EUROPEAN
COMMISSION

Brussels, 10.1.2017
SWD(2017) 5 final

COMMISSION STAFF WORKING DOCUMENT

Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC

Accompanying the document

Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

{COM(2017) 10 final}
{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 6 final}

Table of Contents

1. INTRODUCTION

1.1. Purpose of the evaluation

This Staff Working Document ("**SWD**") provides the results of the evaluation carried out under the Regulatory Fitness and Performance Programme ("**REFIT**") of the ePrivacy Directive ("**ePD**"), announced under the Commission Work Programme 2015.

The purpose of the REFIT evaluation is to assess the regulatory fitness of the current rules and to examine whether they have contributed to the achievement of their main objectives, as well as to identify possible redundancies (i.e. in case the same obligations are covered by another EU legal instrument), inconsistencies and simplification potential. In line with the "Better Regulation" requirements[1], the evaluation assesses 1) the effectiveness, 2) efficiency, 3) relevance, 4) coherence and 5) EU added-value of the ePD.

This evaluation also seeks to meet the reporting obligation set out in Article 18 of the ePD.

The Commission Communication "A Digital Single Market Strategy for Europe" announced that once the new rules on data protection would be adopted, in particular with the newly adopted General Data Protection Regulation (EU) 2016/679[2] ("**GDPR**") and the Law Enforcement Directive (EU) 2016/680[3], the Commission would conduct the evaluation and review of the ePrivacy Directive[4].

Pursuant to this commitment, this REFIT evaluation has been carried out back to back with the Impact Assessment on policy options for the future of the ePD. The conclusions of this evaluation have – where relevant – fed into that Impact Assessment.

1.2. Scope of the evaluation

The evaluation focuses on the objectives, areas and provisions set out in the ePD.

This evaluation covers the period from December 2009, when the Directive resulting from the last revision entered into force, to July 2016. The period between 2004, when the original version of the ePrivacy Directive entered into force, up to December 2009 is not covered by this evaluation.

---

[1] REFIT is the European Commission's Regulatory Fitness and Performance programme launched in December 2012. Under REFIT, action is taken to make EU law simpler, lighter, more efficient and less costly, thus contributing to a clear, stable, least burdensome and most predictable regulatory framework supporting growth and jobs.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and *repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, p. 1–87.*

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. OJ L 119, 4.5.2016, p. 89–131

[4] European Commission, "A Digital Single Market Strategy for Europe", COM(2015) 192 final, 10, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf.

However, whenever longer datasets were available and where they could be useful in showing impacts (i.e. in those provisions with little or no modifications during the 2009 review), these were adequately used. The geographic scope of the evaluation is the whole territory of the EU.

2. BACKGROUND

This section details first the successive steps towards the adoption of the ePrivacy Directive as last amended in 2009 (see Section 2.1), it then explains the relationship of the ePD with the Data Protection Directive (Section 2.2), then, it presents the general and specific objectives pursued by the Directive (Section 2.3). The last section concludes with the baseline situation at the time of the adoption of Directive 2002/58 review (Section 2.4).

2.1. Successive review towards the adoption of Directive 2002/58 as last amended in 2009

2.1.1. Telecommunications Privacy Directive 97/66/EC

The origins of the ePrivacy Directive are set in Directive 97/66/EC, the Telecommunications Privacy Directive[5]. The adoption of Directive 97/66/EC was prompted, on the one hand, by the implementation of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data[6] and, on the other hand, by the development of new technologies in the telecommunications sector.

Directive 97/66/EC sought the harmonisation of Member States' provisions to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community. As *lex specialis* to Directive 95/46/EC, Directive 97/66/EC relied on and were functionally bound by the former, particularly with regard to the definition of personal data[7].

Directive 97/66/EC focused on the telecommunications sector only and applied to the processing of personal data in connection with the provision of publicly available services in public telecommunications networks in the Community. Specific reference was made to the Integrated Services Digital Network (ISDN) and public digital mobile networks[8]. four terms were specifically defined in the Directive: these were "subscriber", "user", "public telecommunications network", and "telecommunications service"[9].

---

[5] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ.L. 24, 30 January 1998, 1–8.

[6] For an explanation of Directive 95/46/EC see section **Error! Reference source not found.**.

[7] Directive 97/66/EC, Article 1(2).

[8] Directive 97/66/EC, Article 3(1).

[9] For the definitions of these terms, see Directive 97/66/EC, Article 2.

2.1.2. ePrivacy Directive 2002/58/EC

In 2002, the Directive on privacy and electronic communications (2002/58/EC)[10] repealed Directive 97/66/EC with a view to adapt its provisions "*to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used*". Essentially, while the Telecommunications Privacy Directive 97/66/EC applied to circuit switched connections (traditional voice telephony), the ePrivacy Directive 2002/58/EC extended its scope to encompass packet switched transmissions (data transmission, use of the Internet).

To this end, definitions of telecommunications services and networks were replaced by definitions of electronic communications services and networks to align the terminology with the proposed Directive establishing a common framework for electronic communications services and networks[11]. The update of these definitions was necessary to ensure that all different types of transmission services for electronic communications were covered, regardless of the technology used.

Other important changes included the specific protection of location data of a user of a publically available electronic communications service. The Commission's Explanatory Memorandum explains that a new type of service is available over cellular and satellite networks which allows the exact positioning of a mobile user's terminal equipment. Given that the location data of a user are far more precise, a new Article 9 was inserted, stipulating that such data may only be used with the consent of the subscriber. A further change was made to introduce the protection of information stored in terminal equipment[12].

The ePD was adopted as part of the Electronic communications Package ("**the ECS Package**"), consisting of five directives and two regulations: the Framework Directive (2002/21/EC), the Authorisation Directive (2002/20/EC), the Access Directive (2002/19/EC); the Universal Service Directive (2002/22/EC); the ePrivacy Directive (2002/58/EC; the Regulation on Body of European Regulators for Electronic communications (BEREC) (1211/2009) and the Regulation on roaming on public mobile communications networks (531/2012). The overall objective of the framework was to promote competition and set forth rules safeguarding end-user interests[13]. The ECS Package was last amended in 2009, including with respect to the ePD.

---

[10] 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 (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, p. 37.

[11] Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector /* COM/2000/0385 final - COD 2000/0189 * *Official Journal C 365 E , 19/12/2000 P. 0223 - 0229*

[12] Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, COM/2000/0385 final - COD 2000/0189, Official Journal C 365 E , 19/12/2000 P. 0223 – 0229.

[13] See the following link for information on the telecom regulatory Framework: https://ec.europa.eu/digital-agenda/en/telecoms-rules.

2.1.3. Citizens' rights Directive amending Directive 2002/58/EC

In 2009 the third reform of the Electronic Communications Framework took place[14] and introduce four fundamental changes to the rules applying to providers of electronic communications services and network: 1) it reinforced the rules on security of the processing, particularly by requiring all electronic communications service providers to notify personal data breaches to authorities as well as to subscribers or customers when they are likely to be adversely affected by the breach (i.e. by identity theft, reputational loss, etc.); (2) it required prior consent for storing or accessing information already stored in the user's terminal equipment such as cookies; (3) it reinforced the legal protection against unsolicited communications by ensuring that any individual or legal person having a legitimate interest may take legal action against infringements before the courts; (4) It specified that data collection and identification devices such as RFID[15] would be covered by the ePrivacy Directive when they are connected or make use of public communication networks or service.

2.2. Related recent legislative developments

2.2.1. Adoption of the General Data Protection Regulation and its relationship with the ePrivacy Directive

The **reform of the data protection legal framework**, initiated in 2012, is a cornerstone of the digital single market. In April 2016, the European Parliament and the Council adopted the **GDPR**". Morever, the Commission committed to **review**, once the new EU rules on data protection would be adopted, the **ePD** with a focus on ensuring a high level of protection for data subjects and a level playing field for all market players.

Issues of data protection in the electronic communications sector not specifically addressed by the provisions of the ePD are covered by the Data Protection Directive and in the future by the newly adopted GDPR once its rules become applicable (as of 25 May 2018)[16]. The ePD needs to be reviewed in the light of the adoption of the GDPR.

The review of the ePrivacy Directive announced in the Commission Digital Single Market strategy, seeks to assess whether the rules of the ePD remain relevant, while at the same time

---

[14] Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. OJ L 337, 18.12.2009, p. 11–36

[15] Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source such as a battery and may operate at hundreds of meters from the RFID reader. Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method for Automatic Identification and Data Capture (AIDC). Definition provided by Wikipedia, see: https://en.wikipedia.org/wiki/Radio-frequency_identification.

[16] This means for instance that the principles related to the processing of personal data defined in the GDPR, the rights of individuals, the obligations of data controllers and processors are also applicable in the context of the electronic communications sector when processing personal data.

evaluating their EU added value, efficiency as well as their coherence with other EU instruments and in particular with the GDPR. Therefore a careful analysis article by article of the coherence with these instruments and the GDPR was conducted in the context of the REFIT evaluation.

2.2.2. Commission proposal for a new European Electronic communications Code

On 14 September 2016, the European Commission published a proposal for a new European Electronic communications Code ("EECC ") which consists of a horizontal recasting of four of the existing Directives (Framework, Authorisation, Access and Universal Service), and bringing them all under a single Directive.

The proposal also follows a REFIT evaluation which overall has shown that the regulatory framework for electronic communications has broadly achieved its general objective of ensuring a competitive sector providing significant end-user benefits. Nevertheless, while its main specific objectives —promoting competition, developing the internal market, and promoting end-user interest —remain relevant, a review of the regulatory framework appeared necessary in order to address the growing need for increased connectivity of the Digital Single Market and to streamline provisions taking into account market and technological developments. The code proposes increased competition and predictability for investments, better use of radio-frequencies, stronger consumer protection, a safer online environment for users and fairer rules for all players.

The ePrivacy Directive is not part of the EECC as its REFIT evaluation and review was pending to the adoption of the GDPR due to the strong need of ensuring consistency of the rules.

2.3. Description of the initiative and its objectives

According to its Article 1, the ePD serves three main objectives (see general objectives in *Figure 1*).

- Its **first objective** is to ensure an equivalent level of protection across the EU of the *fundamental right to privacy and confidentiality* with respect to the processing of personal data in the electronic communications sector. This protection is also granted to subscribers who are legal entities[17].
- Its **second objective** is to ensure an equivalent level of protection with respect to the processing of personal data in the electronic communications sector to protect the *fundamental right to data protection.*
- Its **third objective** relates to the internal market and is to ensure free movement of personal data processed in the electronic communications sector and the free movement of electronic communications terminal equipment and services in the EU.

These objectives are closely intertwined and rely on one another (e.g. the free flow of personal data depends on the existence of common standards to protect such data).

The three main objectives of the ePD are supported by a series of specific provisions (see Intervention logic described in *Figure 1*). These specific provisions, each of which pursues

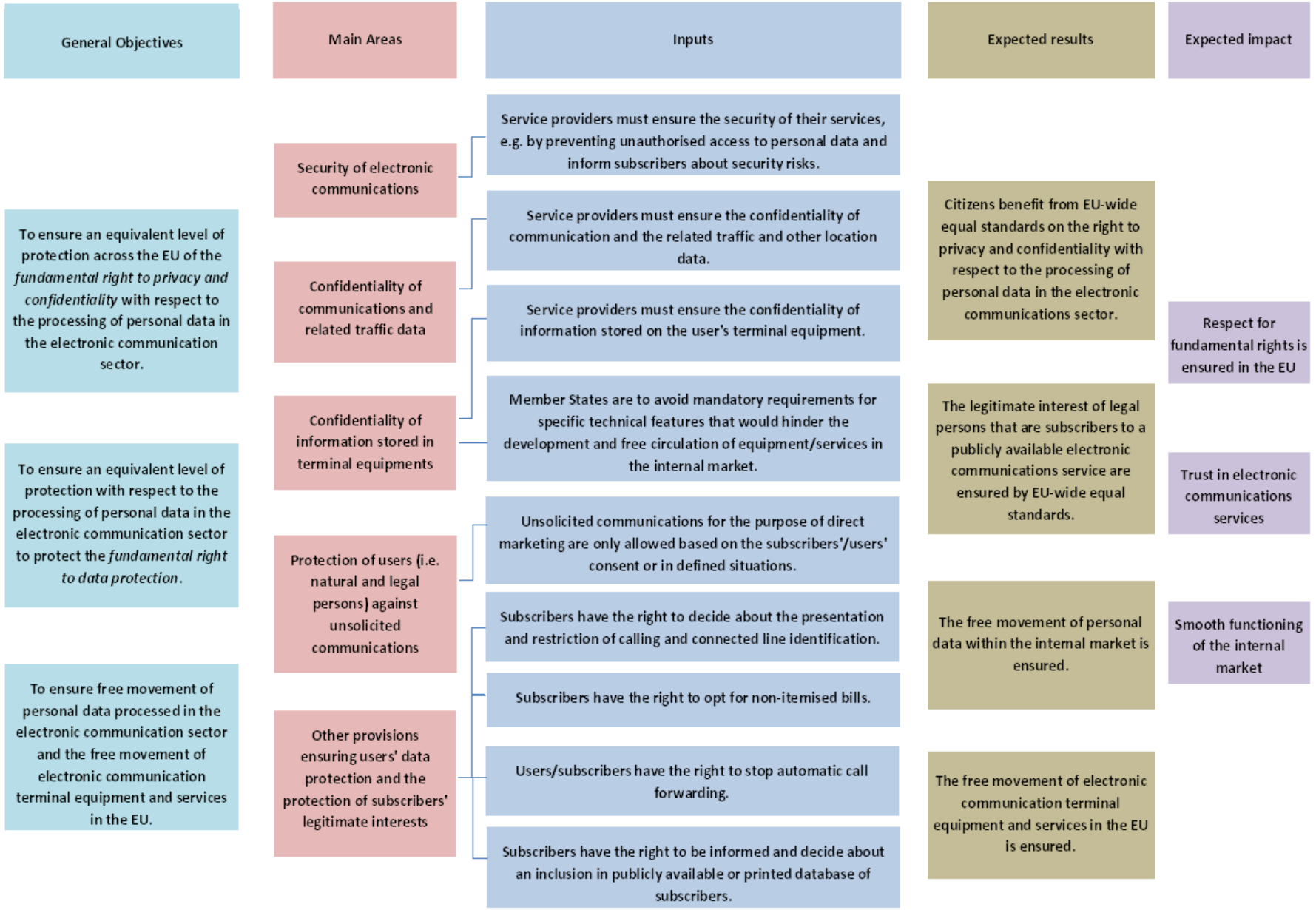
[17] Subscribers are defined in Article 2 of the Framework Directive 2002/21/EC.

one or several of the ePD main objectives, can be classified around 5 main areas harmonised by the ePD, namely:

- Security of electronic communications;
- Confidentiality of communications and related traffic data;
- Confidentiality of information stored in terminal equipment;
- Protection of users (i.e. natural and legal persons) against unsolicited communications;
- Other provisions ensuring users' data protection and the protection of subscribers' legitimate interests.

The main objectives, the 5 areas and the specific provisions ('inputs') attached to them as well as the expected impacts are detailed below in *Figure 1* – Intervention logic

Figure 1 - Intervention logic



2.4. Baseline situation at the time of the adoption of Directive 2002/58/EC

Until the end of the 90's, the electronic communications industry was characterised by separate sectors specialised in the provision of distinct services: voice telephony, data transmission and broadcasting. Each of these services was delivered over a determined network. And the user accessed it via a given terminal: the telephone, the computer or the TV set. Digital technologies that emerged early 2000 changed that situation with any service being offered over any network or accessed via any terminal. The focal point of this convergence process was the advent of the Internet, which created a platform bringing together all communications services and terminals, a key vector of economic growth and innovation in Europe.

The consequence of such revolution is that telecom networks started to carry data, rather than only voice, using Internet protocol and packet switching. While this ensured that the end user could be always connected – anywhere, anytime, such situation drew concerns as to the key position of electronic communications service providers in having access to crucial information about internet users,.

All of this called for a step-change in the Community's policy on telecoms and other transmission networks, which led to the so-called 1999 Review – made up of proposals for a regulation and five directives, including the ePrivacy Directive 2002/58/EC - adopted in July 2000 and which entered into force in 2002. The mentioned package aimed at creating a new framework for all electronic communications for which a key objective was to ensure a high level of user rights and privacy protection, in the light of the privacy challenges which recently emerged. In this context Directive 2002/58 tackled this issue by extending the principle of ensuring confidentiality of communications to all electronic communications service providers while that principle was extending to traffic and location data.

The uptake of mobile internet around 2005-2006 confirmed the importance of protecting traffic and location data in a similar manner as the content of communications given that the collection of these data allow ECS providers to draw very intrusive conclusions about one's life. In parallel a rise of security breaches and the evolution around the delivery of online advertising that started to rely more and more on internet users' behaviour triggered a new range of provisions in the context of the 3rd review of the Electronic Communications rules that led to the adoption of the 2009 Electronic Communications Package. Directive 2002/58/EC was specifically amended to address those issues.

3. EVALUATION QUESTIONS

Pursuant to the Commission Better Regulation Framework[18], the ePrivacy Directive has been evaluated against the five evaluation criteria.

Relevance

[18] http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm.

- To what extent are the general and specific objectives of the ePD still relevant?
- To what extent do the objectives of the ePD – ensuring an equivalent level of protection across the EU of fundamental rights and freedoms, in particular the right to privacy in the electronic communications sector and ensuring the free flow of personal data and services – still correspond to the needs and problems in this sector within the EU?

Effectiveness

- To what extent have the objectives of the ePD been met? Have the ePD rules proved relevant to the privacy needs of citizens and legitimate interest of legal persons as well as the needs of the electronic communications market? What are the major constraints to the attainment of the ePD objectives?

Coherence

- Is the ePD coherent both internally and in relation with other existing regulations? The interplay (covering an assessment of possible overlaps, contradictions and synergies) with in particular the General Data Protection Regulation, the review of the Electronic communications Regulatory Framework and the Radio Equipment Directive will be an essential element of this analysis.

Efficiency

- Do the provisions of the ePD allow for an efficient implementation by Member States?
- What costs have the provisions of the ePD produced and what benefits for the different stakeholders? Could the objectives be achieved at a lower cost?
- To what extent are the costs proportionate to the benefits achieved? To what extent has the intervention been cost-effective, including for SMEs?

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 level?

4. METHOD

4.1. Timing and Sources

The evaluation took place between **December 2015 and July 2016** and drew from the following main data sources:

- **Stakeholder consultations:**
  - A **Eurostat community survey on ICT usage by households and individuals** of December 2015, (specific questions on citizens' level of awareness of cookie tracking)[19];
  - A **public consultation** on the evaluation and review of the ePrivacy Directive (open from 12 April - 5 July 2016);
  - A **Eurobarometer survey** on e-Privacy, targeting citizens (conducted in July 2016);

[19] http://ec.europa.eu/eurostat/data/database?node_code=isoc_cisci_prv.

- **Ad hoc consultations** of (and discussions with) relevant EU expert groups: BEREC[20], ENISA[21], the Article 29 Working Party[22], the European Data Protection Supervisor, the REFIT stakeholder platform, Europol[23], COCOM and the CPC Network between January and July[24];
- **2 workshops organised by the Commission** – one open to all stakeholders and one limited to the national competent authorities in April 2016;
- A **Round Table** organised by the Commission – a closed meeting with 17 key stakeholders from all fields, the European Data Protection Supervisor and the Article 29 Working Party to gather views at a later stage of the review (October 2016);
- **Ad hoc meetings** with representatives of the affected industry, public authorities as well as with Digital Rights (Human Rights), consumer and citizens associations, as well as written input received from these stakeholders;

- **Evidence gathered through COCOM:** Already as of September 2014, the Commission sent a questionnaire to the Communications Committee (COCOM), which gathers the representatives of authorities responsible for electronic communications, requesting Member States to detail how they have implemented Article 4.2 of the ePrivacy Directive**.** More generally speaking, regular discussions took place in the COCOM on the implementation of the ePD in the context of bi-annual meetings of the COCOM[25];

- **Evidence gathered through publicly-tendered studies:**
  - The first comprehensive study on the Directive, titled *"ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation"*[26], was finalised in January 2015. The study did not encompass the entire ePrivacy Directive but focused on Article 3 on scope, Article 5 on confidentiality of communications, Articles 6 and 9 respectively on traffic and on location data (other than traffic data); and Article 13 on commercial communications;

---

20 It is the Body of European Regulators for Electronic communications.

21 ENISA is the European Union *Agency* for Network and Information Security.

22 The Article 29 Working Party is composed of all the data protection authorities of the EU.

23 Europol is the European Union law enforcement agency.

24 The CPC Network is s a network of authorities responsible for enforcing EU consumer protection laws. Some of these authorities are in charge of enforcing the national provisions implementing Article 13 of the ePD. http://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/consumer_protection_cooperation_network/index_en.htm.

25 https://ec.europa.eu/digital-single-market/en/communications-committee.

26 European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071).

- A second study was commissioned to help the evidence gathering exercise to evaluate the ePrivacy Directive (by covering the provisions not evaluated in the first study)[27]. The final report was received in October 2016[28];
- A Study on future trends and business models in communication services[29], was also used. This study investigates competitive pressures on Electronic Communications Service providers from companies offering internet-based communication services, Over-the-Top providers ("**OTTs**")[30], which end-users increasingly regard as substitutes for traditional telecom services;

- **Literature review of relevant reports.** This includes among others Opinions of Article 29 Working Party, Opinions of BEREC, Opinions of the Berlin Group on Telecommunications, Opinions of the European Data Protection Supervisor ("**EDPS**") as well as reports and studies from the Industry, many sent in the context of the public consultation. See Annex I for a detailed overview of these reports and studies.

- **REFIT Platform[31] opinion** (see Annex II for the full overview of the opinion)[32].

4.2. Method-used for the analysis and overall evaluation exercise

The data gathering followed **a participatory approach and strived for triangulation,** cross-checking of desk research, consultation covering both qualitative and quantitative data. As

---

[27] This study focuses on the transposition of the articles which were not covered by the first study. It focuses on (i) Article 1 and 3 on scope; (ii) Article 2 on definitions; Article 4 on security; (iii) Article 7 on itemised billing; (iv) Article 8 and 10 on presentation and restriction of calling and connected line identification; (v) Article 11 on automatic call forwarding and (vi) Article 12 on directories of subscribers.

[28] European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080).

[29] European Commission Study carried out by ECORYS, TNO and others (2016), Study on future trends and business models in communication services, (SMART 2013/0019).

[30] (Over The Top) is a generic term commonly used to refer to the delivery of audio, video, and other media over the Internet without the involvement of a multiple-system operator in the control or distribution of the content. The term over-the-top (OTT) is commonly used to refer to online services which could substitute to some degree for traditional media and telecom services. Definition provided in the study of the European Parliament, Directorate-General for internal policies, policy department A: Economic and Scientific Policy, Over-the-Top (OTTs) players: Market dynamics and policy challenges, dd. December 2015,

http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf.

[31] The REFIT Platform was announced in the 2015 Better Regulation Agenda. It consists of a Stakeholder Group, with 18 members and two representatives from the European Social and Economic Committee and the Committee of the Regions, and a Government Group, with one high-level expert from each of the EU's 28 Member States. Members will be supported in their work by the Commission's Secretariat-General. The members of the Stakeholder Group were selected through a public call for applications. The Commission has sought a balanced representation of different sectors, interests, regions and gender.

[32] The REFIT platform is an advisory group to the European Commission, which role is to provide views on evaluations and identify simplification potentials of existing legislation in line with the Better Regulation guidelines.

further explained below, the Commission collected evidence from different sources and proceeded to cross check them.

Citizens' views were specifically collected via easy to understand questionnaires in the context of a **Eurostat survey** of December 2015 and a **Eurobarometer on e-Privacy** conducted over the phone in July 2016.

A 12 week open **public consultation** on the ePD gathered a total of **421** replies from stakeholders in all Member States as well as from outside the Union, among which **162** contributions from citizens, **33** from civil society, **186** from the industry and **40** from public bodies. For more details see Annex II covering the synopsis report.

The consultation was supported by 2 **stakeholder workshops** (of which one was limited to competent public authorities only) and a Round Table. The views of the public consultation were supplemented by expert opinions of EU expert groups of national competent authorities. Such opinions were issued on the basis of targeted questionnaires sent by the Commission. All in all, stakeholders were consulted in several occasions. For example, the electronic communications industry and public authorities were consulted both via the public and targeted consultations but also though targeted questionnaires sent by the Commission via its contractor.

In addition to the public consultation, study SMART 2016/0080 also relied on two online surveys in order to collect additional information and stakeholders views on the ePD, looking in particular for precise quantitative elements, practical costs and benefits that business and competent authorities have experienced while implementing the ePD.

The formulation of all questions (both in the public and targeted consultations) took into account concerns or views expressed in previous occasions by various stakeholders (industry, citizens, public authorities etc.) as well as the state of the art in terms of technological developments and economic aspects. The data gathered from the sources above were analysed in house. Most of the data was also analysed by external contractors, in cooperation with the Commission, in the context of the 3 above-mentioned studies. Whenever possible, the Commission compared the consistency of the views received from different stakeholders, gathered through the above channels.

Finally, it should be emphasised that the evaluation exercise was coordinated by the European Commission Directorate-General Communications Networks, Content and Technology with the support of a Steering Group, chaired by the SG, (with representatives of European Commission Directorates-General[33]). The Group steered and monitored the progress of the exercise, ensuring the necessary quality, impartiality and usefulness of the evaluation (**see Annex I**).

4.3. Limitations

The evaluation faced limitations in the collection of data:

[33] SG, DG CONNECT, DG COMP, DG JUST, DG GROW, DG ECFIN, DG FISMA, DG TAXUD, DG TRADE, DG RTD, DG JRC, DG EMPL, DG EAC, DG HOME, DG ENV, LS, DG REGIO, DG HOME, DG ENER, DG MOVE, EUROSTAT, EPSC.

Quantitative data on the **costs for businesses to comply with some of the articles of the ePD** is scarce. The majority of stakeholders consulted as part of this initiative (including in particular businesses and business associations consulted as part of online survey and interviews) were not able to estimate relevant figures for the provisions.

The reasons for such difficulties relate primarily, according to businesses, to the fact that the necessary capital expenditures have been incurred right after the entry into force of the ePD in 2002 and have since then amortised themselves[34]. Another explanation is the difficulty for businesses to distinguish the costs incurred due to the ePD from the ones arising from other legislations such as the Data Protection Directive (e.g. security requirements). Finally, difficulties stem from the fact that an important part of the costs are not compliance costs but opportunity costs, given that the ePD imposes negative obligations (e.g. not to process), which are the opportunities providers of public telecommunications services or operators of public electronic communications networks are not able to pursue.

In relation to (recurring) operational expenditures, the feedback from businesses suggests that today, small costs are incurred in relation to e.g. itemised billing, presentation and restriction of calling and connected line identification and automatic call forwarding directories as these services are built-in features by design.

Most costs related to other provisions of the ePD which had not been amortised yet, for example the requirement to set up security measures, the requirement to place cookie banners (to obtain consent), or the rules on commercial communications were mostly based on qualitative calculations and on available studies offering limited quantitative data. The external study supporting the present REFIT evaluation provided an estimation of costs for all the provisions based on a series of assumptions, including a quantification of benefits (see Annex VIII of the Impact Assessment) [35].

5. IMPLEMENTATION STATE OF PLAY

5.1. Transposition

Member States were required to transpose the 2009 ePD in their national legislation by the 25th of May 2011. This implementation suffered from delays in some Member States.

In May 2012, 5 non-communication infringement cases were opened by the European Commission, which referred Belgium, the Netherlands, Poland, Portugal, and Slovenia - to the Court of Justice of the European Union because they had not implemented the revised EU telecoms rules into their national laws, including the Citizens' Rights Directive 2009/136 which amended the ePrivacy Directive[36].

---

[34] European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080). p. 31.

[35] SMART 2016/0080, cited above.

[36] EUROPEAN COMMISSION IP 12-524 " Digital Agenda: Commission asks Court of Justice to fine five Member States for missing telecom rules implementation deadline".

By January 2013 the Commission noted that all Member States had notified full transposition measures. No case led to a judgment of the Court of Justice of the European Union ("**CJEU**").

To avoid divergences in transposition of Article 5.3 of the ePrivacy Directive, the Commission lead discussions on this specific article in COCOM which resulted in Commission guidance on Article 5.3 of the ePrivacy Directive[37].

On 24 June 2013 the Commission made use of its powers to adopt implementing measures by adopting Regulation 611/2013 on notification of personal data breaches.

As regards the transposition of the ePrivacy rules itself, it took place in a very diverse manner[38].

A large majority of Member States have transposed most of the ePD provisions in a national legal instrument regulating "electronic communications", containing the rest of the provisions of the Electronic communications Package. But several provisions have been transposed by Member States in the context of another legal framework, such as the legislative instrument applicable to information society services, the general personal data protection law or the legal framework for consumer protection.

