P

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 6/2017

EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)

EDPS

24 April 2017

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion provides comments and recommendations on how to better safeguard the right to privacy, confidentiality of communications and the protection of personal data in the proposed Regulation on Privacy and Electronic Communications, which is intended to repeal and replace the ePrivacy Directive (2002/58/EC).

Executive Summary

This Opinion outlines the position of the EDPS on the Proposal for a Regulation on Privacy and Electronic Communications, which is to repeal and replace the ePrivacy Directive.

Without the ePrivacy Regulation, the EU privacy and data protection framework would be incomplete. While the GDPR -the General Data Protection Regulation- is a great achievement, we need a specific legal tool to protect the right to private life guaranteed by Article 7 of the Charter of Fundamental Rights, of which confidentiality of communications is an essential component. The EDPS therefore welcomes and supports the Proposal which aims to do just that. The EDPS also supports the choice of legal instrument, i.e. a regulation which will be directly applicable and contribute to a greater level of harmonisation and consistency. He welcomes the ambition to provide a high level of protection with respect to both content and metadata and supports the objective of extending the confidentiality obligations to a broader range of services - including the so-called 'over the top' services (OTTs) - which reflects the progress of technology. He also considers that the decision to grant enforcement powers solely to data protection authorities, and the availability of the cooperation and consistency mechanisms within the future European Data Protection Board (EDPB), will contribute to more consistent and effective enforcement across the EU.

At the same time, the EDPS has concerns whether the Proposal, as it stands, can in fact deliver on its promise to ensure a high level of protection of privacy in electronic communications. We need a new legal framework for ePrivacy, but we need a smarter, clearer and stronger one. There is still a lot to do: the complexity of the rules, as outlined in the Proposal, is daunting. Communications are sliced into metadata, content data, data emitted by terminal equipment. Each being entitled to a different level of confidentiality and subject to different exceptions. This complexity may bring a risk of -perhaps unintended- gaps in protection.

Most of the definitions on which the Proposal relies will be negotiated and decided in the context of a different legal instrument: the European Electronic Communications Code. There is no legal justification today for linking the two instruments so closely and the competition and market-focused definitions from the Code are simply not fit for purpose in the fundamental rights context. The EDPS therefore argues for including a set of necessary definitions in the ePrivacy Regulation, taking into account its intended scope and objectives.

We also need to pay particular attention to the question of processing of electronic communications data by controllers other than providers of electronic communications services. The additional protections offered to communications data would be pointless if they could easily be circumvented by, for example, transferring the data to third parties. It should also be ensured that the ePrivacy rules do not permit a lower standard of protection than that enshrined in the GDPR. For example, consent should be genuine, offering a freely given choice to users, as required under the GDPR. There should be no more 'tracking walls'. In addition, the new rules must also set strong requirements for privacy by design and by default. Finally, in this Opinion, the EDPS also addresses other pressing issues, including the restrictions to the scope of the rights.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,
Having regard to the Treaty of the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and to 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),

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular Articles 28(2), 41(2) and 46(d) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

This Opinion (Opinion) is in response to a request of the European Commission (Commission) to the European Data Protection Supervisor (EDPS), as an independent supervisory authority and advisory body, to provide an opinion on the Proposal for a Regulation on Privacy and Electronic Communications[1] (the Proposal). The Proposal is intended to repeal and replace Directive 2002/58/EC on privacy and electronic communications (the ePrivacy Directive)[2]. The Commission also requested the opinion of the Article 29 Data Protection Working Party (WP29), to which the EDPS contributed as a full member[3].

This Opinion follows upon our Preliminary Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC)[4], issued on 22 July 2016. The EDPS may also provide further advice in subsequent stages of the legislative procedure.

The Proposal is one of the key initiatives of the Digital Single Market Strategy[5], aimed at reinforcing trust and security in digital services in the EU with a focus on ensuring a high level of protection for citizens and a level playing field for all market players across the EU.

The Proposal seeks to modernise and update the ePrivacy Directive as part of the wider effort to provide a coherent and harmonised legal framework for data protection in Europe. The ePrivacy Directive particularises and complements Directive 95/46/EC[6], which will be replaced by the recently adopted General Data Protection Regulation (GDPR)[7].

The EDPS first, in Section 2, summarises his main observations about the Proposal, focusing on the Proposal's positive aspects. Second, in Section 3, he raises his remaining key concerns and provides recommendations how to address them. Additional concerns and recommendations for further improvements are described in the Annex to this Opinion, discussing the Proposal in more detail. Addressing the concerns raised in this Opinion and its Annex and further improving the text of the ePrivacy Regulation would not only serve to better

protect end-users and other data subjects concerned, but also introduce more legal certainty for all stakeholders involved.

2. NEED FOR A DEDICATED LEGAL INSTRUMENT FOR ePRIVACY

2.1 The main positive aspects of the Proposal

The EDPS welcomes the Commission's proposal for a modernised, updated and strengthened ePrivacy Regulation. He shares the view, repeatedly expressed also by the WP29 both in its preliminary and more recent opinions[8] as well as by civil society groups in their preliminary and more recent joint analysis[9], that there is a continued need to have specific rules to protect the confidentiality and security of electronic communications in the EU and to complement and particularise the requirements of the GDPR. He also considers that we need simple, targeted and technologically neutral legal provisions that provide strong, smart and effective protection for the foreseeable future.

The EDPS also welcomes the fact that many of his comments outlined in his Preliminary Opinion as well as in his informal comments have been taken into account, which has notably contributed to the quality of the Proposal. He welcomes the declared ambition to provide a high level of protection with respect to both content and metadata, in particular:

- the choice of a regulation over a directive as the form of legal instrument, which may ensure a more consistent level of protection across the European Union;
- the extension of the scope to cover OTT ('*over-the-top*') providers;
- the approach of allowing processing only under clearly defined conditions;
- the modernisation of the current consent requirements under the new Articles 9 and 10;
- focusing security provisions on issues specific to communications services and ensuring full alignment with the GDPR on data breaches;
- the choice of making the same authorities responsible for supervision of the rules under the GDPR and the ePrivacy Regulation;
- and the opt-in rule for all unsolicited commercial communications.

2.2 Confidentiality of electronic communications must remain protected

The right to the confidentiality of communications is a fundamental right protected under Article 7 of the Charter of Fundamental Rights of the European Union (the Charter) - the modern-day equivalent of traditional (postal) statutes guaranteeing the secrecy of correspondence[10].

Confidentiality of communications is essential for the functioning of modern societies and economies: without trustworthy messengers who deliver information to the recipients without using it for their own purposes, disclosing it to third parties, modifying the content, suppressing or delaying the delivery, many private and public activities could only be conducted face to face.

While the economic and social importance of trustworthy communications cannot be overstated, the protection of the fundamental right to privacy against any interference, especially from state authorities, is its central legal function.

In order to ensure legal certainty, it is crucial to have clear and specific legal rules in secondary legislation to put into practice the principle of confidentiality of electronic communications. Relying merely on a single article in the Charter -at the EU level- is insufficient. In the current legal framework the ePrivacy Directive is the instrument of EU secondary legislation that lays down the necessary, specific legal requirements.

The recognition of confidentiality of communications as a fundamental right in the Charter is in line with European constitutional traditions: the majority of EU Member States also recognise confidentiality of communications as a distinct constitutional right[11]. New more harmonised provisions at EU level contribute to greater legal certainty. As such, they benefit individuals, who are provided equal protection across Europe, as well as businesses, especially those operating in multiple jurisdictions.

2.3 Current level of protection must not be reduced

In addition to implementing the fundamental right to privacy for electronic communications, the ePrivacy Regulation must also serve to maintain the fundamental right to the protection of personal data according to Article 8 of the Charter. This is of particular importance for those situations for which the ePrivacy Directive provides more specific safeguards than those foreseen in the GDPR in order to ensure a higher level of protection for personal data to counter specific risks related to communications data.

For example, whereas the GDPR does not specifically regulate which one of the possible legal grounds for processing may be permitted in which situations, the ePrivacy Directive, and the proposed ePrivacy Regulation, are more precise in some specific contexts by requiring consent as a legal basis[12].

It is similarly crucial that the new rules should not lower the level of protection below the protections provided by the GDPR, by creating derogations from GDPR rules.

Further, in addition to the fundamental rights of individuals, the Proposal maintains the protection of certain rights of legal persons. This applies with regard to unsolicited communications as well as in other aspects in their role as subscribers or users of electronic communications services. While the GDPR does not cover these needs[13], this protection is important in view of the crucial importance of trustworthy and secure electronic communications for the functioning of our society and economy[14].

2.4 Simple, straightforward rules are needed to ensure consistency and legal certainty

The ePrivacy Regulation must also ensure that the new rules will provide simple, straightforward rules across Europe, which are effectively and uniformly enforced. From this perspective, the following aspects of the Proposal are particularly welcome.

The choice of a regulation versus a directive

The EDPS welcomes, as he recommended in his Preliminary Opinion, that the legislators chose a regulation rather than a directive as the form of the new legal instrument. This is consistent with the approach taken in the GDPR; ensures a more consistent and equal level of protection for individuals and other entities protected by its provisions; helps ensure a level playing field for organisations that need to comply with its provisions, and reduces their compliance costs.

Supervision and enforcement

The EDPS welcomes the fact that, as recommended in his Preliminary Opinion, Article 18 of the Proposal gives data protection authorities the power to monitor the application of the ePrivacy Regulation; as well as the application of the cooperation and consistency mechanism under the GDPR to matters falling under the scope of the ePrivacy Regulation. Harmonisation with regard to enforcement powers, including the level of fines, is also welcome[15].

Need for simple, straightforward rules

The ePrivacy Directive, and now also the Proposal, provide rules for a number of situations in which the assessment of whether the processing of personal data is involved, who is the controller or processor, and who would be the data subjects, could be extremely complex. This concerns, among others, technical circumstances related to some network operations (e.g. caller identification), the integrity of the users' end points (information on user terminals) and use of communications services for direct marketing purposes.

It is therefore welcome that the Proposal, as did the ePrivacy Directive, resolves such situations by covering the roles and actions related to the use of communications services without requiring any analysis under the GDPR. Given that the provisions of the ePrivacy Directive have been subject to diversity in interpretation, the ePrivacy Regulation provides an opportunity to clarify certain terms or concepts.

2.5 Extension of scope of the ePrivacy Regulation is essential

We welcome the Commission's ambition to extend the scope of the protection and update the rules so that they cover new ways of providing communications services. Merely maintaining currently available protection would empty these rights of their substance for an increasingly large portion of our everyday communications.

