**BACKGROUND TO THE PUBLIC CONSULTATION ON THE EVALUATION and REVIEW OF THE ePRIVACY DIRECTIVE**

The purpose of this background document is to help stakeholders answer the public consultation. To this end, after an introduction to the ePrivacy Directive in Section I, Section II describes the purposes of the consultation and its structure. Section III explains the main provisions of the ePrivacy Directive: its scope of application, the security provisions, the provisions on confidentiality of communications, the rules regulating the calling line identification and exceptions, directories of subscribers, unsolicited commercial communications and competent authorities. It also describes when/if a given provision appears to raise specific issues needing to be addressed in the review.

## I. INTRODUCTION

### I.1 The ePrivacy Directive in Context

The Data Protection Directive 95/46/EC (hereinafter "**Data Protection Directive**" or "**Directive 95/46/EC**")[1] is the central legislative instrument in the protection of personal data in Europe.

Directive 95/46/EC is the legislative basis for two long-standing aims of European integration: the Internal Market (in this case the free movement of personal data) and the protection of fundamental rights and freedoms of individuals. In the Directive, both objectives are equally important. The General Data Protection Regulation (hereinafter "**GDPR**") will replace Directive 95/46/EC in 2018 with new modernised rules fit for the digital age[2].

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[3] (hereinafter "**ePD**"). The ePD is part of the EU Regulatory Framework for Electronic Communications which comprises four specific directives including the Framework Directive 2002/21/EC. The Framework was last amended in 2009[4] and is currently under revision.

The ePD sets forth rules concerning the protection of privacy in the electronic communications sector. One of the main elements of the ePD is to ensure protection of confidentiality of communications, in line with the fundamental right to the respect of private and family life (including communications) enshrined in Article 7 of the EU Charter of Fundamental Rights (hereinafter "**Charter**").

---

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ, L 281, 23.11.1995.

[2] http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector , J L 201, 31.7.2002, p. 37; Amended by Directive 2009/136/EC.

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF.

Furthermore, the ePD particularises and complements Directive 95/46/EC by, among others, setting up specific rules concerning the processing of personal data in the electronic communication sector. It does so, for example, by requiring users' consent before their phone numbers can be listed in a public directory.

At the same time all matters concerning the protection of personal data in the electronic communications sector which are not specifically addressed by the provisions of the ePD are covered by the Data Protection Directive (and in the future by the GDPR). This means for instance that the privacy principles defined in the GDPR[5] on how processing can legally take place, the rights of the data subjects, the obligations of data controllers and processors, including the rules on international data transfers are also applicable in the context of the electronic communications sector when processing personal data.

## II. EVALUATION AND REVIEW OF THE ePRIVACY DIRECTIVE

The purpose of this consultation is twofold. ***First***, it aims to gather input for the REFIT evaluation of the ePD. This corresponds to Section I of the questionnaire. ***Second,*** it seeks views on possible changes to the current ePrivacy Directive. This corresponds to Section II of the questionnaire.

### II.1 REFIT Evaluation of the ePrivacy Directive

The review of the ePD will be preceded by a Regulatory Fitness and Performance Programme (REFIT), which is a retrospective performance evaluation of the ePD. A REFIT evaluation will "*identify, assess, adopt, and monitor the implementation of initiatives which will result in significant regulatory cost reduction or simplification*" so that the policy objectives that have been set are delivered upon and the benefits of EU legislation are reaped at the lowest cost and with the minimum regulatory burden. The REFIT evaluation of the ePD is part of the Commission's 2015 Work Programme and is expected to end in 2016[6].

The REFIT exercise aims at evaluating the performance of **all** the provisions of the ePD, against the five mandatory criteria enlisted in the Commission Better Regulation Guidelines:

1. **effectiveness** (to what extent have the objectives of the ePD been achieved?),
2. **efficiency** (to what extent has the ePD been cost effective?),
3. **relevance** (are all the provisions of the ePD still relevant today?),
4. **coherence** (is the ePD coherent both internally and in relation with other existing regulations?),
5. **EU added value** (what is the additional value resulting from the ePD compared to what could be achieved by Member States at national and/or regional levels?).

### II.2 The review of the ePrivacy Directive

[5] Personal data must, inter alia, (i) be processed fairly and lawfully, (ii) be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed and (iii) be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected (Article 5 of the GDPR).