When the transposition was done into the national legal framework on electronic communications, some Member States have **widened the scope of particular provisions of the ePrivacy Directive at national level** (especially the confidentiality of communications provisions), considering that these provisions should not only apply to providers of electronic communications services *stricto sensu* but cover also providers of functionally equivalent services.

In Germany, the section of the Federal Telecommunications Act with regard to the processing of personal data – including e.g. traffic data – is not only applicable to services in the context of public networks but applies also to closed user groups[39].

Overall, seven Member States took a wider approach with regard to the scope of the ePD provisions extending the rules to cover so called OTT services[40]. As of 1 January 2015, the new Finnish Information Society Code entered into force[41]. The new Code renders the

---

37 Commission working document to the COCOM on the Implementation of the revised Framework – Article 5.3 of the ePrivacy Directive, June 2010.

38 European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071),

39 European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071), Finnish country profile.

40 European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080), Final Report, p. 91.

41 Finnish law, Information Society Code (917/2014); European Commission Study carried out by ECORYS, TNO and others (2016), Study on future trends and business models in communication services, (SMART 2013/0019), p. 86.

obligations of the ePrivacy Directive also applicable to communications services other than ECS including instant messaging services.

In France the Digital Republic Law was recently adopted and extends the scope of the rules on confidentiality of communications to so called "*online providers of communications services to the public*"[42].

The assessment of the reasons for these implementation/transposition difficulties and their consequences are assessed under Section 6.

5.2. Monitoring of national measures

Once the transposition measures had been put in place, the Commission carried out targeted actions to ensure appropriate transposition of the ePD.

The Commission engaged in an assessment of the transposition measures, through evidence and analysis carried out in the context of the first implementation study mentioned under Section 4. The study includes country reports detailing the transposition of the ePD rules in all the Member States and an analysis of whether national transposing laws are in line with the ePD.

On the basis of this information, the European Commission has conducted discussions in the period 2013-2016 with a few Member States on their transposition of the ePD.

The Commission has also monitored compliance and took proactive measures to ensure harmonised application of the ePD. This has been done through informal contacts with stakeholders and through more systematic actions. For example, the Commission has actively promoted self and co-regulatory actions, including the so-called 'Online Behavioural Advertising Roundtable[43]' and the development of the W3C Do-Not-Track Standard[44], which is still being discussed at international level.

The Commission has also engaged with national authorities responsible for the enforcement of the ePD, through bi-annual meetings to discuss specific issues such as the implementation of the data breach provision and of the Commission Regulation 611/2013 of 24 June 2013 on personal data breach; national experiences on confidentiality of communications and law enforcement; issue of applicable law etc.[45].

Other than the above, it is worth noting that prior to the transposition of the 2009 ePD in national law, one infringement procedure was launched against the United Kingdom in

---

[42] "*any person or company carrying out professional activities consisting in classifying or referencing content, services or goods, and which are proposed or put online by third parties, or putting in relationship parties by electronic means with a view to sell goods, supply services (including free of charge), or to exchange/share goods or services*".

[43] Online Behavioural Advertising roundtable meetings sought to support the (OBA) self-regulatory programme, launched in April 2011.

[44] The DNT policy is implemented technically using an HTTP header field binary option where 1 means the user does not want to be tracked and 0 (default) means the user allows tracking in the website.

[45] Meetings of the competent authorities for personal data breaches took place in 2013, on 10 December 2014 and on 6 October 2015.

September 2010. This case referred to the UK rules on the confidentiality of electronic communications.

The Commission identified three issues in the United Kingdom legislation relating to the confidentiality of electronic communications, which did not transpose the European legislation correctly:

- There was no independent national authority to supervise interception of communications;
- The UK law did not comply with EU rules defining consent as a freely given, specific and informed indication of a person's wishes;
- The UK legislation prohibiting and providing sanctions in case of unlawful interception of communications were limited to 'intentional' interception only, whereas the ePrivacy Directive requires Members States to prohibit and sanction any unlawful interception, regardless of whether committed intentionally or not.

The procedure was closed by the Commission in 2012 following the announcement by the UK government of amending its legislation with a view to bring it in line with European law.

5.3. Choice of competent authorities

The enforcement of the ePD provisions at national level is entrusted to a "*competent national authority*" (Article 15a of the ePD), without further defining that authority or body. This has led to a fragmented situation in the EU and within Member States.

As illustrated in the table provided under Annex V, Member States have often allocated competences to enforce the provisions of the ePD to multiple authorities within their country rather than to one: data protection authorities ("**DPAs**"), telecom national regulatory authorities ("**NRAs**"), other types of bodies (consumer protection bodies).

Overall, in the majority of Member States DPAs are the most appointed as enforcers of the ePD[46], but they are the sole competent authority in charge of EPD rules *only* in Italy, Luxembourg, Spain and Romania and the main authority in Portugal, Lithuania and Czech Republic[47]. For further details see **Annex V**.

This situation causes overlapping competences between authorities as well as a certain degree of legal uncertainty which contributes to hamper harmonised interpretations of the ePD provisions and cooperation in cross-border cases – more details under Section 6.

6. ANSWERS TO THE EVALUATION QUESTIONS

The evaluation questions (relevance, effectiveness, coherence, EU added value, and efficiency) will be answered *vis-à-vis* the five main areas of the ePD sketched under Section

[46] Only in one country the DPA is not at all competent to enforce the ePD provisions: Slovakia.

[47] Analysis of the Commission based on the country tables of European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071).

2.3 above, namely, (i) security of electronic communications; (ii) confidentiality of communications and related traffic data; (iii) confidentiality of information stored in terminal equipment; (iv) protection of users against unsolicited communications and, (v) other provisions ensuring users' privacy and the protection of subscribers' legitimate interests.

Prior to this, the horizontal problems specifically affecting the effectiveness of the ePrivacy Directive, i.e. the definition of the scope and the choice of the competent authorities, will be discussed in the outset of this section.

6.1. Horizontal effectiveness issue: Scope of the ePD and choice of competent authorities

6.1.1. Scope of the ePD

The ePrivacy Directive regulates "*the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community*"[48]. In particular, its provisions apply to providers of "electronic communications networks and services"[49].

To be covered by the Directive:

(1) the service should be an *electronic communications service*,
(2) the service should be offered in an *electronic communications network*,
(3) the aforementioned **service and network** should be *publicly available*, and
(4) the network or service should be provided *in the Community*.

The ePD applies, for the most part, to **traditional telecommunication service providers**, i.e. those providers that are responsible for carrying signals over an electronic communications network. Services which are functionally equivalent to ECS[50], over the top services are not covered.

A series of stakeholders, in particular competent authorities, consumer and civil society associations as well as traditional telecom providers, have criticised that the scope of the ePD in relation to the types of services covered in their view is **too narrow based on the definition of electronic communications services**, potentially hindering the achievement of the right to privacy and confidentiality in the electronic communications sector. This view is also supported by the Deloitte survey towards businesses for which 14 out of 26 replied that

[48] Articles 1 and 3 of the ePD.

[49] Defined in Article 2 of Directive 2002/21/EC (the Framework Directive).

[50] An electronic communication service (ECS) is defined by the current telecom regulatory framework as a 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 excludes 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. Under the interpretation offered by the European Court of Justice (ECJ, 7 November 2013, C-518/11 – UPC Netherland BV; ECJ 30 April 2014, C-475/12 – UPC/Nemzeti Média), ECS cover communication services of providers that bear the responsibility for the conveyance of signals over the underlying electronic communication network vis-à-vis end-users. Being responsible implies that the service provider must have a certain degree of control over the conveyance of signals. Operators of traditional electronic communications services usually also own and run (parts of) the underlying network, which consequently puts them into a "controlling" position.

the scope was too narrow, whereas 16 respondents out of 28 agreed the scope was out of date[51].

The scope of the rules set out in the ePD was also considered **ambiguous and lacking coherence** by the same stakeholders. While Article 3 of the ePD expressly limits the scope to publicly available electronic communications services in public communications networks, other provisions have a different scope, which may create legal uncertainty such as:

- the provision on confidentiality of terminal equipment is **nevertheless applicable to providers of information society services**[52] (Article 5.3);
- the **rule on unsolicited communications** applies to anyone who sends commercial communications (Article 13).

Furthermore, as the ePD only applies to *publicly available* electronic communications networks, this means that **closed (private) user groups and corporate networks** are excluded from the scope of the ePD. In this context, there is a lack of clarity as to which services qualify as a publicly available electronic communications services in public communications networks. Indeed, Member States have diverging views on whether **Wi-Fi access offered by an airport or internet access provided in internet cafes and shopping malls** qualify as publicly available electronic communications services in public communications networks[53].The Article 29 Working Party also noted that the distinction between public and private networks is not always clear, as private and public elements are increasingly intertwined[54]. Examples of such ambiguous services according to the Article 29 Working Party include:

- Internet access provided to ten thousands of students at a university;
- Internet access provided by multinational companies to their employees; and
- Internet access provided to any visitor of a cybercafé.

The **definition of "electronic mail"** is also unclear, as demonstrated by the opinion of the Nordic Ombudsman regarding whether messages appearing to a Facebook user under 'News Feed' can be deemed as 'electronic mail' (and thus be subject to the rules on unsolicited commercial communications). The Nordic Consumer Ombudsmen say: "*It is uncertain*

---

51 European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080), Final Report, p. 92.

52 This is in incoherent with the definition of "electronic communications service" enshrined in Article 2c of the Framework Directive, which expressly excludes information society services. Note that information society services are defined in Art 1.2 of Directive 98/34/EC as amended by Directive 98/48/EC.

53 See Report from the Swedish Post and Telecom Agency (PTS) '*Which services and networks are subject to the Electronic communications Act? Guidance'*, 2009. Available at: https://www.pts.se/upload/Rapporter/Internet/2009/services-e-com-act-2009-12.pdf.

54 Article 29 Working Party, Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)' (WP150), p. 4. See also: J. van Hoboken and F. Zuiderveen Borgesius, "Scoping Electronic Communications Privacy Rules: Data, Services and Values" *JIPITEC*, Vol. 6 (2015), pp. 198-210, para. 16.

whether messages from traders appearing under a Facebook user's 'News Feed' fall within the definition of electronic mail"[55].

Finally, it remains unclear to which extent the **electronic communications** of the **Internet of Things**[56] is covered by the ePD scope as its Article 3 expressly refers to "*public communication networks supporting identification devices*"[57]. According to the EDPS, this seeks to clarify that the communications provider normally should not be concerned with the purpose or content of communications, nor should it even be aware of such specificities of the messages and other communications being transmitted through their services[58].

Recital 56 of Directive 2009/136/EC provides that the provisions of the ePD, in particular those on **security, traffic and location data and on confidentiality of communications** apply to Radio Frequency Identification.

Overall, it can be concluded that the effectiveness of the ePrivacy Directive was partially hampered by its unclear scope and definitions.

6.1.2. Applicable law and cross-border situations

Contrary to the Data Protection Directive, the ePrivacy Directive **does not contain an explicit provision** with regard to the **applicable national law**. This may create legal uncertainty as to which law should apply in a cross-border context. In particular, it is unclear whether the rules on applicable law of the DPD apply (country of origin)[59] or whether the ePrivacy Directive should be considered as following the applicable law rules set forth in the directives belonging to the ECS package (country of destination).

The unclear situation derives from the lacking of a specific applicable law rule, which hinders an effective application of the rules in a cross-border situation.

---

55 See *Position of the Nordic Consumer Ombudsmen on social media marketing of 3 May 2012*, available at: http://www.consumerombudsman.dk/~/media/Consumerombudsman/dco/Guidelines/Position%20of%20the%20Nordic%20Consumer%20Ombudsmen%20on%20social%20media%20marketing.pdf.

56 Based on existing communication technologies like the Internet, the IoT represents the next step towards digitisation where all objects and people can be interconnected through communication networks, in and across private, public and industrial spaces, and report about their status and/or about the status of the surrounding environment (Commission SWD(2016) 110/2 Advancing the Internet of Things in Europe, p. 6).

57 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 radio frequencies like RFID.

58 EDPS Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 22.07.2016, p. 11.

59 Article 4 of the Data Protection Directive provides that "*each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State*".

6.1.3. Diversity of competent authorities

The ePrivacy Directive entrusts the enforcement of its rules to a "*competent national authority*" (Article 15a of the ePD), without further defining that authority or body.

Each of these authorities has **different responsibilities, structures and inherent specificities** not conducive to reaching the same views on the interpretation and enforcement of the ePD, so that the same processing is treated divergently across Member States and thus impacts cross-border processing activities.

This situation fosters different interpretations across Member States and this is reinforced by the fact that there is no recognised EU group to gather together all authorities responsible for the enforcement of the ePD. **DPAs meet through the Article 29 Working Party (which is tasked with providing advice and guidance on the Data Protection Directive and the ePD[60]) and NRAs through BEREC**. In practice, this diversity of competent authorities, whose competences often overlap, has led in many countries to an ineffective enforcement of the rules as evidenced by the lack of compliance of companies in practice with some of the provisions (e.g. the so called "cookie" rule) further supported by the inexistence of case-law[61].

This is confirmed by the views of a strong majority of stakeholders in the public consultation: Consumers and industry converge in thinking that because Member States have allocated enforcement powers to different authorities, this has caused divergent interpretation of the rules.[62] A majority of citizens and consumers and their representative associations believe that this has led to significant or moderate divergent interpretation of the rules in the EU and to non-effective enforcement. Of those that have reported significant and moderate problems, the main source of confusion is for citizens, and then the providers themselves, followed by the competent authorities.

The REFIT platform opinion expressly calls on the Commission to address the fragmentation generated from the diversity of allocation of competences throughout Member States.

Overall, it appears that the **effectiveness of the rules in cross-border cases is hampered** due to the allocation of enforcement competences to a wide range of authorities that often overlap.

---

60 It should be noted that the ePD has tasked the Article 29 Working Party to provide advice and guidance on the ePD.

61 European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071).

62 The majority of citizens, consumer and civil society organisations believe that the significantly or moderately divergent interpretation of the rules in the EU (64.4%) and non-effective enforcement (61.9%) is due to some Member States allocating enforcement powers to several authorities. Of those that have reported significant and moderate problems, the main source of confusion is for citizens, the providers themselves, followed by the competent authorities. Industry also believes that the allocation of enforcement powers to several authorities has caused divergent interpretation (65.4%) but is more divided on the effectiveness of enforcement, with 41.3% believing that this has significantly or moderately caused non-effective enforcement.

6.2. Security of electronic communications

The ePD requires providers of electronic communications services to take appropriate technical and organisational measures to safeguard the security of their services (Article 4). In case of a particular risk of a breach of the security of the networks, the service providers must also **inform their subscribers of this risk** (Article 4.2).

Publicly available electronic communications service providers must **also notify personal data breaches to relevant authorities**, and in certain cases (if the breach is likely to adversely affect that person) also to the subscribers and individuals concerned (Article 4.3).

6.2.1. Relevance of the current rules

Ensuring the security of information processed remains an **essential pre-condition to achieve the objectives of this directive**, e.g. privacy and confidentiality of communications as well as the free flow of personal data and services. If one takes into account that the numbers of deliberate or accidental security incidents is increasing[63], the relevance of the security requirements are even bigger today than in 1997, when this requirement was first adopted.

The fact that similar obligations have been imposed in other sectors, such as those covered by the Directive concerning measures for a high common level of security of network and information systems across the Union ("**NIS Directive**")[64] and the strengthened general rules on security relating to processing of personal data in the GDPR, highlights the importance and increased relevance of security requirements in general.

Nevertheless, the existence of these new provisions has put into question the relevance of maintaining security requirements within the ePrivacy Directive. Therefore a careful assessment of overlaps with relevant EU legislation has been conducted under the coherence criteria under section 6.2.3. Such assessment has shown that most of Article 4 (except Article 4(2)) is covered by the security provisions of the GDPR and therefore such article remains only partially relevant.

6.2.2. Effectiveness

Under this criterion it is assessed whether Article 4 has achieved its objectives and proved effective. The evaluation shows that Article 4 **has only been partially effective in** ensuring security of services.

Before the review of 2009, the Directive provided little guidance on the measures appropriate to fulfil the security requirements while there was no obligation to report breaches at EU level. The security rules introduced in 2009 brought more clarity and a degree of uniformity regarding security of telecommunication services insofar as they spelled out with a high degree of detail the specific security measures to be applied by electronic communication providers to protect communication services.

---

63 Figures on recent data breaches and losses can be found at: http://datalossdb.org.

64 Directive 2016/1148/EU of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.

Nevertheless, as regards the contents of the provision itself, **some uncertainties remain**. For instance, it is not specified whether **the security obligations in Article 4.1 and 4.2 should apply to personal data only or also to non-personal data.** Although some explicit references to "personal data" are made e.g. in Article 4(1a), the "security of services" refers rather to the overall functionality and provision of the service, including personal data but possibly also other aspects. As concerns the **obligation to inform subscribers of security risks (Article 4.2)**, ENISA pointed out that there are difficulties relating to its practical application. In particular, there is **little guidance** about the type of risks and proposed mitigating measures that the providers should be informing for[65]. On this basis, the quality of information provided to subscribers may vary. A questionnaire sent to Member States through the Communications Committee (COCOM) about the application of Article 4.2 indicated that Member States have little experience on the application of this provision as well as important divergences on how it is being applied. For example, in some Member States the providers must notify subscribers about the risks through the provider website (e.g. Poland). In some Member States, the notification must be provided directly to the subscriber (e.g. Sweden). Several countries such as Belgium, Greece, Ireland, Malta, Romania and Spain have transposed the data breach requirements under 4.2 and 4.3 literally[66].

The **obligation to inform subscribers of security risks (Article 4.2)** and the rules on the **notification of personal data breaches (Article 4.3)** may positively contribute to the security of processing as they ensure that any breach must be notified to the competent authorities and in some cases to individuals. Only 13% of industry respondents to the public open consultation indicated that they have faced problems[67].

Public bodies expressed difficulties in enforcing the data breach rule as reflected by the online survey conducted by Deloitte in the context of study SMART 2016/0080. According to some authorities, **the breach notification provision is good on theoretical level but its effectiveness has not been fully achieved yet**. This seems to be confirmed by the inexistent or very low numbers of breach notifications in many Member States (see Table 1 on Reported incidents of personal data breaches in selected EU Member States below). Some authorities explained that **businesses in some cases have failed to report personal data breaches** but the degree of compliance is difficult to verify given that most authorities rely on information provided by companies themselves. This might be caused by the lack of defining criteria to determine what type of breaches needs to be notified.

Table 1 -Reported incidents of personal data breaches in selected EU Member States

Member State	2010	2011	2012	2013	2014	2015
Belgium	/	/	0	0	4	1
Croatia				0	0	0
Cyprus	0	0	0	0	0	0

[65] ENISA (June 2016). *Working paper on the review of the ePrivacy Directive. Article 4 – Security of processing*, p. 12-15.

[66] Smart STUDY 2016/080 Final Report, p 68.

[67] Question: "Have you encountered problems in applying/understanding the rules (in your role of provider or as individual)?". 120 respondents answered "Yes", 106 answered "No" and 104 did not have an opinion.

Member State	2010	2011	2012	2013	2014	2015
Estonia				1	2	5
Germany	-	-	17	66	112	261
Greece (HDPA)[68]	n/a	n/a	0	0	0	4
Greece (ADAE)	4	7	5	16	30	11
Ireland	410	1167	1592	1507	2188	2317
Romania					1	3
Sweden			5	4	16	24
United Kingdom			491	381	308	550
Total	**414**	**1174**	**2110**	**1975**	**2661**	**3176**

Source: Deloitte - Responses of competent authorities to Deloitte online survey

In addition, there have been **in the recent years some major cyber-attacks** and other breaches[69], which further put into question the extent to which the rules are applied in practice and adequately enforced. A few authorities also expressly reported to the Commission that they do not have the power to impose penalties in case of violation[70]. On a positive note, the transposition check carried out by one of the supporting studies of the REFIT[71] shows that most Member States transposed all relevant parts of this article. On this basis, the effectiveness of this article in achieving secure processing is not hindered in most Member States. Indeed, almost half of the Member States[72] appear to have transposed this article more or less literally[73].

Quantitative data about the incidents reported may be interpreted in different ways: it may be read as **a sign of greater responsiveness from operators**. A study published by university researchers in the United States found that in the US, the adoption of personal data breach notification laws resulted in a reduction of identity thefts by 6.1 % in average[74]. There is no similar information available for the EU.

To conclude, it can be concluded from the above that Article 4 was relatively effective in imposing adequate security obligations upon providers of electronic communications but that

[68] HDPA: minor incidents only; Obligation for providers to submit a Data Breach Notification to the supervising authorities (both the HDPA and ADAE) has only been imposed in 2012.

[69] Some security breach cases reported in the press include Gemalto, Talk Talk, Carphone, Belgacom.

[70] European Commission workshop with competent authorities, April 2016.

[71] SMART study 2016/0080.

[72] Belgium, Croatia, Denmark, Greece, Ireland, Poland, Portugal, Romania, Slovenia, Spain, and United Kingdom.

[73] Such is the case of Austria, Bulgaria, Cyprus, Czech Republic, Estonia, France, Hungary, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Slovakia, and Sweden.

[74] Acquisti; Telang and Romanosky, "Do Data Breach Disclosure Laws Reduce Identity Theft?" (Updated), *Journal of Policy Analysis and Management* (2011), Vol. 30, No. 2, pp. 256-286.

such effectiveness could be increased with more clarity on security breach notification and powers to competent authorities,

6.2.3. Coherence

This section assesses whether the rules of Article 4 are coherent both internally and in relation with other existing EU legal instruments. Article 4 is closely linked to Article 13a of the **Telecom Framework Directive 2002/21/EC** and **Articles 32, 33 and 34 of the GDPR**[75] and other instruments[76].

In the table below, the connection between the ePD and the GDPR as well as the Electronic communications package is presented. For each relevant provision[77] a brief summary is provided, using the following colour code:

- Green: positive relationship (e.g. synergies);
- Yellow: potential challenges.

Table 2 - Comparison of Article 4 with the similar security provisions in the GDPR and Framework Directive[78]:

Provision in the ePD	Provision in the other instrument	Main findings
GDPR		
Security of Processing (Article 4.1 and 4.2)	- Principles relating to processing of personal data (Article 5) - Security of processing (Article 32) - Data protection by design and by default (Article 25) - Data Protection Impact Assessment (Article 35)	The measures provided in Paragraphs 1 and 1a of Article 4 of the ePD are covered by the GDPR. The **GDPR goes into greater detail** than the ePD, providing further references to measures such as pseudonymization, encryption, confidentiality, integrity, availability, and resilience of processing systems, as well as disaster recovery plans, regular testing, and adherence to codes of conduct and standards. **However, the requirements of Article 4.2 regarding the breach to the security of the network are not addressed under the GDPR.**

[75] European Commission (2016). *Background to the public consultation on the evaluation and review of the ePrivacy Directive*, p. 10.

[76] It is also linked to Directive 2014/53/EU on Radio Equipment (so called "**RED Directive**") applicable as of 13 June 2016 and Directive 2016/1148/EU of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (so called "**NIS Directive**"), OJEU 19.07.2016, L194/1.

[77] Only those instruments and provisions that a have connection to the ePD are listed.

[78] Table based on European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080).

Notification of personal data breaches (Article 4.3 and 4.4)	- Notification of a personal data breach to the supervisory authority (Article 33) - Communication of a personal data breach to the data subject (Article 34)	The **procedures for personal data breaches vary considerably** between the ePD and the GDPR; thus, an ECS may need to follow different procedures in case it offers electronic communications and other services, with divergences on: • Conditions for notification to authorities; • Conditions for notification to data subjects; • Content of the notification; and • Exceptions to the notification to data subject.
Electronic Communications Package (Framework Directive)		
Framework Directive		
Security of processing (Article 4.1 and 4.2)	Security and integrity (Article 13a.1 and 13a.2)	Article 4.1, 4.1a and 4.2 of the ePD focus on ensuring the integrity and confidentiality of the personal data both stored and in transit. Article 13.a and 13.b of the FD focus on security matters affecting the continuity of the service and of the network. **It works in synergy with Article 4 of the ePD.** The requirements of Article 4.2 are not addressed under the Article 13a.1 and 13a.2.
Security of processing (Article 4.3 and 4.4)	Security and integrity (Article 13a.3 and 13a.4)	The breach notifications under Article 4.3 and 4.4 of the ePD focus on the privacy impact such a breach would have on the individual. The breach notifications under 13.a.3 and 13.a.4 are requested when a breach will significantly impact the operation of networks or services (e.g. server down, no access to internet). Thus, the provisions do not overlap or contradict each other, but rather work on synergy.

Many of the **competent authorities interviewed by Deloitte criticised that with the adoption of the GDPR there will be two different data breach notification regimes**, if the regime detailed under Article 4 of the ePD remains[79]. This view was supported by ENISA, which argued that the **data breach requirements of the ePD overlaps with Articles 33 and 34 of the GDPR and that these provisions achieve the same objective in a more efficient and flexible way than in the ePD**. The deadline for notifying the supervisory authority of breaches is more flexible in the GDPR than in the ePD (72 versus 24 hours). ENISA therefore concludes that the **GDPR scheme seems to be preferable** to the one of the ePD as it has the potential to achieve the same objective, allowing for more efficiency and better quality of results but with a more flexible regime.[80] Conversely, ENISA confirms that Article 4(2),

[79] SMART study 2016/0080, Final Report, p 104.

[80] ENISA (June 2016). *Working paper on the review of the ePrivacy Directive. Article 4 – Security of processing*, p. 13-15.

which relates to notification of risks, is not part of the GDPR; it is specific to the electronic communications sector. For more details on coherence with GDPR, see **Annex IV**.

On the coherence of these security provisions with the Framework Directive and GDPR, around one third of citizens and consumers reported that they do not know, whether such coherence is achieved.

In the light of the above, and in particular of the coherency check with other existing instruments, it can be summarised that Article 4.1, 4.1a and Article 4.3 and 4.4 **are redundant with the security provisions of the GDPR**. **Article 4.2 remains relevant** as it is neither covered by the Framework Directive nor by the GDPR.

6.2.4. Efficiency

Businesses have indicated that they incurred most of compliance cost with Article 4 after the adoption of these rules (some in 1997, some in 2002 and also as for the data breach notification in 2009). This provision is one of the more costly provisions for businesses and competent authorities, as it entails several concrete obligations. For businesses, the provision entails costs as to the implementation of security standards, potential interaction with competent authorities in the context of audits and since 2009, the obligation to notify security breaches as detailed further below..

The SMART study provided a detailed calculation of the compliance costs as for the data breach notification regime. It explains that excluding any estimates on the costs of setting up necessary internal business organisation (assumed to be already included in any adequate risk management approach), the **notification costs** are estimated using staff costs and time requirements. The costs for a staff person entrusted with reporting and follow-up activities are assumed to be EUR 60,000.[81] Presupposing that reporting activities are similar to those under Article 13a of the Framework Directive 2002/21/EC and that no further analysis within the organisations are necessary, time required for notification is assumed to be one 0.5 working days. Combining these two factors, the average cost for reporting one incident is **EUR 125.**[82] While this number is not considered to be very significant for businesses, it may underestimate the expenses due to a very narrow definition of work steps and staff involved in the notification process. With regard to **post data breach response costs**, investigations are considered as a significant driver of costs.[83] In relation to administrative burden, mostly stemming from the notification obligations for telecommunication service providers, it is estimated that an annual amount of around **EUR 28** per affected business per year[84].From the

[81] This number is based on information gathered in the "Action Programme Reducing Administrative Burdens in Europe", using the salary information category "Professional" in the EU27 (increased by 25% to include overhead costs).

[82] Calculating the number includes the following steps: EUR 60.000 /12 months / 20 days / 2 = EUR 125.

[83] It is important to note that the frequency and cause of audits differs between the NIS context and the situation under the ePD. The impact assessment only considers investigations following notifications (thus not covering regular audits by authorities) and assumes that they only take place in 10 to 20 per cent of all cases.

[84] European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080), p. 281.

perspective of competent authorities, Article 4 tends to be one of the most time-consuming provisions, with variations across Member States.

Other studies have evaluated these costs differently and allude to higher figures.[85] Nevertheless, it should be noted that the costs of notifying breaches are by definition **only incurred in case of an actual breach**; **so real costs incurred** must be estimated in the light of the **(very low level of) notification of such breaches** in the Member States[86].

Regarding the requirements to implement security measures, several studies reported that large organisations are progressively increasing their spending on IT security. The same research finds that organisations who have invested more in security defences have fewer breaches. This seems to indicate a positive effect associated to the security requirements.

To monitor compliance of such security requirements, available information suggests that the actual time spent by public authorities depends on the Member State. Three authorities indicated that this takes less than one working day, four indicated that it takes between 1 day and less than a week and three authorities indicated that it takes 1 week or more[87].