Instant Messaging and Voice over IP

As already mentioned in our Preliminary Opinion, individuals must be afforded the same level of protection for all functionally equivalent services, irrespective whether they are provided by traditional fixed line or mobile telephone and messaging (SMS, MMS) services on one hand, and OTT communications services such as Voice over IP (VoIP)[16] and instant messaging apps on the other hand.

Users' expectations are often similar with regard to the privacy and confidentiality of these messages and any breach of confidentiality may be equally intrusive. For example, a user may begin a conversation using the messaging function of a game, then move to an OTT instant messaging service, exchange mobile SMS' and MMS' and eventually launch a call between two phones. All these different types of communications may be performed by using the same devices, i.e. smartphones, and for the user the different legal frameworks for the services used are by no means evident or even understandable.

In light of the above, the EDPS welcomes the fact that recital 11 of the Proposal recognises the need to extend the scope to functionally equivalent services and also provides some examples of such services, in particular '*Voice over IP, messaging services and web-based e-mail services'*.

As also recommended in our Preliminary Opinion, there is a need to go further: protect not only communications that are '*functionally equivalent'* with services offered by traditional telecommunications service providers, but also those services that offer new opportunities for communication, possibly as an addition to other services. As part of these efforts, it is necessary to ensure that communications functionalities integrated into other services (e.g. messaging functionalities in gaming, dating apps) should also benefit from the same protection.

For this reason, the EDPS specifically welcomes the fact that so-called *'ancillary'* services are explicitly referred to and covered by Article 4(2) of the Proposal.

Internet of Things (IoT)

While we commonly refer to the 'Internet of Things', in reality it is mostly an *'Internet of Things which are connected to people'*: IoT includes sports trackers, health sensors, personal communications devices, smart TVs, intelligent cars and many other devices. They are equipped with sensors for sound, video, movement and physical parameters of their owners. The fact that they launch their data transfers and communications sometimes without the owner triggering it (or even being aware) cannot be a reason to give lower protection to such often sensitive communications.

The protection of communications privacy should not be dependent on whether humans themselves speak or listen, type or read the content of a communication, or whether they simply rely on the increasingly smart features of their terminal devices to communicate content on their behalf. 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.

EDPS welcomes the fact that Article 2(1) of the Proposal[17] clarifies that the purpose and content of a communication must not affect its protection under the right to privacy. The EDPS also welcomes the fact that recital 12 specifically refers to the Internet of Things, machine to machine communications and aims to ensure that the Proposal will unambiguously cover machine-to-machine communications in the context of the Internet of Things, irrespective of the type of network or communication service used, on all networks and services which are otherwise within the scope.

Covering networks of different types

The EDPS also welcomes the Commission's ambition to bring all publicly accessible networks and services within the scope of the confidentiality requirements. These should cover, for example, Wi-Fi services in hotels, restaurants, coffee shops, shops, trains, airports and networks offered by hospitals, universities to the users of their main services (patients or students respectively), as well as corporate Wi-Fi access offered to visitors and guests, and hotspots created by public administrations[18].

3. KEY CONCERNS AND RECOMMENDATIONS

Whilst welcoming the Proposal, the EDPS remains concerned about a number of provisions that risk undermining the intention of the Commission to ensure a high level of protection of privacy in electronic communications. In particular, the EDPS has the following key concerns:

- the definitions in the Proposal must not depend on the separate legislative procedure concerning the Directive establishing the European Electronic Communications Code[19] (the EECC Proposal);
- the provisions on end-user consent need to be strengthened. Consent must be requested from the individuals who are using the services, whether or not they have subscribed for them and from all parties to a communication. In addition, other data subjects who are not parties to the communications must also be protected;
- it must be ensured that the relationship between the GDPR and the ePrivacy Regulation does not leave loopholes for the protection of personal data. Personal data collected based on end-user consent or another legal ground under the ePrivacy Regulation must not be subsequently further processed outside the scope of such consent or exception on a legal ground which might otherwise be available under the GDPR, but not under the ePrivacy Regulation;
- the Proposal lacks ambition with regard to the so-called '*tracking walls'* (also known as *'cookie walls'*). Access to websites must not be made conditional upon the individual being forced to '*consent'* to being tracked across websites. In other words, the EDPS calls on the legislators to ensure that consent will be genuinely freely given;
- the Proposal fails to ensure that browsers (and other software placed on the market permitting electronic communications) will by default be set to prevent tracking individuals' digital footsteps;
- the exceptions regarding tracking of location of terminal equipment are too broad and lack adequate safeguards;
- the Proposal includes the possibility for Member States to introduce restrictions. These call for specific safeguards.

These main concerns -along with recommendations how to address them- are outlined in this Section 3.

3.1 Scope and definitions

The EDPS welcomes the intention to define the material scope of the ePrivacy Regulation based on its objective to ensure consistent and comprehensive protection of the fundamental rights of privacy, confidentiality of communications and data protection. By creating a self-standing instrument, no longer integrated into a framework for competition and market rules, it becomes possible to define the scope of the new ePrivacy Regulation in such a way that the focus of scope and definitions be on the protection of fundamental rights, rather than on economic factors and concerns relating to fair competition and efficient use of resources.

The core concepts used in the ePrivacy Regulation must be carefully defined to achieve its full effectiveness. The EDPS is concerned that this effect could be weakened or undermined by the lack of precision and clarity of some of the definitions, and unnecessary dependencies on the EECC Proposal. This could take away rights from the individuals concerned or restrict the scope of the Regulation in an unjustified manner.

Avoid dependence on EECC definitions

When the comprehensive framework for electronic communications was adopted in 2002, the ePrivacy Directive was an integral part of that framework. Nevertheless, the legislators realised that a set of definitions needed for a competitive and fair market for electronic communications services and related purposes was not fully adequate for the protection of fundamental rights.

Accordingly, central terms of the framework –such as '*user'* and *'communication'*– were specifically defined in the ePrivacy Directive for the purposes of that instrument, deviating from the general definitions of the Framework Directive[20]. The 2009 reform of the framework kept the connection between the instruments intact, but also maintained the separate definitions of the ePrivacy Directive.

With the current legislative process, the legislators are faced with proposals for instruments which are much more independent of each other:

- The EECC Proposal comprises rules for the electronic communications market to ensure a true single market for communications, efficient use of spectrum, incentives for investment in broadband, a level playing field for market players and effective regulation;
- The ePrivacy Proposal aims to provide a high level of privacy protection for users of electronic communications services, and to increase trust in and security of digital services[21].

Unlike the exercises of 2002 and 2009, the 2017 review does not intend to preserve the synchronicity of the legislative process for the different areas, but clearly separates between the rules relating to markets and those on the protection of fundamental rights. Accordingly, the configurations in which the legislative bodies work on these proposals are not always identical, so that coordination of the two procedures becomes even more unlikely.

The EDPS welcomes the separation of the fundamental rights aspect from the economic aspect and the creation of a dedicated and independent instrument focused on the protection of the fundamental rights of privacy and data protection of individuals using electronic communications services. The EDPS appeals, however, to the legislators to fully apply the logic of this approach. In this light the EDPS does not see the need for the EECC Proposal definitions to be automatically applicable in the present context. Indeed, the distinguishing criterion for defining the scope of the ePrivacy Regulation should be protection of fundamental rights, and not exclusively the economic factors related to fair competition and efficient use of resources. Furthermore, even where definitions might be identical in the text of the two proposals, it would be preferable to include fully standalone definitions in the ePrivacy Regulation, where necessary particularised because of the specific context of the protection of fundamental rights. This, also in order to avoid changes to the meaning of its provisions being caused by amendments in the legislative process on the EECC, and without prejudice of the necessary consistency of the two areas of legislation.

The dependence of key definitions in the Proposal on the separate parallel legislative procedure for the EECC Proposal creates unnecessary and avoidable risks for the clarity and effectiveness of the ePrivacy Regulation: as long as the EECC Proposal is not adopted, its definitions can still change, and where these definitions are used in the ePrivacy Proposal, this would affect the meaning and impact of its provisions. As already seen in the past, it cannot be generally expected that the definitions created for purposes of economic regulation are as such adequate for the protection of fundamental rights. **For these reasons, the EDPS recommends removing the unnecessary dependencies on the EECC Proposal and defining central terms in the ePrivacy Regulation itself, consistent with the EECC Proposal though not necessarily identical. This, would also facilitate the reading of the ePrivacy Regulation by an average user.**

Clearly identify the individuals concerned

For instance, the definition of *'end-user'* has a central function in the ePrivacy Proposal, as it should designate the entity whose fundamental rights are to be protected. However, the definition of *'end-user'* in the EECC Proposal refers to natural persons *or legal entities* who have a contract with an electronic communications service provider and do not provide electronic communications services[22]. Using the term *'end-user'* with this meaning does not guarantee that the fundamental rights of all individuals using electronic communications services are adequately protected. Where individual fundamental rights are concerned, the proposal should use a term properly defined for this objective, referring to *a natural person using electronic communications services without necessarily having subscribed to it*. This would be appropriate for many provisions, including in Articles 6 and 8, while there are some provisions where the reference to an entity which has a contractual relationship with a service provider is useful (e.g. in Article 15 on public directories). Section 3.2 analyses in more detail the risks resulting from allocating decisions on fundamental rights to other entities than the individuals concerned.

Create clarity on the services covered

As highlighted in Section 2.5, the EDPS emphasizes that the extension of the *material* scope is a long-needed adjustment of the legislation to the technological and economic developments. Individuals should be able to rely on the confidentiality of their communications, regardless of whether they use SMS or an internet messenger service. Definitions referring to the different subsets of services are critical for the determination of the scope of the instrument. The adjustment of the definition of *'interpersonal communications service'* in Article 4(2) to include also ancillary services is therefore very much welcome. This adjustment illustrates very clearly that the scope of the ePrivacy Regulation is not intended to be identical to that of the EECC Proposal and that it may need specific or different definitions than the EECC. For the protection of the confidentiality of communications it is not relevant whether the service used to communicate is central or ancillary from the point of view of its provider.

Make sure that all communications data is covered

When defining communications metadata, in its Article 4(3)(c), the Proposal refers only to '*data processed in an electronic communications network'*. This could create a gap of protection when some of the data determining the processing of communications content is processed by equipment, which is part of the service infrastructure, but not considered part of the network. This could be the case when such data is processed by equipment, which is considered *'associated facilities'* within the meaning of the EECC.

In order to avoid such gaps in protection, the definition of metadata in Article 4(3)(c) should encompass not only any data that is processed *'in an electronic communications network',* but also any data that is processed by any other equipment for the provision of the service and which is not considered content.

