only one answer, unless stated differently.**

## 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.

29508582413-52

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

European Gaming and Betting Association

**Question III:** Please enter your organisation's address:

Rue Gray 50, 1040, Brussels

**Question IV:** Please enter your organisation's website:

www.egba.eu

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

Maarten Haijer

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

+32/2/554 0890

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

egba@egba.eu

**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 A:** What is your name?

**Question VIII B:** What is your e-mail address?

**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 VIII D:** Please specify what kind of internet content provider

- Publisher
- Providers of digital platforms and service aggregators
- Broadcasters
- Advertisers
- Ad network providers
- Other**

**Question VIII E:** Please specify what type of internet content provider:

**EGBA members are EU-regulated online gambling operators.**

**Question VIII F:** Please specify the level of the government authority:

- National
- Regional
- Local

Question VIII G: Please provide the name of the public body or institution:

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

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

**Question VIII I:** Please indicate the provisions of the e-Privacy Directive you are in charge of (e.g. confidentiality of communications, traffic and location data, commercial communications):

**Unsolicited communications and confidentiality of the communications.**

**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

Question IX A: Please specify:

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

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

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

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

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

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

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

Free movement of electronic communications equipment and services in the EU	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
---	-------------------------------------	--------------------------	--------------------------	--------------------------	--------------------------

**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.

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

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

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

**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?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
to non-effective enforcement?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

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

*Please note the field is between 1 and 1500 characters*

EGBA strongly advises against any redundant broadening of the scope of the e-Privacy Directive because the General Data Protection Regulation (“GDPR”) already provides risk-based rules. As a matter of fact, the enforcement of national legislation on e-Privacy Directive made by different types (in nature, priorities and expertise) of authorities across Member States (DPAs, telecom regulators, consumer protection agencies) is a source of legal uncertainty for online gambling operators, a cross-border economic activity by nature. It creates divergent interpretations of the directive and a fragmented regime with inefficiencies and unnecessary costs to the detriment of both consumers and business, impacting negatively the protection of consumers.

Confusion produced by this particular kind of fragmentation is likely to increase if Member States are allowed to appoint a specific, separate body to monitor the data protection activities of online gambling operators. This is due to the fact that these agencies are excluded from common bodies such as the Article 29 Working Party or the forthcoming European Data Protection Board, which seek, inter alia, a common interpretation of EU privacy rules. The protection of gambling consumers should not rely on the practices and interpretations of the EU law adopted by the different national authorities, but instead there should be a high level of consumer protection equal to all EU consumers.

**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
<input type="text"/>			

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The free movement of personal data processed in connection with the provision of electronic communication services	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Free movement of electronic communications equipment and services	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

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

*Please note the field is between 1 and 1500 characters*

EGBA considers that the level of protection that personal data is granted should not depend on whether this data is related to an electronic communication, but rather on its sensitivity, on the one hand, and on the nature of the operations carried out by each company, on the other.

The forthcoming GDPR already encompasses this idea, and provides detailed and stringent rules for the processing of sensitive personal data, as well as enhanced information obligations towards data subjects. It also will provide the obligation to carry out privacy impact assessments, and to modify internal privacy practices accordingly. The legislation based on a risk-based approach is simultaneously flexible and effective. Because of that, companies will be obliged to put in place wide safeguards when performing data processing operations.

In the context of the online gambling industry, any communication between the operator and the player respects data protection rules, as well as the content of any communication done primarily by the player either with the operator or a third party (e.g.



another player). Moreover, during the registration procedure and the use of the website, the player is given comprehensive and full information about data processing and privacy rules followed by the consumer's clear consent.

### 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
<b>The Framework Directive (Article 13a):</b> requiring providers of publicly available electronic communication services and networks to take appropriate measures to manage the risks posed to the security and integrity of the networks and services and guarantee the continuity of supply.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>The future General Data Protection Regulation setting forth security obligations applying to all data controllers:</b> imposing on data controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, as appropriate, the pseudonymisation and encryption of personal data and the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>The Radio Equipment Directive:</b> imposing privacy and data protection requirements upon all terminal equipment attached to public telecommunication networks.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>The future Network and Information Security (NIS) Directive:</b> obliging Member States to require that digital service providers and operators of certain essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in their operations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Please note the field is between 1 and 1500 characters

There are several inconsistencies between the security obligations of the GDPR and the ones of the current e-Privacy Directive (e.g. data breach notification period). Both legal instruments impose security measures on the processing of personal data. We believe that this duplication should be avoided, and that the rules put forward by the GDPR are more in line with the new digital reality and that, therefore, are appropriate to ensure the protection of personal data.

Furthermore, as stated above (Question 6A), we believe that the level of protection that personal information should be granted must depend on its sensitivity, and not on the channel through which is collected.

For these reasons, we also consider, once again, that the approach taken by the GDPR, which requires the carrying out of data protection impact assessments before the performance of risky operations on personal data, and the adoption of appropriate security measures (in article 35(7)(D)) will oblige data processors to enact enough safeguards to protect the privacy of individuals.

**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.

**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)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
I find it more reasonable to apply to marketing messages sent through social media opt out rules (Art 13)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### 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.