Several stakeholders in the online survey and interviews conducted by Deloitte pointed out that the efficiency may be hindered based on the interaction of the ePD with other instruments. More specifically, it was argued that there might be **to many overlapping requirements** (GDPR, ePD, Network and Information Security Directive, Framework Directive), creating administrative burden.

Overall, Article 4, in particular the requirement to notify personal data breaches, appears to be one of the most costly provisions, both for businesses and competent authorities, while this provision mostly overlaps with the GDPR. Keeping overlapping provisions between the ePD and the GDPR **could potentially entail additional costs, administrative burden and legal uncertainty for ECS providers.** It would also add extra costs for competent authorities given that more than one authority may have to investigate the same data breach.

6.2.5. EU added value

Having different levels of national security requirements, including different procedures and circumstances under which personal data breach notifications are required to be notified may lead to uncertainty and to more cumbersome procedures and significant administrative costs for providers operating across borders. Operators are moving towards offering cross-border services; hence, having harmonised security EU rules becomes more relevant as otherwise they may have to comply with different national rules. Furthermore personal data breaches are not confined to the borders of one Member State, an operator may have to notify personal data

---

85 Ponemon Institute (June 2016): Cost of Data Breach Study. Global Analysis, p. 8 (around EUR 155) and Commission Staff Working Paper on Impact Assessment on the General Data Protection Regulation proposal, 25.01.2012, SEC 2012(72), Annex 9 and p101.

86 See Table 1 on Reported incidents of personal data breaches in selected EU Member States, p 25.

87 European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080), Deloitte online survey to public authorities, p 111.

breaches in various Member States. This highlights the need for harmonised procedures to notify personal data breaches.

When the security obligations of the ePD were streamlined in 2009 with new personal data breach obligations the intention was to render electronic communications service providers more accountable across the EU while such rules did not exist in any other EU instruments.

The **added value of having harmonised rules at EU level** is **confirmed by a majority of public bodies, citizens and civil society** that responded to the public consultation[88]. However, as for the personal data breach notification, a great majority of industry did not see any EU added value[89], which appears to be due to the fact that **the recently adopted GDPR sets forth similar rules** (see section on coherency).

The above leads to the conclusion that there is EU added value to have rules requiring notification of personal data breaches but **there is no added value in having these requirements in the ePD, given that similar rules exist under the GDPR**.

KEY FINDINGS:

The **pertinence of having security requirements at EU level** to protect personal data from loss or unauthorised access as well as data breach notification was **demonstrated**; the scarce evidence on the related costs and benefits is not sufficient to estimate whether such costs have been fully proportional vis-à-vis the benefits and objectives pursued

At the same time, the above confirms that the security provisions of the ePD (Articles 4.1 and 4.1a, 4.3, 4.4 and 4.5) overlap with other legislation and cause duplication.

The **effectiveness** of the security provision under the ePD **has been partly limited** due to various reasons, such as the lack of enforcement powers of competent authorities in some Member States. Moreover, keeping overlapping provisions between the ePD and the GDPR could potentially entail additional costs, administrative burden and legal uncertainty for ECS providers.

In light of the above, it can be concluded that **Articles 4.1, 4.1a, 4.3 and 4.4. appear redundant while the requirement of Article 4.2 to report risks is still relevant and coherent with the GDPR and Framework Directive**.

6.3. Confidentiality of communications and related traffic data

The **principle of confidentiality of communications and related traffic data and location data** is spelled out respectively in **Articles 5.1, 6 and 9 of the ePD** (hereinafter we refer to these provisions as "**confidentiality of communications and related traffic data**").

Member States must ensure confidentiality of communications and of related traffic data in public communication networks and services. Therefore, **listening, tapping, storing or engaging in other kinds of interception or surveillance of communications** and the related

[88] Question 6 of the public consultation.

[89] Question 6 of the public consultation.

traffic data without the consent of the citizen concerned (except when legally authorised) is **prohibited**[90].

The principle relates **both the content of communications and their related traffic data**[91]. Article 6 of the ePD specifies that ECS providers must ask for their subscribers'/users' consent in order to use traffic data for the purpose of marketing electronic communications services as well as to provide "value added services"[92]. If individuals have not consented or if the data is not anonymised, **the data must be erased** after the period during which the bill may be challenged or payment pursued.

Article 9 of the ePD requires users' consent for ECS providers to process location data other than traffic data. It can be processed to provide value added services to the extent and for the duration necessary for the provision of such services. These data **can be processed** for other purposes, without consent, as long as the **data are made anonymous**.

6.3.1. Relevance of the current rules

The *rationale* behind the rules protecting the content of communications is the need to ensure that **one's communications** (what is written or said) **is kept private**. These rules not only seek to protect privacy, but also support other fundamental rights, such as the freedom of speech. The rules ensure as well the secrecy of communications *per se,* independently of the protection of privacy, for example **to exchange business information,** which may not qualify as personal data.

The prohibition to access communications covers indifferently the content of the electronic communications and the traffic and location data attached to it (so called "meta-data"). The latter is justified by the dangers caused by the **ECS unobstructed view of citizen's daily behaviour online** and physical moves. The **European Court of Justice has acknowledged** in recent rulings that traffic data may allow very precise conclusions to be drawn concerning the private lives of persons[93].

Rules on confidentiality of communications under Article 5(1) and (2) have **no direct equivalent in Directive 95/46/EC or the GDPR**. The general data protection instruments do not refer to the prohibition of listening, tapping, storing, or otherwise intercepting

---

[90] Following the judgment of the CJEU in which it annulled the Data Retention Directive (CJEU 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*), currently two cases were brought before the Court concerning the conditions for Law Enforcement authorities to access data, the conditions under which data can be retained and addressing the question of EU competence in this area (C-203/15, *Tele2 Sverige* and CC-698/15, *Davis*).

[91] Traffic data relates to websites visited, phone numbers of people called, time of the call, location of where the device were checked for new emails etc. Communications data is the content of the communication (voice, content of SMS).

[92] The processing of traffic data is allowed when needed by the ECS for billing purposes without consent.

[93] CJEU 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* paragraph 27: "*Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*".

communications and their related data. The need for such reules and the fact that they are not replicated elsewhere is confirmed by several stakeholders interviewed by Deloitte[94] as well as BEREC[95] and the EDPS. Similarly, the Article 29 Working Party argues that ensuring confidentiality of communications is a key objective of the ePD and that it is still relevant to have a "general prohibition of the interception/surveillance/monitoring of the content of electronic communications". [96]

.

6.3.2. Effectiveness

According to stakeholders, the **ePD has not been fully effective in ensuring protection of privacy and electronic communications**. In the public consultation, 76% of the citizens and civil society do not believe, or believe only to a limited extent, that Article 5.1 has ensured full protection of privacy and confidentiality of communications. Citizens and organisations representing consumers and civil society report that the application/understanding of the rules on confidentiality of electronic communications is problematic, citing various reasons, including the fact that they do not cover OTT services. 60% of the industry recognised that they **had encountered difficulties** in understanding or applying the rules on confidentiality of communications and related traffic data[97].

As further described below, this lack of effectiveness could result from a variety of factors, including:

- A series of p**roblems and flaws in the wording and implementation** of Article 5.1 and 5.2, which prevented the full achievement of the key objective of ensuring the confidentiality of communications detailed below[98]:

---

94 SMART study 2016/080, Final Report p 120.

95 BEREC, in its response to the ePrivacy Directive questionnaire, argues that confidentiality of communication is one of the fundamental provisions of the ePD, and that Article 5 therefore remains relevant.

96 Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf, p. 9.

97 Question 2 of the public consultation.

98 Notably, an online survey carried out by Deloitte for European Commission in the context of the Study Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080) with competent authorities showed that there are several ambiguities in relation to the scope and application of this provision. For example, 43% of the respondents (12 authorities) considered a serious problem that it is not sufficiently clear what type of communications data is in scope. On this basis, the application of this provision varies across Member States leading to unequal standards for citizens. Closely related is the fact that there is ambiguity as to which types of services are covered by these provisions. On this basis, at least in some Member States Article 5.1 and 5.2 only apply to the electronic communications sector. As more and more citizens regularly use online communications services (cf. 2016 Eurobarometer survey (EB) 443 on e-Privacy addressing citizens, (SMART 2016/079)), important services that are part of citizens' everyday life are not covered, weakening the effectiveness of this provision.

- the wording of the provisions (Article 5.1. and 5.2) appears **partially outdated.** It should be clarified that the **confidentiality** of electronic communications **should also apply against "automatic" intrusions** without human intervention. **None of the Member States** has provisions that deal explicitly with **automated data processing, without human involvemen**t, in the context of a breach of confidentiality of electronic communications. Moreover, diverging interpretations exists across Member States. For example, Sweden requires the involvement of a person in order to qualify for an illegitimate breach of confidentiality. Belgium, Germany and other Member States will consider the **interception of MAC addresses a breach of confidentiality** while in France there will need to be additional data captured that link the MAC to an individual[99].
- Some Member States **treat traffic data and content differently**[100]; others have one provision/instrument covering both types of data[101]. For eleven Member States only when content is in transit is it considered *a communication* of which the confidentiality should be protected[102].
- Member States have also taken **very different approach** in transposing the **lawful business exception (**Article 5.2), due to the confusing wording of the provision, written in too broad terms.

- the limited scope of application and related uneven playing field, a problem described in Section 6.1.1. Indeed, while the **ePD covers some parts of consumers' everyday communication means**, **new communication means** that are expected to become more important over the next couple of years are not covered by the confidentiality rules[103].

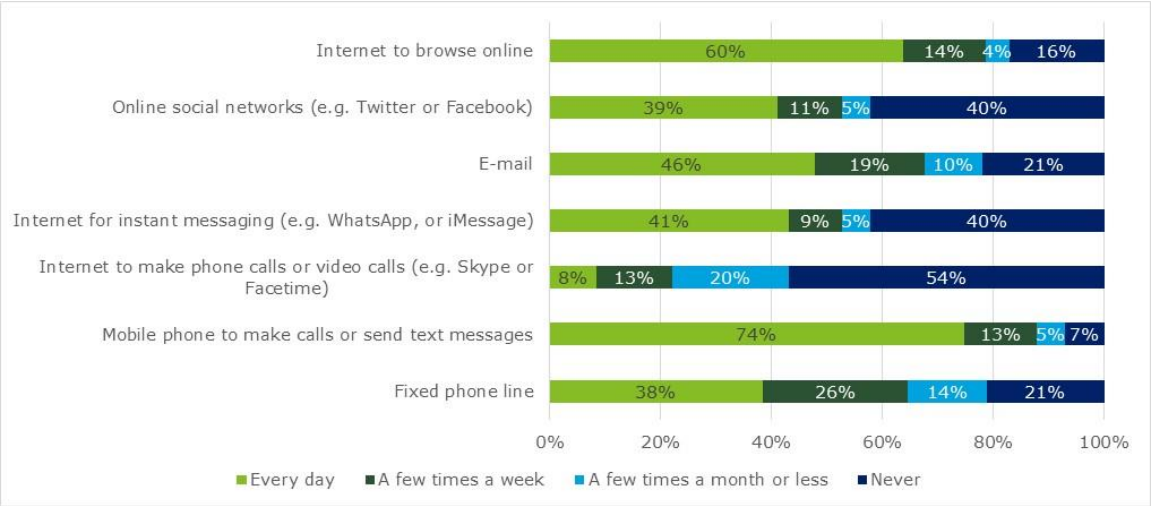
99 AU, FI, HU, IT, L, NL, RO and SV (European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071)).

100 CY, EL, IE and RO (European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071)).

101 AT, BG, CZ, DK, EE, ES, FI, HR, IT, LT, LU, LV, MT, NL, PT, SK and SV (European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071)).

102 BG, CZ, EE, ES, IT, LT, MT, NL, PT, SK and SV (European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071)).

103 European Commission Study carried out by ECORYS, TNO and others (2016), Study on future trends and business models in communication services, (SMART 2013/0019).



Source: 2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079)

Over-the-top providers**, which provide functionally equivalent communications services** over the Internet (e.g. Voice over IP, instant messaging) have become prominent in the field, supported by the Eurobarometer survey table above on the usage of these services, and they **are not covered by the current definition of ECS**. For instance, as highlighted above, the Eurobarometer on ePrivacy shows that a large part of consumers also uses OTT services every day that are not covered by the ePD:

- Email is used by 46% of consumers every day;
- OTTs for the purpose of instant messaging (e.g. WhatsApp) are used by 41% every day[104]; and
- Online social networks are used by 38% every day.

Considering actual traffic volumes, the use of OTT services has increased considerably: The OTT's share of overall messaging traffic has already increased from 8.31% (2010) to 66.96% (2013) and is projected to rise to 90% until 2020[105]. Conversely, the use of SMS continues to decrease in almost all EU MS since 2010, albeit at a different pace: In Finland and Germany. On the individual level, the average WhatsApp user is reported to send approximately 40 (while receiving around 80) messages per day as opposed to an estimated number of 4.5 SMS

[104] Interestingly, the Eurobarometer data shows that for instant messaging OTTs, two large groups of consumers seem to exist: Those that use instant messaging every day and those that never use it. The proportion of consumers that uses it a few times per week / month is comparatively small. It can be assumed that age is an important factor with regard to the take-up of such services. While younger generations use instant messaging every day, the majority of older consumers do not use it at all. Therefore, it can be expected that the share of consumers who use instant messaging on a daily basis will increase over the next years.

[105] DG for Internal Policies, "Over-the-Top players (OTTs), Study for the IMCO Committee", 2015, 31.

This ratio of approximately 1:10 for daily SMS versus OTTs messages is likely to be much higher in practice, due to the reported parallel use of multiple messaging apps[106]..

Given the strong penetration of OTT services in the electronic communications market[107], the fact that the rules only apply to traditional ECS providers and not to these new players strongly questions the effectiveness of the rule as **such situation deprives citizens from the very protection the Directive intends to provide**.

While the processing of personal data in deploying these services is covered under the GDPR (rights of data subjects, principles relating to processing of data, etc.), the specific, additional, protection provided by the ePD, which in the case of confidentiality of communications requires the consent of both communicating parties to interfere in the content of communications, is not applicable to OTTs.

This situation also raises concerns as to the fact that the current legal framework has resulted in **an uneven level playing field** among different market players due to market and technological changes. The public consultation shows that 76% of citizens and civil society and public bodies find that **OTTs should provide the same level of protection when they provide functionally equivalent communication services as ECS providers**, while only very few think that this should not be the case (5.6%). Industry is more divided as 42% does not want the scope to be broadened while 36% does[108]. This may be explained by the fact that OTT providers replied and belong to industry. Nevertheless, extension of the rules to cover OTT services is the second priority of industry (29%) after the option of not keeping any provision anymore.

The **need to guarantee confidentiality of communications regardless of the technology used** is also confirmed by the Eurobarometer survey on e-Privacy:

> More than **nine in ten** (92%) say it is **important** that the **confidentiality of their e-mails and online instant messaging is guaranteed**.
>
> ***Source*:** *2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079)*

The Article 29 Working Party[109], BEREC and the EDPS[110] also support **an extension of the scope of Articles 5.1, 6 and 9** to cover at least OTTs.

Wi-Fi tracking is another gap in the protection guaranteed by the ePD. When a Wi-Fi enabled device is switched on, it continually broadcasts unique identifiers called MAC (Media Access Control) addresses. **WiFi (and in a comparable way Bluetooth) tracking** may be used to

---

106 European Commission Study carried out by ECORYS, TNO and others (2016), Study on future trends and business models in communication services, (SMART 2013/0019), p. 42.

107 European Commission Study carried out by ECORYS, TNO and others (2016), Study on future trends and business models in communication services, (SMART 2013/0019), p. 54, 56, 60.

108 Question 17 of the public consultation.

109 Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240 adopted 29.07.2016.

110 EDPS opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 22.07.2016.

count people, to track and observe their movements within the area covered by a private network, such as airports or shopping malls. This includes the trajectories they follow as well as the time they spend at certain locations.[111] It is not clear in all MS whether the current ePD protects the information emitted from the devices, such as MAC addresses. Similarly, it remains unclear to which extent the **electronic communications** of the **Internet of Things[112] ("IoT")** is covered by the ePD.

Finally, the effectiveness of the rules on confidentiality of communications was also affected by the **fragmentation generated by the competence of Member States to derogate to these rules**. Indeed, Article 15 of the e-Privacy Directive sets out rules that allow national rules to be created to restrict the rights and obligations provided for under the general rules. This means that rules can be set, for example, forcing electronic communications service providers to retain data. This can be done for the purposes of *"safeguard(ing) national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communications system*"[113]. It must be "necessary, appropriate and proportionate" and must comply with the EU Charter (e.g. interference with privacy rights must be "strictly necessary").

To sum up, the effectiveness of Article 5.1, 6 and 9 has been hindered by the problems described above.

6.3.3. Coherence

Under this criterion it is relevant to assess the extent to which the principle of confidentiality of communications is coherent with the GDPR, meaning whether the protections provided by Article 5.1, 6 and 9 are also provided by the GDPR, causing a possible overlap.

Article 7 of the EU Charter specifically protects the *confidentiality of communications*. This is separate from Article 8 of the EU Charter which protects *personal data*. The rules on confidentiality of electronic communications are only enshrined at EU level in the ePD.

The GDPR contains a number of obligations upon data controllers and processors and rights of data subjects to ensure appropriate confidentiality, integrity and security of *personal data* under the principles of processing personal data (Article 5.1.f)[114], and in the specific security

---

[111] See, e.g., Information Commissioner's Office, *Wi-Fi location analytics*, February 2016: https://ico.org.uk/media/for-organisations/documents/1560691/wi-fi-location-analytics-guidance.pdf; Rice S., *Be wary of public Wi-Fi* (ICO Blog), September 2015, https://iconewsblog.wordpress.com/2015/09/25/be-wary-of-public-wi-fi/; Korolov M., IEEE group recommends random MAC addresses for Wi-Fi security, http://www.csoonline.com/article/2945044/cyber-attacks-espionage/ieee-groups-recommends-random-mac-addresses-for-wi-fi-security.html; Hill S., *How Dangerous is Public Wi-Fi? We Ask an Expert*, http://arstechnica.com/tech-policy/2016/06/advertiser-that-tracked-100-million-phone-users-without-consent-pays-950000/.

[112] Based on existing communication technologies like the Internet, the IoT represents the next step towards digitisation where all objects and people can be interconnected through communication networks, in and across private, public and industrial spaces, and report about their status and/or about the status of the surrounding environment (Commission SWD(2016) 110/2 Advancing the Internet of Things in Europe, p. 6).

[113] European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071).

[114] This principle is referred to as the principle of 'integrity and confidentiality', although only security obligations are mentioned in Article 5.1.f.

provision (Article 32 of the GDPR). The provisions of the GDPR seek to update, strengthen and modernise the Data Protection Directive. While the DPD and GDPR rules mentioned above are extremely relevant towards ensuring that personal data is kept secure, these rules **do not regulate explicitly the principle of confidentiality** of communications and related traffic data as laid down in Article 5. Therefore it is important to stress that the **GDPR does not specifically cover** the right to confidentiality of *communications*.

In its opinion, the REFIT platform recommends that the two pieces of legislation are fully aligned and that the provisions ensuring confidentiality of communications of the ePD are revised to ensure that they are fit for the digital age and the new technology reality.

Regarding the specific rules on traffic and location data, by requiring consent for the processing of these data, the ePD offers a single legal basis to permit processing of personal data. The GDPR, at least potentially, allows other legal grounds, such as legitimate interests, performance of a contract, or the data subject's vital interest. Furthermore, the ePD also limits the validity of consent to the duration necessary for such services and the data must be used for the 'value added services' only. Furthermore, unless the individual has consented, the data must be anonymised or deleted after the period during which the bill may be lawfully challenged or the payment pursued.

The above leads to the conclusion that the ePD rules on confidentiality of communications and related traffic data are coherent with the GDPR.

6.3.4. Efficiency

Under this criterion it is important to assess whether the costs involved in fulfilling the confidentiality requirements are proportionate to the benefits achieved. According to the study SMART 2016/0080, there is **scarce information as to the cost of compliance with the confidentiality of communications rules**, partly due to the fact that these rules had to be applied as of 1997 and they appear to have been amortised by now.

The proportionality of these costs was addressed in the public consultation. A proportion of citizens and civil society (57.1%) think that the cost of compliance is proportional to the objectives of the ePrivacy Directive, while a majority of industry players (65.3%) report disproportionate compliance costs. A majority of public bodies (72.7%) believes that the costs of compliance are in line with the objectives pursued.

Evidence collected by the study SMART 2016/0080[115] shows that rather than compliance costs, the costs incurred by ECSs appear rather as **lost business opportunities**[116], given that the ePD places limitations on the re-use of traffic data for purposes that are not related to the

[115] European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080).

[116] In interviews and in an online survey with businesses conducted within the scope of the European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080), several stakeholders indicated that there are no significant on-going compliance costs or administrative burden in relation to these provisions. However, some stakeholders indicated that there are **opportunity costs** as the provisions render certain business models invalid. For example, telecom providers indicated that ECS lose out on potential business activities and opportunities in possible Big Data services, in particular compared to providers of OTTs.

conveyance of communications, whereas functionally equivalent OTTs remain out of the scope of such rules[117].

In the public consultation most consumers believe that the price of compliance is justified in order to reach the objectives of confidentiality of the ePD.

6.3.5. EU added value

The rules on confidentiality of communications aim at ensuring the right to confidentiality of communications across the EU, by introducing harmonised standards. It can be argued that this cannot be achieved by Member States alone, as communications are not bound by borders (in particular within the internal market) and Member States' standards on this varied before the introduction of the ePD. The EU added value also lays in the **harmonisation of concepts and rules** on confidentiality of electronic communications, traffic and location data.

This EU added value of the rules on confidentiality of communications is confirmed by citizens and civil society (90%) and Member States and public authorities (90%) responding to the public consultation, while overall two thirds of respondents recognise this EU added value[118]. These views are shared by Article 29 Working Party, EDPS and BEREC. Conversely, a vast majority of industry does not agree to the necessity to have rules on confidentiality of communications at EU level (63.34%). Although in August 2016, ETNO, an association representing Europe's leading telecom operators, published a report which stated that *'privacy related provision of the ePrivacy Directive, i.e. the article on confidentiality of communications, may still be relevant today'*[119].

KEY FINDINGS:

Confidentiality of communications is only ensured at EU level by the ePD, which key purpose is to **specifically spell out** the fundamental right to private life, correspondence and communications enshrined in **Article 7 of the EU Charter**. The relevance and EU added value of the rules on confidentiality primarily lay in their goal to afford an **equivalent level of protection** and confidentiality of the electronic communications throughout the EU. **Specific rules ensuring confidentiality of communications are all the more needed** according to citizens, civil society and public bodies in the light of technological changes and growing risks posed by online tracking.

With regards to traffic/location data of electronic communications, the evaluation confirmed its high degree of sensitivity, given that such data may allow very precise conclusions to be drawn concerning the private lives of persons involved. This is repeatedly stressed in recent rulings of the EU Court. Hence, Article 29 Working Party, the EDPS and BEREC have recommended to **keep the rules on confidentiality** and to **regulate any processing of traffic and location data within the ePD**. All of them recommend extending its scope to OTTs providing functionally equivalent services. It is argued that new technologies **would allow**

[117] See EC synopsis report on the Public Consultation, p. 8.

[118] Question 5 to the public consultation.

[119] Study on the revision of the ePrivacy Directive – ETNO, August 2016.

ECS to analyse network traffic in real time causing greater threats to privacy and confidentiality of communications.

Furthermore, the rules are fully aligned with the GDPR, and constitute a complement to it. However, the assessment of the ePD has shown that it **has not been fully effective in ensuring the protection of privacy and electronic communications in the EU.** This is due to a series of problems and flaws in the wording and implementation of Article 5.1 and 5.2, 6 and 9 including their limited scope of application.

Compliance costs faced by companies appear negligible as the costs have already been amortised.

6.4. Confidentiality of information stored in terminal equipment

Article 5.3 of the ePD aims to ensure the **confidentiality of information stored on the users' terminal** equipment (i.e. computers, smartphones), in particular by increasing awareness and empowering users.

Under Article 5.3, Member States are required to ensure that "*the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent…* 'Information' includes technologies and applications such as cookies, web-beacons or spyware but also contact lists, pictures, content of emails, etc. This requirement stems from the revision of the ePD in 2009.

6.4.1. Relevance

Under this criterion it is necessary to assess whether the specific objectives of Article 5.3 are still relevant. Information transferred through electronic communications networks is increasingly stored in terminal equipment. This would normally include the content of emails, SMS, pictures, contact lists, videos, etc.

The relevance of this article is evident if one takes into account that the more information is stored in devices, the higher the sensitivity of such information is and the greater the damaging consequences for individuals if such information were released without their consent.

This is confirmed both in the public consultation and in the Eurobarometer survey on e-Privacy, where a large majority of citizens considered that **requesting their consent** before accessing or storing information on their terminal equipment **remains valid, given the sensitivity of the information stored** on users' terminal equipment (e.g. pictures, contact list, etc.).

More specifically, **more than nine in ten** respondents to the Eurobarometer survey on e-Privacy **(92%)** considered **important that their permission be asked** before:

- their personal information (e.g. photos, calendar, contacts) on their computer, smartphone or tablet can be accessed;
- tools are used to monitor their activities online (such as cookies).

***Source*:** *2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079)*

In addition to privacy issues, protecting the information in devices is relevant as a measure to minimise information theft and subsequent abuse of such information, for example to engage in theft (stealing from bank accounts) and identity theft.

At the same time, the **need for a more flexible consent rule** was also supported by the Eurobarometer survey on e-Privacy and by a **majority of the respondents** to the public consultation.

However the relevance of this provision is partially diminished by the fact that it is both over-inclusive with a scope that covers a non-privacy invasive practice, namely first party analytic cookies. For example, some stakeholders have argued that the provision should **not cover technologies that are not privacy invasive**. In its opinion, the **REFIT Platform** expressed a similar view and stressed the need to review the rules to allow greater flexibility for those tools that do not pose any privacy risks.

For example, respondents to the Eurobarometer survey on e-Privacy are globally in favour of a request from a website to access their information, the first time or each time they visit the website (while 39% think this should happen each time they enter the website). Also in all but one country, the absolute majority of respondents to the Eurobarometer survey totally agree the **default browser settings should stop their information from being shared**.

6.4.2. Effectiveness

In assessing the effectiveness of Article 5.3 we note that this provision is applicable not only to cookies but also to any other technology used to store or gain access to information on individuals' technical equipment (spyware, malware, etc.)[120].

However, its effectiveness has been hindered because it is unclear whether it covers new techniques where identifiers emitted by the device are used for tracking purposes. For example, there is at least a lack of clarity relating to the coverage of some techniques, hindering its effectiveness: **Wi-Fi tracking**, and device fingerprinting[121]. These techniques must comply with the GDPR when the processing involves personal data; however, it is unclear whether Article 5.3 would also apply[122].

In its opinion, the REFIT Platform recommended the elaboration of rules that are future proof and support privacy-friendly technologies (see Annex III). It also points out that the GDPR rules remain applicable if the information stored or collected from the device entails the processing of personal data. Therefore, the user or the subscriber should be informed about the identity of the entity that wishes to store information or gain access to information that is already stored in his terminal equipment and about the purposes of the processing. Moreover, users should be provided with any information relating to the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, and the existence of their right of access.

---

120 Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, adopted 22.06.2010.

121 The Article 29 Working Party has recognised the applicability of Article 5.3 to device fingerprinting in its opinion 9/2014 on device fingerprinting (25 November 2014).

122 *Ibid*, p. 1.

According to the study SMART 2013/0071 on the ePD[123], cookies that are exclusively used for website usage statistics ("**first party analytics cookies**") should not require consent, as recommended by the Article 29 Working Party[124].

To implement the obligation of Article 5.3, websites have set up cookie banners in their websites, often with boxes, which users have to click to agree to receive cookies. The fact that users are given a choice whether to allow access to information stored on their terminal equipment, theoretically empowers users. However, **several issues hindering the effectiveness of this mechanism** have been identified. One point of criticism relates to the **transparency of the consent mechanism.** More specifically, there are often no transparent tools to withdraw or manage consent. Information notices are not granular and sufficiently clear for average users. Indeed, for some users it may not be clear that giving mere consent can provide a justification to comprehensively track their behaviour in the online environment ("profiling")[125], giving users a false sense of protection[126]. There is a need for more clarity about these practices.

As there is a widespread use by websites of cookies[127], this means that consent is required for a very large number of websites. As a result, citizens are constantly exposed to requests to give consent, **causing consent fatigue,** frustration, while affecting negatively their Internet experience. From this perspective, the method of using banners to which users are requested to click to accept cookies appears ineffective. Alternatively, more streamlined procedures, for example expressing consent through browser settings, appear as better options.