Further, from the point of view of a communications provider who is subject to the ePrivacy Regulation, the content or purpose of a communication cannot play a role for the treatment of its confidentiality and security. The provider should not be concerned whether the message transmitted is the reading of a heart rate monitor or a stock exchange transaction order from a smart trading application, or a photo of a flower bouquet accompanying a wedding invitation. Effective and efficient service, and respect for privacy and security, must be ensured

accordingly for all communications. Where certain types of communications require specific actions by the network, many existing communications protocols permit the specification of these requirements as part of the communications metadata. In the interest of trustworthy services, this method should be applied rather than breaching confidentiality for this purpose.

Protecting communications data in the 'cloud'

An additional concern is that the ePrivacy Regulation must not only clearly provide for the confidentiality and security of communications while in transit but must also protect the confidentiality and security of end user equipment and communications data stored in the *'cloud'*. **The EDPS recommends that Article 5 and Recital 15 of the Proposal should be revised to clearly cover both situations.**

Recital 15 of the Proposal, as currently drafted, seems to cover only data in transit: it provides that '*the prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the communication by the intended addressee'.*

While Article 8(1) and 8(2) would also protect communications stored on terminal equipment, the Regulation should also be clear in providing the same level of protection for communications stored on other equipment than user terminals, e.g. in mailboxes operated by a service provider or any cloud storage used as part of the communications service[23]. Indeed, the EDPS would emphasise that new technical paradigms (e.g. cloud computing) further increase the importance of confidentiality[24].

As explained by the WP29 in its Opinion 1/2017[25], the scope of the protection outlined in the quoted text in recital 15 is based on a conceptual framework of communications, which is outdated. Today most communications data remain stored with service providers, even after receipt. It should be ensured that the confidentiality of these data remains protected. In addition, communication between subscribers of the same cloud-based services (for instance webmail providers) will often entail only very little conveyance: sending an email would mostly involve reflecting this in the database of the provider, rather than actually sending communications between two parties.

More generally, the EDPS recommends that thorough scrutiny be applied to the entire body of definitions used in the proposed Regulation, in order to avoid unnecessary dependencies on the EECC Proposal and to ensure that the level of protection is not lowered compared to that under the current ePrivacy Directive.

3.2 Consent should be requested from the individuals whose rights are affected

The EDPS welcomes the declared ambition of the Commission to provide a high level of protection to both content and metadata by giving consent, as defined in the GDPR, a central role for the processing of electronic communications data under Articles 6 and 8 of the Proposal.

However, these provisions, in some situations, would allow third parties to provide consent for, and thus make decisions about, the fundamental rights of others, going against the self-determination of individuals and the very essence of the concept of *'consent'* as defined in the GDPR.

For example, using the definitions of the Proposal, consent by the end-user could mean that an employer as a subscriber may give consent instead of the employees who are using the services. This would generally also apply in other situations where an organisation subscribes to services

then used by individuals on the basis of this subscription, or when landlords provide certain communications services to their tenants.

Adding to the complexity, the Proposal does not simply require *'end-user'* consent for data processing. Rather, it uses various terms when it refers to who should provide consent:

- under Article 6(2)(c), for metadata, it is the '*end-user concerned'*;
- under Article 6(3)(a) and (b), for content, it is either '*the end-user or end-users concerned'* (in case of the provision of a specific service to an end-user) or
- *'all end-users concerned'* (in all other cases);
- under Article 8(1)(b), protecting terminal equipment, it is the '*end-user';*
- while under Articles 15 & 16 (publicly available directories and unsolicited communications) it is '*end-users who are natural persons'*.

In light of the foregoing, considering the unclear definition of *'end-user'* and the inconsistent use of language among the various consent provisions in the Proposal, it is not clear whose consent is required in any given situation. Under the following three subheadings the EDPS explains his three main concerns relating to the notion of end-user consent, and provide recommendations to address each.

Consent must be given by the individuals using the service

First, the Proposal must ensure that it is those individuals who are in fact using a communications service who are the ones entitled to make the decision whether or not to allow processing of their communications data.

As highlighted above, those who subscribe for a service may not always be the ones (or the only ones) using the service. For example, an employer may contract services that are then used by its employees and visitors, or a hotel chain may contract communications services for use by its guests. Similarly, a landlord or a head of household may contract the services, which are then used by several individuals (e.g. family members, tenants) living on the same premises (as well as by visitors).

We assume that the intent of the Commission was to ensure that it is the individuals effectively using the service, rather than those subscribing to it, whose consent is required. However, this should be made clearer in the Proposal.

To this end, the EDPS recommends including a stand-alone definition of *'end-user'* in the ePrivacy Regulation, for purposes of providing consent to processing of communications data. The definition should build on the following four elements: (i) *natural person (ii) using a publicly available electronic communications service (iii) for private or business purposes, (iv) without necessarily having subscribed to this service'*[26].

In addition, we recommend including a recital in the Proposal making it clear, by also providing specific examples, that end-users include for instance employees, tenants, hotel guests, family members, visitors, and any other individuals who are -as a matter of fact- using the services, for private or business purposes, without necessarily having subscribed to it.

Consent must be requested from all parties to a communication

The proposed rules must also make it clear that -as a rule- all parties to a communication, such as, for example, both senders and receivers of an electronic mail and all individuals participating

in a video-conference, must be given the opportunity to decide whether or not to allow processing of their communications data.

The EDPS presumes that it was the Commission's intention to require -in most typical cases such as for scanning email content for purposes of market research or targeted advertisement- the consent of all parties to a communication. At the same time, the EDPS acknowledges that there may be some specific circumstances when consent of one party may be sufficient (e.g. when an individual's location data is tracked in such a way that no other person's personal data is involved, or when an individual requests specific limited services such as the ability to search and organise her own incoming emails, according to key words or by senders). For these cases, any necessary exceptions may be specifically provided for[27].

In light of the above, and also with a view to simplify the complexity of the Proposal, the EDPS recommends that in each case where end-user consent is required, the same phrase, *'all end-users'* be consistently used throughout the Proposal[28]. This consistent approach is particularly important with regard to all metadata and content under Article 6 as well as for any processing under Article 8[29].

Rights of individuals other than the communicating parties must also be protected

Finally, the EDPS is also concerned about the protection of those individuals who are not parties to a communication but whose personal data are included in those communications[30]. Under the GDPR, any processing of such data (beyond the household and other exceptions) is subject to the requirement of having a legal ground for processing under Article 6[31].

In order to ensure there is no ambiguity to what extent the provisions of the GDPR also apply in these situations, **the EDPS recommends that a substantive provision be added to confirm that *'any processing based on end-user consent must not adversely affect the rights and freedoms of individuals whose personal data are related to the communication, in particular, their rights to privacy and the protection of their personal data'.***

3.3 Relationship between the GDPR and the ePrivacy Regulation

The EDPS welcomes the fact that, as he previously recommended, the relationship between the GDPR and the ePrivacy Regulation remain complementary, as is currently the case. The current language: '*complements and particularises',* which has now been also included in Article 1(3) of the Proposal, is satisfactory to define this relationship[32].

The EDPS also welcomes the fact that recital 5 now clearly states that the Proposal *'does not lower the level of protection enjoyed by natural persons under [the GDPR]'.* The EDPS recommends that this sentence be further strengthened by adding the following phrase in order to frame the message in a more positive way *'- to the contrary, where appropriate, it aims to provide additional, and complementary, safeguards considering the need for additional protection for the confidentiality of communications'.*

The EDPS notes, however, that this relationship raises the following issue: in cases where the end-user has given consent to a service provider to transfer metadata and/or content data to a third party which will then act as a controller, will the processing of the data by the third party be governed by the GDPR or by the ePrivacy Regulation?

The consequences are significant. If the GDPR applies to the further processing, all the legal grounds for processing under Article 6 of the GDPR would be available to the third party. In

contrast, if the Proposal were also to apply, processing would only be possible based on consent (or another specific exception under the Proposal).

If the Proposal is interpreted to mean that third parties may rely on any legal ground under the GDPR for processing, this would create a loophole which could significantly lower the level of protection provided in the ePrivacy Regulation. For example, communications service providers (who would be covered by the Proposal) might be tempted to set-up subsidiaries to circumvent the stricter regime of the ePrivacy Regulation.

To ensure legal certainty, the EDPS recommends that the Proposal specify, in a substantive provision, that '*neither providers of electronic communications services, nor any third parties, shall process personal data collected on the basis of consent or any other legal ground under the ePrivacy Regulation, on any other legal basis not specifically provided for in the ePrivacy Regulation.'*.

The EDPS further recommends that a recital be included to explain that '*when the processing is allowed under any exception to the prohibitions under the ePrivacy Regulation, any other processing on the basis of Article 6 of the GDPR shall be considered as prohibited, including processing for another purpose on the basis of Article 6(4) of the GDPR. This would not prevent controllers from asking for additional consent for new processing operations'*.

This should not prevent the legislators from providing additional, limited and specific exceptions in the ePrivacy Regulation, for example, to protect the '*vital interests'* of individuals pursuant to Article 6(d) of the GDPR or to allow processing for purposes of scientific research or (official) statistics under Article 89 of the GDPR[33].

Further, the proposed last sentence of recital 5 provides that *'processing of electronic communications data by providers of electronic communications services should only be permitted in accordance with this Regulation'*. This sentence creates ambiguity as it could arguably suggest that processing electronic communications data by parties other than providers of electronic communications services does not come under the scope of the ePrivacy Regulation. This would be contrary to the text of Article 2(1) itself, and would reduce the level of protection under the ePrivacy Regulation. What matters is not *who* processes the data, rather, *what type of data* is protected. Processing of electronic communications data and information related to the terminal equipment of users should unambiguously come under the scope of the ePrivacy Regulation, irrespective of which entity processes such data. **Accordingly, the EDPS recommends replacing the quoted sentence in recital 5 as follows: *'processing of electronic communications data should only be permitted in accordance with, and on a legal ground specifically provided under, this Regulation'*.**

3.4 Consent must be freely given: '*tracking walls*' must come down

'Tracking-walls' and the notion of freely given consent

Article 8(1), modeled upon Article 5(3) of the current ePrivacy Directive, prohibits *'the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware'*. Exceptions include the case, under Article 8(1)(b), where '*the end-user has given his or her consent'.*

While the EDPS welcomes these new provisions and recommends maintaining the current consent requirement, he also acknowledges that Article 5(3) of the ePrivacy Directive, as currently applied, has failed to live up to its potential to provide a genuine opportunity to choose, and to give control to the individuals. Instead, consent mechanisms have been developed by businesses and other organisations with the objective of arguably meeting the bare legal requirements for compliance under the ePrivacy Directive but failing to give users a genuine choice and control over what is happening to their data.

