QUESTIONNAIRE FOR THE PUBLIC CONSULTATION ON THE EVALUATION AND REVIEW OF THE E-PRIVACY DIRECTIVE (EN)

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

New Section

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.

The current e-Privacy Directive (ePD) is outdated, does not align with the new General Data Protection Regulation (GDPR) and can no longer be justified in a world of converged and globally connected online services. Therefore, a Review should focus on measures that are necessary both in order to protect the confidentiality of consumers' communications and to enhance consumer trust.

ISPA believes that more than assessing the ePrivacy Directive against its past application, the Commission would need to evaluate if this sectorial law is still relevant. Indeed, since its adoption and revision, a number of new legal instruments have been adopted that contribute to and achieve the same objectives.

The General Data Protection Regulation (GDPR) imposes extensive restrictions on the use of personal data and is applicable to all sectors (thereby extending the obligations originally outlined in the ePrivacy Directive to all sectors). Other legislative initiatives, such as the Network and Information Security Directive, but also the proposed overhaul of consumer rules should also be taken into account.

ISPA believes that there is no more need of sector-specific privacy rules that govern the commercial use of personal data. Some provisions of the ePrivacy, such as the confidentiality of communications, could find a more effective application in the revision of the Framework Directive, which is going to have a more horizontal scope.

For example concerning data breach notification (Art.4 Pr. 3) the GDPR introduces similar obligations though with differences in terms of the reporting deadlines. As a result there is no need for telecoms-specific legislation in this matter (see Q 7 A).

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.

ISPA would like to highlight the lack of harmonization and interpretation of the obligations under the ePrivacy Directive across the EU (i.e. implementation of the breach notification requirements, the cookies rules or the definition of traffic data).

ISPA furthermore suggests that ambiguities in the application and understanding of such provisions should be clarified by the GDPR, making these provisions redundant. Being a regulation, the GDPR should address the challenges of harmonization and provide for a uniform interpretation of the law. This approach would secure that for instance webmail services are treated in the different member states legally the same, which was not always the case as the decision of the administrative court in Cologne(1) recently has shown.

Source: (1) Administrative Court Cologne, 21 K 450/15, 11.11.2015.

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.

According to Article 15 ePD it is up to each Member State to ensure that an appropriate national authority was competent to investigate an enforce the national laws.

The lack of harmonization has been indeed a challenge. However, the GDPR should address these challenges given the real overlap with the ePD. The GDPR also sets out a comprehensive regime for penalizing companies that violate EU data protection law.

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.

As the Commission noted in its press release (1), with the GDPR "[…] *our work in creating first-rate data protection rules providing for the world's highest standard of protection is complete. Now we must work together to implement these new standards across the EU so citizens and businesses can enjoy the benefits as soon as possible* […]" (underlining added by ISPA). This underlines how comprehensive the new regime is, making additional sector specific rules redundant. Furthermore, any new privacy rules in this space might create conflicting requirements, decreasing the legal certainty which the Commission suggested would be ensured by the GDPR.

ISPA sees no need for specific rules for instance on traffic/location data as the GDPR provides strict rules and strengthens the consumer rights. Furthermore in ISPA's opinion the best way to ensure consumer rights (e.g. itemised billing) is through effective competition, which is provided in this high competitive sector.

Like the data protection rules, the EU consumer protection rules are also being overhauled. This reform focuses on improving consumer rights in the digital space. Consumer rules that are currently outlined in the ePD, to the extent they are still needed, may sit more sensibly in consumer specific legislation or within the rest of the telecom package.

Sources:

(1) EU-Commission press release on the GDPR: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm (24.06.2016)

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.

When the Commission published its proposal on the GDPR, it underlined the need to "[…] *introduce a general obligation for data controllers to notify data breaches without undue delay to both data protection authorities and the individuals concerned*.[…]" (1) The Commission noted that at that time such obligations were only compulsory in the telecommunication sector, "based on the ePrivacy Directive" (2). It is thus crystal clear that the GDPR obligations are actually based on and extend the obligations of the ePrivacy Directive.

The Network and Information Security Directive (NISD) in Article 1 Parg. 3 also clarifies that security and notification requirements provided for in the Directive shall not apply to undertakings, which are subject to the requirements of the Framework Directive (Article 13a and 13b). This provision was introduced given the overlap between the two legislative instruments, making it clear that entities falling under the scope of the NISD are subject to the same legislation as those subject to the Framework Directive. Therefore the entities subjected to the Framework Directive were explicitly excluded from the scope of the NISD.

As stated above the GDPR, the NISD as well as the Framework Directive provide sufficient security regulations, which have broad horizontal impact and make the security provisions in the ePD redundant.

It is thus clear that the ePD's security provisions are no longer needed.

Sources:

(1) and (2) Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions (COM (2012) 9 final): http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF (24.06.2016)

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.

When evaluating the provisions relevant to direct marketing, it is important to underline that the GDPR provides specific rules on direct marketing as well - ensuring a higher level of harmonization that existed in the past. The GDPR thus also regulates any messages sent through other means, like social media.

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.

As noted by the previous questions and our responses above, a number of legislative instruments provide for ensuring a high level of protection of personal data or aiming to increase users' trust.

In ISPA's opinion the recently approved GDPR should sufficiently address any user's concerns regarding the protection of their data.

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.

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.

In ISPA's opinion the regulatory objectives of the directive could be best promoted through effective competition and self regulation.