Statistics on the type of cookies actually used

The 2014 "Cookie Sweep" analysis initiated by the Article 29 Working Party and carried out in eight Member States[128] found that **the majority of the cookies are persistent third-party cookies**. In the Cookie Sweep, 16555 cookies were recorded on 478 sites, 70% of which were third-party cookies. 86% were persistent cookies and 14% were session cookies. In addition, it was found that 74 out of 474 websites only used first party cookies. In addition, 15 out of 474 only used session cookies (first and third party).

Source: Deloitte

123 European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071).

124 Article 29 Working Party, Opinion 4/2012 cookie consent exemption, 7.07.2012.

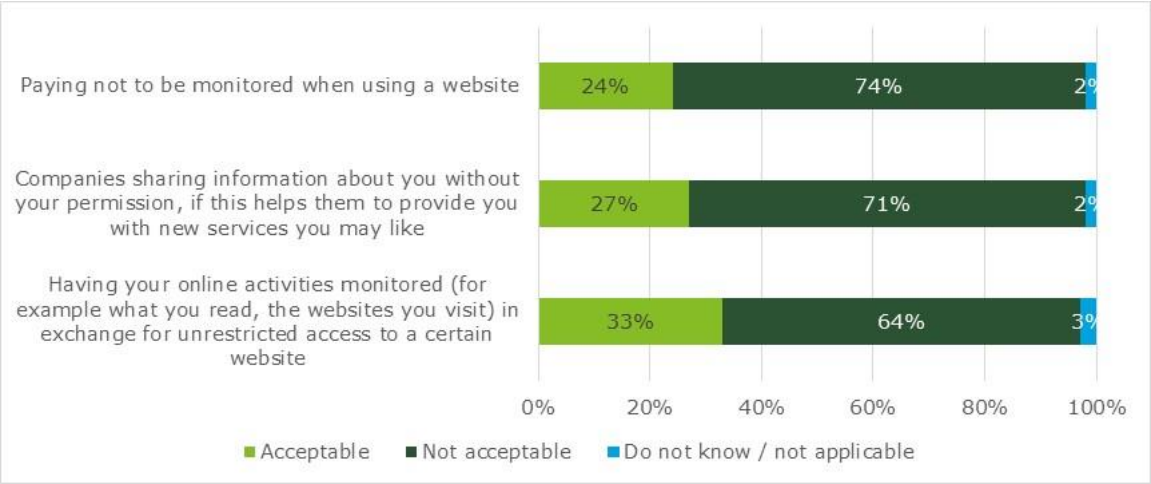
125 *Ibid*, p. 13.

126 *Ibid*. p. 8.

127 European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080) estimates, according to available evidence, that the share of websites in the EU using cookies is of 50% (medium scenario), with 55% (maximum scenario) and 45% (minimum scenario).

128 CZ, DK, FR, GR, NL, SI, ES, UK.

Furthermore, some allege that Article 5.3 does not ensure that users have a real choice when it comes to cookies as most of the time they are constrained to consent to cookies if they want to access the content of websites (so called "cookie wall" practice). This is confirmed by **research that has shown that when confronted to a 'take it or leave it' approach, most users will end-up consenting**[129]. A laboratory test conducted by the JRC on cookie banners has shown that whereas with a simple banner that allows entering the website without accepting cookies only 57% of the participants accepted cookies; almost 100% users gave their consent when presented with a 'take it or leave it' approach[130]. In this respect, the results of the public consultation are also relevant, while reflecting a disparity of views. Indeed, a **great majority of citizens, civil society and public bodies** replying to the public consultation agreed that information service providers **should not have the right to prevent access** to their non-subscription based services in case they refuse the storing of identifiers in their terminal equipment. On the other hand, a great majority of industry did not agree with this option, arguing that this would contradict the freedom to trade[131]. These results are confirmed by the Eurobarometer survey on e-Privacy according to which a strong majority of respondents **does <u>not</u> consider acceptable** to have their online activities monitored (for example what they read, the websites they visit) in exchange for unrestricted access to a certain website.



Source: 2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079).

A technical solution envisaged to address some of the inefficiencies related to consent through banners consists in enabling individuals to consent through browser settings. To this end, browsers should be configured to enable consent as a true expression of the individual's will. The proposal to impose **privacy by default in browser settings** was strongly supported by **89%** of the respondents to the Eurobarometer survey on e-Privacy. The concept of privacy by

[129] To verify the existence of cookie wall, the 8 DPAs checked around 100 of the most visited web in various Member States (BE, FR, DE, PT, PL, UK, IT). Only one web site could not be open but it was not clear that it was due to a cookie problem or a technical one.

[130] The lab experiment conducted over 602 participants in Valencia by JRC early 2016 sought to determine whether changes/clarifications to cookie banners affected: a) the decision to accept cookies, (b) the decision to learn more about a website's cookie policy, and (c) the amount of attention paid to the information in the cookie policy page.

[131] E.g. IAB Europe supplementary paper as contribution to the public consultation.

default in browser settings is similar to the data protection by design principle in the GDPR, which includes appropriate technical measures.

An Eurostat survey suggests that the rule may have had an overall **positive effect** on the level of **citizens' awareness** on the use of tracking techniques online[132].

Finally, the effectiveness of Article 5.3 is further hampered by the fact that the rule has been implemented and interpreted in different ways by various EU countries, thereby generating fragmentation in the legal framework.

Enforcement actions in some countries have proved limited, as highlighted by country profiles from Study 2013/071.

This problem has also been highlighted by the REFIT Platform, which adopted an opinion on the ePrivacy Directive in which it calls on the Commission to addresses national implementation problems and to facilitate the exchange of best practice amongst Member States.

6.4.3. EU added value

Whilst Member States can enact rules to ensure confidentiality and integrity of terminal equipment, such a protection could not be achieved in a uniform way in the absence of common EU rules.

The **EU added value** of the rule on confidentiality of terminal equipment derive from the fact that tracking techniques rising from the Internet, may often relate to companies located in another Member States. This common cross-border nature of navigating online supports the enactment of rules at EU level to better achieve the objective of ensuring online privacy. Uniformed rules within the EU are hence key to achieve the objective of protection. If this matter were solved at the national level, businesses would need to adjust their approach for every EU Member State and consumers would face a lack of transparency.

6.4.4. Efficiency

The last review of the ePD brought additional administrative and compliance costs for Information Society Providers (i.e. website providers) due to the transformation of a duty to inform users of tracking tools and give the possibility to opt-out into an obligation to collect prior users' consent.

In the public consultation as well as interviews and an online survey with businesses conducted in the context of one of the supporting studies to this REFIT evaluation[133], industry highlighted that the costs for compliance with Article 5.3 are the main cost factor regarding the ePrivacy Directive[134]. In terms of the cost of compliance for businesses, industry respondents to the public consultation reply that the costs are significant (62%) or moderate

---

[132] According to a **Eurostat survey of December 2015**, two third of European internet users (65%) know that cookies are being used by websites in order to trace their online activities; but, wide disparities remain according to the internet penetration, with Finland close to 80% of awareness, compared to Romania 30%.

[133] European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080).

[134] *Ibid 160*

(20.8%), while public authorities do not know (56%) or respond that they are moderate (17%).

An assessment of compliance costs[135] using quantitative and qualitative data concludes that the price per website to notify of the use of cookies and similar devices stored in users' terminal equipment is of 300 Euro, per year. It estimates that the website will require adaptations each year, which will amount to 300 Euro. Thus, it concludes that over a period of 3 years, a company would have to spend a total of 900 Euro[136]. This includes costs for legal advice, updates to privacy policies, and technical updates to websites and would be incurred once per website, i.e. at the time of the introduction of the new policy[137]. The study calculated that the overall cost for businesses operating in the EU a website using cookies amounted to approximately EUR 1.8 billion in 2015. However, this cost is projected to gradually decrease until 2030 to approximately EUR 1.4 billion per annum.

From the consumer perspective, the benefits of having such rules seem to be confirmed in particular by the Eurobarometer on ePrivacy. It is important to 82% of consumers that tools for monitoring their activities online (such as cookies) can only be used with their permission. In a similar vein, 89% of consumers think the default settings of their browser should stop the information stored on their terminal equipment from being shared.

The above costs indicates that there is scope for finding more efficient ways to comply with the objectives of the rule, protecting privacy and empowering individuals, in more cost efficient ways, such as, for example, centralised consent mechanisms through the browser.

6.4.5. Coherence

Article 5.3 is meant to protect the privacy of individuals extended to their terminal equipment. The *rationale* of the rule is based on the understanding that the terminal equipment is part of the private sphere of an individual, in the same way as his or her domicile and communications. Recital 24 of the ePD captures the *rationale* of this article by stating that *"terminal equipment of users (…) and any information stored on such equipment are part of the private sphere of these users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms*". This purpose has been recognised by Article 29 Working Party[138].

---

135 *Ibid 160*

136 The figure of 900 Euro of compliance costs needs to be understood as an average value across all size classes of businesses, across all industries, and across all Member States. It is only an average, i.e. not a median value or a fixed value that all businesses incur in any case. Quite naturally, differences exist between smaller and larger businesses, as well as between businesses in different industries and Member States – a Romanian start-up for instance has different costs than a global IT enterprise. This is due to the differences in their websites' complexity, as well as the operations behind administrating the respective website. Therefore, it is by no means a contradiction if stakeholders indicated that compliance costs would be significantly higher or lower than the 900 Euro.

137 European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080).

138 Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, adopted 22.06.2010.

Thus, Article 5.3 is not concerned about the protection of personal data *per se*, in fact, Article 5.3 applies independently of whether the information stored or accessed in the device is personal data.

If the information accessed is personal data, any subsequent use and processing of such personal data collected from the device, for example, to build profiles of individuals, will be governed by the Data Protection Directive and in the future by the GDPR. This means that all the rights and obligations contained in the GDPR such as the right to have the data rectified (Article 16) or the right to erasure (Article 17) of the GDPR will apply to such further processing of personal data[139].

In practice this means that the role of Article 5.3 is to empower users *vis-à-vis* their private sphere, giving them the possibility to decide over the content and access to their device. The goal of Article 5.3 is limited to this specific purpose. Then, the GDPR complements the protection offered by Article 5.3 if/when the data collected from the device is personal data. The interplay between the applications of both set of rules is illustrated in various opinions of Article 29 Working Party[140].

In this respect, it should be stressed that the adoption of the GDPR will have an impact on the definition of consent under the ePD, and thus on Article 5.3. Under the GDPR consent requires **a clear affirmative action establishing freely given, specific, informed and unambiguous indication of the data subject's agreement** to the processing of personal data relating to him or her, such as by a written statement, including by electronic means (Article 4.11 of the GDPR). Recital 32 of the GDPR illustrates the meaning of consent[141].

To conclude, **it follows from the above that Article 5.3 rule is fully coherent with the rules of the GDPR.**

KEY FINDINGS:

We conclude that the **objective pursued by the rule remains relevant** given the sensitive information stored on users' own device and need to protect them from being tracked online.

However, the effectiveness of Article 5.3 is hindered due to various reasons, which include its scope and the challenges related to make consent truly effective. **Critics were made on the**

[139] Recital 30 of the GDPR explicitly recognises the possibility to associate cookie identifiers with personal data by saying: '*Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses,* ***cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them****".*

[140] Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, adopted 22.06.2010; Article 29 Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, adopted 16.09.2014; Article 29 Working Party, Opinion 02/2013 on apps on smart devices, adopted on 27.02.2013.

[141] "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent".*

ineffectiveness of consent as consumers may feel compelled to accept cookies if, not doing so, means that they are not able to access the web site. From this perspective, some have raised the question of whether consent is freely given because of the 'take it or leave it approach', where refusing cookies would prevent the access to a certain website**. Furthermore, in many cases, the information given regarding online tracking is, in the view of some stakeholders, not considered to be sufficiently clear.** Last, **the method of using banners is perceived by some as detrimental to an optimal browsing experience**.

The coherent application of Article 5.3 and the rules of the Data Protection Directive have been illustrated in many opinions of Article 29 Working Party. As explained above, Article 5.3 complements the GDPR in a fully consistent manner.

6.5. Protection against unsolicited communications (so called "spam")

Article 13 seeks to give individuals a right not to be disturbed in their privacy by unsolicited commercial communications. This is increasingly important as the costs of making such communications decreases and the technology is more capable of delivering new, more privacy invasive ways, to reach individuals.

To this end, the ePD prohibits 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**")[142].

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). For example, this is the case regarding person to person telephone communications.

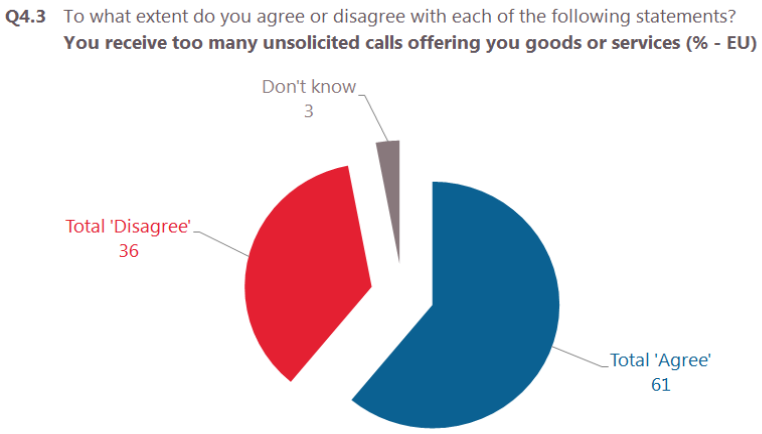
The ePD also **protects legal persons, i.e. companies, against unsolicited commercial communications** but leaves it to Member States to define the legitimate protection they deserve (i.e. whether opt-in or opt-out regime).

6.5.1. Relevance of the current rules

While technology advances and is increasingly capable of reaching users at very low costs, for example, by instant messaging or VoIP calls, users are becoming more and more distressed by unsolicited commercial communications, including emails, banners, newsfeeds, voice calls, etc. Hence, the rules limiting the ability to contact users for marketing purposes increase in relevance.

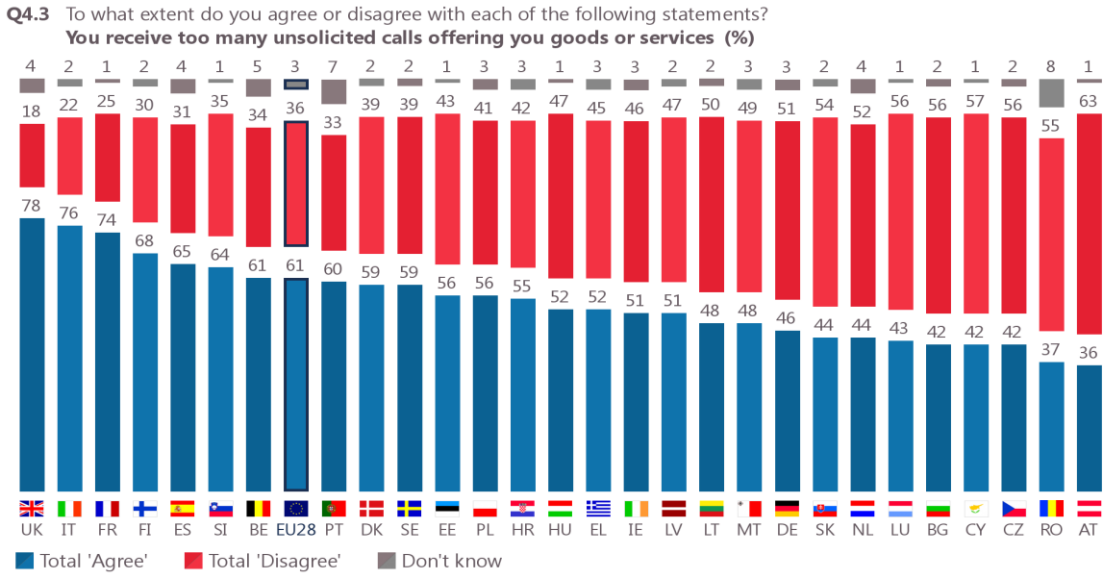
[142] The protection applicable to electronic e-mails is also applicable to SMSs, MMSs and other kinds of similar applications (Recital 67 of the Citizens' Rights Directive).

In the Eurobarometer survey on e-Privacy, just over six in ten respondents (61%) agree that they receive too many unsolicited calls offering them goods or services, while 36% disagree[143].



Base: respondents who use a fixed phone line or a mobile phone (N=26,241)

There is a reasonably large variation in opinion across the EU about unsolicited calls. Respondents in the UK (78%), Italy (76%) and France (74%) are the most likely to agree they receive too many unsolicited calls offering them goods or services. This compares to 36% of respondents in Austria (where customers can opt-in to these calls).



Base: respondents who use a fixed phone line or a mobile phone (N=26,241)

In the public consultation, almost two thirds of respondents from civil society, citizens and public bodies (62%) **agree with the relevance of the rules** on unsolicited communications.

[143] Q4.3 To what extent do you agree or disagree with each of the following statements? You receive too many unsolicited calls offering you goods or services. Respondents were those who use a fixed line or a mobile phone.

Industry disagrees (63%) with the need to have specific rules and appears to favour horizontal opt-out rules applying to all communication channels.

The above confirms **the relevance of rules on unsolicited communications**, **yet the views of citizens and civil society as well as public bodies on the one hand and the industry on the other hand diverges on the type of protection that such rules should provide.**

6.5.2. Effectiveness

There is evidence showing that the current rules on unsolicited advertising have not proven completely effective in protecting citizens. Available statistics show that the number of nuisance calls in Europe is very high. UK authorities[144] estimates that UK consumers as a whole receive around 1.7 billion live sales calls, 1.5 billion silent calls, 940 million recorded sales messages, and 200 million abandoned calls[145]. Another recent survey conducted over a selected number of countries around the world showed that the number of people registering to do-not-call lists (referred to as Robinson lists) is constantly increasing[146].

The statistics of complaints in MS against unsolicited advertising (including all means) are impressive. As highlighted in Table 3, the German Bundesnetzsagentur has received around 60,000 complaints related to spam in 2013, i.e. more than twice as many as in 2012. The majority of these complaints (68%) concerned telephone spam. In the UK, 180,000 complaints reached the various competent authorities in 2014 against nuisance marketing calls and texts. For the 12-month period ending October 2015, the ICO received an average of 14,343 complaints monthly about nuisance calls.[147]In comparison with the other provisions of the ePD, most competent authorities received the highest number of complaints for Article 13. For example, the Greek DPA estimates that around 90% of all complaints received in relation to the ePD relate to Article 13.

Table 3 - Complaints by citizens concerning Article 13 by Member State and year

Member State	2010	2011	2012	2013	2014	2015
Belgium	170	284	453	289	316	218
Bulgaria	0	0	0	87	100	45
Croatia	N/A	N/A	N/A	0	0	0
Cyprus	660	465	251	332	122	128
France	Not available	Not available	Not available	1071	932	2057
Germany	55,778	35,829	24,063	59,018	60,953	72,099
Greece	87	118	229	193	211	117

144 Ofcom is the communications regulator in the UK.

145 ICO-OFCOM, Tackling Nuisance Calls and messages (December 2015): A survey conducted on UK customers revealed that more than four in five (86%) of participating UK adults reported experiencing unsolicited communications in the observed period. The majority of the calls (89%) were considered to be annoying by participants across all ages, socio-economic group and working status.

146 Step Change Debt Charity, Combating Nuisance Calls and Texts, by Claire Milne.

147 http://stakeholders.ofcom.org.uk/binaries/consultations/silentcalls/JAP_Update_Dec2015.pdf.

Member State	2010	2011	2012	2013	2014	2015
Ireland	231	253	606	204	176	104
Poland	Not available	Not available	Not available	Not available	Not available	91
Slovakia	128	91	132	288	155	95
Sweden	Not available	Not available	Not available	46	49	66
United Kingdom	Not available	Not available	79,018	199,376	175,248	166,663
Total	**57,054**	**37,040**	**104,752**	**260,904**	**238,262**	**241,683**

Source: Deloitte based on data made available by the competent authorities.

In the public consultation, Article 13 appears one of the three rules that the industry expressed (most) difficulties in understanding/implementing (see Table 4). In general terms, a significant number of stakeholders have expressed to have faced problems with this provision. As part of the EC's public consultation, almost half of the respondents indicated that they faced problems in applying or understanding the rules on unsolicited marketing communications. The share of those stating they faced problems is highest for citizens and civil society (55%). In the group belonging to the industry, slightly more respondents stated that they did not face problems (39%) compared to those who did face problems (37%).

Table 4– Extent to which respondents encountered problems in relation to the rules on unsolicited marketing communications, per stakeholder group

Stakeholder group	Yes	No	No opinion	Total nr. of responses
Industry	37,4%	38,8%	23,7%	139
Citizens & civil society	54,5%	28,1%	17,4%	178
Public bodies	44,4%	33,3%	22,2%	18
All replies	46,9%	32,8%	20,3%	335

Source: Deloitte based on EC public consultation.

The challenges identified include the following:

- ✓ The rules on unsolicited communications **give leeway to Member States** to decide whether legal persons are protected by an opt-in or opt-out regime (see Article 13.3, 13.5), **which have led to very different approaches across the EU** for unsolicited communications. As a result, the protection afforded to legal persons widely diverges among Member States. It is not fully clear if "direct marketing" encompasses as well political marketing or fundraising activities.

- ✓ The **rules differ widely according to the technology used**, which adds a layer of complexity and does not ensure legal certainty.

- ✓ There is **legal uncertainty** as to whether commercial communications received by users of a social medium (e.g. in their **News Feed page**) fall under the regime of new means of communications under Article 13.3 or whether such practices are covered by the opt-in regime applicable to e-mail under Article 13.1. In its opinion, the REFIT platform calls on the new rules to provide effective and appropriate protection when it comes to new means of online commercial communications, for instance social media.

- ✓ It is not fully clear if "direct marketing" encompasses as well political marketing or fundraising activities.

The table below provides for an overview of the regime for voice-to-voice unsolicited marketing calls to natural persons in the various Member States and shows that 10 countries provide for an opt-in regime whereas the remaining countries, at least in part, have chosen an opt-out regime (i.e. equivalent to a right to object to receiving these calls).

Table 5 - Overview opt-in or opt-out regime for voice-to-voice unsolicited marketing calls to natural persons used by Member States, in relation to the percentage of people agreeing to receive too many unsolicited marketing calls (*Sources: Eurobarometer on ePrivacy of 2016 and Deloitte study):*

Member State	Opt-out	Opt-in	% of people agreeing they receive too many unsolicited commercial calls (Eurobarometer)
United Kingdom	X		78%
France[148]	X	X	74%
Finland	X		68%
Italy	X		66%
Spain[149]	X	X	65%
Slovenia[150]	X		64%
Belgium	X		61%
Portugal		**X**	**60%**
Denmark[151]	X	X	59%
Sweden	X		59%
Estonia	X		56%
Poland	X		56%
Croatia	X		55%
Greece	X		52%
Hungary		**X**	**52%**
Ireland[152]	X	X	51%
Latvia		**X**	**51%**
Lithuania		**X**	**48%**
Malta	X		48%
Germany		**X**	**46%**
Netherlands	X		44%
Slovakia		**X**	**44%**
Luxembourg		**X**	**43%**
Bulgaria		**X**	**42%**
Cyprus		**X**	**42%**

148 Opt-out for person-to-person marketing calls to fixed lines, opt-in in respect of calls to mobile phones.

149 Opt-out for person-to-person marketing calls to fixed lines, opt-in in respect of calls to mobile phones.

150 The situation in Slovenia, following the provision of the Electronic Communications Act, is at the moment quite confused, but the law is currently being amended so that opt-out regime will be in place for both fixed and mobile telephony.

151 There are a few exceptions to the opt-in consent for consumers.

152 Opt-out for person-to-person marketing calls to fixed lines, opt-in in respect of calls to mobile phones.

Czech Republic	X		42%
Romania		**X**	**37%**
Austria		**X**	**36%**

In bold are the countries with only opt-in regimes in place

The percentages of citizens receiving too many unsolicited calls are particularly high in three large MS, such as the **UK**, **Italy** and **France** where it is on average around 75%, in which an opt-out regime applies.

NB. Such calls are partly under opt-in in France for voice-to-voice calls towards mobile phone.

***Source*:** *2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079)*

Citizens, consumers and civil society organisations believe that Member States should not be able to choose between an opt-in or an opt-out system for direct marking calls with human intervention directed towards individual citizens (72.3%) or for direct marketing to legal entities (67.7%). According to them, **Member States should be forced to apply the opt-in solution** for marketing calls to citizens (88%) and for legal entities 75%). Citizens and civil society believe that the opt-in system is by far a better option for all types of communications. They find that opt-out regimes do not function adequately, despite the fact that they have existed for a number of years.

Member States themselves and public authorities also agree that Member States should not be allowed to choose between an opt-in or an opt-out regime for marketing calls sent to individuals (73%) and legal entities (66%). They largely favour an opt-in for calls to individuals (87%). Industry is aligned with the fact that Member States should not be given the choice but would prefer an opt-out system (74%).

The above leads to the **conclusion that the effectiveness of the rules on unsolicited communications is affected by:**

- the lack of clarity of the provisions;
- the large discretion left to the Member States as to the choice between an opt-in and opt-out regime, (e.g. with regard to the protection afforded to voice-to-voice telephony);
- the distinction made according to the technology used (e.g. difference between Article 13.1 and 13.3).

6.5.3. EU added value

The rules under Article 13 seek to guarantee that natural and legal persons enjoy an equivalent level of protection across the EU. Having different rules in the Member States would lead to different degree of protection of citizens in the EU regarding commercial communications. The borderless nature related to the placing of commercial communications emphasizes the need for such harmonised rules.

The specific added value of unsolicited communications rules rely on the **intrusive impact of such communications over privacy** and the **economic burden caused to businesses** and lost productivity due to the reception of such communications.

6.5.4. Efficiency

The study SMART 2016/0080 reports that overall, **five of eleven businesses** indicated in the online survey that they **incurred significant costs** in relation to the provisions concerning

unsolicited communications. But three out of the five businesses stated that they would have implemented some of the measures in a similar fashion, also without the ePD in place.

As concerns the costs for businesses, according to Deloitte business survey, **five of eleven businesses** indicated in the online survey that they **incurred significant costs** in relation to the ePD's provisions concerning unsolicited communications. Article 13 was one of the three provisions that most businesses associated costs with.[153] In the public consultation, while no specific numbers were provided, it was indicated that costs related to adaptations in telemarketing procedures, e.g. initial costs to check opt-out registers (Robinson lists) the revision of lists, offering text-script on opt-out possibility and assistance in registering with related registers.

In addition to the compliance costs related to the direct implementation of the ePD, businesses contend that they incur in **opportunity costs**[154]. It was explained that unsolicited communication is in some ways the backbone of the entire industry in terms of marketing and sales. The necessity of prior consent by users in order to be contacted reduces potential business opportunities in marketing and sales. Furthermore, based on the high number of complaints received on these provisions, competent authorities have to dedicate substantial resources to this issue.

The study SMART 2016/0080 collected a limited number of quantitative information, on the basis of which quantitative calculations were developed[155]. Compliance costs related to Article 13 were calculated in association with the compliance costs related to Article 5.3, which amounted to 300 Euro per year, as clicking or unclicking an online box is a very common way to request consent for direct marketing. It concluded that a 25% should be added to the 300 annual costs, plus some additional expenses, making a total amount of **EUR 490** per year[156].

From the consumer perspective, the high level of complaint shows the high citizens/consumer interest in these rules.

6.5.5. Coherence

The rules of Article 13 of the ePD details under which conditions **citizens and legal persons** can be contacted through **electronic communications** (opt-in consent). It sets forth specific rules for fax, email and automated calling machines.

---

[153] After the rules on confidentiality of communications (six businesses) and the rules on traffic and location data (five businesses).

[154] In the business survey for European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080), all five businesses that indicated to have incurred costs in relation to Article 13 agreed that these costs included opportunity costs. This was also raised by several respondents to the public consultation as well as in interviews carried out for SMART 2016/0080.

[155] European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080).

[156] European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080).

As regards the overall internal coherence of Article 13, the divergence of the regimes[157] according to the technology used to make unsolicited communications is mostly pointed as incoherent by a large proportion of citizens and civil society responding to the Public Consultation (61.5%)[158].

The **GDPR regulates the legal grounds to process personal data**. It also clarifies that where personal data are processed for the purpose 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).

The ePD only covers the specific requirement that applies to ***the sending*** of commercial communications **by the electronic means outlined above** (fax, email and automated calling machines). The GDPR covers any processing of personal data, including for marketing purposes. Thus, if an email and a phone number are put together with other information in order to create a profile of an individual, this processing is covered by the GDPR. However, the sending of marketing material is covered by the ePD.

Thus, the GDPR and the rules on unsolicited communications of the ePrivacy Directive do not overlap but are fully complementary.

The **eCommerce Directive 2000/31/EC**[159] mainly **imposes informational requirements upon information society services** (e.g. to clearly display the marketing nature of emails and identity of the natural or legal person on whose behalf the commercial communication is made)[160]. The rules of the eCommerce Directive have not been updated and still refer to Directive 97/66/EEC. Nevertheless, the provisions of the eCommerce Directive are not incoherent with those of the ePrivacy Directive and mainly complement these rules.