This phenomenon is sometimes referred to as the issue of *'tracking-walls'.* Tracking walls, in effect, mean that users who do not accept tracking across other sites will be denied access to the websites that they are seeking to access[34]. Cookies, or other techniques, such as device fingerprinting are used to continuously track users as they leave their digital trail over the internet, and companies having access to them further use the information obtained for profiling, advertisement and other commercial purposes. This purportedly consent-based and generalised tracking carries high privacy risks and takes control over their personal data completely out of the hands of the individuals concerned.

Tracking walls undermine the idea that consent must be freely given, a key requirement both under Directive 95/46/EC and the GDPR. The GDPR improves upon Directive 95/46/EC by not only requiring that consent be freely given but also providing further guidance as to what this means in practice. In particular, it provides that consent is not considered to be freely given in situations where the provision of a service is made dependent on an individual giving her consent to the processing of her personal data despite the fact that such processing is not necessary for the performance of that service[35]. This is precisely the case of tracking walls, which often oblige the user to consent to the use of third-party tracking cookies, which are unnecessary for the performance of the service concerned. It is crucial that users be able to use a service without being tracked - especially by third parties and in situations where the user depends on, and has no real alternative to, using the service. On the basis of the GDPR it is possible to argue that such tracking walls are not allowed at all, because a *'freely given'* informed consent is lacking. To provide legal certainty, it is important that this be made explicit in the ePrivacy Regulation.

Considering the importance of freely given consent, and the often insufficient implementation of the current Article 5(3) by operators of websites, the EDPS recommends a complete and explicit ban on so-called *'tracking walls'*.

Accordingly, the EDPS recommends that the ePrivacy Regulation provide, in a substantive provision, that *'no one shall be denied access to any information society services (whether these services are remunerated or not) on grounds that he or she has not given his or her consent under Article 8(1)(b) to the processing of personal data that is not necessary for the provision of those services'*.

To complete this provision, the EDPS further recommends an additional, explicit prohibition on the practice of excluding users who have ad-blocking or other applications and add-ons installed to protect their information and terminal equipment.

For the avoidance of any doubt, the EDPS also recommends that a recital should explicitly confirm that *'processing of data for purposes of providing targeted advertisements cannot be considered as necessary for the performance of a service'*.

A related concern is that end users may also be confronted with forced consent mechanisms before they can use smart devices (e.g. smart TVs). In the context of the Internet of Things, it should be ensured that the functionality of smart devices is not conditional on consent that is not necessary for the functionality requested. This particularises the conditions of Article 7(4) of the GDPR to the context of the Internet of Things, where end users buy and use physical products and may reasonably expect certain functionalities of these products.

The EDPS recommends therefore that a similar, specific ban be also included in the Proposal, in the form of a substantive provision requiring that *'no one shall be denied any functionality of an IoT device (whether use of a device is remunerated or not) on grounds that he or she has not given his or her consent under Article 8(1)(b) for processing of any data that is not necessary for the functionality requested'.*

This comprehensive approach would ensure the highest level of protection for individuals, as well as legal certainty and a level playing field for all market players.

Alternative business models based on transparency and user empowerment

This approach does not prevent innovative use and re-use of personal data in the world of *'big data'*. Rather, it aims at strengthening fundamental rights at the same time as opening new opportunities for businesses to develop innovative personal data based services built on mutual trust. The way how organisations use and reuse personal data must become more transparent and individuals must be given more control over what is happening to their data. As the EDPS stated in his Opinion on *'Meeting the challenges of big data'*[36], companies and other organisations that invest a lot of effort into finding innovative ways to make use of personal data, should use the same innovative mind-set when implementing data protection principles.

Telephone companies, internet service providers, as well as other organisations who provide communications services that come under the scope of the ePrivacy Regulation are often in a unique position to build a mutually beneficial relationship based on trust with their customers. On the basis of this trust relationship customers may be willing to enter into a partnership and share their personal data for new innovative uses for the benefit of all concerned[37].

3.5 Privacy must be protected by default

The EDPS strongly supports the clarification in Article 9 that consent could be expressed via technical settings where technically possible and effective. To make this effective, however, the requirements regarding privacy by default are also essential. Such tools must be offered to the user at the initial set-up with privacy-friendly default settings, and at other moments when users make significant changes to their devices or software. Moreover adherence to accepted technical and policy compliance standards by all parties concerned, including the operators of the website, should become obligatory[38].

As stated in the EDPS Preliminary Opinion[39], users must have user-friendly and effective mechanisms to provide and revoke their consent. The EDPS therefore welcomes the fact that the Proposal provides that the user's consent to the processing could be expressed by using the appropriate settings of a browser or another application.

In principle, Article 9(2) of the Proposal provides for a meaningful approach to using technical configuration features of a user device and the software installed on it for expressing consent. The wording in Article 9(2) of the Proposal: '*without prejudice to paragraph 1'*, is designed to ensure that any user-friendly mechanism to provide consent must also meet the requirements

of the GDPR including in particular sufficient specificity and the possibility for the individual concerned to withdraw it.

In contrast, Article 10 of the Proposal requires that end users be given the *'option'* to determine through software settings whether they allow third parties to access or store information on their devices. The EDPS considers that this provision is inconsistent with Article 25 of the GDPR on '*Data protection by design and by default'*. **Instead, the EDPS recommends that Proposal impose an obligation on hardware and software providers to implement default settings that protect end users' devices against any unauthorised access to or storage of information on their devices.**

Furthermore, the EDPS recommends that a substantive provision provide for adherence to accepted technical and policy compliance standards by all parties concerned, including operators of websites.

Article 10(2) requires software providers to inform users about the availability of privacy settings upon first use of the software. It is crucial that users should, during this process, be able to make a simple choice to avoid being tracked. However, the same '*all or nothing'* approach should not be applied to their consent to tracking. As noted above, any technical means used to provide consent must meet the requirements for consent as required under Article 4(12) GDPR, including not only consent being *'freely given'*, but also '*specific'* and *'informed'*. Providing general information about the privacy settings during the first use of software that will have an *'all or nothing'* impact on any future use, will not meet the requirements of consent as provided for in the GDPR.

Further, it is also important that users should not only be informed about the privacy settings during installation or first use of the software, but also at other moments when users make significant changes to their devices or software. Such notices should also be provided, for example, when users reset their devices to factory settings. The settings should, at such times also, remain set privacy by default. They must also be easily accessible during use.

3.6 Devices must not be tracked without their users' consent

The EDPS is also concerned about the proposed exception in Article 8(2)(b) of the ePrivacy Regulation for tracking users of communication devices in public spaces in the physical world (sometimes referred to as '*device tracking'*). This type of technology is already in use, for example, to measure footfall in busy shopping areas or to map traffic flows on roads. The collected data, while often intended to be used for statistical purposes only, may reveal the location and behavioural patterns of individuals. In some contexts, such as in the vicinity of a religious establishment or a medical clinic, location information is highly sensitive in itself, even in its raw form without extensive profiling and analytics.

Considering the potential privacy risks, it is worrisome that the Proposal provides a nearly blanket permission for any purpose for this type of tracking, provided there is a notification to the user alerting her to the measures she can take to *'stop or minimise collection'*.

It is difficult to see why this form of use of location data deserves weaker protection than others. Elsewhere in the Proposal, providers of communications services are not allowed to process information about the location of the users unless those users have given their consent. The data processed in the context of device tracking in a physical world should not be considered to be less sensitive.

Compared to a processing based on an opt-in consent, any opt-out solution offers less protection due to the power of the *'default':* most people simply will not have the time, or interest to take

action: they will accept the default option and not opt out. Beyond this more general concern, the proposed approach, notification, coupled with a weak and ineffective form of '*opt-out'* is problematic for several reasons.

Firstly, an unsuspecting user may not even notice the sign in a busy area. In addition, in cases of large-scale application of such technology the user might be notified only at the outer edges of such an area, which would render the existence of the technology even more invisible.

Secondly, based on the Proposal's language, it may not be possible for users to evade this type of tracking other than by switching off the basic functionalities of their own devices, such as wireless internet access on their mobile phones. The user cannot be expected to opt-out - possibly multiple times- when entering an area where device-tracking technologies are used. This is especially so if avoidance of tracking comes at the expense of the functionalities of their devices. In this context, it is also important to highlight the message in recital 18, which discusses consent: '*Basic broadband internet access [...] [is] to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. Consent for processing data [...] will not be valid if the subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment'.*

Further, if it is technically possible to opt out, for example by registering the device Wi-Fi MAC address in a database which the provider of the location-tracking service must check, the same method can be used for an opt in scheme. Informed, freely given consent, as required under the GDPR is preferred in all situations.

In light of the foregoing, the EDPS recommends that the current Article 8(2)(b), as well as Article 8(3) and 8(4) be deleted and replaced by a -simpler- requirement of consent (by all end-users[40] concerned). Additionally, as in Article 6 regulating the processing of content and metadata, the ePrivacy Regulation also should specify that processing based on consent is only possible if the purposes *'cannot be fulfilled by processing information that is made anonymous*[41]*'.*

If necessary, limited and targeted exceptions can be provided for purposes of scientific research and (official) statistics under Article 89 of the GDPR and to protect 'vital interests' of individuals pursuant to Article 6(d) of the GDPR[42].

An additional, also limited and narrowly-tailored, exception may be provided for purposes of people counting (such as measuring footfall and traffic flows), subject to appropriate safeguards, including technical and organisational measures to ensure that data processed for these purposes should not be processed for any other purposes and in particular, should not be processed to support any measures or decisions that are taken with regard to the individual concerned ('*functional separation'*)[43]; as well as an effective horizontal opportunity to opt-out of the processing (similar to 'do not call' registers in the context of unsolicited communications or 'do not track' in the context of online tracking); and strict limitations on the period for which data may be retained.

The EDPS further recommends that the ePrivacy Regulation make specific reference to the possibility for the EDPB to provide further guidance as to the safeguards that must be implemented. These more detailed guidelines may recommend, for example, in typical use cases for statistical purposes, that the identifiers from the end-user device should never be stored and processed directly but only used as the basis for calculating new pseudonymous identifiers

and that these identifiers cannot be cross-linked across different tracking services and must have a short persistence, limited to what is strictly necessary to carry out the statistical calculations.

3.7. Restrictions must be limited and subject to safeguards

Article 11 of the Proposal broadly corresponds to the current Article 15 of the ePrivacy Directive. Article 15(1) of the ePrivacy Directive allows Member States, among other things, to introduce a national data retention regime providing for the mandatory storage of electronic communication data by providers for the purposes of detecting, investigating, and prosecuting serious crime, including terrorism. Following the invalidation in the 2014 *Digital Rights* judgment[44] of the 2006 Data Retention Directive (2006/24/EC)[45], Member States are no longer under a legal obligation deriving from a specific Union legal instrument to introduce or maintain a data retention regime.