[6] Annex 3 of CWP-2015 (COM(2014) 910 final of 16.12.2014

In the Digital Single Market Strategy[7] (hereinafter "**DSM Strategy**"), the Commission announced its intention to review the ePD as one of the initiatives aimed at reinforcing trust and security in digital services in the EU with a focus on **ensuring a high level of protection for citizens and a level playing field for all market players**.

Without prejudice to the outcome of the REFIT evaluation, several policy issues have emerged as potentially needing to be addressed in the review of the ePD:

First, *ensuring consistency*. Given that the ePD complements Directive 95/46/EC, which is being replaced by the General Data Protection Regulation (GDPR), full coherence between the two instruments needs to be ensured. This implies considering whether some of the provisions of the ePD are already sufficiently covered by the GDPR (e.g. personal data breach notifications).

Second, *updating the scope of the ePD in light of the new market and technological reality*. The ePD applies to traditional telecommunication service providers (i.e. providers responsible for carrying signals over an electronic communications network). It does not apply to the so called over-the-top providers (hereinafter "**OTTs**") that provide (functionally equivalent) communications services (e.g. Voice over IP, instant messaging) over the Internet. The review should assess whether this situation should be changed.

Third, *enhancing security and confidentiality of communications*. Cyber-attacks, reports of covert surveillance and online tracking for commercial purposes have highlighted the growing risks for the confidentiality of communications and the protection of information stored in users' equipment. The review will consider options to improve the effectiveness, efficiency, and coherence of the relevant provisions.

Fourth, *addressing inconsistent enforcement and fragmentation*. Institutional issues concerning the governance of the ePD at national level, such as the co-existence of multiple authorities and its impact in enforcement and harmonisation, must be evaluated.

## III. CONTENT OF THE ePRIVACY DIRECTIVE AND ISSUES TO BE TACKLED

### III.1 Aim of the ePrivacy Directive

According to its Article 1, the ePD provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data and the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the EU. Moreover, it provides for protection of the legitimate interests of subscribers who are legal persons.

The ePD serves therefore thee main objectives. ***First*** it seeks to ensure the full respect of fundamental rights set out in Articles 7 and 8 of the Charter. In particular, one of its main objectives is the respect for the fundamental right of confidentiality of communications, guaranteed under Article 7 of the Charter, Article 8 of the European Convention on Human Rights as well as under other international instruments relating to human rights.

[7] Commission Communication "A Digital Single Market Strategy for Europe", COM(2015) 192 final.

Next to the fundamental rights aim, the ePD pursues also important internal market objectives. The ***second*** objective of the ePD is thus to ensure free movement of data processed in the electronic communication sector. Just as Directive 95/46/EC, the ePD aims to harmonise legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and legitimate interests of legal persons, in order to avoid obstacles to the internal market for electronic communications in accordance with Article 26 of the TFEU.

The ***third*** main objective of the ePD, which is also connected to the EU internal market, is ensuring the free movement of electronic communication terminal equipment and services in the EU. The ePD pursues this objective by harmonising the rules on privacy and confidentiality in the electronic communication sector in the EU, but also by providing specific rules on technical features and standardisation. For example, Article 14 of the ePD provides that in implementing the provisions of the ePD, Member State may not impose mandatory requirements for specific technical features on terminal or other electronic communication equipment which could hinder the free circulation of such equipment in the EU.

**III.2 Scope of application of the ePrivacy Directive**

**a) Information society services providing functionally equivalent services**

The ePD applies, according to the wording of its Article 3, "*to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community including public communications networks supporting data collection and identification devices*."

The Framework Directive defines electronic communications services as entities that are responsible for conveyance of signals on electronic communications networks.[8] It explicitly excludes information society services.

Many modern forms of communications taking place "over the Internet", such as Voice over IP, instant messaging, webmail and the like, may be defined as "information society services". The ePD would thus not apply, in principle, to these kinds of online communication services.