The **Consumer Rights Directive** also provides for the need to ensure that consumers are adequately informed[161]. But it does not address the issue of unsolicited communications.

The above confirms that the **rules on unsolicited communications are coherent** with other EU legal instruments.

KEY FINDINGS:

The **relevance and EU added value** of having rules on unsolicited communications **have been clearly supported** by stakeholders, including a majority of the respondents to the public consultation as these rules pursue a very valid purpose of protecting citizens and businesses against invasive communications.

[157] Under Article 13.1 opt-in is imposed but under Article 13.3 Member States can choose to apply opt-in or opt-out.

[158] See Synopsis Report to the Public Consultation, p. 6.

[159] Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ.L.* 178, 17 July 2000, 1-16.

[160] Articles 6 and 7 of the eCommerce Directive.

[161] Directive 2001/83/EU of 25 October 2011 on Consumer Rights, OJEU, L304/64, 22.11.2011.

Article 13 has proven to be **coherent with other existing EU legal instruments**, including the newly adopted GDPR and eCommerce Directive and the costs of compliance proportionate to the objectives pursued.

Nevertheless, the effectiveness of the rules has not been optimal. Difficulties in the enforcement of such rules **and lack of legal clarity** have been shown, while Member States may choose **between an opt-out and an opt-in regime regarding voice-to-voice telemarketing calls.**

6.6. Other provisions ensuring users' privacy and the protection of subscribers' legitimate interests

The ePD provides for the right for subscribers to receive **non-itemised bills** (Article 7). 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. Hence, Article 7 recognises the right to non-itemised bills (i.e. not showing the complete numbers called).

The ePD also gives callers the **right to prevent the presentation of the calling-line identification** if they wish so to guarantee their anonymity (Article 8) exceptions apply when the provide may override the user choice (Article 10)[162]; while subscribers have the possibility to **stop automatic call forwarding** by a third party to their terminals (Article 11).

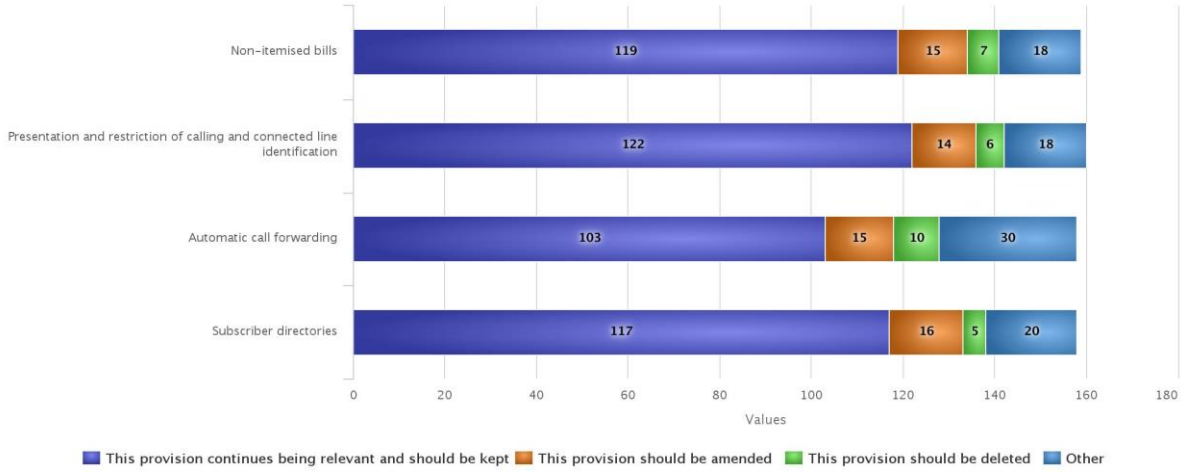
Finally pursuant to Article 12, subscribers must be given the opportunity to determine whether their personal data is **included in a public directory** (printed, electronic or obtainable through directory inquiry services). Furthermore, they must be informed about any further usage possibilities based on search functions embedded in electronic versions of the directory.

6.6.1. Relevance

As regards the relevance of the rules, a **wide range of stakeholders that responded to the public consultation indicated that all the above provisions continue to be relevant** and should be kept. Citizens, consumers, civil society, Member States and public authorities generally believe that the provisions on itemised billing (75%) calling line identification, (76%) automatic call forwarding (65%) and directories (74%) should be kept and are still relevant.

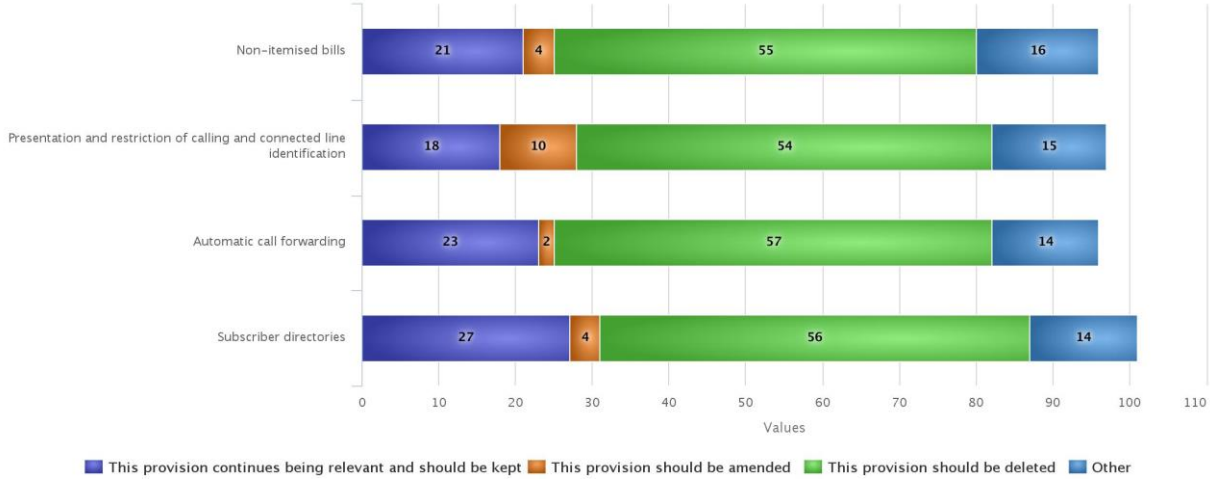
Give your views on the following aspects – **Citizens and civil society**:

[162] There are two cases when the caller decision to hide the presentation of the calling line identification may be overridden according to Article 10: (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.



The majority of the industry considers these provisions should not remain. In particular, the **traditional telecom providers**, currently under the obligation to comply with these provisions **called on the repeal of all these provisions**, arguing that they are not relevant anymore in the light of technological developments and highly competitive telecommunications market where operators would not be in a position to refuse a request related to the topic covered by the mentioned provisions[163]. The ECS and Electronic Communications Network ("**ECN**") providers argue that the rules should either be removed completely or moved from the e-Privacy Directive to other horizontal consumer protection instruments or elsewhere in the ECS/ECNs framework or in the citizens' rights directive. These rights, where relevant should be extended to all communications services, but it is not clear how this applies to non-voice services.

Give your view on the following aspects – **Industry**:



Specifically, the **provision on non-itemised bill** (not showing the complete numbers called on bills) **appears outdated for various reasons.** First, in view of the penetration of cost flat rates, itemised billing ceases to be relevant. Secondly, the same applies considering the increase of communications service providers that provide a calling service for free

163 ETNO "*Study on the revision of the ePrivacy Directive*"; August 2016, p. 35.

(especially among OTT functionally equivalent services relaying on the internet for providing voice calls). Last but not least, arguably, the increase of mobile subscriptions and the decrease in the use of fixed lines suggests an increase of individual subscriptions, diminishing (if not totally eliminating) the privacy risks. Still, some of the mobile subscriptions may relate to family packages[164].

The **automatic call forwarding provision** and **calling line identification** are seen as still relevant. However, there is scope for simplification of the automatic call forwarding rules. The EDPS sees this provision as a tool giving individuals the capacity to take action against those engaging in unsolicited communication in violation of applicable law[165]. Article 29 Working Party underlines the importance to keep this provision to ensure obedience of ECS providers with user's request to display or withhold CLI but suggests **updating the provision to ensure that identification cannot be spoofed or falsified**[166].

It should also be noted that **similar rules on calling line identification exist in many countries around the world**; such as for instance the United States where the Federal Communications Commission's[167] caller ID rules require telephone companies to make available at no cost to the user, simple and uniform per line blocking[168].

Some telecom providers have argued that it would be unlikely they would refuse to act against the nuisance which may be caused by automatic call forwarding by others, meaning that despite the absence of a legal obligation, operators could either act on the basis of contractual obligation or with the view to keep their customers satisfied. Furthermore, responses underlined that nowadays smart devices allow users to block callers, raising the question of whether there is a need for regulation.

On the other hand, while smartphones may have these functionalities, the exceptions when this choice may be overridden (emergency services) have to be implemented at network level by the ECS provider. Furthermore, as shown in the Eurobarometer survey on e-Privacy, there are still many Europeans using non-smart phones and also fixed lines, which often use terminal equipment that does not offer this functionality. This means that a great number of subscribers would not be able to reject calls with no identified number or block forwarded calls.

The particular relevance of the **subscriber directories** is stressed by the EDPS, which recommends maintaining the provision while extending its scope to include all kinds of

---

164 European Commission Study carried out by ECORYS, TNO and others (2016), Study on future trends and business models in communication services, (SMART 2013/0019).

165 EDPS opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 22.07.2016, p. 20.

166 Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240 adopted 19.07.2016, p. 21.

167 The Federal Communications Commission (FCC) regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the commission is the United States' primary authority for communications laws, regulation and technological innovation.

168 See FCC Consumer guide – protecting your privacy.

directory services[169].

In light of the above, it can be summarised that there are arguments pointing towards the following:

- The rules on **calling and connected line identification** and **subscribers directories as well as automatic call forwarding** are considered relevant despite the need of simplification and adapting them to technological changes in particular as **these rules complement the rules on unsolicited communications**;
- The rules on **itemised bills** may generally be considered outdated and not relevant anymore in the light of technological and market changes.

6.6.2. Effectiveness

Respondents to the public consultation **did not have particular difficulties in understanding the rules** on non-itemised billing, presentation and restrictions of calling line identification automatic call forwarding, subscribers' directory. These provisions were considered relatively clear[170].

The clarity of the rule on **non-itemised billing** (Article 7) seems to be confirmed by respondents to the EC's public consultation: only 19% of citizens and civil society and 16.3% of the industry indicated that they have faced problems in applying/understanding the rule[171]. However, **limited data exist as to whether this provision actually reached its objective** of ensuring privacy of subscribers.

As for the provision on **calling and connected line identification** (Article 8), no serious issues could be identified. Only few respondents to the public consultation reported to have faced problems in applying or understanding the rules on control over calling line identification, whereas almost half respondents stated that they did not face problems[172]. According to the competent authorities responding to Deloitte's online survey, this article functions rather well. When asked about the functioning of this provision, the majority of respondents indicated that Article 8 functions well (23.3%) or very well (13.3%). Similarly, when asked about problems in relation to this provision, few serious challenges are reported by the responding national competent authorities[173].

The results of the public consultation as to the effectiveness of the **automatic call forwarding** provision shows that although 44% of the respondents did not have an opinion on this, close to 70% of the respondents that had an opinion had not encountered any problems in applying / understanding the rules.

---

169 *Ibid* p. 150.

170 Less than 20% of the respondents expressed difficulties in understanding or applying these rules (Question 2 of the public consultation).

171 Question 2 of the public consultation.

172 It has to be noted in this regard that quite a high number of respondents (127) did not have an opinion in this regard.

173 SMART Study 20016/080, Final Report, p 152.

- *Industry:* Of the overall 63 respondents that had an opinion, 57% had not encountered any problems, while 43% answered in the affirmative;
- *Citizens and civil society organisations:* Of the overall 108 respondents that had an opinion, 72% stated that they had not encountered any problems, while 28% answered in the opposite;
- Only one of ten *public bodies* that had an opinion indicated that they had encountered problems.

Based on Deloitte online survey with businesses, the provision on automatic call forwarding was a problem for only 25% of respondents that indicated this particular provision is of practical relevance for them. According to the competent authorities responding to Deloitte's online survey, this article functions rather well. When asked about the functioning of the different provision, the majority of respondents indicated that Article 11 functions well (26.7%) or fair (20%). Similarly, the competent authorities did not point to any serious challenges as part of the online survey or interviews[174].

Finally, the majority of stakeholders across the different groups stated that they had not encountered any problems of understanding or applying **Article 12 on subscribers' directories**. According to Deloitte online survey with businesses, the Directive's provisions regarding directories of subscribers were a problem for one of six businesses that indicated this particular provision is of practical relevance for them, while the competent authorities responding to Deloitte's online survey, considered that this article functions rather well. Similarly, the majority of competent authorities indicated that there are only moderate challenges in relation to this provision[175].

In light of the above, it can be summarised that the mentioned rules (rules on itemised bills, calling and connected line identification, automatic call forwarding, and subscribers' directories) appear overall to have been effective in achieving their specific objective of protection.

6.6.3. EU added value

The **EU added value** of having uniformed rules on **calling and connected line identification** or **subscribers directories** lies in the fact that often unsolicited marketing calls may come from a person or company located in another Member States. Furthermore, it should be stressed that **subscribers' directories** are nowadays mostly available on the Internet, which increases the chances that unsolicited calls may come from a person or a company located in another Member State, relying on these directories to conduct direct marketing. The EU added value of these rules is confirmed by the public consultation with a majority of citizens, consumer and civil society organisations seeing an added value in having special uniformed rules on public directories (54%) and special rules on calling line identification (56%).

In this context, having rules defined at **EU level** in a unformed way on **calling and connected line identification** and **subscribers' directories** would greatly increase the chances of

[174] SMART Study 20016/080, Final Report, p 158.

[175] SMART Study 20016/080, Final Report, p 163.

ensuring effective rules that do not diverge from one Member State to the other, reducing as well compliance costs for companies.

6.6.4. Efficiency

The **transposition** of the above provisions was overall uniform in the Member States throughout the EU, with no important divergences[176].

The information available to the Commission on compliance costs for businesses related to these provisions remains limited. The significant costs involved in the initial implementation of these provisions have been offset over time. Some small recurrent costs exist but they appear negligible. The study SMART 2016/0080 reports that respondents to its survey asserted that the development of the technical solutions is already built in by default in the services.

As concerns the rule on **directories of subscribers**, it was pointed out in the public consultation that it involves significant information duties to subscribers. However, no information is available as concerns the magnitude of such costs.

From the consumer perspective, the public consultation has shown that **citizens seem to value these provisions with 75% supporting this rule; although the support is less obvious than for the rules on confidentiality of communications (90%) or unsolicited communications (78%)**. This may be due to the fact that some of these provisions are used in few occasions. For example, Article 10 is only relevant when people receive anonymous nuisance calls or when individuals call emergency services hiding their number.

6.6.5. Coherence

In the table below, the connection between the ePD and the GDPR as well as the Electronic Communications package and the Radio Equipment Directive is presented. For each relevant provision a brief summary is provided[177], using the following colour code:

- Grey: neutral relationship/no challenges nor positive aspects identified; and
- Yellow: potential challenges.

Comparison of the so called "consumer" provisions of the ePrivacy Directive with the similar provisions in the GDPR and Universal Service Directive and Radio Equipment Directive:

Provision in the ePD	Provision in the other instrument	Main findings
GDPR		
Itemised bills (Article 7)	- No specific provision in the GDPR	The ePD particularises a specific situation that is not otherwise regulated in the GDPR
Calling and connected line identification (Articles 8 and 10)	- No specific provision in the GDPR	The ePD particularises a specific situation that is not otherwise regulated in the GDPR.

[176] European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080).

[177] Only those instruments and provisions that a have connection to the ePD are listed.

Automatic call forwarding (Article 11)	- No specific provision in the GDPR	The ePD particularises a specific situation that is not otherwise regulated in the GDPR
Subscribers' directories (Article 12)	- Conditions for consent (Article 7) - Transparent information(Article 12), - Information when personal data collected from data subject (Article 13) - Information provided where personal data not obtained from data subject (Article 14) - Right to object (Article 21) and the right to be forgotten (Article 17)	Article 12 of the ePD provides for a more specific protection that in the GDPR. In addition, it protects the interests of legal persons. Under Article 6 of the GDPR consent would be one legal ground among others. However, the GDPR ensures that data subjects are informed when their data are processed (Articles 12, 13 and 14). It provides for a right to object and a right to be forgotten.
Electronic communications Package		
Universal Service Directive		
Itemised bills (Article 7)	- End users interests and rights (chapter IV) - Control of expenditure (Article 10 and Annex I) - Contracts (Article 20)	This provision seeks to ensure that privacy is protected when receiving itemised bill (a right not to show numbers called). It is closely related to consumer protection rules for electronic communications services set forth in the Universal Service Directive.
Calling and connected line identification (Articles 8 and 10)	- End users interests and rights (chapter IV) - Contracts (Article 20)	No specific challenges
Automatic call forwarding (Article 11)	- End users interests and rights (chapter IV) - Contracts (Article 20)	No specific challenges
Subscribers' directories (Article 12)	- Telephone directory enquiry services (Article 25)	Article 12 of the ePD and Article 25 of the U.S Directive do not overlap as they pursue different objectives: Article 12 ensures the privacy of users and subscribers of ECS (right to consent or to be aware of their introduction in directories), Article 25 seeks to ensure that telephone directories are available and that completion of ECS providers over the making available of telephone directories is protected.
Radio Equipment Directive		
Non-itemised bills (Article 7)	- No specific relevant provision	Neutral
Calling and connected line identification (Articles 8 and 10)	- Essential requirements (Article 3e)	According to Article 3 of the RED, **radio equipment** shall be constructed so as to ensure it incorporates safeguards to guarantee that the personal data and privacy of the user and of the subscriber are protected. The Commission shall be empowered to adopt delegated acts but only to specify which categories or classes of radio equipment are concerned. The delegated acts cannot specify which privacy safeguards should be enshrined. Article 8 and 10 set forth specific requirements which apply upon ECS providers, not upon the equipment itself. Article 10 sets forth exceptions when the choice made by the caller may be overridden. Theoretically it would be possible to use the RED to impose requirements upon radio equipment similar to those set forth by Article 8. This has been raised by some stakeholders. However, the exceptions to Article 8, overriding the choice made by the provider (e.g., calls to emergency services), must be done by the ECS provider. To illustrate this point: if a caller places an emergency call hiding his phone number, art 10 recognises the possibility for the emergency services to identify the caller (and eventually help him/here). A smartphone cannot identify

		unanimous calls. Only the ECS can identify the number and stop the nuisance calls, which is inherent to the provision of the ECS service. Moreover, even if theoretically the requirements of Art 8, could be imposed by RED, it would not affect terminal equipment that does not allow the use of radio frequency spectrum. For such type of equipment, it would not be possible to use the RED to impose Article 8 requirements. Therefore Article 3 of the RED does not overlap with Articles 8 and 10.
Automatic call forwarding (Article 11)	- Essential requirements (Article 3e)	According to Article 3 of the RED, radio equipment shall be constructed so as to ensure it incorporates safeguards to guarantee that the personal data and privacy of the user and of the subscriber are protected. The Commission shall be empowered to adopt delegated acts but only to specify which categories or classes of radio equipment are concerned. The delegated acts cannot specify which privacy safeguards should be enshrined. Recipients of forwarded calls must be able to stop such calls. If the calls are anonymous, the ECS can identify the number and stop the automatic call forwarding. This cannot be done by the smartphone. Thus, RED cannot be used to achieve the goal of Article 11. Therefore Article 3 of the RED does not overlap with Article 11.
Subscribers' directories (Article 12)	- No specific relevant provision	Neutral

In light of the above, most of the above rules appear to be coherent with other relevant EU instruments.

KEY FINDINGS:

It can be summarised from the information above that:

- The rules on **calling and connected line identification** and **subscribers directories** are considered to be relevant.

- The **rules on non-itemised bills would be considered as outdated** and not needed anymore in the light of technological and market changes.

The rules have functioned well and it is confirmed that they are fully coherent with other EU instruments.

7. CONCLUSIONS – KEY FINDINGS

The evaluation found that **the ePD general objectives** of ensuring (i) an *equivalent level of protection across the EU of the right to privacy and confidentiality* with respect to the processing of personal data in the electronic communications sector and (ii) ensuring *free movement of personal data and of terminal equipment* in the EU **remain relevant.**

Most of the specific provisions implementing these objectives are also relevant, including the principle of confidentiality of communications (**Article 5.1 5.2, 6 and 9),** the confidentiality of terminal equipment (**Article 5.3**), the rules on unsolicited commercial communications (**Article 13),** etc.

At the same time, **some of the provisions appear no longer needed** to attain these objectives, primarily due to changes in legislation and to some extent due to technological developments. In two particular cases, it is obvious that the ePD overlaps with the GDPR. This is the case of the security requirement and the obligation to notify personal data breaches (**Article 4.1, 4.1a**, **4.3 and 4.4)**. These obligations have basically the same content as the new security provisions of the GDPR and therefore **have become redundant**.

Moreover, the provisions on automatic call forwarding (**Article 11**) and the provisions on presentation and restriction of calling and connected line identification (**Article 8 and 10**) **may benefit from simplification** whereas the provision on non-itemised bills (**Article 7**) **appears to be out-of-date** in the light of technological and market developments; keeping it as a legal obligation would not fulfil any clear purpose.

The ePD has been **partially effective** in ensuring a satisfactory and coherent level of **privacy protection for citizens**, as well as ensuring an **adequate protection of legal persons.** This is because:

- The perceived limited scope of the rules on confidentiality of communications **(Article 5.1, 5.2, 6 and 9) which** cover traditional ECS providers and telecommunication companies, but do not apply to OTTs offering functionally equivalent services.

- The **limited transparency about cookies used for tracking** and **the shortcommings related to the common method used to seek consent – take it or leave banners--(Article 5.3)**. Additional measures to enhance transparency about tracking and how to control the browser to limit such tracking appear needed. Such measures could include requiring information at browser level and mandating default privacy settings.
- The **scope** of the provision under Article 5.3 was considered **both too large** (it should not include first party analytics) and **too narrow (it should include all tracking techniques).**
- **Rules on** unsolicited commercial communications (**Article 13**) **differ partially according to technology used** while they **leave leeway to Member States** to select between opt-in or opt-out requirements for a variety of communication channels, including voice-to voice telephony. The assessment shows scope to improve the current rules, including via provisions such as calling line identification and/or making the rules to enable blocking unwanted calls more effective.

As regards the **efficiency,** reliable and representative quantitative data has not been found. On the basis of the limited information gathered, it appears that most of the compliance costs experienced today relate to the rules on security, commercial communications and to the "cookie" consent provision. The **evaluation showed** scope to improve the efficiency of the cookie provision, for example, by centralising users' ability to consent through browsers or other applications.

The evaluation **confirmed the EU added value of the ePD**; indeed, as electronic communications, have a global reach, it is necessary to ensure harmonisation of national rules

and an equivalent level of protection across the whole EU. The evaluation further showed that **most of the ePD rules are coherent with other pieces of legislation**, mainly the GDPR, Framework Directive, Radio Equipment Directive, or eCommerce Directive. However, in some cases, **adjustments appear necessary to ensure consistency between the GDPR** and the ePrivacy rules. This includes the need to (i) **delete the security provisions** mentioned above and (ii) to introduce **more coherence as regards enforcement authorities** and their powers.

8. ANNEXES

1. **Annex I**: Procedural information concerning the process to prepare the evaluation including stakeholders consultations
2. **Annex II:** Stakeholder consultation, including synopsis report on the public consultation
3. **Annex III** on REFIT Platform opinion
4. **Annex IV:** Overview of the evolution of the electronic communications market
5. **Annex V**: REFIT analysis of coherence of the ePrivacy Directive with the GDPR
6. **Annex VI**: Competent national authorities to enforce the ePrivacy Directive implementing provisions (Articles 5, 6, 9 & 13)

Annex I: Procedural Information

Identification

This Staff Working Paper was prepared by Directorate H Digital Society, Trust and Cybersecurity' of Directorate General 'Communications Networks, Content and Technology'.

Organisation and chronology

Several other services of the Commission with a policy interest in the review of the ePrivacy Directive have been associated in the development of this analysis. The ePrivacy Inter-Service Steering Group ('ISSG') met for the first time on 25 February 2016 and discussed the draft public consultation on the evaluation and review of the ePrivacy Directive, which was launched on 12 April 2016. At that meeting a draft inception impact assessment on ePrivacy was also presented.

A second ePrivacy Inter-Service Steering Group meeting took place on 26 July 2016 to discuss a draft evaluation report and the problem definition of the IA. Comments were received by 29 July 2016.

A third ePrivacy Steering Group took place on 26 August 2016 to discuss the draft Impact Assessment as well as remaining comments to the revised draft REFIT evaluation report.

The ISSG, chaired by SG, DG CONNECT, was flanked by DG COMP, DG JUST, DG GROW, DG ECFIN, DG FISMA, DG TAXUD, DG TRADE, DG RTD, DG JRC, DG EMPL, DG EAC, DG HOME, DG ENV, LS, DG REGIO, DG HOME, DG ENER, DG MOVE, EUROSTAT, EPSC.

Regulatory Scrutiny Board

This staff working document was submitted, together with the Impact Assessment for the Review of the ePrivacy Directive, for discussion at the regulatory scrutiny board meeting of 28 September 2016.

Evidence

This evaluation took into account the following main inputs:

- The contributions to the public consultation on the evaluation and review of the ePrivacy Directive;
- Meetings and workshops with stakeholders, including a workshop with national authorities (April 19) and another one with all stakeholders (April 12);
- Targeted consultations with EU expert groups which led to the following contributions*:*
  - *Article 29 Working Party Opinion*[178]
  - *EDPS*[179]

[178] Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240 adopted 19.07.2016.

- *BEREC*[180]
- *ENISA*[181]
- *JRC*[182]
- *CPC network*[183]

- It also builds on two studies dedicated to the evaluation and review of the ePrivacy Directive:
  - *The first comprehensive study on the Directive, titled "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation"*[184] *(SMART 2013/071). The study covered Article 3 on scope, Article 5 on confidentiality of communications, Articles 6 and 9 respectively on traffic and on location data (other than traffic data); and Article 13 on commercial communications;*
  - *A second study entitled "Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector" (SMART 2016/80) was commissioned. The study covered the provisions not evaluated in the study SMART 2013/071 and helped the evidence gathering exercise*[185]*;*
- Other recent DG Connect studies in the area of electronic communications have been used where appropriate:
  - *Study on future trends and business models in communication services (SMART 2013/0019);*
- In addition to the review and other studies quoted above the following studies and surveys in the area of Data Protection and Online Privacy was considered:
  - *2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079);*
  - *2015 Eurobarometer survey (EB) 431 Data Protection;*
  - *2011 Eurobarometer survey (EB) 359 Data Protection and Electronic Identity in the EU;*

---

179 EDPS opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 22.07.2016.

180 BEREC response to the ePrivacy Questionnaire, 29.07.2016.

181 ENISA working paper on the review of the ePrivacy Directive - Article 4 – security of processing, July 2016; ENISA working paper on the review of the ePrivacy Directive – Article 5.3 – cookies and similar techniques, July 2016.

182 Informal inputs were requested from JRC on experience in lab with cookie banners and on technical aspects related to security.

183 The CPC network did not reply collegially but invited its members to reply to the ad hoc consultation. Repliers were received from Spain, Norway, Denmark and Romania.

184 European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071).

185 European Commission Study carried out by Deloitte (2016), Evaluation and review of Directive 2002/58 on privacy and the electronic communications sector (SMART 2016/0080).

- *Commission Staff Working Paper on Impact Assessment on the General Data Protection Regulation proposal, 25.01.2012, SEC 2012(72);*
- *The other relevant sources quoted in the document, ranging from academic papers to industry.*

- **Literature review of relevant reports.** This includes among others Opinions of Article 29 Working Party, Opinions of BEREC, Opinions of the Berlin Group on Telecommunications, Opinions of the European Data Protection Supervisor as well as reports and studies from the Industry[186], many sent in the context of the public consultation.