The EDPS would like to take this opportunity to reiterate that any national data retention regime has to comply with the requirements of the Charter, in particular Articles 7, 8, 11, 47 and 52, as set out in the relevant case law of the Court of Justice. In particular, Member States would have to comply with the *Digital Rights Ireland* jurisprudence, including the latest judgment in *Tele 2 Sverige* and *Watson and others*[46].

In addition, the EDPS supports the approach of the Proposal by which only selected grounds listed in Article 23(1) GDPR can be accepted as grounds for restricting the scope of certain rights and obligations set out in Articles 5 to 8 of the Proposal. Indeed, incorporating *all* the grounds of exception under Article 23 GDPR would not be appropriate, given the particularity of the Proposal as compared with the GDPR[47].

In any event, the EDPS considers that the mere fact that the intended scope of the Proposal is extended compared to the ePrivacy Directive today, should not be understood as a general mandate for the Member States to automatically extend the scope of application of any -existing or future- data retention regimes beyond the traditional electronic communications services which fall within the scope of Article 15(1) ePrivacy today. At the very least, the necessity and proportionality of any such data retention obligations would have to be demonstrated, in line with the Charter and the case law of the Court referred to above[48].

Additional safeguards

Article 23(2) of the GDPR requires that legislative measures imposing restrictions must contain certain specifically listed provisions such as, for example, explanation of the purposes of the processing and provision of safeguards to prevent abuse or unlawful access or transfer. There should be no doubt that these additional specifications and safeguards foreseen in Article 23(2) must also apply in cases where restrictions are imposed under the ePrivacy Regulation. This should be made clear in a substantive provision of the Proposal[49].

In addition, the EDPS **recommends that legislators carefully verify what specific safeguards are required under the Proposal**, considering that any restrictions will not only affect the rights of individuals to the protection of their personal data but also constitute an interference with the confidentiality of communications.

In particular, in cases where Article 23(1)(e) of the GDPR applies, the EDPS recommends that the Proposal should provide that legislative measures imposing restrictions should require prior judicial authorisation for any access to content or metadata[50].

Transparency regarding government access requests

In global networks, communications cross borders without users being aware. Communications between EU Member States may pass through third countries, whilst communications between third countries may be transmitted via EU territory. Communications service providers established or operating in the EU may be subject to requests for information or access to their users' data from law enforcement or security services of other Member States and non-EU countries, based on applicable national laws and practices laying down exceptions to the right to confidentiality of communications. Following the entry into force of the GDPR, such requests requiring personal data to be transferred to a third country may only be based on an international agreement, such as a mutual legal assistance treaty[51].

The use of security and law enforcement powers to breach the confidentiality of communications must be in line with the principles of necessity and proportionality. While informing the individuals subject to such measures may be restricted for instance in order to safeguard the objectives of an on-going investigation, a general awareness about the frequency and volume of disclosure requests addressed to communications service providers would give citizens in general and also public bodies the possibility to benchmark and assess the general practice in the use of these instruments. Transparency regarding government access requests may thus play an important role in helping ensure respect for fundamental rights.

In consequence the EDPS has already recommended in his Preliminary Opinion that the ePrivacy Regulation should provide specific rules enhancing transparency[52]. In particular, he recommended a new provision creating an obligation for organisations to disclose, at least periodically and in an aggregate form, law enforcement and other government requests for information. This should cover requests from both inside and outside the EU. We also explained that with regard to such requests from third countries, the service providers should observe the legality condition provided for in Article 48 of the GDPR.

While the EDPS welcomes the fact that Article 11(2) takes some steps towards transparency, by allowing on demand access to the competent supervisory authority of some information about these procedures, we recommend that legislators take transparency one step further and require publication of the same information.

In addition, the EDPS recommends that the supervisory authorities not only have '*on-demand*' access to this information, but also receive periodic reports, *ex officio*.

4. CONCLUSIONS

The EDPS welcomes the Commission's Proposal for a modernised, updated and strengthened ePrivacy Regulation. He shares the view that there is a continued need to have specific rules to protect the confidentiality and security of electronic communications in the EU and to complement and particularise the requirements of the GDPR. He also considers that we need simple, targeted and technologically neutral legal provisions that provide strong, smart and effective protection for the foreseeable future.

The EDPS welcomes the declared ambition to provide a high level of protection with respect to both content and metadata, in particular the key positive elements outlined in Section 2.1.

Whilst welcoming the Proposal, the EDPS remains concerned about a number of provisions that risk undermining the intention of the Commission to ensure a high level of protection of privacy in electronic communications. In particular, the EDPS has the following key concerns:

- the definitions under the Proposal must not depend on the separate legislative procedure concerning the Directive establishing the European Electronic Communications Code[53] (the EECC Proposal);
- the provisions on end-user consent need to be strengthened. Consent must be requested from the individuals who are using the services, whether or not they have subscribed for them and from all parties to a communication. In addition, data subjects who are not parties to the communications must also be protected;
- it must be ensured that the relationship between the GDPR and the ePrivacy Regulation does not leave loopholes for the protection of personal data. Personal data collected based on end-user consent or another legal ground under the ePrivacy Regulation must not be subsequently further processed outside the scope of such consent or exception on a legal ground which might otherwise be available under the GDPR, but not under the ePrivacy Regulation;
- the Proposal lacks ambition with regard to the so-called '*tracking walls'* (also known as *'cookie walls'*). Access to websites must not be made conditional upon the individual being forced to '*consent'* to being tracked across websites. In other words, the EDPS calls on the legislators to ensure that consent will be genuinely freely given;
- the Proposal fails to ensure that browsers (and other software placed on the market permitting electronic communications) will by default be set to prevent tracking individuals' digital footsteps;
- the exceptions regarding tracking of location of terminal equipment are too broad and lack adequate safeguards;
- the Proposal includes the possibility for Member States to introduce restrictions; these call for specific safeguards.

These main concerns -along with recommendations how to address them- are outlined in this Opinion. Beyond our general comments and key concerns detailed in the main body of the Opinion, the EDPS also provides further -and sometimes more technical- comments and recommendations on the Proposal in an Annex, in particular, to facilitate the work of legislators and other stakeholders who wish to further improve the text during the legislative process. Finally, we also note the importance of a swift processing of this important dossier by the legislators, to ensure that the ePrivacy Regulation, as intended, may apply as of 25 May 2018, the date when the GDPR itself will also become applicable.

The importance of confidentiality of communications as laid down in Article 7 of the Charter is growing with the increased role that electronic communications play in our society and economy. The safeguards outlined in this Opinion will play a key role in ensuring the success of the Commission's long term strategic objectives outlined in its DSM Strategy.

Done in Brussels, 24 April 2017

(**signed**)

Giovanni BUTTARELLI

European Data Protection Supervisor

ANNEX: FURTHER ANALYSIS AND RECOMMENDATIONS

Beyond our general comments and key concerns detailed in the main body of the Opinion, the EDPS also wishes to provide further -and sometimes more technical- comments and recommendations on the Proposal, in particular, to provide a working tool to facilitate the work of legislators and other stakeholders who wish to further improve the text during the legislative process.

For ease of reference, the order of these comments follows the structure of the Proposal, starting with the recitals and discussing relevant Articles in order.

1. Covering different types of networks (recital 13)

As noted above in Section 2.5, the EDPS welcomes the Commission's ambition to bring all publicly accessible networks and services within the scope of the confidentiality requirements. Recital 13 includes some examples, such as *'... "hotspots" situated at different places within a city, department stores, shopping malls and hospitals'*.

For the sake of avoidance of ambiguity, the EDPS would encourage further clarifications and examples. These should include Wi-Fi services in hotels, restaurants, coffee shops, shops, trains, airports and networks offered by universities to their students, as well as corporate Wi-Fi access offered to visitors and guests, and hotspots created by public administrations.

In addition, the EDPS further recommends that recital 13 also clarify what should be considered *as 'publicly accessible'.* For example, it should be made clear that a service remains considered publicly accessible even if the provider limits the service to registered users such as in the case of an organisation offering Wi-Fi access to its customers and visitors[54].

2. Personal data cannot be considered as counter-performance (recital 18)

Recital 18 of the ePrivacy Proposal provides that *'in the digital economy, services are often supplied against counter-performance other than money, for instance by end-users being exposed to advertisements'*. This may imply that end-users' data are used as counter-performance, especially if this recital is read together with recital 16 of the EECC Proposal, which more directly suggests that *'electronic communications services are often supplied against counter-performance other than money, for instance by giving access to personal data or other data'*.

The EDPS emphasises that personal data cannot be considered as *'counter-performance'* for a requested service such as access to a website or an app. This is because consent is valid only if freely given and withdrawn without detriment to the individual concerned. As the EDPS recently explained in his Opinion 4/2017 on the Digital Content Proposal[55], the notion of '*counter-performance'* creates additional obligations for the individual and is not consistent and compatible with the notion of consent under the GDPR. The notions of *'paying with personal data'* and offering personal data as *'counter-performance'* would indeed therefore undermine the current legal grounds for lawful processing as set out in Article 6 of the GDPR.

The EDPS, therefore, recommends deleting the quoted phrase from recital 18 and amending it as follows: '*In the digital economy, services are often supplied with remuneration paid by a third party rather than by the recipient of the service'.*

3. All individuals, not only citizens, require protection (recital 33)

The EDPS recommends replacing the term '*citizen*' with the term '*individual*' in recital 33. The concept of citizenship is not appropriate when it comes to protecting fundamental rights, since all individuals in the EU are entitled to protection under the Charter, not only citizens.

4. Protection of legal persons (Article (1))

While it is clearly justified that legal persons also have rights regarding their electronic communications and the protection of these should be integrated into the Proposal, the language of the Proposal needs to be adjusted. The reference in Article 1(1) to fundamental rights and freedoms of *'legal persons'* should be deleted. Instead, as regards legal persons, the EDPS recommends using language similar to the language used in Article 1(2) of the current ePrivacy Directive.

5. Territorial scope should match GDPR (Article 3)

The EDPS recommends that the ePrivacy Regulation have unambiguously the same *territorial* scope as the GDPR (including the extra-territorial scope provided for in Article 3(2)[56]) and follow the same approach in terms of applicable law about personal data processing. The current wording of Article 3 does not prevent such an interpretation, but it is not sufficiently clear whether an identical territorial scope is intended, and therefore the provision should be amended in order to cover the same area. A recital would further clarify the legislator's intentions.