The non-application of the ePD may result in both a void of protection and in an uneven playing field in the market as functionally equivalent services are not subject to the same regulatory constraints, meaning they do not have to comply with the provisions of the ePD (such as for confidentiality of communications). It is worth noting that some Member States have broadened the scope of application of their national laws to regulate OTTs.[9]

Nevertheless, OTT providers have to comply with the Data Protection Directive (and in the future with the GDPR). The latter requires for instance that in order to lawfully process

[8] Article 2 (c) of Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services defines them as "service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks."

[9] For example, since January 2015, the Finnish Information Society Code has included a new provision pursuant to which the confidentiality of communication rules apply to all electronic communication distributors, including social media companies.

personal data, data controllers or data processors must rely on one lawful ground enshrined in Article 7 (e.g. consent, processing is necessary for the legitimate interests of the controller, processing is necessary for the performance of a contract to which the data subject is party, processing is necessary for the performance of a task carried out in the public interest etc.).

They also need to comply with the principles relating to data quality (Article 6 of the Data Protection Directive 95/46/EC) as well as respect data subjects' rights (right to be informed, right to rectify, right of access, right to erasure, right to object etc.), which will be enhanced by the GDPR.

**b) Exclusion of private networks**

The ePD only applies to "*publicly available electronic communications services in public communications networks*" (Article 3). Recital 55 of the Citizens' Rights Directive expressly excludes closed user groups and corporate networks.

There may be situations where it is unclear whether a service qualifies as a publicly available electronic communications services in public communications networks. Not all Member States hold the same views regarding whether cases such as WIFI access offered by an airport, Internet access provided in internet cafes and shopping malls qualify as publicly available electronic communications services in public communications networks.[10] With the growing importance of such networks, some may argue that some privacy safeguards defined in the ePD should apply to all electronic communications, including in the examples mentioned above.

**(c) Public communication networks supporting data collection and identification devices**

The last revision of the ePD clarified that the Directive covers "*public communication networks supporting identification devices*". This means that the collection of information, including personal data, using radio frequencies, such as RFID, is subject to the ePD when such devices are connected or make use of public communication networks or services. Recital 56 of the Citizens' Rights Directive explains that the provisions of the ePD, in particular those on security, traffic and location data and on confidentiality of communications apply to such devices.

While such clarifications are welcome, arguably more legal certainty may be needed with regard to the application of the ePD to Internet of Things solutions (i.e. internet connecting devices among themselves), including to components, products, services and platforms that integrate everything in a communications network for digital processing.

Last but not least, it is worth noting that a few provisions of the ePD are worded in such a way that effectively broadens their application to other actors. This is the case of Article 5(3) dealing with the use of cookies and similar techniques, which applies to anyone storing information or gaining access to information already stored, in the terminal equipment (i.e. computer, smart phone) of a subscriber or user.

**III.3 Security of electronic communications**

[10] PTS Report, Which services and networks are subject to the Electronic Communications Act?

The ePD requires providers of electronic communication services to take appropriate technical and organisation measures to safeguard security of their services, if necessary in conjunction with the provider of the public communications network (Article 4). Publicly available electronic communication service providers must also notify personal data breaches to relevant authorities, and in certain cases also to the subscribers and individuals concerned (Article 4.3).

**a) The Telecom Framework Directive**

Article 13a of the Framework Decision complements this provision by requiring providers of publicly available electronic communication networks and services to take appropriate measures to manage the risks posed to the security of the networks and services. It also requires them to guarantee the integrity of their networks and continuity of supply.

**b) The Radio Equipment Directive**

This Directive imposes certain privacy and data protection requirements upon all terminal equipment attached to public telecommunication networks. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements: incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected. To this end, the Commission may adopt delegated acts.

The notion of terminal equipment which is used, for example in Article 5,3 of the ePrivacy Directive is defined in Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment as follows: (a) equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network. This would include smart phones, computers, but also smart meters and smart cars.

**c) The GDPR**

The future General Data Protection Regulation will introduce security obligations applying to all data controllers: controllers and processors will have to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This includes, 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, having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals.

In addition, the GDPR introduces a general personal data breach notification obligation to all data controllers. Controllers must notify the data protection authority of a data breach "*without undue delay and, no later than 72 hours after having become aware of it*" unless technical measures are in place. Moreover, they must notify data subjects of a breach where it creates a "high risk" to their privacy.

**(d) The Network and Information Security Directive**

The future **Network and Information Security (NIS) Directive** will oblige 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.