I.5. EU ADDED VALUE OF THE ERIVACY DIRECTIVE

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

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

- ○ Yes
- ○ No
- ○ No opinion

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

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

II. REVISING THE E-PRIVACY DIRECTIVE: LOOKING AHEAD

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

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

- ☐ Widening the scope of its provisions to over-the-top service providers (OTTs)
- ☐ Amending the provisions on security
- ☐ Amending the provisions on confidentiality of communications and of the terminal equipment
- ☐ Amending the provisions on unsolicited communications
- ☐ Amending the provisions on governance (competent national authorities, cooperation, fines, etc.)

☐ Others

☑ None of the provisions are needed any longer

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

○ Yes

○ No

○ Other

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

As noted above, there is indeed a need to improve harmonization. However, as the Commission suggests, the main benefit of the GDPR is that it provides "*a single set of rules*". As it broadly covers processing of personal data, it should address this concern and require no sectorial instrument anymore.

If the rules of the current ePrivacy Directive were simply made to apply to all market players without regard to technology or sector, many of its provisions would overlap with or conflict with the GDPR or other legislation. For example considering that location data is legally defined as a category of personal data under the GDPR and that it has particular potential risks associated, it could be concluded that there is no need to regulate it further and specifically under the revised ePD, as controllers and processors already have significant duties under the GDPR to treat the data accordingly.

Similarly, data breach reporting rules under the ePDwill be inconsistent with equivalent rules under the GDPR. If there is no justifiable reason for the rules to be different, they should be rendered the same in which case there is no need for them to appear twice. Otherwise, the coexistence of two different sets of rules creates legal uncertainty and confusion for consumers, which does not play in favor of a coherent consumer policy online.

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.

ISPA agrees provided law enforcement actions are in tension with the Charter of Fundamental Rights and thus appropriate safeguards need to be provided by law. We however also believe that enforcement related considerations would be better addressed in the revision of the Framework Directive given that the needed safeguards are already foreseen in Article 1.

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.

This question dictates a technology and business model approach and would result in a radical change of the present business environment. Additionally, the ePrivacy Directive contains a clear provision on technology neutrality and we suggest the Commission to remain consistent with such principle. This approach would be consistent also with other legislation such as the Network and Information Security Directive.

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

☐ Identifiers placed/collected by a third party information society service (not the one that you are visiting) for online behavioural advertising purposes

☐ Identifiers placed/collected by an information society service you are visiting – when their purpose is website analytics, measuring number of website visitors, where visitors go within the website, etc. (e.g. "first party" cookies or equivalent technologies)

☐ Identifiers placed/collected by an information society service you are visiting whose purpose is to support user experience, such as language preference cookies[1]

☐ Identifiers collected/placed by an information society service to detect fraud

☐ Identifiers collected/placed by and information society service for frequency capping (number of

times a user sees a given ad)

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

☐ 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.

As noted above, it is important to maintain the spirit of Article 14 of the ePrivacy Directive and avoid any technology mandate. Also, the GDPR includes the requirement of adopting internal policies and implement measures, which meet in particular the principles of data protection by design and data protection by default. Article 25 GDPR underlines that controllers shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural actors.

Furthermore, Article 21 GDPR specifically states that individuals shall have the right not to be subject to a decision based on automated processing, such as profiling, which produces legal effects or similarly significant effects.

These provisions provide a comprehensive protection for individuals, making any further regulation redundant. ISPA welcomes the recognition of ongoing industry initiatives. Indeed, these initiatives should be encouraged, as the GDPR does so.

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.

The definition of personal data in GDPR is broad, specifically calling out location data and online identifiers, making these provisions in the ePrivacy Directive redundant. Relying on the GDPR for these provisions would also significantly reduce legal uncertainty.

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.

As noted above, the current revision of the consumer rules should also be taken into account. To the extent these provisions are still needed as for example the provisions concerning subscriber directories (Art. 12), they could be transferred e.g. to the telecom Package or other appropriate legislation.

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.

The GDPR contains detailed provisions on direct marketing, introducing a robust right to object. Given that the GDPR is a Regulation and as such directly applicable, Member States will have to implement these provisions, annulling the current differences.

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.

In line with the logic of our approach, ISPA considers that while the ePD as sectorial law is not anymore needed, some of its obligations are valid and could be better applied in the

context of other legislative frameworks whose enforcement would be delegated to single authorities. For instance, to the extent some provisions are transferred to the rest of the Telecommunication Package, the telecom regulatory authorities will likely to continue to have jurisdiction over these matters, as much as DPAs will have jurisdiction over privacy matters already covered by the GDPR.

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.

In contrast to the GDPR, the current ePD protects not only natural persons, but also legal persons. Some provisions, for example, the confidentiality of communications which corresponds to the fundamental right enshrined in Article 7 of the Charter of fundamental rights and Article 8 of the European Convention of Human rights might continue to be relevant to legal persons. In ISPA's opinion the fundamental rights approach to protect the rights of legal persons is sufficient and other sector specific provisions are not necessary or desirable anymore, for example to allow legal persons to be able to withhold their calling number.

Additional Information to Question 16A: Other ePDprovisions that are mostly consumer rights related (such as itemized billing (Article 7) or unsolicited communications) should firstly be evaluated on their continued necessity. If that is still found to be the case they may be better addressed in consumer protection legislation. In this line, it is interesting to mention the recent CERRE Study on Consumer Privacy(1) which states that sector-specific privacy regulations are inadequate in a dynamic environment and should be withdrawn.

Source:

(1) CERRE Study on Consumer Privacy: http://www.cerre.eu/publications/consumer-privacy-network-industries (24.06.2016)

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

Confirmation Page Text

Thank you for your contribution

Escape Page Text

This survey has not yet been published or has already been unpublished in the meantime.