**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.

*Please note that the amount of text permitted is between 1 and 1500 characters*

Currently, there is a divergence between national laws implementing the e-Privacy Directive. For this reason, online gambling operators are obliged to adapt their internal privacy policies to the national legislation (implementing the directive) of each of the countries in which they offer their services. Extending the current scope of the e-Privacy Directive, in addition to the EU data protection regulation (and subsequently the GDPR) would create additional administrative compliance costs, additional costs in the area of marketing and web design, and additional personnel costs to the online businesses (staff and regular training). This results in a substantial increase of the compliance costs of online gambling operators, but does not, in practice, elevate the level of consumer protection. Again, the right balance would be struck by using the GDPR's risk-based approach.

In addition, as a result of the adoption of the GDPR, which also allows great discretion to Member States, online gambling operators will have to modify again their privacy practices. This will result again in high initial financial costs, and so will any further modification of the e-Privacy Directive. For this reason, EGBA would like to draw the attention of the European Commission to the fact that further requirements beyond the GDPR are not needed.

**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.**

*Please note that the amount of text permitted is between 1 and 1500 characters*

While costs related to the compliance with the e-Privacy Directive were initially high, these costs are now lower as EU-regulated online gambling operators have adapted their privacy policies accordingly. Any modification of this regime would again oblige businesses to carry out costly investments in order to re-adapt these policies. For this reason, we advise against any modification of the e-Privacy Directive that would create unnecessary additional burdens.

Furthermore, there is a partial overlap between the e-Privacy Directive and the GDPR, as both of them provide obligations that protect personal data. As the GDPR provides enough safeguards for operations that may affect sensitive personal data, we consider that maintaining both regimes will lead to an increase of data controllers' compliance costs while not leading to any further relevant protection and indeed may reduce protection due to confusion and resulting inconsistencies.

#### **I.5. EU ADDED VALUE OF THE E-PRIVACY DIRECTIVE**

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

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

- Yes**
- No
- No opinion

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

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

## 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.**

*Please note the field is between 1 and 1500 characters*

As mentioned previously, EGBA considers that the GDPR will provide enough safeguards in what concerns the protection of personal data. For this reason, no further legislation is needed.

## II.1. REVIEW OF THE SCOPE

The requirements set forth by the e-Privacy Directive to protect individual's privacy apply to publicly available electronic communication services (**ECS**). Such rules do not apply to so called Over-The-Top (**OTT**) services (e.g. unmanaged Voice over IP, instant messaging, web mail, messaging in social networks). This may result in both a void of protection for citizens and in an uneven playing field in this market. Although the rules to protect personal data of Directive 95/46/EC and the future GDPR apply to OTT communications services, some specific rules of the e-Privacy Directive, such as the principle of confidentiality of communications, do not apply to these services. See background document for more details (see Section III.2).

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

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

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

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

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

	All networks, whether public, private or closed	Non-commercial WIFI Internet access (e.g. ancillary to other activities) provided to customers/public in, e.g. airport, hospital, mall, universities etc.	Only publicly available networks (as currently)
Security obligations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Confidentiality of communications	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Obligations on traffic and location data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 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.**

**Question 21:** While an important number of laws imposing security requirements are in place, numerous publicly reported security breaches point to the need for additional policy measures. **In your opinion, to what extent would the following measures improve this situation?**

	significantly	moderately	little	not at all	do not know
Development of minimum security or privacy standards for networks and services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Extending security requirements to reinforce coverage of software used in combination with the provision of a communication service, such as the operating systems embedded in terminal equipment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Extending security requirements to reinforce coverage of Internet of Things devices, such as those used in wearable computing, home automation, vehicle to vehicle communication, etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Extending the security requirements to reinforce coverage of all network components, including SIM cards, apparatus used for the switching or routing of the signals, etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

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

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

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



times a user sees a given ad)

- Identifiers collected and immediately anonymised in a way that it is impossible to identify the users' device
- Other

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

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

**Question 24:** It has been argued that requesting users' consent to the storage/access of information in their devices, in particular tracking cookies, may disrupt Internet experience. **To facilitate this process and users' ability to consent, a new e-Privacy instrument should (several options possible):**

- Require manufacturers of terminal equipment including operating systems and browsers to place on the market products with privacy by default settings (e.g. third party cookies off by default)
- Adopt legislation, delegated acts for example, defining mechanisms for expressing user preferences regarding whether they want to be tracked
- Mandate European Standards Organisations to produce standards (e.g. Do Not Track; Do not Store/Collect)
- Introducing provisions prohibiting specific abusive behaviours, irrespective of user's consent (e.g. unsolicited recording or filming by smart home devices)
- Support self-co regulation
- Others

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

**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.**

*Please note: between 1 and 1500 characters answer possible*

The current set of exemptions provides an accurate balance between the rights of individuals and values that, such as national security, are necessary for the well-functioning of society. Broadening the scope of the exemptions would undermine this balance and threaten the privacy of EU citizens.

EGBA would like to stress that online gambling operators are unfortunately, in some cases, obliged by national gambling legislation to process traffic and location data in order to geo-locate consumers, so as to block players from other countries or to re-route player to national websites from the .com offer.

**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
<b>Non-itemised bills</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Presentation and restriction of calling and connected line identification</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Automatic call forwarding</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Subscriber directories</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

## II.4. UNSOLICITED COMMERCIAL COMMUNICATIONS

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

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

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

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

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

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

## 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.**

*Please note the field is between 1 and 1500 characters*

As stated in our answer to question 4A, the enforcement and monitoring of data protection legislation should be attributed to a single national authority. Due to the complexity and sensitivity of the issue, national data protection authorities should be entrusted with this task. Furthermore, by allowing such authorities to carry out this task, legal uncertainty resulting from diverging interpretations of the same provisions would be mitigated.

**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.**

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