A verbatim copy of the provisions of the GDPR would not achieve the objective, as the application of the ePrivacy Regulation should not be conditional on the parties concerned being qualified as *'controller'* or *'processor'* within the meaning of the GDPR.

6. 'In platform messages' (Article 4(1)(b) and recital 1)

The EDPS welcomes the fact that recital 1 confirms that the principle of confidentiality applies to '*current and future means of communication'* and provides examples such as *'calls, internet access, instant messaging applications, e-mail, internet phone calls and personal messaging provided through social media'.*

The EDPS supports the call for clarification by the WP29 in its Opinion 1/2017[57] that the Proposal should specifically and unambiguously include all in-platform messages between users of a social network (such as Facebook or Twitter).

The EDPS further recommends that this recital more clearly specifies that the notion of communication does not only include electronic communication between two individuals (or machines) but also any communications within a defined group (e.g. a conference call, or messages sent to a defined group of recipients).

In addition, as the EDPS highlighted in Section 3.1 above when discussing scope and definitions, the EDPS recommends independent, standalone definitions better suited for the protection of privacy and confidentiality of communications, to help ensure that in-platform messages are unambiguously included in the notion of '*interpersonal communications service'*, and thus, within the definition of *'electronic communications service*[58].

7. Definition of *'electronic mail'* (Article 4(3)(e))

The EDPS recommends that the defined term *'electronic mail'* be replaced by a more general term, such as, for example, *'electronic message'* in Article 4(3)(e). This is to ensure that there is no confusion with the term '*electronic mail or email'* as these words are commonly understood. Clarity of the definition is crucial in order to provide legal certainty with regard to the scope of the protection against all unsolicited communications in Article 16[59].

The proposed recital 33 correctly highlights the need for the provisions on unsolicited communications to be technologically neutral. The EDPS welcomes the specific mention in this recital of *'instant messaging applications, emails, SMS, MMS, [and] Bluetooth'* as examples. We would also encourage providing further examples in this recital. For example, in the context of protection against unsolicited communications, it should be ensured that individuals are protected against unsolicited messages irrespective whether these are delivered via the *'timeline'* feature or the messenger feature of a social network or the messenger feature of a gaming application.

To ensure legal certainty, the definition itself must also be sufficiently clear and broad to ensure that the defined term encompasses all relevant communications channels in addition to traditional email communications[60].

8. Processing under exceptions must be '*strictly'* necessary (Articles 6 and 8(1))

The EDPS supports the recommendations of the WP29 that with regard to all exceptions set forth in Articles 6 and 8(1) of the Proposed Regulation the word *'strictly'* should be added before *'necessary'*[61].

9. Exception for security purposes (Article 6(1)(b))

Article 6(1)(b) allows processing of both content and metadata for security purposes. The EDPS emphasises -as noted in this Annex, Section 8 above- that this exception must be narrowly construed and limited to what is strictly necessary. According to these principles, content could only be processed to recognize and remove elements that could be dangerous to the network or user terminal itself, e.g. viruses and other malicious elements, but not for other purposes. This does not exclude that some additional processing for these purposes may be authorised based on the consent of the individuals concerned and subject to other safeguards such as those mentioned in Article 6(3)(b). The EDPS would also recall Opinion 2/2006 of the WP29 on privacy issues related to the provision of email screening services[62].

10. Protection of communications metadata must be strengthened (Article 6(2))

The EDPS calls attention to the fact that the distinction between content and *'metadata' is* not clear-cut in a multiple service environment as the Internet, where the service provided to the user often combines different technological components in such a way that what, for one component, is considered content constitutes metadata for another[63].

The processing of data about the communication (such as URLs of websites accessed, e-mail header, telephone numbers called, location of terminal equipment) are often equally revealing than the actual contents of the communication. Metadata about communications can provide a very detailed profile of an individual and processing it can be just as intrusive as processing content of communications.

For instance, metadata allow for the identification of targets in military drone operations[64]. Metadata can also identify structures in political attacks and criminal investigations[65]. Research has also shown that individuals can be identified from a very limited set of mobile phone location data[66]. It has also been shown that intimate details about a person's lifestyle and beliefs, such as political leanings and associations, medical issues, sexual orientation or habits of religious worship can be discovered through mobile phone traffic data[67].

In addition, for certain types of data, it has been arguable under the ePrivacy Directive whether they should be considered as content or metadata. Recital 2 of the Proposal now clarifies that a full URL (specifying the visited webpage) is considered metadata. However, considering the sensitive nature of this data, this type of data deserves the same high level of protection as content data.

As also explained by the WP29 in its Opinion 1/2017[68], the ePrivacy Regulation therefore must clearly provide for a high level of protection of the confidentiality of communications of both *'content'* and *'metadata'*. The Proposal, in recital 2, recognises this need, which the EDPS welcomes.

Despite its ambition to provide a high level of protection for metadata, the Proposal nevertheless allows its processing subject to less stringent safeguards. To ensure a high level of protection, the EDPS recommends that the same rules apply for consent for both content and metadata under Article 6.

11. Protecting the terminal equipment: need for technologically neutral and inclusive wording (Article 8)

The EDPS welcomes that a wording has been chosen for Article 8(1), which can be considered as technologically neutral and inclusive, as recommended in the Preliminary Opinion[69].

The EDPS recalls the need to ensure that all current and future tracking techniques used via smartphones and in IoT applications are fully covered. The rules, in particular, should cover device fingerprinting, as well as all forms of '*passive tracking'*, that is, the use of identifiers and other data broadcasted by devices. With the development of the Internet of Things, more and more data will likely to be broadcast '*by default'*. Rather than considering the condition that information is *'already stored, in the terminal equipment'*, the condition could cover all information that *can be obtained* from the device. Such operations would require consent with the exceptions for transmission and provision of a service, as currently laid down, with a possible extension for a very limited case of processing directly related to a service requested by the user and performed exclusively by the service provider.

12. Exception for '*web-audience measuring'* (Article 8(1)(d))

In the Preliminary Opinion, the EDPS recommended that the ePrivacy Regulation should also create an additional exception for first party analytics cookies, subject to adequate safeguards[70]. This should help ensure that data can be processed when this causes little or no impact on the rights of users to the confidentiality of their communications and private life. The EDPS recommended that any such exceptions be limited to cases where the use of such first party analytics cookies is strictly limited to aggregated statistical purposes. In addition, adequate safeguards must be applied including clear information provided to the individuals concerned, a user-friendly mechanism to opt out from any data processing, and appropriate anonymisation

techniques applied to collected information such as IP addresses. The WP29 in its Opinion 04/2012 on Cookie consent exemption[71] already called legislators to create such an exception.

The EDPS also recommended that for more guidance on the safeguards to be applied and the conditions under which a first party analytics cookie can be exempted from the consent requirement, the ePrivacy Regulation may refer to future guidance to be provided by the EDPB.

The EDPS welcomes the fact that a new exception has been created. However, in order to ensure that the exception remains limited, the EDPS recommends adding the phrase *'and further provided that no personal data is made accessible to any third parties'* at the end of the paragraph. This is to ensure that the exception is narrowly construed, and specifically excludes the use of third party services, as intended and recommended by the WP29.

The EDPS also notes that the exception must not create a loophole for long-term storage or further processing of personal data for additional purposes. Allowing the storage of information on the user's equipment and reading information from the user's equipment for statistical purposes is acceptable only when a number of conditions are met. For example, the resulting information may not constitute a detailed picture of individual users and the information obtained must not be used for any other purpose than to obtain insight into the functioning and use of a service in an aggregated and general manner. The information must also not be merged with other information to build a profile of a user, or be used to target the user.

The Proposal should be updated to include essential safeguards and refer to the possibility of additional guidance to be provided by the EDPB[72]. For example, as in the case of device tracking (as discussed in Section 3.6 of the main body of this Opinion), the EDPS recommends that this exception be subject to additional safeguards including technical and organisational measures to ensure that data processed for these purposes should not be processed for any other purposes and in particular, should not be processed to support any measures or decisions that are taken with regard to the individual concerned; as well as an effective horizontal opportunity to opt-out of the processing; and strict limitations on the period for which data may be retained.

13. Additional recommendations relating to device tracking (Article 8(2))

First, the EDPS recommends deleting the phrase *'to enable it to connect to another device and, or to network equipment'* from the first sentence of Article 8(2). This is to ensure a technologically neutral coverage and full protection of all data emitted by terminal equipment irrespective of the purpose.

Second, the EDPS recommends adding the phrase *'which the end-users concerned have authorised'* (or similar language) after the phrase *'for the purpose of establishing a connection'*. The objective is to ensure that the connection established is the one the user actually is aware of and has given his or her prior consent to. For example, some individuals may have approved, via the appropriate settings on their device, that whenever they are near a Wi-Fi hotspot, their devices are automatically looking for (and perhaps automatically connecting) to (previously specified) available networks. At the same time, they may not authorise that their medical or fitness tracker communicate their medical or fitness information to any and all devices designed to capture and process this information. With increased availability of IoT devices, including medical devices, often the mere fact whether one is wearing or not a particular device can be indicative of very sensitive, for example, health information, and therefore caution is needed.

14. Withdrawal of consent (Article 9(3))

With regard to Article 9(3) (possibility to withdraw consent), the EDPS recommends adding a reference to Article 8(1)(b), in addition to the references already made to Article 6.

15. *'Feasibility'* of expressing consent via technical settings (Article 9(2)

Article 9(2) provides that *'... where technically possible and feasible, ... consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet'*.

The phrase *'where technically possible and feasible'* lacks sufficient clarity. It is open to a broad range of interpretations and risks empting out this obligation altogether. In one reading, the drafting may simply be redundant by requiring that offering consent via technical setting must be both *'technically feasible'* and *'technically possible'*. Alternatively, the drafting may be read to impose an additional condition of general (rather than technical) *'feasibility'*, with a scope which might be read strictly or broadly, and might arguably even include commercial considerations such as the effect of expressing consent this way on existing business models or on relevant markets in general.

The EDPS therefore recommends that the phrase *'where technically possible and feasible'* should be replaced by *'where technically feasible'* to ensure legal certainty as to the scope of this obligation[73].

16. Calling line identification (CLI) and incoming call blocking (Articles 12-14)

The Proposal includes a right for call recipients to be informed about who is calling them and take action against those calls, which withhold their CLI. The EDPS welcomes maintaining this right, also considering that this is one of the protections enabling individuals to take action against those engaging in unsolicited communication in violation of applicable law.