[186] E.g. EDPS Opinion for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC, 18 July 2008, C181/1 OJ; 2nd EDPS Opinion on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, 9 January 2009, C128/04; EDPS Opinion on net neutrality, traffic management and the protection of privacy and personal data 7 October 2011; Article 29 WP Opinion 1/2003 on the storage of traffic data for billing purposes of 29 January 2003; Article 29 WP Opinion 8/2006 on the review of the regulatory Framework for Electronic communications and Services, with focus on the ePrivacy Directive; Article 29 WP Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC of 27 February 2004; Article 29 Working Party, Opinion 2/2006 on privacy issues related to the provision of email screening services, WP 118 adopted 21.02.2006; Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, WP 171 adopted 22.06.2010; Article 29 Working Party, Opinion 13/2011 on Geolocation services on mobile devices, WP 185 adopted 16.05.2011; Article 29 Working Party, Opinion 04/2012 on Cookie Consent Exemption, WP 194 adopted 07.06.2012; Article 29 Working Party, Opinion 02/2013 on apps on smart devices, WP 202 adopted 27.02.2013; Article 29 Working Party, Working Document 02/2013 providing guidance on obtaining consent for cookies, WP 208 adopted 02.10.2013; Article 29 Working Party, Opinion 9/2014 on the application of Directive 2002/58/EC to device Fingerprinting, WP 224 adopted 25.11.2014; Article 29 Working Party, Report Cookie Sweep Combined Analysis, WP 229 adopted 03.02.2015; Berlin International Working Group on Data Protection in Telecommunications Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential of 15-16 April 2013; Norway Datalsynet THE GREAT DATA RACE How commercial utilisation of personal data challenges privacy; Report, November 2015; ENISA (June 2016) Working paper on the review of the ePrivacy Directive. Article 4 – Security of processing; Working Paper: Update on Privacy and Security Issues in Internet Telephony (VoIP) and Related Communication Technologies, 59th meeting, 24-25 April 2016, Oslo (Norway). DLA Piper, ETNO "*Study on the revision of the ePrivacy Directive"*; August 2016 and previous versions; VDAV study Quelle Ipso November 2015; CERRE, "Market Definition, Market Power and Regulatory Interaction in Electronic communications Markets", 2014, 15; European Commission Study carried out by ECORYS, TNO and others (2016), Study on future trends and business models in communication services, (SMART 2013/0019), p. 54, 56, 60; The Information Technology & Innovation Foundation, Daniel Castro and Alan McQuinn, "*The Economic Costs of the European Union's Cookie Notification Policy"*, November 2014 (US); Directorate-General for Internal Policies, "Over-the-Top players (OTTs), Study for the IMCO Committee", 2015.

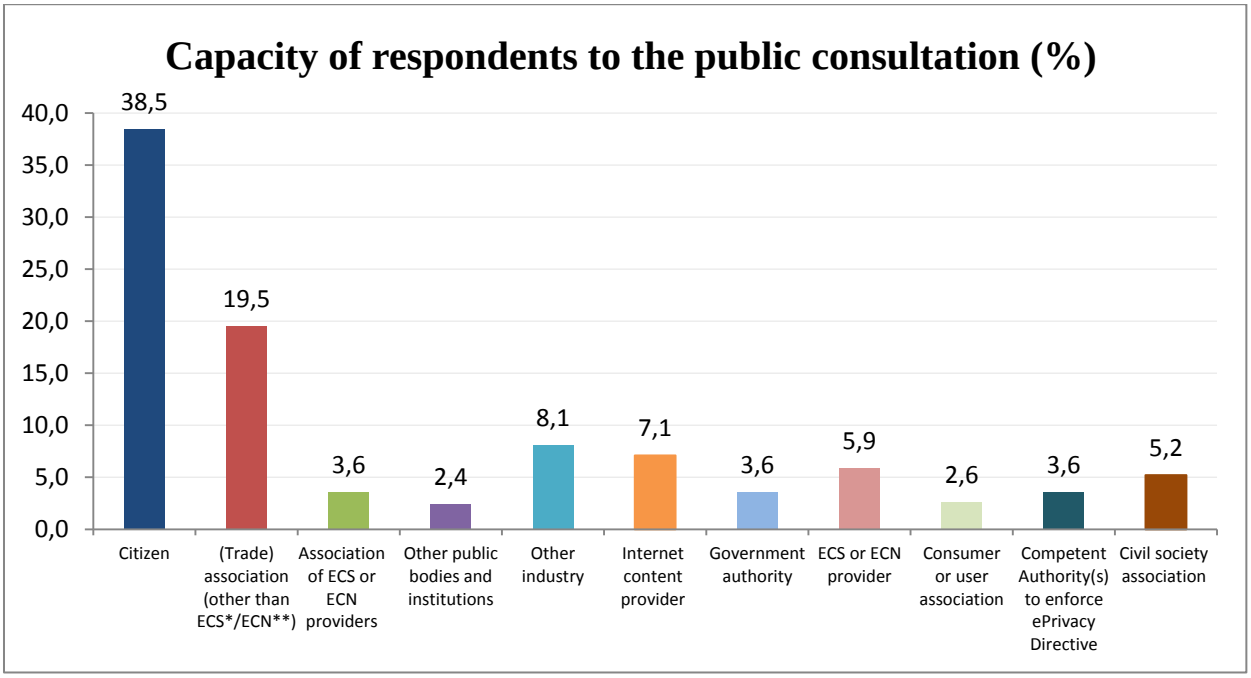
Annex II: Stakeholder Consultation on the evaluation and review of the ePrivacy Directive

I- Results of the public consultation – SYNOPSIS REPORT

The public consultation on the review of the ePrivacy Directive[187] ran from 12 April to 5 July 2016. The questions gathered input on: (1) the evaluation of the ePrivacy Directive; (2) the possible solutions for its revision. The results of the consultation will feed into the REFIT Evaluation (Regulatory Fitness and Performance Programme) and Impact Assessment Staff Working Documents in preparation of a legislative proposal.

OVERVIEW OF RESPONDENTS

The consultation received **421** replies from stakeholders in all Member States and outside the EU. The largest number came from Germany (25.9%), UK (14.3%), Belgium (10%) and France (7.1%). The Commission received **162** replies from citizens; **186** contributions from industry actors such as electronic communications, network providers, Internet content providers, trade associations and others; **40** replies from public authorities including competent authorities which enforce the ePrivacy Directive at national level; **33** contributions from consumer and civil society associations.



This report categorises the responses into the following groups:

[187] 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 (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37).

- **Citizens, consumer and civil society organisations**: citizens' answers were compared to those of civil society and consumer associations. As their positions did not differ, these categories are grouped together and referred to as "citizens, consumer and civil society organisations";
- **Public authorities**: government authorities, competent authorities enforcing the ePrivacy Directive, other public bodies and institutions;
- **Industry**: trade associations of electronic communication service ("**ECS**") or electronic communication network ("**ECN**") providers, ECS or ECN providers; trade association other than ECS/ECN, Internet content providers e.g. publishers, providers of digital platforms and service aggregators, broadcasters, advertisers, ad network providers, other industry. The position of ECS/ECN was compared to the other industries'. The report indicates where the positions differ.

As questions were optional, the percentages in the report refer to the amount of respondent per group that answered the particular question.

The contributions of stakeholders who consented to publication are available online.

This analysis does not represent the official position of the Commission and its services, and does not bind the Commission in any way.

- **REFIT EVALUATION OF THE EPRIVACY DIRECTIVE**
    - **EFFECTIVENESS OF THE ePRIVACY DIRECTIVE**

The first part of the questionnaire sought to assess whether the objectives of the ePrivacy Directive have been achieved.

The majority of citizens, consumer and civil society organisations (76.2%) do not think that the ePrivacy Directive has achieved the objective of ensuring full protection of privacy and confidentiality of communications across the EU, or has done so to a small extent. 58.3% of the ECN/ECS industry agrees with this statement while the industry at large (57.4%) thinks this objective has been achieved to a significant or moderate extent.

The most frequently cited reasons for this assessment are the following:

- The ePrivacy Directive has a limited scope of application since most of its rules do not apply to over-the-top services ("**OTTs**")[188];
- The principle of confidentiality should be included in an overarching, horizontal legal instrument instead of a sector specific one;
- Some of the rules allow for divergent national interpretation;
- The rule on cookies does not result in adequate protection for consumers: consumers are not offered a real choice to accept cookies and some new tracking applications are not captured;
- The ePrivacy Directive has been enforced in a fragmented manner.

[188] E.g. Voice over IP, instant messaging, web mail services.

Both categories of citizens, consumers and civil society organisations and industry are internally divided on the question whether the objectives of ensuring the free movement of personal data, equipment and services in the EU have been achieved.

42.3% of citizens, consumers and civil society organisations believe the objective has been achieved for the free movement of personal data. 36.3% do not believe that (or only to a little extent); the other respondents have no opinion (21.4%). The proportions are relatively similar on the free movement of equipment with 45.3% stating that the objective has been met and 30.9% disagreeing.

48.7% of industry representatives said that the objectives have been met for the free movement of personal data, while 37% disagree. For the free movement of equipment and services, 41.6% responded that the objective has been met while 26.2% disagree. On the question on the free movement of equipment around one third responded that they did not know.

The most frequently quoted reasons relate to differences in implementation (especially on cookies), hence high compliance costs, unfair competition between those subject to the rules and those that are not and divergent enforcement at national level.

Public authorities are more positive. The majority assesses that the Directive has significantly or moderately achieved its objectives in all areas: 74% for confidentiality, 68% for free movement of data; 62.5% for free movement of equipment and services.

- *MOST PROBLEMATIC RULES*

- **Citizens, consumer and civil society organisations** report that most difficulties stem from the application/understanding of the rules on:
    - unsolicited commercial communications (unclear application to non ECS, unclear mix of opt-in and opt-out system, 'spam continues');
    - confidentiality of electronic communications (unclear scope, OTT services are not covered, general distrust);
    - traffic and location data (unclear application of rules when data is both location and traffic data, scope only covers ECS whereas data is generated by apps and services which are not ECS);
    - notification of data breaches (ePrivacy Directive and General Data Protection Regulation ("**GDPR**")[189] are not aligned, different competent authorities).
- **Industry** reports most difficulties with the rules on:
    - confidentiality of communications (unclear scope of application; rules on cookies cause a disrupted Internet experience for users and are costly for businesses due to divergent interpretations throughout the Member States);
    - traffic and location data (overlap with the GDPR; even with consent of users, ECN/ECS industry cannot extract value from this type of data in the same way

[189] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

as operators not subject to the rules of the ePrivacy Directive; the rules hinder innovation and cause fragmented national implementation);
    - unsolicited commercial communications (fragmented situation at national level).
- More specifically, **ECS/ECN providers** report most difficulties with the rules on:
    - traffic and location data (overlap with the GDPR, call for same rules as applicable to OTTs, rules are too strict and hamper new business models);
    - notification of data breaches (inconsistent rules with the GDPR, lack of uniform interpretation across the EU);
    - and confidentiality of communications (scope of application).
- **Public authorities** report most difficulties with the rules on
    - processing of location and traffic data (unclear definitions, overlaps between both types of data);
    - unsolicited commercial communications (definition of direct marketing is controversial, unclear relationship with Electronic Commerce Directive).
        - *DIFFICULTIES LINKED TO DIFFERENT ENFORCEMENT AUTHORITIES*

Citizens, consumer and civil society organisations and industry agree that divergent interpretation of the rules is due to Member States giving enforcement powers to several authorities. However, a relevant percentage of public authorities hold different views.

The majority of citizens, consumer and civil society organisations believe that the significantly or moderately divergent interpretation of the rules in the EU (64.4%) and non-effective enforcement (61.9%) is due to some Member States allocating enforcement powers to several authorities. Of those that have reported significant and moderate problems, the main source of confusion is for citizens, the providers themselves, followed by the competent authorities.

Industry also believes that the allocation of enforcement powers to several authorities has caused divergent interpretation (65.4%) but is more divided on the effectiveness of enforcement, with 41.3% believing that this has significantly or moderately caused non-effective enforcement. Industry notes that companies are the main party affected by the situation, followed by citizens and the authorities. A larger majority of ECN/ECS believes that attribution of enforcement powers to several authorities has caused divergent interpretation (83%) and non-effective enforcement (63.8%).

Public authorities are more optimistic: 36.3% believe that the allocation of enforcement powers to several authorities has caused divergent interpretations, 47.8% consider that it has caused non-effective enforcement to a significant or moderate extent. This category believes that it is a source of confusion mostly for citizens, followed by industry.

- **RELEVANCE OF THE ePRIVACY DIRECTIVE**

Given the recent adoption of the GDPR, the questions sought to assess the relevance of the objectives of the ePrivacy Directive and its articles, taking into account technological, social and legal developments.

- *PERTINENCE OF EU SECTOR SPECIFIC RULES*

The majority of citizens, consumer and civil society organisations (90.3%) see an added-value in having rules on EU-level to ensure the right to privacy and confidentiality in the electronic communications sector.

61% favour EU rules to ensure the free movement of personal data in the electronic communications sector and 62.8% see the need to ensure the free movement of equipment and services.

A majority of citizens, consumer and civil society organisations consider it relevant to have specific rules for the electronic communications sector on confidentiality (83.4%), traffic and location data (73%), unsolicited commercial communications (78%) and notification of personal data breaches (72.8%). For directories (54.4%) and calling line identification (55.5%), a smaller majority supports the need for special rules. The respondents were more divided on the need for special rules on itemised billing, (47.3% support it, while 31.3% have no opinion and 21.4% do not support it) and automatic call forwarding (48.4% support it, while 31.9% have no opinion and 19.8% do not support the need).

Citizens, consumer and civil society organisations believe that the rules are needed because they protect the personal data of consumers and they believe they should be in control of the data they communicate to the public. If taken out, the rules should be included in the revised Universal Service Directive.

90% of public authorities agree that having rules on EU-level in the electronic communications sector are needed to ensure privacy and confidentiality.

72.4% believe that they are needed to ensure free movement of data; 67.8% see a need to ensure the free movement of services and equipment.

Public authorities believe that specific rules for the electronic communication sector are needed on confidentiality (88.9%) and on traffic and location data (92.3%). By a majority, public authorities support special rules for the electronic communications sector in all areas of the consultation (specified above).

A majority of industry does not see the benefit of EU sector-specific rules. 63.4% replied that EU rules are not needed to ensure the protection of privacy and confidentiality, 64.6% said that rules are not needed to ensure the free movement of data and 58.3% do not see the need for rules to ensure the free movement of services and equipment. This is echoed by the ECS/ECN providers who by a larger majority do not believe that rules are necessary (72-86%).

The area that industry quotes as not requiring special rules for the electronic communications sector is the notification of personal data breaches (78.1%), followed by the rules on traffic and location data (66.2%), confidentiality (63.4%), and on unsolicited commercial communications (63.1%).

A few industry respondents argue however that rules on direct marketing and directories should be maintained in the ePrivacy Directive and that specific rules are needed for the ECS/ECN sector because it collects data inherently more sensitive than the data OTT services collect.

The ECS/ECN industry argues that special rules are not needed because some are covered by the GDPR and all actors are collecting and processing similar personal data. Inconsistent regulation of the same services leads to discrimination between types of businesses and this is also confusing for consumers, they argue. The rules that the GDPR does not cover could be covered by consumer protection legislation or by the telecom package.

o COHERENCE OF THE ePRIVACY DIRECTIVE

This section aimed to assess whether the existing rules are coherent with one another and with other legal instruments.

▪ *COHERENCE WITH OTHER EU INSTRUMENTS*

On the coherence of the ePrivacy Directive with other instruments on security (i.e. Framework Directive, GDPR, Radio Equipment Directive and Network and Information Security (NIS) Directive) **around one third of citizens, consumer and civil society organisations reported that they did not know**. Among those that had an opinion, most reported that the provisions are significantly or moderately coherent with each other.

Industry in general reported that the strongest level of coherence is with the GDPR (65.5% reported significant or moderate levels of coherence), followed by the Framework Directive (51%) and the NIS Directive (50%). On the Radio Equipment Directive, most industry respondents were unaware of its coherence; 24.6% reported significant/moderate coherence.

ECS/ECN providers report general coherence with the Framework Directive and the NIS Directive (60% for both) but less with the GDPR (40%). Many respondents reported that they did not know about coherence with the Radio Equipment Directive.

Public authorities reported general coherence except on the Radio Equipment Directive for which they also did not know.

▪ *TELEMARKETING*

Citizens, consumer and civil society organisations and public authorities think that the freedom left to Member States to decide on opt-in or opt-out for telemarketing is not coherent.

On telemarketing calls, a majority of citizens and civil society (61.5%) report that it is not coherent to allow Member States to make telemarketing calls subject either to prior consent or to a right to object, while Article 13.1 requires opt-in consent for email, fax, and automatic calling machines.

41.4% of industry say this is coherent while the rest find it is not (31.8%) or have no opinion (26.8%).

A majority of public authorities also report that this is not coherent (61.5%); around 30% report that this is coherent, the rest have no opinion.

- *MARKETING MESSAGES VIA SOCIAL MEDIA*

Citizens, consumer and civil society organisations and public authorities want an opt-in rule for marketing messages sent via social media, while industry wants an opt-out system.

On the legal uncertainty regarding the legal treatment of messages sent through social media, a majority of citizens, consumers and civil society organisations (82.4%) and public authorities (74.1%) would like an opt-in system for marketing messages sent through social media (like for email) and they are largely against applying the opt-out system of Article 13.3.

Industry largely prefers the opt-out system (71%).

- **EFFICIENCY OF THE EPRIVACY DIRECTIVE**

This part sought to assess the costs and benefits of the ePrivacy Directive, including for citizens at large.

- *USERS' TRUST*

A majority citizens, consumer and civil society organisations (61.1%) do not believe that the national provisions implementing the ePrivacy Directive have raised the level of trust in the protection of their data when using electronic communications services (or has only done so to a slight extent). **50% of responses from industry also point to this finding, while 44% of public authorities report that there has been a significant/moderate increase in the level of trust** (most of the other respondents in this category do not have an opinion).

- *ADDITIONAL COSTS FOR BUSINESSES*

In terms of the cost of compliance for businesses, 43.5% of citizens, consumer and civil society organisations respond that they do not know and 24.9% say that the cost is little. Some state that the costs are excessive for SMEs and start-ups. A regulation would be cheaper to comply with than a Directive, they believe.

Industry replies that the costs are significant (62.3%) or moderate (20.8%), while public authorities do not know (56.5%) or respond that they are moderate (17.4%).

Precise costs are not provided by ECS/ECN and do not appear in their accounting systems. The ECS/ECN industry argues that the ePrivacy Directive has prevented them from offering new services launched by actors not subject to the rules (opportunity costs), due to an uneven playing field under the current legal framework.

Some report that the costs are disproportionate for SMEs, that the fragmentation at national level raises costs, technical and legal advice costs and costs to check Robinson registers are significant, litigation procedures for Article 5.3 and Article 13.3 are lengthy and disproportionate. Another SME points that the overall costs are relatively small for complying with cookie rules, no more than the annual hosting cost of a website. A few have expressed concerns regarding the excessive costs of compliance for SMEs and start-ups. They argue that large “fixed cost” of compliance should not become a barrier for new businesses.

Public authorities do not appear to have much information. They say that the costs are indirect and that there are legal setbacks.

- *PROPORTIONALITY OF COSTS*

A majority of citizens, consumer and civil society organisations (57.1%) find that the cost of compliance is proportional to the objectives of the ePrivacy Directive. Most consumers believe that the price of compliance is justified in order to reach the objectives of confidentiality of the ePrivacy Directive.

A majority of industry players (65.3%) report disproportionate compliance costs to meet the objectives. 22% of industry players did not have an opinion and 12.7% agreed to the cost of compliance.

ECS/ECN providers argue that compliance costs are creating a clear competitive disadvantage as compared to OTTs, which are not in the scope of the directive.

Some of them demand a level playing field with OTTs. They argue that the current approach is creating legal uncertainty and an asymmetry of data protection/privacy law, as consumers are not protected in the same way when they use functionally equivalent communication services, e.g. Internet based service providers. According to them, a highly competitive market such as ECS/ECN can provide effective solutions without regulation.

Moreover, some entities have expressed the concern that personal data protection rules are already fully covered by the GDPR and that the answer to this issue lies in best practice of GDPR guidance and not in more law.

Finally, some of these ECS/ECN operators insist that a competitive disadvantage creates significant loss of competitiveness and business opportunities for the concerned organisations, with a negative impact on innovation and on the time needed to market new services. Moreover, investments that would have been made in the absence of sector-specific regulation are delayed or discarded.

Most public authorities (72.7%) believe that the costs of compliance are in line with the objectives pursued.

Some have highlighted the right to privacy as one of the most important rights guaranteed by the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. In order to protect it, actors involved in data collection and manipulation must accept the cost of compliance.

o EU ADDED-VALUE OF THE EPRIVACY DIRECTIVE

This section seeks to assess the EU added-value of the ePrivacy Directive in order to evaluate whether EU action is needed for this specific sector.

A majority of citizens, consumer and civil society organisations (86.7%) believe that national measures would have been necessary if the ePrivacy Directive had not existed. 65% of public authorities agree but 50.4% of industry (60% of ECN/ECS) disagree.

A majority of citizens, consumer and civil society organisations think that the ePrivacy Directive has had clear added-value for increasing/harmonising the confidentiality of

communications (55.4%) and the free flow of personal data (54.4%). Less than half (47.4%) believe this is the case for the free movement of services and equipment. Public authorities believe there is added-value for the 3 areas (respectively, 91.6%, 80% and 56%).

Industry at large is more critical. Only 40.1% believe that the Directive has had added-value for the confidentiality of communications, 34% for free flow of personal data and 39.6% for the free movement of services and equipment. ECN/ECS providers are more critical: 20.2% believe that the Directive has had added-value on the confidentiality of communications, 17.6% for free flow of personal data and 11.7% for the free movement of services and equipment.

- **REVISING THE EPRIVACY DIRECTIVE: LOOKING AHEAD**

This section covers forward-looking questions to assess the possible solutions in case there is a need to revise the ePrivacy Directive.

PRIORITIES FOR REVISION

- Citizens, consumer and civil society organisations believe that the priorities (with the option to select several) of any future instrument should be the following (in the most frequently quoted order):
    - Amend the provisions on confidentiality of communications and of terminal equipment (68.5%);
    - Widen the scope of the provisions to cover OTTs (62.9%);
    - Amend the rules on governance (61.8%);
    - Amend the provisions on unsolicited commercial communications (57.9%);
    - Amend the provisions on security (55.6%);
    - None of the provisions are needed any longer (3.9%);
    - Others (11.8%).
- For industry, top priorities should be:
    - None of the provisions are needed any longer (55.6%);
    - Widen the scope to cover OTTs (28.8%);
    - Amend the rules on unsolicited commercial communications (22.9%);
    - Amend the provisions on governance (22.9%);
    - Amend the provisions on unsolicited commercial communications (22.9%);
    - Amend the provisions on confidentiality of communications and of terminal equipment (19.6%);
    - Amend the provisions on security (17%);
    - Others (12.4%).

  The position of ECN/ECS is broadly in line with this.

- For public authorities, top priorities should be to:
    - Widen the scope to OTTs (72.4%);
    - Amend the rules on unsolicited commercial communications (58.6%);
    - Amend the rules on confidentiality (51.7%);
    - Amend the provisions on security (41.4%);
    - Amend the provisions on governance (41.4%);

- Other (6.9%).

CHOICE OF LEGAL INSTRUMENT

A very clear majority of citizens, consumer- and civil society organisations (66.3%) and of public authorities (66.7%) believe that a regulation would be a better instrument than a Directive.

47% of industry representatives suggest other options. 24.1% are against the idea of a regulation, while 28.9% are in favour of a regulation. Among the ECS/ECN, 67.7% favour other options, while only 15% are in favour of a regulation.

When referring to the other options, industry often states that the ePrivacy Directive should be repealed and not replaced, the GDPR is sufficient. According to this category of stakeholders, consumer related questions are thought to be better covered under consumer protection instruments.

- **REVIEW OF THE SCOPE**

  - *EXTENSION OF SCOPE TO OTTs*

Citizens, consumers and civil society organisations think that the rules should be broadened to cover OTTs (76%), a few believe it should in part (8.4%) while a few think that it should not be broadened (5.6%). They would like the rules on security, confidentiality, traffic and location data and on unsolicited marketing communications to be extended to messages sent via OTT services by close to 100% support. **Public authorities are aligned with the opinion that the rules should be extended but in slightly different proportions (62.1% in favour**, 31% in part, none answered not at all). Those in favour also support with close to 100% that all the rules mentioned should be extended.

Industry is more divided as 41.6% do not want the scope to be broadened while 36.2% do and 7.4% believe it should in part. Of the respondents that said that the rules should be broadened entirely or in part, 98.4% said so for the rules on confidentiality, 95.1% for the security obligations, 85.2% said so for the rules on security and traffic and location data and 72.1% for the rules on unsolicited commercial communications.

45% of the ECS/ECN industry answered that the scope should be broadened to OTTs, while 15% said no. The rest said in part (7.5%) or did not know (12.5%).

  - *TYPE OF NETWORKS TO BE COVERED*

A majority of citizens, consumer and civil society organisations believe that the rules on security (58.2%), confidentiality (64.7%) and on traffic and location data (58.2%) should apply to all networks: public, private and closed. A smaller proportion (20-24%) advocates that these rules should apply to Wi-Fi internet access provided to customers or the public such as in airports, hospitals etc. ("**non-commercial Wi-Fi**"), while a smaller proportion (11-20%) opts for the current situation i.e. that they should only apply in relation to publicly available networks.

Industry is equally divided between advocating that the rules on security should apply to all networks on the one hand (48.6%) and to only publicly available networks on the other (48.6%). On the confidentiality of communications, slightly over half (51.4%) think that the rules should apply only to publicly available networks, and the other half to all

networks. As for the rules on traffic and location data, significantly more (57.7%) believe that the rules should only apply to publicly available networks. A few respondents say that non-commercial Wi-Fi should be covered (2-2.5%, depending on the area i.e. security, confidentiality and the rules on traffic and location data).

The ECS/ECN industry (slightly over 70%) favours the rules applying to all networks.

Public authorities are more divided as on applying the rules on security, an equal number (37.5%) opt for all networks and non-commercial Wi-Fi, slightly less (25%) for publicly available networks. On the confidentiality of communications, slightly more opt for all networks (44%). With regard to the applicability of the rules on traffic and location data, more opt for application to non-commercial Wi-Fi (44%).

- **ENSURING SECURITY AND CONFIDENTIALITY OF COMMUNICATIONS**

  - *SECURITY*

A majority of citizens, consumer and civil society organisations (87.2%) believe that legislation should ensure the right for individuals to protect their communications, e.g. by securing Wi-Fi connections or by using encryption apps.

Public authorities agree (72%) with user empowerment measures.

Industry is divided between those that agree (41.5%), those that do not (31.1%) or that do not know (27.4%). The ECS/ECN industry is also divided between those that agree (30%) and that do not (37.5%). Many in this category did not answer (17.5%) or did not know (15%).

Those from industry (at large) that disagree highlight that legislation is not needed, that user solutions can be developed by industry and it is in their interest to do so. Some also explain that when traffic is encrypted, operators cannot detect malware and viruses and cooperate with law enforcement and detection of illegal and harmful content. Others point that the obligation to secure communications is covered in other instruments such as the GDPR and the NIS Directive.

The consultation document put forward the following policy options to improve security:

- 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 communications 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.

A majority of citizens, consumer and civil society organisations support the options for additional policy measures to improve the security requirements in all the areas suggested by the Commission and each option received support with largely the same proportions: development of minimum security or privacy standards for networks and services (86%),

followed by Internet of Things (79.8%), network components (74.8%) and software used in combination with the provision of a communication service (73.7%).

Industry is much less receptive to these additional policy measures on security. The development of minimum security or privacy standards for networks and services received support from 29% of industry, followed by the Internet of Things (28.8%), network components (23.6%) and software used in combination with the provision of a communication service (20.5%).

Public authorities are broadly in favour except for the idea to extend security to cover software used in combination with communications services, where only 46.2% think that this will significantly or moderately improve the situation. The development of minimum security or privacy standards for networks and services received most support (80.7%), followed by extending the security requirements to include all network components (65.3%) and Internet-of-Things devices (61.5%).

- *COOKIES*

The practice of websites to deny access to those users who refuse to accept cookies (or other technologies) have generated criticism that citizens do not have choice. The Commission asked in the consultation whether:

- Information society services should be required to make available paying service (without behavioural advertising) as an alternative to the services paid by users' personal information (**option 1**);
- 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 (**option 2**).

Citizens, consumer and civil society organisations support option 1 (55.5%) less than option 2 (76.6%), while public authorities do not agree with option 1 (55%) but agree with option 2 (70%). Industry disagrees or strongly disagrees with option 1 (78.7%) and option 2 (75.8%).

Those in favour of a paying service argue that this would enable users to enjoy an online experience without intrusion into their personal lives. Those against the pay option say this would be discriminatory between those who can afford to pay and those who cannot, that this is not commercially possible for many online companies and would be contrary to the fundamental right to conduct a business.

Those in favour of the solutions whereby online service providers should not be allowed to prevent access to the service argue that a pay option should be available. Those against the option argue that the law should not impose a certain business model. Online behavioural advertisement, enabled through the use of cookies, is a way to ensure sustainability.