While therefore an important number of laws exist imposing security requirements, reports of electronic mass surveillance, news about users of computers and smart phones being infected with virus and malware, hacking of connected cars, etc. raise questions about whether the current security of communications should be enhanced, for example, by developing minimum security and/or privacy standards for networks and services.

Therefore, the evaluation and review of the ePD will assess the rules of the Directive and their interplay with the other legal instruments, including assessing whether they continue having an added value as well as whether additional actions are needed to effectively guarantee the security and confidentiality of communications.

### III.4 Confidentiality of electronic communications

#### a) Confidentiality of communications: Main Principle

The ePD 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 (Article 5.1).

#### b) Confidentiality of the information stored in computers, smart phones and similar devices

This principle is extended to users' terminal equipment, i.e., computers, smart phones and similar devices (Article 5(3)). Given that citizens may have very sensitive information in their phones and computers, their equipment is considered part of their privacy sphere, which warrants enhanced privacy protection. As a consequence, consent (as defined in Directive 95/46/EC) is needed before someone can store or access information in such equipment, and having been provided with clear and comprehensive information, inter alia, about the purposes of the processing.

This covers all types of information stored or accessed such as user's list of contacts, cookies, local shared objects ('flash cookies'), web beacons,[11] bugs, viruses, etc.

There are two derogations to the consent rule. One exception covers information used (i) "*for the sole purpose of carrying out the transmission of a communication over an electronic communications network*", the other exception concerns information which is (ii) "*strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*".[12]

[11] Object embedded in a web page or email, which unobtrusively (usually invisibly) allows checking that a user has accessed the content.
[12] Article 5(3).

The group of national data protection authorities, the Article 29 Working Party, recommended that first party analytics cookies[13] should not require prior consent of website visitors. Some Member States (e.g. the Netherlands) have legislation that already includes such an exemption.

The ePD clarifies in a recital that where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application.[14] This recital has been integrated into the text of the implementing law of 9 Member States,[15] while others refer to it in guidance documents issued by national data protection authorities. The Article 29 Working Party has provided guidance as to the conditions for browser settings to deliver valid and effective consent in its Opinion 2/2010[16].

**c) Online tracking through identifiers stored in terminal equipment to serve targeted advertising**

Given the overwhelming use of cookies and other technologies for online behavioural advertising (hereinafter "**OBA**") purposes,[17] websites owners have increasingly deployed consent mechanisms, such as banners, to comply with the prior consent requirement. In particular the advertising industry claims that banners disrupt users' Internet experience.

The World Wide Web Consortium (**W3C**) is working to standardize the technology and meaning of Do Not Track, by defining mechanisms for expressing user preferences around Web tracking and for blocking or allowing Web tracking elements. The DNT Standard has not been finalized yet.

The online industry has developed a cross-industry self-regulatory initiative to introduce pan-European standards to enhance transparency and user control for OBA.[18]

The common 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 and that consent gives a false sense of protection.

**d) Confidentiality of traffic and location data**

In most cases traffic and location data are 'personal data', as defined by the Data Protection Directive 95/46/EC and the GDPR.

The ePD contains specific privacy protections that apply when providers of publicly available communication services process traffic and location data. More particularly, under Articles 6

[13] Cookies set up by the web site one is visiting, which, among others, aim at measuring websites audience (number of visitors, where they go within the web site, etc.
[14] Recital (66) of the Citizens' Rights Directive.
[15] ePrivacy study, SMART 2013/0071, p12.
[16] Only browsers or other applications that require the user to engage in an affirmative action to accept both the setting of and continued transmission of information contained in cookies by specific websites are able to deliver valid and effective consent.
[17] Behavioural advertising encompasses a variety of techniques used by online advertisers to present targeted ads to consumers. The ads fit the profile of each user. Such profile has been previously created by collecting information about the user's browsing behaviour.
[18] http://www.youronlinechoices.eu/.

and 9 of the ePD, traffic[19] and location data must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication. Nevertheless, traffic data necessary for the purposes of billing and interconnection payments may be processed without prior consent but only up to the end of the period which the bill may lawfully be challenged or payment pursued.

The rules allow that providers of publicly available electronic communications services process traffic and location data for the provision of value-added services (e.g. route guidance, traffic information, weather forecasts and tourist information) in so far as the subscriber or the user to whom the data relate has given his prior consent (which may be withdrawn at any time).