To help make call blocking an effective tool to protect against unsolicited communications, the EDPS further recommends that the phrase *'or having a specific code/prefix identifying the fact that the call is a marketing call, as foreseen in Article 16(3)(b)'* be added after the words *'to block incoming calls from specific numbers'* in Article 14(1)(a).

17. Publicly available directories (Article 15)

Article 15 of the Proposal requires that *'providers of publicly available directories shall obtain the consent of end-users who are natural persons to include their personal data in the directory'*, while legal person have the right to object.

In the Preliminary Opinion the EDPS recommended maintaining this provision and extending its scope to include not just telephone directories, but also all other kinds of directory services. Further, the EDPS recommended that the consent requirement for *'reverse lookup'* should also be explicitly extended to other service identifiers such as email address or user name. We welcome the clarifications that have been made to this effect in recital 30 and that mobile phones, email addresses and enquiry services are thereby now explicitly included in the scope of Article 15.

We nevertheless support the recommendations of the WP29 in its Opinion 1/2017 that it should be made clearer in the Proposal that a specific separate (i.e. granular) consent is required for search and for reverse search. We further recommend that the *phrase 'as determined by the provider of the directory'* be deleted from Article 15(1).

18. Unsolicited communications (Article 16)

The EDPS welcomes the fact that Article 16 of the Proposal has maintained, updated and strengthened the current protection against unsolicited communications. The means by which unsolicited communications are conducted have evolved since the ePrivacy Directive first came into force. As an example, an unsolicited voice call can start with an automated dialler, play a recorded message and then use a chat-bot to interact with the called individual via a series of automated screening questions. The chat-bot can then use the answers to transfer the called individual to a live operator. This type of direct marketing call is now treated the same way as making fully automated calls.

As this example shows, the EDPS welcomes the Proposal's ambition to adopt a technology neutral approach and modernise the rules. The general requirement of consent - irrespective of the technology used - is particularly welcome.

However, there is room for further improvements. The text must be strengthened both to prevent loopholes and to ensure legal certainty with regard to borderline cases.

Concerns regarding the scope of protection

Article 16 of the Proposal addresses *'direct marketing communications'* only. Yet not all spam and malicious communications can be considered as '*direct marketing'* in any usual business sense, or in the meaning of Article 4(3)(f), which defines this term for the purposes of the ePrivacy Regulation.

As an example, the following very significant categories of unsolicited communications appear to have been left outside the scope of protection:

- Some communications related to crime attempts, e.g. phishing attacks and fraudulent financial proposals, which may not always be covered by the definition of direct marketing.
- Some types of marketing communications, which may or may not fall under the definition of direct marketing.
- Communications that are of non-commercial nature, or where it is otherwise not obvious whether a communication can be considered as direct marketing (such as, for example, some types of communications sent by political parties, religious or charitable organisations to seek donations or promote political, religious or other views[74]).

For these reasons, the EDPS recommends that the legislators provide a more comprehensive protection to cover all types of spam, unsolicited telephone calls and marketing messages, phishing and other malicious attempts. To this end, the EDPS recommends both broadening and clarifying the scope of '*direct marketing communications'*, and introducing additional terms such as, for example, *'unsolicited communications'*.

First, providing comprehensive protection cannot be simply achieved by providing specific rules for *'direct marketing communications'*. Instead, before providing specific rules for direct marketing communications, the EDPS recommends a clear prohibition for all types of unsolicited communications to prevent loopholes for a variety of malicious or otherwise undesirable unsolicited communications.

Another concern related to the scope is the need for technologically neutral rules. Article 16 should unambiguously require the prior consent of recipients for all types of unsolicited electronic communications, independent of the means e.g. electronic mail, voice or video calls, fax, text but also direct in-platform messaging (within an information society service). To this end, the recitals provide further examples.

Further, the EDPS recommends that the recitals should clarify that whenever a direct marketing message is sent to a natural person *working for* legal persons, the provisions applicable to natural persons will apply[75].

As far as the current exceptions regarding existing relationships and similar products and services, the EDPS welcomes the fact that Article 16(2) of the Proposal preserved them, but the EDPS recommends that the Proposal clarify, perhaps in a recital, what is meant by '*similar products and services'* and explain also the notion of *'existing relationship'.*

Withdrawal of consent

The EDPS recommends that Article 16 clarify that the withdrawal of consent for direct marketing is free of charge and as easy as to give consent. This is to ensure consistency with the GDPR[76] and improve protection of recipients. We note that the term '*free of charge'* is used in Article 16(2) of the Proposed Regulation, but only with regard to the opt-out of direct marketing on the basis of contact data obtained in the context of a sale.

Safeguards for direct marketing calls (Article 16(3)

Under Article 16(3), those placing direct marketing calls must additionally either (i) present the identity of a line on which the natural or legal person placing the call can be contacted (Article 16(3)(a)) or (ii) use a specific code/prefix to identify it as a marketing call (Article 16(3)(b)). The code/prefix-requirement for direct marketing calls is thus presented as an alternative to the contact line identification requirement.

The EDPS welcomes both requirements, however, insist that, in order to enable effective withdrawal of consent, it is crucial that the requirements must not be alternatives, but must rather, be complementary to each other. Both must be mandatory. To this effect, the word *'or'* between paragraphs (a) and (b) should be replaced by *'and'*.

Information to end-users (Article 16(6)

Another concern is that the Proposal does not explicitly prohibit the use of false identities when sending direct marketing communications. It is noted in recital 34 that *'the masking of the identity and the use of false identities, false return addresses or numbers while sending unsolicited commercial communications for direct marketing purposes'* is prohibited. In Article 16(6), however, it is merely stated that end-users shall be informed of *'the identity of the legal*

or natural person on behalf of whom the communication is transmitted'. This obligation to inform recipients about the identity should be complemented with a clear prohibition on the use of masked or false contact addresses for direct marketing purposes in a substantive provision.

Europe-wide opt-out register for voice-to-voice calls

Based on Article 16(4) of the Proposal, Member States may choose an opt-out regime for voice to voice marketing calls. Recital 36 further specifies that Member States *should be able to* establish and/or maintain national opt-out systems.

These provisions, unless further improved, maintain a significant loophole for the protection of personal data, and also do not live up to the ambition of creating a more harmonised legal framework across Europe, which would benefit both businesses and individuals. In principle, the EDPS is in favour of an opt-in regime. Nevertheless, for those individual Member States oriented to create or maintain their own systems, the EDPS recommends that legislators take this opportunity to create a Europe-wide system for opting-out from unsolicited direct marketing calls, with the ePrivacy Regulation itself specifying the arrangements for the opt-out for voice-to-voice marketing calls. For the Member States choosing an opt-out regime for voice to voice marketing calls, a uniform system such as a European Do Not Call register, may therefore represent a benchmark.

Alternatively, the Regulation should at least clearly require that each Member State shall create a national Do Not Call register. It is crucial that situations could no longer exist where a user would have to opt-out with each individual communication provider, instead of simply registering via a Do Not Call register.

Additionally, the EDPS recommends that the Regulation specify that recipients of voice-to-voice calls should be given two options to withdraw their consent: for future calls from the organisation placing the call (and any affiliated organisations) and the possibility during these calls to register in a national (or European) Do Not Call register.

19. Protecting security of communications (Article 17)

It is essential that the current level of protection be maintained: legislators should not create a regulatory gap by removing the existing security obligations in the ePrivacy Directive.

The EDPS welcomes that the Proposal in its Article 17 maintains the ePrivacy Directive obligation of service providers to inform those using their services about any known security risks, which have to be taken into account when using the service. As regards the addressee of this information, it is certainly appropriate to inform the end-users (within the meaning of the definition from the EECC) about such risks, however, a clarification that ultimately the natural persons using the services have to be informed would increase the effectiveness of the security warning. The adjustment of definitions, as suggested in Section 3.1 above, may help to clarify this, but in addition a reference in the relevant recital may be useful.

The EDPS recognizes that provisions of the ePrivacy Directive on data breaches are not needed in the proposed Regulation, as the issue is covered by the corresponding provisions of the GDPR.

The EDPS is also aware that the security provisions of the EECC, as well as those of the Radio Equipment Directive (RED)[77] should contribute to the security of communications networks, services and terminals. Furthermore, the NIS Directive[78] and –to a lesser extent– the EIDAS Regulation[79] may cover some of the services in the scope of the proposed ePrivacy Regulation. However, it has to be noted that even the combined scope of services of all these different instruments may not include all services in the scope of the ePrivacy Regulation. In particular, as the material scope of the ePrivacy Regulation is wider than that of the EECC Proposal, the obligations of the EECC Proposal do not apply to all services covered by the ePrivacy Regulation. The security requirements in the GDPR only apply to cases where the processing of personal data is concerned and the responsible entity is identified as controller or processor. However, there is a need to ensure that confidentiality of all communications data is protected.

Therefore, there remains a need for specific provisions on security also in the ePrivacy Regulation[80]. The EDPS recommends adding the clarification to the ePrivacy Regulation that the security related obligations of Article 40 of the EECC Proposal should apply *mutatis mutandis* to all services in the scope of the ePrivacy Regulation, regardless of whether they are also within the scope of the EECC Proposal or not. This general security provision could be complemented by a recital listing some specific additional security measures, which were mentioned in the public consultation of the Commission[81] and supported by the EDPS in its preliminary opinion on the review:

- development of minimum security or privacy standards for networks and services;
- extending of security requirements to reinforce coverage of software used in combination with the provision of a communication service, such as the operating systems embedded in terminal equipment;
- extending security requirements to reinforce coverage of IoT devices, such as those used in wearable computing, home automation, vehicle to vehicle communication, etc; and
- 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.

These requirements could assist in the proper implementation of principles of security by design, data protection by design and data protection by default, and would provide more guidance for manufacturers and software providers. Furthermore, they could have the effect to encourage the producers of the products, services and applications used in electronic communications services to take into account the rights to privacy and data protection when developing and designing them, in a similar way as this is envisaged in Recital 78 of the GDPR.

Encryption

As it has also been pointed out by both the EDPS and the WP29 in their Preliminary Opinions, encryption has grown into a critical tool to protect the confidentiality of communications within electronic communications networks. The use of encryption has increased after the revelations about efforts by public and private organisations and governments to gain access to communications'[82].

The EDPS continues to recommend that the ePrivacy Regulation clearly allow users to use end-to-end encryption (without *'back-doors'*[83]) to protect their electronic communications. The

EDPS further recommends, as also suggested by the WP29, that decryption, reverse engineering or monitoring of communications protected by encryption should be prohibited.

In addition, the use of end-to-end encryption should also be encouraged and when necessary, mandated, in accordance with the principle of data protection by design. In this context the EDPS also recommends that the Commission consider measures to encourage development of technical standards on encryption, also in support of the revised security requirements in the GDPR.