The consultation asked for which options among the following (with several options available), consumers should be asked for their consent before personal data and other information is processed when stored on their smart devices:

- Identifiers placed/collected by a third party information society service (not the one you are visiting) for online behavioural advertising purpose (‘third party cookies’);

- Identifiers placed/collected by an information society service which the consumer is 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 the consumer is visiting whose purpose is to support user experience, such as language preference cookies;
- 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 identifiers.

Citizens, consumer and civil society organisations replied most often (96.5%) that they want to be asked to consent before third party cookies are used. 69.4% said they want to be asked before cookies are used for frequency capping, 62.3% for website analytics and 60% before identifiers are used by information society services to detect fraud.

Although the other stakeholders did not have to answer these questions, some did. Industry mostly refers to others solutions (62%) and says that consent should be sought for use of third party cookies (36.7%). The other options received between 11.4% and 19% of support by industry.

Public authorities believe that consent should be sought for third party cookies (85%), for frequency capping (55%). The least support was for consent to be given when the data is immediately anonymised (15%).

On the solutions proposed to the cookie consent issue, citizens, consumer and civil society organisations supported some options (respondents could select multiple answers):

- Introducing provisions to prevent specific behaviours, irrespective of users' consent (86.7%);
- Imposing obligations on manufacturers of terminal equipment to market products with privacy-by-default settings activated, preventing operators from collecting and storing data (81.2%);
- Mandating EU standards organisations to produce do-not-track or do-not-collect/store types of standards (74%);
- Adopting legislation e.g. delegated acts on defining how to express user preferences regarding whether they want to be tracked (60.2%);
- Supporting self/co-regulation (34.8%);
- Other (9.4%).

This contrasts with the solutions preferred by industry:

- Supporting self/co-regulation (58.3%);
- Other (36.8%);
- Imposing obligations on manufacturers of terminal equipment to market products with privacy-by-default settings activated, preventing operators from collecting and storing data (18.4%);
- Introducing provisions to prevent specific behaviours, irrespective of users' consent (16%);

- Mandating EU standards organisations to produce do-not-track or do-not-collect/store types of standards (14.1%);
- Adopting legislation e.g. delegated acts on defining how to express user preferences regarding whether they want to be tracked (9.8%).

The most common solution industry put forward was to repeal the ePrivacy Directive and refer to the rules of the GDPR. They believe that horizontal rules are needed, technology-neutral and future-proof. Some also argued in favour of an opt-out approach.

The options most **public authorities preferred were the introduction of rules prohibiting specific abusive behaviour (70.4%) and placing obligations on manufacturers (63%).**

- *TRAFFIC AND LOCATION DATA*

The ePrivacy 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. Furthermore, consent of users should be asked in order to use them for value-added services e.g. 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. Under the current regime, traffic data cannot be processed for any other purpose than those mentioned.

On the question if the exemptions to consent for processing traffic and location data should be amended (possibility to choose several options), **citizens, consumer and civil society organisations' preference was not broadening the rules (49.1%)** but they accept that the use of this type of data should be allowed for other purposes if it is fully anonymised (45.1%). A proportion considers that the provisions should be broadened to include the use of such data for public purposes (27.4%) or statistics (20%) provided certain guarantees are included (the argument being that this is the case already in practice). They argue that traffic and location data provide a detailed picture of individuals' habits and that this type of data should only be processed with their prior consent. Some would also like the principles of data minimisation and purpose limitation to be included in sector-specific legislation. They also flag the difficulty of ensuring full harmonisation.

Industry considers that the provisions on the processing of location and traffic data should be removed (63.2%). A substantial proportion considers that the provisions should be broadened to include the use of this data for statistical purposes (with the required safeguards) (36.1%), and/or to include the use of this data for public purposes (with required safeguards) (31.6%). Some consider that the data should be allowed to be used for other purposes if fully anonymised (25.6%) and a few (6.8%) do not want the use to be broadened.

Industry appears in favour of removing the provisions to achieve a level playing field, and argues that the GDPR provides enough safeguards. In the event that special rules still exist, the possibilities to process traffic and location data should be extended and aligned with the GDPR especially on the possibility of pseudonymisation. Some traffic and location data will not fall under the scope of personal data and this data should not be made subject to processing restrictions as this could limit the EU's ability to build a data-driven digital economy.

Public authorities favour in roughly an equal manner the solutions proposed (27.3% - 42.4%) except the option to delete the provisions on traffic and location data (6%).

36.4% is not in favour of broadening the rules. They highlight the importance of being able to use data from new sources for statistical purposes. Some also highlight that the definition of traffic data should not refer to subscriber billing.

- **Non-itemised billing, calling line identification, automatic call forwarding, directories**

The ePrivacy Directive provides for the right of subscribers to receive non-itemised bills. It also gives callers the right to prevent the presentation of the calling line identification ("CLI") if they wish to guarantee their anonymity. Subscribers have the possibility to stop automatic call-forwarding by a third party to their terminals. Finally, subscribers must be able to determine whether their personal data is included in a public directory.

Citizens, consumers, civil society and public authorities generally believe that the provisions on non-itemised billing (74.8%) calling line identification, 76.3% automatic call-forwarding (65.2%) and directories (74%) should be kept and are still relevant.

Consumer organisations and civil society believe that the rules are needed because they protect the personal data of consumers who should be in control of the data they communicate to the public. If repealed, the rules should be included in the revised Universal Service Directive.

Citizens argue that they want their say in directories, automatic forwarding should cover other types of communications, but some also argue that CLI masking should be banned.

Industry replied that they would like the rules on non-itemised billing (57.2%) calling line identification (55.7%), automatic call-forwarding (55.3%) and directories (55.4%) to be scrapped. The ECS/ECN industry favours that view by a larger proportion (around 75%).

The ECS/ECN industry argues that the rules should either be removed completely or moved from the ePrivacy Directive to other horizontal consumer protection instruments, elsewhere in the ECS/ECNs framework or in the citizens' rights Directive. Where relevant, these rights should be extended to all communications services, but it is not clear how this applies to non-voice services. The argument is made that the rules should not apply to business users. The obsolete nature of printed directories was also brought up and that it is no longer included in the scope of universal service obligations in most Member States. They also argue that the development of search engines and online services have changed the ability to search for professional services. CLI is appealing to customers but the rules should be amended to cater for cross-border communications and to cover new VoIP technologies. The GDPR provides sufficient safeguards.

Internet companies and other industries either see no need for these rules to be extended to OTTs or consider that they should be included elsewhere. Some respondents do not want commercial companies to be allowed to withhold their calling and connected line identification number because this is generally used for direct marketing calls. Many argue that the rules are not needed or are obsolete.

There are dissenting views on the possibility for subscribers to have their data listed and to have data bases with accurate information. Provisions on non-itemised billing may be needed

to protect the privacy of sensitive communications such as helplines. These are valuable consumer rights according to the advertising industry.

Public authorities (84%) favour maintaining the rules on non-itemised billing, CLI (72%), call-forwarding (79.1%) and directories (60%).

Some note that the rules on CLI should be amended to prevent withholding CLI for sales and marketing purposes to avoid 'spoofing'; that the rules in general should be modernised for the digital age. More studies are needed to see if end users have used the possibility to have non-itemised billing and restrictions on CLI. If this is not widely used, the rules should be repealed.

o UNSOLICITED COMMERCIAL COMMUNICATIONS

The ePrivacy Directive requires prior consent to send commercial communications through electronic mail (including SMS), fax and automatic calling machines without human interaction. However, companies which have acquired an end-user's email as a result of a sale of products/services can do direct marketing by email to advertise similar products or services, provided that the end-user is given the possibility to object (**opt-out**). Member States can decide whether to require opt-in or opt-out for marketing calls with human interaction. The protection against all types of commercial communications also benefits legal persons but the ePrivacy Directive leaves it to Member States to decide whether they are protected by an opt-in or opt-out regime.

Citizens, consumers and civil society organisations believe that Member States should not be able to choose between an opt-in or an opt-out system for direct marketing calls with human interaction directed at individual citizens (72.3%) or for direct marketing to legal entities (67.7%). **Member States should apply the opt-in solution** for marketing calls to citizens (88.2%) and for legal entities (74.8%).

Consumers and civil society believe that the opt-in system is a better option for all types of communications. They find that opt-out regimes do not function adequately, despite the fact that they have existed for a number of years.

Public authorities agree that they should not be able to choose between an opt-in or opt-out for marketing calls sent to individuals (73.3%) and legal entities (65.5%). They favour opt-in for calls to individuals (86.9%) but opinions are nearly equally divided between the opt-in and the opt-out for marketing messages to legal entities.

Of public authorities that commented, most argued in favour of an opt-in system, because it is simpler to understand. The others either recommend an opt-out system or do not have an opinion but stress the need for flexibility or coherence with the GDPR.

Industry is aligned on their preference that Member States should not be given the choice (52%). It diverges with the other two categories in so far as industry would prefer an opt-out system for marketing calls made to individuals (73.5%) and to legal entities (77.3%).

The ECS/ECN industry argues that sector-specific legislation needs to be abolished, rules need to be aligned with the GDPR which includes rules on direct marketing (right to object). Those should be clarified in guidelines from the European Data Protection Board (EDPB). If maintained, these rules should either be in the GDPR or in the Unfair Commercial Practices

Directive. The system should be harmonised but kept flexible. The fact that opt-out lists exist at national level shows that users trust and rely on them. There could be more harmonisation on the existing codes of practice and opt-out models.

Many marketing companies and other companies argue that this is not sector-specific legislation and that rules should either be in the GDPR or in the Unfair Commercial Practices Directive. They argue for a single opt-out regime for all types of communication channels, and that this would also help SMEs. Other tools to protect against direct marketing exist: smartphone settings blocking push notifications and/or calls from callers identified as nuisance, some email platforms automatically filter commercial communications into a secondary space.

- **FRAGMENTED IMPLEMENTATION AND INCONSISTENT ENFORCEMENT**

Some provisions of the ePrivacy Directive may be formulated in too general terms. Consequently, Member States may have implemented key provisions differently. The result is a fragmented situation. While the Data Protection Directive entrusts its enforcement to data protection supervisory authorities, the ePrivacy Directive leaves it to Member States to designate a competent authority or other national bodies. The result is a fragmented situation. Some Member States have allocated competence to data protection supervisory authorities, whereas others to the ECS/ECN national regulatory authorities, others to yet another type of body such as consumer authorities. See section III. 7 of the background document.

- *AUTHORITIES IN CHARGE*

A majority of citizens and consumer and civil society organisations consider that enforcement of the ePrivacy Directive should be allocated to a single authority (69.3%). 18.2% do not favour that solution, the rest do not know.

Of those that favour a single authority, consumers and citizens think that the national data protection authority would be most appropriate (67.2%) while 20.4% would prefer the national consumer protection authority to be in charge.

Industry is in line with the position of citizens and consumers in roughly the same proportion. They think that the national data protection authority would be best suited but the proportion is not as high (51.7% for the industry at large, 30% for the ECS/ECN) as many prefer other options (38.8%).

Public authorities are less convinced as only 38.5% agree while 50% disagree, and the rest do not know. Of those that agree with a single authority, they think that the best authority would be the national data protection authority (53.3%) while 26.7% would prefer the national ECS/ECN authority to be in charge.

21.3% of the total respondents answered 'other'. Close to all of them (94.7%) commented and their options and arguments vary. Some would like the DPA at EU level to be competent (EDPB or an EU agency), that the sector-specific rules should be repealed altogether, or placed in other instruments, consumer protection rules should be moved to consumer protection acquis and enforced by consumer protection authorities, ENISA is also mentioned for the security aspects, one mentions the use of the consistency mechanism.

Those that support giving responsibility to telecom NRAs argue that they have a deeper understanding of the ECS market. If everything is given to the DPAs, the non-privacy values could be forgotten or given less priority.

Of those that say that the DPA should be responsible, some stress that this should only be the case for privacy-related issues, and that the other issues should be covered in other instruments. There is strong emphasis on harmonised guidance. Some also call for the independence, powers and funding of national DPAs to be strengthened.

- *CONSISTENCY MECHANISM*

A majority of citizens, consumer and civil society organisations believe that the consistency mechanism created by the GDPR should apply to cross-border matters covered by the ePrivacy instrument (71.9%). Slightly over 60% (55.5% of ECS/ECN) of industry agree, while public authorities appear more divided: 37.5% have not provided an answer, 27.5% agree and 17.5% disagree.

- *SANCTIONS*

On the question of sanctions, 82.9% of citizens, consumer and civil society organisations believe that the future instrument should include specific fines and remedies. 68.5% of industry disagrees, while exactly half of public authorities agree and one third disagrees. The rest do not know.

III. Ad hoc consultations of EU expert groups and workshops

In parallel to the public consultation, the European Commission conducted ad hoc consultations of the following EU expert groups in the course of the summer 2016. It also organised a series of workshops to receive additional inputs from stakeholders.

III.1 The REFIT Platform

The REFIT Platform was announced in the 2015 Better Regulation Agenda. It consists of a Stakeholder Group, with 18 members and two representatives from the European Social and Economic Committee and the Committee of the Regions, and a Government Group, with one high-level expert from each of the EU's 28 Member States.

The task of the Platform is to:

1) invite and collect suggestions from all available sources on regulatory and administrative burden reduction,
2) assess the merits of the collected suggestions in terms of their potential to reduce regulatory and administrative burden without endangering the achievement of the objectives of the legislation;
3) forward with any comments, the suggestions considered to merit most attention to the Commission or, in the case of an implementing measure, to the Member State concerned; and
4) respond to each person making a suggestion and to publish the suggestions it receives and the response from the Commission or Member State.
5) The Commission can also consult the Platform on any matter relating to its better regulation work and REFIT programme.

On 27/28 June 2016, the REFIT platform adopted an opinion on the review of the ePrivacy Directive

Overall, the REFIT Platform has considered the need to align the ePD with the recently adopted GDPR and to harmonise the 'cookie provision', suggested by Danish Business Forum. The Platform recommends that the Commission gives due consideration to the issues identified by the Platform such as ensuring that the revised ePD (adopted in 2002 and amended in 2009) is aligned and consistent with the GDPR adopted in 2016 or that additional exceptions to the 'consent' rule for cookies are envisaged under certain conditions, provided that they do not create any privacy risk. The Platform also recommends that the Commission addresses national implementation problems and facilitates the exchange of best practice amongst Member States.

a) Considerations of the REFIT Platform Stakeholder group

The Stakeholder group recommended that the so called "cookie" rule in Article 5.3 be amended in a manner which would both decrease industry costs of implementation and raise awareness of privacy among users. The Commission, Member States and Data Protection Authorities should ensure that the future instrument is aligned and consistent with the GDPR, in terms of approach and of choice of legal instrument.

The Commission and Member States should seek greater harmonisation in the implementation and enforcement of the rules, including the provisions related to cookies and the enforcement mechanisms, while promoting the use of European standards. The rules related to cookies and tracking technologies, as well as the rules on unsolicited communications, should be reviewed to ensure that they are future proof. Reforming the legislation should not open any back doors for tracking users and any exceptions to the consent rule should only affect cookies which do not create any privacy risks.

b) Considerations of the REFIT Platform Government group

The government group drew a special attention to the so called "cookie" provision. It stressed the importance of assessing whether that rule has achieved its specific objective of raising citizens' awareness, in the light of the costs incurred by businesses. In this respect, the group underlined the importance of taking into account the feedback gathered throughout the consultation exercise. To conclude, the opinion recommends that the Commission amends Article 5.3 when putting forward a legislative proposal; while other EU institutions are invited to speed-up the legislative process on this file and competent authorities to share best practices on enforcement.

III.2 Article 29 Working Party

The Article 29 Working Party was expressly consulted by the Commission. It adopted an opinion on the evaluation and review of the ePrivacy Directive (2002/58/EC)[190]. The key findings of this opinion are the following:

- it supports maintaining specific rules on confidentiality of communications;

[190] Article 29 Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240 adopted 19.07.2016.

- it clarifies that the GDPR will not apply "in cases where the ePrivacy Directive contains specific obligations with the same objective";
- the new ePrivacy instrument should at least maintain and reinforce its current principles, to guarantee the confidentiality of electronic communications[191];
- the scope of the rules on geo-location and traffic data should be extended to all parties;
- the new instrument must seek to protect the confidentiality of functionally equivalent electronic communications services (such as WhatsApp, Google, Gmail, Skype and Facebook Messenger);
- the broad scope of the consent requirement under Article 5.3 should be clarified while there is a need to create more specific exceptions to allow for the processing of data that causes little or no impact on the privacy of users;
- it acknowledges the high intrusiveness of tracking over time of traffic and location data and call on a uniformed regime suggesting the merger of the current Articles 6 and 9 and the introduction of more exceptions to the consent rule;
- when consent is the applicable legal basis, users must be provided with truly easy (user friendly) means to provide and revoke consent.

III.3 European Data Protection Supervisor

The views of the EDPS were expressly requested by the European Commission.

In his opinion on the review, the EDPS expresses similar views to those of the Article 29 Working Party, of which he is a member. In particular, the EDPS also endorses the need to **keep specific rules to ensure confidentiality of communications** at EU level that would complement the GDPR. In this respect, he made the following recommendations:

- the scope of new ePrivacy rules needs to be broad enough to cover all forms of electronic communications irrespective of network (public or private[192]) or communication services used;
- individuals must be afforded the same level of protection for all types of communications regardless of the technology used (e.g. telephone, Voice over IP, services, mobile phone messaging app, Internet of Things);
- no communications should be subject to unlawful tracking and monitoring without freely given consent, whether by cookies, device-fingerprinting, or other technological means. This means that the so called cookie rule should be revised to address any tracking techniques;

[191] This means that it should be clear that the consent should be the only legal basis permitted.

[192] The updated rules should ensure that the confidentiality of users is protected on all publicly accessible networks, including Wi-Fi services in hotels, coffee shops, shops, airports and networks offered by hospitals to patients, universities to students, and hotspots created by public administrations.

- users must also have user-friendly and effective mechanisms to give, or not their consent. In this respect cookie walls (where users are forced to give their consent to access a webpage) should be prohibited;
- in order to increase confidentiality and security of electronic communications, the consent requirement for traffic and location data must be strengthened and apply horizontally (i.e. to any processing of such data);
- the new rules should complement, and where necessary, specify the protections available under the GDPR;
- the rules should also maintain the existing, higher level of protection in those instances where the ePrivacy Directive offers more specific safeguards than in the GDPR. In this respect, the EDPS supports maintaining the rules on subscribers' directories and calling and connected line identification;
- the rules protecting against unsolicited communications, such as advertising or promotional messages, should be updated, made technology neutral and strengthened by mandating the recipient's prior consent for all forms of unsolicited electronic communications.

III.4 CPC Network

The European Commission also specifically consulted the Consumer Protection Cooperation Network through a tailored questionnaire. The network was not in a position to provide a coordinated reply and invited its members to reply individually.

Replies were received from consumer authorities from Spain, Romania, Norway, and Denmark. The key points of their replies are summarised below:

- all respondents considered that the ePD only partially achieved its objectives;
- as to which provision in particular is problematic, several authorities refer to Article 13. Some considered that the high number of complaints received regarding unsolicited calls show the need to review. Others emphasised some flaws of the rules, such as difficulties to apply the rules to new technological development such as social media; difficulties to prove unsubscribing to a mailing list and difficulties for companies to understand the rules;
- one authority considered that Article 5.3 failed to achieve its objectives in the light of diverging interpretation and enforcement;
- overall the respondents agreed that the wide diversity of competent authorities has created difficulties that have led to diverging interpretation and/or fragmented enforcement. One authority specifically referred to the uncertainty that this created among competent authorities as to which authority should act. Another considered that this may cause a concurrent action of authorities leading to increased cost of enforcement;
- a majority of respondents agreed that a regulation would be the better suited instrument to achieve the objectives of the current ePD;
- they all agreed that the rule on unsolicited communications should be reviewed and that the choice left to Member States between opt-in and opt-out is not coherent under Article 13.3 with the opt-in rule under Article 13.1. While a majority of them

considered that opt-in should apply to all situations for unsolicited communications towards individuals; the position is not clearly defined for legal persons. A majority support the opt-in rule to apply to social media. All respondents that expressed a view, considered that Member States should not retain the possibility to choose between opt-in and opt-out for individuals (under Article 13.3), while 2 out of 3 considered that they should not retain this possibility for legal person as well[193].

III.5 BEREC

BEREC, the EU body gathering NRAs (competent telecom authorities) was expressly consulted by the Commission and sent its views on the 31st of July.

Overall, BEREC considered that:

- there is still a need to have data protection rules and privacy rules addressing the electronic communications sector;
- the rule on confidentiality of communications should apply equally to ECS and OTT players, while its wording should be adapted to technological changes;
- there is a still a special interest to regulated traffic and location data over the GDPR given the sensitiveness of these data[194];
- so called consumer provisions (on itemised bill, calling & connected line identification etc.) should be maintained and extended to OTT players.
- the security rule, including the notification requirement, should be maintained and aligned with the ones of the GDPR;
- regarding the question of extending the protection of the rules to semi-private network (e.g. airport, cafes etc.), the authority underlined the need to ensure that the rules should be adjusted so that they do not act as a detriment to the further development of non-commercial Wi-Fi-access;
- regarding Article 5.3 the authority underlines that the current system does not allow a meaningful consent and that the rules needs to be revise and focus more on the purpose of tracking rather than on the access and storing of information.

III.6 Workshops, Round Table and meetings with stakeholders

The European Commission organised **two workshops** in April 2016 to collect further views of stakeholders, using participatory techniques.

The **first workshop** was open to all stakeholders and took place on 12 April. There were around 120 participants, representing industry, competent authorities and civil society. The main views that were expressed are summarised below:

---

193 One respondent did not express his views on this.

194 BEREC reply p. 6: "*As technology has developed, so have the threats to confidentiality of communications. Nowadays, it is for instance possible* ***to automatically analyse network traffic in real time (i.e. Deep Packet Inspection), even on a core network level****. Such analysis could be used for anything from traffic management to profiling of the network users for marketing purposes*."

- representatives of the telecom industry argued for the need to push for the economic growth, emphasising job opportunities and innovation by removing specific provisions of the ePD, such as those on traffic and location data;
- representatives from the OTT players underlined the difficulties for these companies operating across border to comply with different national rules on access to communications by law enforcement authorities;
- representatives from consumer organizations, argued for keeping the requirement for user consent on tracking, location and traffic data while promoting privacy by design/default;
- representatives from competent authorities underlined the benefit of supporting user friendly measures such as Do-Not-Track (DNT) to protect privacy and called for fully harmonising privacy rules in a regulation;
- academics supported an extension of the ePrivacy rules to OTT providers, while stressing the interdependence of privacy with other fundamental rights like the freedom of expression or right to private property.

The **second workshop** gathered the **national competent authorities** in order to receive their specific inputs to the review. The discussions focused on the cookie rule, rules on traffic and location data, the need of a security provision and the provisions on consumer protection (subscriber directories and unsolicited communications).

The **round table** with 17 key stakeholders from all fields, the EDPS and the Article 29 Working Party gathered views at a later stage of the review. Stakeholders expressed their views on, *inter alia*, the preferred legal instrument, the extension of the scope to OTT providers, the need of having sector specific rules on traffic and location data, how to simplify the requirement to obtain consent before placing cookies or other identifiers and on how to address online tracking.

IV. Eurobarometer on e-Privacy

Between the 7th and 8th July 2016, around 27,000 citizens from different social and demographic groups were interviewed throughout the EU via telephone (mobile and fixed line) on questions related to the protection of their privacy. Below is a summary of the results of this Eurobarometer survey[195].

Citizens' use of tools to protect their privacy online:

- 60% of the respondents acknowledge that they have changed their privacy settings on their internet browser for instance to delete browsing history or delete cookies;

- 41% of respondents avoid certain websites because they are worried their online activities would be monitored while roughly a third of the respondents acknowledge using software that protects them from seeing online adverts and/or being monitored online.

[195] 2016 Eurobarometer survey (EB) 443 on e-Privacy (SMART 2016/079).

Citizens' assessment of importance of measures protecting their privacy online and confidentiality of their communication[196]:

More than nine in ten respondents throughout the EU consider the following as important:

- Personal information (e.g. photos, calendar, contacts) on their computer, smartphone or tablet can only be accessed with their permission[197];
- The confidentiality of their emails and online instant messaging is guaranteed[198];
- Tools for monitoring their activities online (such as cookies) can only be used with their permission[199].

Almost nine in ten respondents (89%) agree with the proposal that the default settings of their browser should stop their information from being shared.

Nine in ten agree they should be able to encrypt their messages and calls, so they are only read by the recipient (90%), with 65% saying they totally agree with this.

A majority of respondents agree that they receive too many unsolicited calls offering goods or services.

Citizens' views on the acceptability of business models around access to information:

A strong majority of respondents do consider it not really acceptable or not acceptable at all to:

- Have their online activities monitored (for example what they read, the websites they visit) in exchange for unrestricted access to a certain website (67%);
- Have companies sharing information about them without their permission (even) if this helps these companies to provide them with new services they may like (71%).

76% of respondents do not want to pay as an alternative not to be monitored when being on a website.

[196] The question was based on the key provisions of the ePrivacy Directive that ensures citizens' confidentiality of communications and of terminal equipment (sometimes referred to as "cookie" provision) and seeks to evaluate the citizens' views on the need to keep and revise these provisions.

[197] 92 % with 78% considering this as very important.

[198] 92% with 72% considering this as very important.

[199] 82% with 56% considering this very important.

ANNEX III:

REFIT PLATFORM OPINION

Date of Adoption: 27/28 June 2016

REFIT Platform Opinion on the submission by the Danish Business Forum on the E Privacy Directive and the current rules related to "cookies"

The REFIT Platform has considered the need to align the ePrivacy Directive with the recently adopted General Data Protection Directive and to harmonise the 'cookie provisions', suggested by Danish Business Forum.

The Platform recommends that the Commission gives due consideration to the issues identified by the Platform such as ensuring that the revised E-Privacy Directive (adopted in 2002 and amended in 2009) is aligned and consistent with the General Data Protection Regulation adopted in 2016 or that additional exceptions to the 'consent' rule for cookies are envisaged under certain conditions, provided they do not create any privacy risk, in the on-going REFIT evaluation of the Directive. The Platform also recommends that the Commission addresses national implementation problems and facilitates the exchange of best practice amongst Member States.

The detailed recommendations of the Stakeholder Group and Government group are provided within the main body of the Opinion.

Detailed Opinion

Contents

The current rules on collection of data (following the e-privacy directive) are meant to enhance the protection of personal data. However, the regulation is very burdensome for businesses given that cookie information and consent mechanisms must be implemented on almost all websites. In addition, the current rules are likely to be counterproductive as the constant stream of "cookie pop-up-boxes" that users are faced with completely eclipses the general goal of privacy protection as the result is that users blindly accept cookies.

Suggestion

The "cookie regulation" should be amended in a manner which will both decrease industry

costs of implementation and raise awareness of privacy among users. Less intrusive types of cookies (for instance cookies used for website statistics) should be exempted and regulation should be reserved for websites using cookies that pose genuine risks of privacy intrusion. The benefits will be fewer burdens to businesses, more alertness to privacy issues among users, and the possibility of more effective and targeted enforcement.

2 Policy context

The DBF submission relates to the so-called "cookie rule" enshrined in Article 5(3) of Directive 2002/58/EC on privacy and electronic communications (the ePrivacy Directive), as amended by Directive 2009/136/EC.

General Data Protection Directive

The right to the protection of personal data has been explicitly laid down in Article 8 of the Charter of Fundamental Rights and in Article 16 of the Treaty on the Functioning of the European Union. The latter gave the EU new responsibilities to protect personal data in all areas of EU law, including police and judicial cooperation.

On 25 January 2012 the European Commission has proposed a comprehensive reform of the EU's 1995 data protection directive (95/46/EC) to strengthen online privacy rights and boost Europe's digital economy.

Technological progress and globalisation have profoundly changed the way data is collected, accessed and used. In addition, the EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement, which in turn created complexity, legal uncertainty and administrative costs.

The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritised. The reform allows European citizens and businesses to fully benefit from the digital economy and a single law (the General Data Protection Regulation) will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The GDPR will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe.

Current State of Play

Regulation 2016/679/EU 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) was published in the Official Journal on 4 May 2016. The regulation entered into force in May 2016 and will be applicable as of May 2018.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA was published in the Official Journal on the same day. The transposition deadline is 6 May 2018.

The e-privacy Directive

The e-Privacy Directive (2002/58/EC) specifies and complements Directive 95/46/EC with respect to the processing of personal data in the electronic communication sector, ensuring the free movement of such data and of electronic communication equipment and services in the Union.

The Commission announced in the Digital Single Market Communication of 6 May 2015 (‘DSM

Communication') that it would prepare the 'review (of) the ePrivacy Directive with a focus on ensuring a high level of protection for data subjects and a level playing field for all market players'. Furthermore, the GDPR requires that Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with the General Data Protection Regulation.