The enhanced protection of traffic and location data i.e. prior consent under the ePD is justified by the fact that: on the one hand, traffic and location information, in particular if stored over time, may allow very precise conclusions to be drawn concerning the private lives of individuals (e.g. their habits in everyday life, permanent or temporary places of residence, daily movements, the activities carried out, the social relationships of those persons and the social environments frequented by them). On the other hand, the needs of modern society require that people have access to electronic communication services for most part of their daily lives[20].

Service providers increasingly use traffic and location data for a variety of purposes. For example, location data is used for value added services such as location services. Traffic data is used for filtering of malicious content, spam detection, etc. Both traffic and location data may be used for the analysis of customer behaviour, to make profiles which can be later used for marketing purposes.

It has been argued that not all the uses of traffic data need consent. For example, the Article 29 Working Party considered that the setting-up and use of filtering systems by email providers for the purposes of detecting virus might be justified by their obligation to take appropriate technical and organisational measures to safeguard security of their services as foreseen in Article 4 of the ePD (and thus consent should not be necessary).[21] Article 26.5 of the Universal Service Directive establishes that location information must be made available to the authority handling emergency calls, which appears to require the disclosure of such information to the relevant authorities, regardless of consent.

Nevertheless, this obligation currently only applies to providers of publicly available electronic communications services in public communications networks. Location services provided by information society services, such as apps providing geo-localisation services, are currently not covered by the ePD provisions.[22] They only have to comply with the rules of the Data Protection Directive 95/46/EC (and in the future with the GDPR). This means that these services may rely on any of the legal grounds to process personal data set forth under Article 7 of the Data Protection Directive (and Article 6 of the GDPR).

[19] "Traffic data": Article 2b) of the Directive defines traffic data as "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*". Traffic data includes, among others, the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services.

[20] See: *Information society statistics - households and individuals*, http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals.

[22] See: Opinion 13/2011 on Geolocation services on smart mobile devices http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

Deleted: ¶

[22] See: Opinion 13/2011 on Geolocation services on smart mobile devices http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

### III.5 NON-ITEMISED BILLS, CONTROL OVER CALL LINE IDENTIFICATION, AUTOMATIC CALL FORWARDING AND SUBSCRIBERS DIRECTORY

The ePD provides for the right for subscribers to receive non-itemised bills. Itemised bills make it easier to verify if the fees charged are correct, but if the service is used by various persons (i.e. a service used by all members of a family), this may jeopardise users' privacy.

The ePD also gives callers the right to prevent the presentation of the calling-line identification if they wish so to guarantee their anonymity; while subscribers have the possibility to stop automatic call forwarding by a third party to their terminals.

There are two cases when the caller decision to hide the presentation of the calling line identification may be overridden: (a) when a subscriber requests the tracing of malicious nuisance calls; (b) in the case of organizations engaged in emergency calls, law enforcement authorities, ambulance, fire brigades, for the purpose of responding to such calls. These provisions are specific to the electronic communication sector. The GDPR does not contain similar specific rules.

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). Furthermore, they must be informed about any further usage possibilities based on search functions embedded in electronic versions of the directory. If this provision were deleted, the legal grounds set forth under Article 7 of the Data Protection Directive (and future Article 6 of the GDPR) would apply. This means that for publishing subscribers' data in public directories rather than consent being necessary, controllers would be able to choose any of the legal grounds contained in such article (e.g. consent, processing is necessary for the legitimate interests of the controller, processing is necessary for the performance of a contract to which the data subject is party, processing is necessary for the performance of a task carried out in the public interest etc.).

### III.6 UNSOLICITED COMMERCIAL COMMUNICATIONS

#### a) Use of electronic mail, fax and automatic calling machines

The ePD prohibits unsolicited commercial communication or more precisely the use of electronic mail, fax and automatic calling machines for direct marketing, unless the user or subscriber has given his prior consent (often referred to as '**opt-in**' – Article 13(1)). However, companies which have acquired an end-user's contact details 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**').

The protection applicable to electronic e-mails, is also applicable to SMSs, MMSs and other kinds of similar applications (Recital 67 of the Citizens' Rights Directive).