Current state of play

The e-Privacy Directive is subject to an evaluation under the REFIT Programme where issues of effectiveness, efficiency, coherence, EU added value and relevance will be thoroughly assessed. A special emphasis on burden reduction is envisaged and the results of this evaluation will feed into the Impact Assessment of its revision and inform the design of the e-Privacy Directive.

3 Opinion of the REFIT Platform

3.1 Considerations of the REFIT Platform Stakeholder group

- The revision of the e-Privacy directive was announced in the Digital Single Market Strategy. The Commission's objective is to ensure a high level of protection for citizens and a level playing field for all market players as the digital economy is borderless.
- The e-Privacy directive regulates the processing of personal data and the protection of privacy in the electronic communication sector. It was originally adopted in 2002 to complement the 1995 Data Protection Directive and was last updated in 2009.
- With the recent adoption of the General Data Protection Regulation (GDPR), which defines the EU general legal framework for the protection of personal data, it is essential to review the e-Privacy Directive to ensure that the two pieces of legislation are fully aligned. Given the importance of the provisions contained in the e-Privacy Directive, such as the one ensuring the confidentiality of communications, it is also necessary to ensure that the e-Privacy rules are fit for the digital age and the new technological reality.
- In terms of the choice of the legal instrument, turning the e-Privacy Directive into a Regulation would help create a coherent and consistent legal framework with the GDPR and facilitate the interplay between the two. In any case, since a Regulation has direct general application and it is also binding in its entirety in the whole of the Union, Member States cannot be requested in a directive to contradict rules contained in a regulation. This must be taken into account not only in revising the e-Privacy directive, but also in implementing the GDPR.
- Several provisions of the Directive, such as those related to cookies and similar techniques (art. 5.3), have been implemented in different ways by different EU countries, thereby generating fragmentation in the legal framework. For example, some countries have added "national flavour" to Article 5.3. Fragmentation has also affected the consistent enforcement of the e-Privacy rules, as the competent enforcement authorities may differ from one Member State to another. Even in the territory of a single Member State, the competence to enforce the Directive may be divided among different authorities depending on the instrument used to implement the different parts of the Directive in national law. All this fragmentation must be corrected in the revision of the e-Privacy Directive to avoid disruptions in the Digital Single Market.
- According to the e-Privacy Directive, browsers should by default reject 3rd parties' cookies and require users to engage in affirmative action to accept the cookies. In addition, as

required by the 1995 Data Protection Directive, the user or the subscriber should be informed about the identity of the entity that wishes to store information or gain access to information that is already stored in his terminal equipment and about the purposes of the processing. Moreover, users should be provided with any information relating to the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, and the existence of their right of access, the right to rectify the data concerning him and the right to refuse the storing of or the access to their information.

- The way the 'cookie consent' requirement, derived from the e-Privacy Directive, is implemented in practice could result in individuals being bombarded by constant requests several times a day. This may create a "tick-the-box" approach, with consumers not being aware any more of what they consent to and not being able to exercise a real choice, as cookies must be accepted to continue browsing. Companies - especially SMEs - also need to find ways to be able to comply easily with the 'consent' requirement without distorting the 'user experience'. At the same time rules should be proportionate and should not create a disincentive for the development of the digital economy.
- It is essential to review the rules applying to cookies and similar techniques to ensure futureproof measures to protect users, promote privacy-friendly technologies and allow greater flexibility for those tools that do not pose any privacy risks whatsoever.

  It is also key to look at how to ensure that, when required, consent is informed and meaningful.
- Exceptions covering, for instance, cookies used for website statistics should be envisaged. However, in that case, it would be fundamental to include all the necessary safeguards to avoid that such an exception is used for tracking users 'through the backdoor' or leading to uncontrolled sharing of personal data with third parties.
- It is also necessary to look at the provisions in the e-Privacy Directive that relate to unsolicited commercial communications to ensure that they provide effective and appropriate protection when it comes to new means of online commercial communications, for instance social media.

Conclusion:

- The Commission must propose amendments to the e-Privacy directive to align it with the general Data Protection Regulation and harmonize cookies provisions.

Recommendations:

- The Commission, Member States and Data Protection Authorities should ensure that the revised E-Privacy Directive (adopted in 2002 and amended in 2009) is aligned and consistent with, and does not overlap with, the General Data Protection Regulation adopted in 2016, both in terms of approach and of choice of legal instrument.

  The Commission and Member States should seek greater harmonisation in the implementation and enforcement of the Directive, including the provisions on cookies and the enforcement mechanisms. The review should also consider whether European standards can be used to implement the revised legislation.
- The European Parliament and Member States, including national Data Protection Authorities, should promote a 'privacy by design' approach. The rules related to cookies and tracking technologies, as well as the rules on unsolicited communications, should be reviewed to

ensure that they are futureproof.

- Additional exceptions to the ‘consent’ rule for cookies and similar techniques could be envisaged under certain conditions. Information provided to consumers in relation to the ‘cookie consent’ requirement should be meaningful, comprehensive and easily to understand.
- Reforming the legislation should not open any back doors for tracking users and any exceptions to the consent rule should only affect cookies which do not create any privacy risks.

On the recommendation of the Government group, it is important to underline that Article 5(3) of the e-privacy directive, which is recommended to be amended, is not only about cookies and that we need future proof measures to deal with tracking tools beyond cookies.

3.2 Considerations of the REFIT Platform Government group

It is necessary to assess the implementation of the latest regulation on "cookies" (approved by Directive 2009/136/EU) to determine if it has achieved its objectives (users to be more aware of the use of these techniques to gather data about their Internet surfing and not to install them if they do not consent to it).

The Commission envisages reviewing the e-Privacy Directive in accordance with Regulation (UE) 2016/679, which strengthened the protection of personal data while reinforcing the digital single market. This is according to the Strategy for a Digital Single Market in Europe (Communication COM (2015) 192 final, of 6 May 2015). Amending the "cookie" law to render it more effective in protecting personal data, while alleviating business' legal compliance burdens, is in harmony with the aim of the said Strategy.

The feedback from the consultation to prepare the new legislative proposal on ePrivacy will be useful to assess the impact of the e-privacy Directive.

If the consultation reveals that the current “cookie regulation” has not achieved a good balance between raising awareness of privacy among users and industry interests in keeping legal compliance costs at bay, that regulation should be amended in the way proposed by Danish Business Forum.

There is broad support to review the e-Privacy Directive once the European Commission consultation and subsequent analysis has been finalized.

RECOMMENDATIONS

- *Recommendations to the Commission (e.g. soft measures; legislative action)*
  Legislative action: amendment of article 5(3) of the e-Privacy Directive, if needed.
- *Recommendations to other EU institutions (e.g. acceleration of legislative process; political commitment)*
  EU Parliament support for this potential reform.
- *Recommendations to Member States (e.g. national implementation; exchange of best practice)*

National implementation of the reforms once approved at the EU level.

ANNEX IV: OVERVIEW OF THE EVOLUTION OF THE ELECTRONIC COMMUNICATIONS MARKET

(since the 2009 review of the ECS regulatory package)

The largest majority of the ePD provisions apply to the electronic communications sector. Within the European Union, the telecommunication sector[200] is one of the crucial industries for the completion of the Digital Single Market. According to Eurostat, around 44.7 thousand enterprises are active in this market, accounting for a share of 0.2% of all businesses active in the EU. Around 90% of these enterprises are micro-enterprises, 99% are SMEs. Around 52% of all EU telecommunication enterprises were established in the United Kingdom, Poland, the Netherlands, Germany and France in 2014.

Overall, approximately one million citizens are employed in the telecommunications sector of which roughly 20% are active in SMEs[201]. In total, 56% of all employees in the EU telecommunications sector worked for enterprises in United Kingdom, France, Germany, Poland, and the Netherlands in 2014. The sector generates an annual turnover of EUR 385 billion. In terms of contribution of the telecommunication sector to the annual GDP of each Member State, Eurostat data shows that the sector is largest in Luxembourg (9.5% of overall annual GDP in 2012), Estonia (4.5%), Bulgaria (4.3%), Croatia (4.1%), and the United Kingdom (3.8%)[202].

Around 151 million fixed broadband subscriptions existed in the EU28 (97.2% of EU households) while the number of mobile communication subscriptions was over 667 million. This means that while one in four EU citizens has fixed broadband subscription, the number of mobile subscriptions even exceeds the total number of EU citizens. In addition, Eurostat data shows that 97.1% of EU households have mobile broadband subscriptions[203].

A 2016 global forecast of the market for Over-The Top (OTT) providers[204] shows that market is estimated to grow from USD 28.04 billion in 2015 to USD 62.03 billion by 2020 with a

---

[200] Eurostat defines this sector as being composed of business activities of providing telecommunications and related service activities, such as transmitting voice, data, text, sound and video.

[201] Figure from 2011. Actual figure today likely to be higher. See: http://ec.europa.eu/eurostat/statistics-explained/images/4/4f/Sectoral_analysis_of_key_indicators%2C_telecommunications_%28NACE_Division_61%29%2C_EU-28%2C_2012_A.png.

[202] Figures relate to 2012. The actual figures today are likely to be higher. See Eurostat: http://ec.europa.eu/eurostat/statistics-explained/images/9/9c/Key_indicators%2C_telecommunications_%28NACE_Division_61%29%2C_EU-28%2C_2012.png.

[203] Latest Eurostat figure available for 2013.

[204] (Over The Top) is a generic term commonly used to refer to the delivery of audio, video, and other media over the Internet without the involvement of a multiple-system operator in the control or distribution of the content. The term over-the-top (OTT) is commonly used to refer to online services which could substitute to some degree for traditional media and telecom services. Definition provided in the study of the European Parliament, Directorate-General for internal policies, policy department A: Economic and Scientific Policy, Over-the-Top (OTTs) players: Market dynamics and policy challenges, dd. December 2015,

CAGR of 17.2%[205]. The report argues that market is in the growing stage in Europe and therefore OTT providers in these regions have immense scope for enhancement. Overall, the North American region is expected to contribute the maximum market share to the overall OTT market[206]. Around 40% of primaries in the OTT market are expected to be established in North America by 2020 while 25% are expected to be European.

According to the report, the European market is expected to grow at a similar pace (i.e. with a similar CAGR) as the North American market – albeit with a smaller overall market size. The Asian-Pacific, Middle East and African, and Latin American markets are smaller than the European and North American markets in terms of absolute size but are expected to grow faster than these two until 2020.

Recent Eurobarometer data shows that mobile phones to make calls or send text messages are used by 74% of consumers every day while more traditional fixed phone line services are used by 38% each day. However, a large part of consumers also uses services every day that are not covered by the ePD: E-mail is used by 46% of consumers every day, OTTs for the purpose of instant messaging (e.g. WhatsApp) are used by 41% every day[207], and online social networks are used by 38% every day[208].

The results of the public consultation on the evaluation and review of the regulatory framework for electronic communications demonstrate that consumers increasingly recognise a functional equivalence between traditional SMS/MMS services and OTT services like *WhatsApp* or traditional voice calls and OTT *Voice-over-IP* (VoIP) services like *Skype* and a potential for their substitution[209].

Considering actual traffic volumes, the use of OTT services has increased considerably: The OTTs share of overall messaging traffic has already increased from 8.31% (2010) to 66.96% (2013) and is projected to rise to 90% until 2020. Today the average WhatsApp users sends around 40 messages per day and receives almost twice as many messages. In comparison, the daily number of SMSs sent per mobile user in the EU is around 4.525. In other words, the average WhatsApp user sends almost ten times more messages than the number of SMSs sent by mobile phone users.

---

[205] http://www.marketsandmarkets.com/Market-Reports/over-the-top-ott-market-41276741.html.

[206] http://www.prnewswire.com/news-releases/over-the-top-market-worth-6203-billion-usd-by-2020-572232561.html.

[207] Interestingly, the Eurobarometer data shows that for instant messaging OTTs, two large groups of consumers seem to exist: Those that use instant messaging every day and those that never use it. The proportion of consumers that uses it a few times per week / month is comparatively small. It can be assumed that age is an important factor with regard to the take-up of such services. While younger generations use instant messaging every day, the majority of older consumers do not use it at all. Therefore, it can be expected that the share of consumers who use instant messaging on a daily basis will increase over the next years.

[208] Flash Eurobarometer 443 (2016): e-Privacy. Data on 26,526 consumers collected between 6 and 8 July 2016. At the stage of drafting this report, the Eurobarometer results are only of provisional character.

[209] DLA Piper 2016: ETNO. Study on the revision of the ePrivacy Directive, p. 11; see also https://ec.europa.eu/digital-single-market/en/news/full-synopsis-report-public-consultation-evaluation-and-review-regulatory-framework-electronic

Conversely, the use of SMS continues to decrease in almost all EU MS since 2010, albeit at a different pace: In Finland and Germany, SMS volumes have dropped to levels of 2006, while the decline has been slower in countries like Spain and France. Few countries observed stagnant volumes (Poland) or even a growth from previously low levels (Estonia).

On the individual level, the average *WhatsApp* user is reported to send approximately 40 (while receiving around 80) messages per day as opposed to an estimated number of 4.5 SMS. This ratio of approximately 1:10 for daily SMS versus OTTs messages is likely to be much higher in practice, due to the reported parallel use of multiple messaging apps.

It appears undeniable that **OTTs have become crucial players of the electronic communications market**, which may correlatively have led to loss of revenues of traditional players[210].

According to Informa, global annual SMS revenues would fall by 20% between 2013 and 2018, and this decline in global SMS revenues would largely be caused by the continuing adoption and use of over-the-top (OTT) messaging applications in both developed and emerging markets[211]. The growth of popularity of OTTs may be one of the sources of the observed erosion of revenues of ECSs over time in service areas that have been substituted by OTTs today, e.g. instant messaging instead of SMS or MMS. Popular examples are WhatsApp, Apple's iMessage and Facebook Messenger.

The study also indicates that between 2008 and 2014 fixed and mobile revenues have been declining in the EU, each with 19% - mainly driven by a decline in traffic related revenues.

[210] E.g. European Commission Study carried out by ECORYS, TNO and others (2016), Study on future trends and business models in communication services, (SMART 2013/0019), p. 60-61 and 64.

[211] Informa's World Cellular Revenue Forecasts 2013-2018 and Informa's World Cellular Revenue Forecasts 2018; 2013. Available from: http://www.telecoms.com/197721/ott-app-use-undermining-sms-revenue/.

ANNEX V: REFIT analysis of coherence of the ePrivacy Directive with the GDPR

As Article 1.2 of the ePrivacy Directive makes clear, its provisions particularise and complement the Data Protection Directive. Article 95 of the General Data Protection Regulation states that it does not impose additional obligations for the processing of personal data on ECS providers in relation to matters for which they are subject to specific obligations with the same objective set out in the ePrivacy Directive. In other words, the ePrivacy Directive should override the GDPR with regard to obligations of a similar nature, while Recital 173 of the GDPR called upon the need to revise the ePrivacy Directive to adapt to the changes brought by the GDPR, and ensure consistency between the two instruments. Finally, the main purpose of this REFIT evaluation is to assess which existing provisions of the ePD may appear redundant, out-of-date or not needed anymore.

In the table below is presented the connection between the ePD and the GDPR. For each relevant provision[212] there is a brief analysis of "**coherency check**", using the following colour code:

- **Green**: positive relationship (e.g. synergies);
- **Grey**: neutral relationship/no challenges nor positive aspects identified; and
- **Yellow**: potential challenges.

PROVISIONS OF THE ePRIVACY DIRECTIVE	PROVISIONS OF THE GDPR	COHERENCY TEST	RESULT
Scope and aim (Article 1)	- Subject-matter and objectives (Article 1) - Material scope (Article 2)	Close connection, as the ePD acts as *lex specialis* in relation to the GDPR. However, the relationship is clear. There is a need to revise the geographical scope of	**NEUTRAL**

[212] Only those instruments and provisions that a have connection to the ePD are listed.

		the ePD in the light of the GDPR.	
Definitions (Article 2)	- Definitions (Article 4)	ePD to be adjusted to refer to the GDPR instead of the General Data Protection Directive and apply GDPR definitions to ePD – e.g. personal data, consent. However, no challenges could be identified.	**NEUTRAL**
Services concerned (Article 3)	- Material scope (Article 2)	There may be a lack of clarity as when the ePD and when the GDPR applies, as to what exactly fall into the definition of "public or publicly available electronic communications services".	**NEUTRAL**
Article 4.1 and 4.1a security requirement ECS must take appropriate measures to safeguard security of its services (e.g. personal data can be accessed only by authorised personnel, protect personal data against accidental or unlawful destruction)	- Principles relating to processing of personal data (Article 5.1e) - Data protection by design and by default principles (Article 25) - Security of processing (Article 32 and recital 39[213])	**Overlap** The provision is mirrored in Article 32 of the GDPR	**NEGATIVE** ➢ **Redundancy**
Article 4.2 Notification of risks	- It is not covered by the security requirements under the GDPR	**No overlap** The aim of the article (notify users of risks, such as	**NEUTRAL**

[213] Recital 39 of the GDPR *"Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing".*

ECS must inform subscribers concerning security risks		virus and other vulnerabilities) remains fully relevant. It is also in line with one of the NIS Directive pillars, namely ensuring a culture of security across sectors and promoting awareness and control among users.	
Article 4.3.; 4.4; 4.5 Notification of personal data breaches	- Notification of a personal data breach to the supervisory authority (Article 33) - Communication of a personal data breach to the data subject (Article 34)	**Overlap** The data breach notification requirements (Article 4.3, 4.4 and 4.5 of the ePD) overlap with the similar obligations under the GDPR (Article 33 and 34).	**NEGATIVE** - **Redundancy**
Article on 5.1 & 5.2 – Confidentiality of Communications Prohibition on 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 users concerned	- Principles relating to processing of personal data (Article 5) - Security of processing (Article 32)	**No overlap** The **GDPR has not specifically addressed** the right to confidentiality of *communications and related traffic data*. It does not contain any prohibition on listening, tapping, storage or other kinds of interception or surveillance of electronic communications. The GDPR contains an obligation upon data controllers and processors to ensure appropriate security, confidentiality and integrity of *personal data* under the principles of processing personal data (Article 5.1.f)[214], and in the specific security provision (Article 32 of the GDPR). The principle of Confidentiality of Communications is also afforded	**POSITIVE**

[214] This principle is referred to as the principle of 'integrity and confidentiality', although only security obligations are mentioned in Article 5.1.f.

		to legal persons (not protected by the GDPR), thus leading to **the protection of business secrets.**	
Article 5.3 on Confidentiality of Terminal equipment No storage of information or access to information already stored (e.g. photos, contacts) in a user's device, unless consent is given.	- Definition of personal data (Article 4.1) - Conditions for consent (Article 7) and recital 42 - Transparent information (Article 12), - Information to be given when personal data collected from data subject (Article 13) - Information to be given where personal data not obtained from data subject (Article 14). - Right to object (Article 21) - Automated individual decision-making, including profiling (Article 22) - Data protection by design and by default (Article 25)	**No overlap** The new definition of personal data clarifies that online identifiers are personal data. Need to rely on the new definition of consent under the GDPR (Article 7 and recitals 42, 43) The GDPR further complements the level of information to be provided to the data subjects under Article 12, Article 13 and Article 14. The obligation to inform about processing of personal data is therefore covered by the GDPR. The objective of protection of Article 5.3 of the ePD should be enhanced by the principle of data protection by design and by default under Article 25 of the GDPR[215].	**POSITIVE**

[215] Article 25 of the GDPR: "*The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed (….) such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*"

Article 6 on Traffic Data Traffic data must be erased or made anonymous when it is no longer needed to transmit the communication or for billing purposes	- Definition of Personal Data (Article 4.1) - Principles relating to processing of personal data (Article 5.1 b and e) - Lawful grounds for processing (Article 6) - Condition for consent (Article 7 and recital 42) - Security of processing (Article 32)	**Potential overlap** The GDPR does not explicitly refer to traffic data nor provide for a specific regime. Regarding the specific rules on traffic data, the ePD provides for a specific protection as it limits the legal basis to consent for the processing of these data by ECS providers. A limited set of derogations apply: billing purposes, anonymised data. It provides for additional safeguards (obligation to erase and timing when this needs to be done). It also provides specific requirements about the handling of traffic data. Given the intrinsic connection between traffic and content data, increasingly it is becoming more difficult to separate both concepts. The GDPR allows other legal grounds, such as the legitimate interest of data controller or the performance of a contract as well as imposing obligations on data controllers and processors and rights for data subjects. But the principles of processing will apply in any case, in particular: • the '**data minimisation' principle** (Art. 5.1(c) GDPR): the processing of personal data needs to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. • the '**storage limitation' principle** (Art. 5.1(e) GDPR): personal data may only kept in a form	**POTENTIAL CHALLENGES** **Specific protection must be demonstrated to remain**

		which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. • The principle of data protection by design and default (Article 25), the requirement for data protection impact assessments (Article 35) • The clarification under Article 6.3 of the ePD that consent can be withdrawn at any time is redundant with Article 7.3 of the GDPR setting the conditions for consent.	
Article 7 on Itemised bills Subscribers have the right to receive non-itemised bills	- Itemised Billing is not expressly regulated in the GDPR. - This provision related to personal data is more specific.	**No overlap** Uncertain there is a need for a legal provision, the possibility to receive non-detailed bills is often proposed contractually and may not require a legal requirement.	**NEUTRAL**
Articles 8 on presentation and restriction of calling & connected line identification and Article 10 on exceptions	- The GDPR does not contain specific references to calling and connected line identification	**No overlap** The ePD particularises a specific situation that is not otherwise regulated in the GDPR. The ePD brings forth greater clarity as to the exercise of such rights (for example, by obliging providers to offer this functionality free of charge).	**NEUTRAL**

Article 9 on Location data other than traffic Data Location data can only be processed when made anonymous or after user's consent	- Definition of Personal Data (Article 4.1) - Principles relating to processing of personal data (Article 5.1b and e) - Lawful grounds for processing (Article 6) - Condition for consent (Article 7) and recital 42 - Security of processing (Article 32)	**Overlap** Location data related to electronic communications is already regulated by Article 6 of the ePD. Article 9 of the ePD covers location data other than traffic data. The clarification under Article 9.1 of the ePD that consent can be withdrawn at any time is redundant with Article 7.3 of the GDPR setting the conditions for consent. However, Article 4.1 of the GDPR clarifies that location data are personal data. Therefore, these data could fall under the GDPR, unless the specific protection afforded by the ePD when location data are processed by ECS is still considered necessary.	**POTENTIAL CHALLENGES** **Specific protection must be demonstrated to remain**
Article 11 on automatic call forwarding	- The GDPR does not contain provisions on automatic call forwarding. - This provision related to personal data is more specific.	**No overlap** Automatic call forwarding is specifically addressed by the ePD. The closest parallel in the GDPR is the right to object to the processing of personal data under Article 21 of the GDPR, which however has a different scope.	**NEUTRAL**
Article 12 on Subscribers' directories	- Conditions for consent (Article 7) - Transparent information(Article 12), - Information when personal data collected from data subject	Article 12 of the ePD provides for a more specific protection that in the GDPR, also **protecting the interests of legal persons**. Under Article 6 of the GDPR consent would be one legal ground among others. However, the GDPR ensures that data subjects are informed when their	**NEUTRAL**

	(Article 13) - Right to object (Article 21) - Right to be forgotten (Article 17) Information provided where personal data not obtained from data subject (Article 14).	data are processed (Articles 12, 13 and 14).	
Article 13 on Unsolicited communications Rules on e.g. automated or person-to-person marketing calls, marketing emails and SMS	- Lawful grounds for processing (Article 6 and recital 47[216]) - Conditions for consent (Article 7) - Right to object (Article 21)	**No overlap but need for clarification of relationship** The GDPR and the rules on unsolicited communications of the ePrivacy Directive **do not overlap but they are complementary.** The **GDPR regulates the legal grounds to process personal data,** including if the purpose is to use them for direct marketing. - It also clarifies 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). - The rules of Article 13 of the ePD details **under which conditions citizens and legal persons can be contacted using electronic communications**	**POSITIVE**

[216] Recital 47 of the GDPR: "*The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.*"

		networks to send them commercial communications.	
Article 14 on standards No mandatory requirements must be imposed on devices which could impede the free movement of goods	- Data protection by design and by default (Article 25)	Paragraph 1 of Article 14 of the ePD seeks to ensure the flow of personal data, in accordance with one of the two overarching objectives of the Directive. This goal, as noted above, is shared with the GDPR, This provision seeks to ensure the free movement of terminal equipment, one of the objectives of the ePD.	**NEUTRAL**
Article 15 on exemption to the ePD for national security purposes, criminal matters etc.	- Article 23 of the GDPR	Article 15 of the ePD details the derogations to the specific provisions on confidentiality of communications of the ePD and the safeguards that must be respected by MS when doing so. Article 23 of the GDPR details these derogations for the provisions of the GDPR. Compared to Article 15 of the ePD, Article 23 sets forth with more precision the specific minimum required content of Union or national laws providing for specific restrictions. In particular, they have to contain specific provisions on a number of elements, such as among others the purposes of the processing or categories of processing, the categories of personal data, the scope of the restrictions introduced, the safeguards to prevent abuse or unlawful access or transfer and the storage periods.	**NEUTRAL**
Article 15a on competent	- **CHAPTER VI on independent**	The ePD leaves it to Member States to decide which	**POTENTIAL CHALLENGES**

authorities and enforcement Leaves it to MS to decide which should be the competent authorities.	**competent authorities** - Competences and powers (Articles 55, 56, 57, 58) - Cooperation and consistency mechanism (Article 60, 61, 62, 63) - Section III (EDPB) - General conditions for imposing administrative fines (Article 83) - Penalties (Article 84)	should be the competent authority. There are differences as concerns the powers, (including fines) and sanctions for the breach of provisions related to the processing of personal data. Modifying the rules and relying on the approach of the GDPR would enhance enforcement.	

ANNEX VI:

Competent national authorities to enforce the ePrivacy Directive implementing provisions (Articles 5, 6, 9 & 13):

The enforcement of the ePD provisions at national level is entrusted to a "*competent national authority*" (Article 15a of the ePD), without further defining that authority or body. This has led to a fragmented situation in the EU and within Member States. Member States have allocated the competence to DPAs, telecom NRAs, to another type of body (e.g. consumer protection bodies) or to several different bodies within the same country.

Moreover, there is no recognised EU group to gather together all authorities responsible for the enforcement of the ePD: indeed, DPAs meet through the Article 29 Working Party, NRAs through BEREC. Some consumer bodies meet through the Consumer Protection Cooperation (CPC) network.

Country	Article 5	Articles 6 & 9	Article 13
Austria	NRA Telecom office	NRA Telecom office	NRA Telecom office DPA
Belgium	NRA Ombudsman for telecoms Regional supervisory authorities for the media sector DPA	NRA Ombudsman for telecoms Regional supervisory authorities for the media sector	NRA Ombudsman for telecoms Regional supervisory authorities for the media sector Ministry for Economy DPA
Bulgaria	NRA DPA Commission for Consumer Protection	NRA Commission for Consumer Protection	NRA Commission for Consumer Protection DPA
Croatia	NRA DPA	NRA DPA	NRA DPA Ministry for Economic Affairs Ministry of Finance
Cyprus	NRA DPA	NRA DPA	NRA DPA
Czech Republic	DPA	DPA	DPA
Denmark	DPA	The Telecommunications Complaints Board	Competition and Consumer Authority Consumer Ombudsman
Estonia	NRA	NRA	DPA
Finland	NRA	DPA	DPA
France	DPA NRA	DPA NRA	DPA NRA Ministry for Economic Affairs
Germany	DPA NRA Data Protection Commissioners of the German Lands (for art. 5.3)	DPA NRA	DPA NRA

Country	Article 5	Articles 6 & 9	Article 13
Greece	DPA NRA	DPA NRA	DPA NRA
Hungary	DPA NRA (except Article 5.3)	DPA NRA	NRA DPA Consumer Protection Inspectorates / National Authority
Ireland	DPA	DPA NRA	DPA
Italy	DPA	DPA	DPA
Latvia	Ministry of Transport NRA DPA - Article 5.3	Ministry of Transport DPA	Ministry of Transport DPA Consumer Protection Authority
Lituania	DPA	DPA	DPA
Luxembourg	DPA	DPA	DPA
Malta	DPA	DPA	DPA
The Netherlands	Consumer Protection Authority DPA NRA (5.1)	DPA NRA	Consumer Protection Authority DPA
Poland	DPA NRA	DPA NRA	DPA Office of Competition and Consumer Protection NRA
Portugal	DPA NRA (5.1)	DPA	DPA
Romania	DPA	DPA	DPA
Slovakia	Ministry of Transport NRA Ministry of Finance (5.3)	Ministry of Transport NRA	Ministry of Transport NRA
Slovenia	NRA	NRA DPA	NRA Market Inspectorate
Spain	DPA	DPA	DPA
Sweden	NRA	NRA	Consumer Agency
UK	NRA DPA	NRA DPA	NRA DPA Financial Authority

Source: on the basis of European Commission Study carried out by time.lex and Spark (2015), Study on the "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071).