#### b) Telephone calls for direct marketing purposes carried out by non-automated calling machines (i.e. individuals making calls)

The ePD leaves it up to Member States to decide whether to impose a prior consent requirement (i.e. **opt-in**) or a right to object (i.e. **opt-out**) for commercial communications sent

by means not mentioned above (Article 13(3)). This is the case of telephone calls for direct marketing purposes carried out by non-automated calling machines (i.e. individuals making calls).[23] Opt-out solutions authorise calls to individuals who prior to the call have not explicitly signed up to a Robinson list, or registered their opposition to being called.

It is unclear whether Article 13(3) covers commercial communications received by users of a social medium (e.g. in their News Feed page) or whether such practices are covered by the opt-in regime applicable to e-mail.

**c) Unsolicited communications to legal persons**

The protection against unsolicited commercial communications also applies to legal persons, but the ePD leaves it up to Member States to decide whether they are protected by an opt-in or opt-out regime.

In addition to the provisions outlined above, the GDPR establishes that where personal data are processed for the purposes of direct marketing, anyone has the right to object to such processing (including to profiling to the extent that it is related to such direct marketing), whether the initial or further processing, at any time and free of charge. Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

## III.7. COMPETENT AUTHORITIES AND ENFORCEMENT

Some provisions of the ePD 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 95/46/EC entrusts the enforcement of its provisions to data protection supervisory authorities, the legislators of the ePD has decided to take a different approach. It leaves it up to Member States to set up the national bodies entrusted with the enforcement of the ePD (Article 15a).

This has led to a fragmented situation in the Union. Some Member States have allocated competence to data protection supervisory authorities (hereinafter "**DPAs**"), whereas others to the telecom national regulatory authorities (hereinafter "**NRAs**") and others to yet another type of bodies, such as consumer authorities. Moreover, in some Member States the competence is scattered across three or four different authorities (e.g. DPA, NRA, Consumer Protection Authority), each one competent for a specific piece of the ePD.

It has been suggested that this situation is a source of confusion for economic operators and citizens. Some indicate that this leads to differing interpretation of the law, given the different nature and sensibilities of the authorities involved. Furthermore, Article 8.3 of the Charter requires that authorities responsible for compliance with data protection rules to be "independent".

The Article 29 Working Party is entrusted with the task of, among others, providing guidance and advising the Commission on matters covered by the ePD. Yet, only data protection authorities are part of the Article 29 Working Party and will be part of the future European Data Protection Board. This means that national authorities, other than DPAs, competent to enforce the ePD may not be permanently represented when guidance is provided on data

[23] Opt-out solutions authorise calls to individuals who prior to the call have not explicitly signed up to a Robinson list or registered their opposition to being called.

protection aspects covered by the ePD. Furthermore, the future GDPR creates a consistency mechanism based on a European Data Protection Board (EDPB) that will play a role, among others, in cases of complaints in cross-border data processing; such a mechanism does not exist under the ePD.[24] The cooperation and consistency mechanism aims to make sure that the rules of the GDPR will be applied consistently throughout the EU in case of cross-border processing operations.

Under this mechanism, the lead DPA will submit its draft decision to the other concerned DPA. If, within four weeks, one of the concerned DPAs "expresses a relevant a reasoned objection to the draft decision", the lead DPA, "if it does not follow the objection or is of the opinion it is not relevant and reasoned", will refer the matter to the European Data Protection Board (EDPB). The EDPB will decide on the case within a one-month period (extendable to two months) and by 2/3 majority of its members. If the adoption is not adopted within this period, it will be adopted by simple majority within the next two weeks. The lead DPA will have to adopt its final decision "on the basis of" the EDPB decision, which will be binding.

Finally, it should also be noted that, the powers and tasks of the DPAs (e.g. including the fines) have been defined in great details and harmonised under the GDPR.[25]

The evaluation and review of the ePD will consider whether this institutional fragmentation jeopardises the harmonised application of the ePD rules or has anyway led to other shortcomings, e.g. in terms of legal certainty, burden on operators, etc. Finally, such evaluation will have to take into account the enforcement and consistency mechanisms introduced under the GDPR.

[24] Article 51 of the General Data Protection Regulation.
[25] Chapter VI – Section 2 of the GDPR