The EDPS further recommends that the ePrivacy Regulation specifically prohibit encryption providers, communications service providers and all other organisations (at all levels of the supply chain) from allowing or facilitating *'back-doors'*.

20 Collective redress mechanisms (Article 21)

Article 21 of the Proposal omits explicit reference to Article 80 of the GDPR, which provides for the right for the data subject to '*mandate a not-for-profit body, organisation or association'*, under certain conditions, to exercise certain rights on the data subject's behalf, as well as for the possibility for Member States to provide that these organisations may perform similar functions independently of a data subject's mandate, at their own initiative. The reason for this omission is not clear, when the ePrivacy Regulation is meant to *'particularise and complement'* the GDPR, which provides for several avenues for remedies, including Article 80 on collective redress mechanisms. Here, the ePrivacy Regulation appears to leave out an important new mechanism for upholding data subjects' rights.

Article 21(2) of the Proposal refers to a possibility for individuals or legal persons *'having a legitimate interest'* to bring legal proceedings, which may have been intended to also include the availability of collective redress mechanisms under the GDPR. The introduction of the concept of legitimate interest and the absence of a reference to Article 80 of GDPR, however, require further clarification. The EDPS recommends that the legislators introduce an explicit provision for collective redress and effective remedies or otherwise clarify the text (e.g. by explicitly confirming the applicability of Article 80 of the GDPR) ensuring full availability of the collective redress mechanisms available under the GDPR.

21 Further harmonisation of fines (Articles 23(4), 23(6) and 24)

The EDPS welcomes harmonisation of enforcement powers, including the level of fines. Further harmonisation of fines, however, would be desirable. Articles 23(4), 23(6) and 24 of the Proposal provide for Member States to lay down the rules on penalties for infringements of certain provisions of the ePrivacy Regulation. The EDPS supports the recommendations of Opinion 1/2017 of the WP29[84] that it would be more consistent to arrange for this also in the ePrivacy Regulation itself.

Notes

[1] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on privacy and electronic communications), COM(2017) 10 final, 2017/0003 (COD).
[2] 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, OJ L 201, 31.7.2002, p.37; amended by Directive 2009/136/EC.
[3] WP29 Opinion 1/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) (WP247), adopted on 4 April 2017. See also WP29 Opinion 3/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC) (WP240), adopted on 19 July 2016.
[4] See https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-07-22_Opinion_ePrivacy_EN.pdf .
[5] A Digital Single Market Strategy for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, 6 May 2015 (COM(2015) 192 final) available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN.
[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.
[7] 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, 04.05.2016, p.1, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.
[8] See WP29 Opinions 1/2017 and 3/2016.
[9] See EDRi, *'EDRi's Position on the proposal of an ePrivacy Regulation'*, available at <https://edri.org/files/epd-revision/ePR_EDRi_position_20170309.pdf> (Position paper, 9 March 2017) and '*E-Privacy revision: An analysis from civil society groups'* <https://edri.org/files/epd-revision/EDRi_ePrivacyDir-final.pdf> (Analysis, 6 July 2016).
[10] Article 7 of the Charter also protects the right to privacy.
[11] See, for example, Article 10 of the German Constitution, Article 37 of the Slovenian Constitution, Article 36 of the Croatian Constitution, Article 19 of the Greek Constitution, Article 43 of the Estonian Constitution, Article 15 of the Italian Constitution, Article 49 of the Polish Constitution, Article 28 of the Romanian Constitution, Article 72 of the Danish Constitution, Article 13 of the Dutch Constitution, Article 29 of the Belgian Constitution, Article 6 of Chapter 2 of the Swedish Constitution, Article 10 of the Finnish Constitution, Article 17 of the Cypriot Constitution, Article 18 of the Spanish Constitution, Articles 10 and 10a of the Austrian Constitution, Article 13 of the Czech Constitution and Article 22 of the Slovak Constitution.
[12] As an example, Article 8(1)(b) of the Proposal requires consent for *'the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment'*. Further, Article 6(2)(c) and 6(3) requires consent for the processing of content and metadata. In addition, Article 16 on unsolicited communications also requires -as a rule subject to certain exceptions- prior consent to be the legal basis for direct marketing communications.
[13] See Article 1 and recital 14 of the GDPR with regard to legal persons, which make it clear that the GDPR grants the right to the protection of personal data only natural persons and not legal persons.
[14] Without protection of confidentiality, the use of electronic communications would be impossible for many business transactions or for exchanges in the public administration. Furthermore, organisations also benefit being protected against unsolicited phone calls, whether those calls are made to specific employees or to a central switchboard. Similarly, legal entities are entitled to the right to have incoming calls blocked not only with respect to calls made to individual employees but also to general telephone numbers used by the organisation.
[15] Further harmonisation of fines, however, would be desirable. See Annex, Section 21 for more detail.
[16] Strictly speaking, VoIP is a family of protocols that supports the provision of telephony services over networks using internet protocols (mainly IP) instead of traditional telephony standards. These technologies are used by so-called OTT providers, but also by traditional network providers. In the regulatory context the term '*VoIP'* is often used as a synonym for internet telephony provided on top of the basic transmission networks. This is the meaning applied in this Opinion.

[17] Article 2(1) of the Proposal provides that the ePrivacy Regulation applies to '*the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users'*.
[18] For further recommended clarifications, see Annex, Section 1.
[19] Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code, COM (2016) 590 final/2, 2016/0288(COD) of 12.10.2016.
[20] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended.
[21] The EEEC Proposal is based solely on Article 114 TFEU, as it aims to achieve the internal market for electronic communications and ensure its functioning. In contrast, the ePrivacy Proposal has a dual legal basis: Article 16 TFEU, the same specific legal basis as that of the GDPR, as well as Article 114 TFEU. Article 16 TFEU alone would have been insufficient, as the new provisions will not only *'particularise'* some provisions of the GDPR, but will also *'complement'* it with provisions that are not limited to the protection of personal data.
[22] The term '*subscriber'* (previously used in the current ePrivacy Directive) is no longer used. It is also useful to compare the proposed new definition with the current Article 2(a) of the ePrivacy Directive, which currently defines '*user'* as '*any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service'*.
[23] For a more detailed discussion, see also page 26, para 40(c) of WP29 Opinion 1/2017.
[24] See, e.g. Science and Technology Options Assessment (STOA), European Parliament, *Potential and impacts of cloud computing services and social network websites*, 2014. PE 513.546. Available at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf
[25] See WP29 Opinion 1/2017, para 40(c).
[26] It is useful in this context to recall Article 2(a) of the ePrivacy Directive, which currently defines *'a user'* as *'any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service'.*
[27] The EDPS recommends that the legislators carefully consider in what way best to achieve narrowly tailored appropriate exceptions to cover these situations. See also in this respect, para 18, bulletpoints 4 of the WP29 Opinion 1/2017, recommending an exception that is built upon the notion of '*domestic exception'* under the GDPR, but also incorporates limited professional use for standard functionalities such as key word search.
[28] This is based on the assumption that the definition of *'end-user'* is amended as set out in Sections 3.1 and 3.2 or otherwise replaced by a more appropriately defined term. The EDPS also notes that the notion of *'concerned'* should be avoided, as it creates unnecessary additional uncertainty as to who should provide consent.
[29] As explained in Section 3.1 discussing definitions, for the purposes of certain provisions, such as, for example, with regard to publicly available directories in Article 15, a different term will be more appropriate, to ensure that those subscribing to the service will be in a position to decide.
[30] Indeed, in everyday communications individuals often share personal data of others, both for private and professional purposes. Some of this personal data, such as, for example, intimate personal matters shared among family and close friends, or the content of communications among physicians, lawyers, fraud investigators, and so forth, can be particularly sensitive.
[31] See also the recommendation in para 18 of the WP29 Opinion 1/2017, suggesting that it should be clarified that the processing of data of persons other than the end- users (e.g. the picture or description of a third person in an exchange between two people) involved also needs to comply with all relevant provisions of the GDPR).
[32] We also note that the GDPR concerns the protection of personal data, which is a separate right, set forth in a different article, Article 8 of the Charter. Further, the legal basis of the two instruments is also not identical. Finally, the scope of the protected persons is different, as the ePrivacy Directive also provides protection for legal persons. Further, whereas it might have been possible to include many provisions of the ePrivacy Directive in the GDPR itself, this has not been the case. Recital 173 and Article 95 of the GDPR call for a clarification of the relationship between the two legal instruments in the new legislative instrument for ePrivacy.
[33] See also para 21, page 16 of WP29 Opinion 1/2017.
[34] A similar phenomenon occurs also in the world of mobile apps where the apps often request permission to access different capabilities and functions of a mobile phone, which are not necessary for the functioning of the app and provision of the service, including access to Wi-Fi, GPS, camera, messages, contacts, browsing history or pictures. An example may be torch app whose functionality is to provide a bright flashlight, but which requests overbroad data access to many of the above data categories clearly unnecessary for the functioning of the service it provides.
[35] The GDPR, in its recital 42, emphasizes that *'[c]onsent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment'*. It also highlights that *'a declaration of consent pre- formulated by the controller ... should not contain unfair terms'.* Further, recital 43 provides that *'[i]n order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller.'* Recital 43 also provides that *'consent is presumed not to be freely given … if the performance of*

a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.' This latter point has also been reiterated in Article 7(1) of the GDPR, which provides that *'[w]hen assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract'.*

[36] EDPS Opinion 7/2015: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf .

[37] On the subject of possibilities of new innovative business models, respectful of EU data protection laws, see, for example, EDPS Opinion 9/2016 on Personal Information Management Systems ('PIMS') subtitled '*Towards more user empowerment in managing and processing personal data*'.

[38] A recent Eurobarometer survey showed that almost 90% of EU citizens indeed want such privacy-friendly default settings. *TNS Political & Social at the request of the European Commission, 'Flash Eurobarometer 443 - July 2016, "e-Privacy" Report, EN'* (December 2016), at p. 43.

[39] See page 16, under the heading *'Mechanisms for providing and revoking consent'.*

[40] On the definition of end-users, see our recommendation in Sections 3.1 and 3.2.

[41] Research by EDRi members shows that most current services built on location metadata are purportedly based on anonymisation, not consent, and have raised concerns that the data, as an actual fact, is not fully anonymised. https://www.openrightsgroup.org/ourwork/reports/mobile-data.

[42] On the possibility of providing for such exceptions, see also Section 3.3 above when discussing the relationship between the GDPR and the ePrivacy Regulation.

[43] On the notion of functional separation and the organisational and technical measures that may be used to help ensure it, see also Section III.2.3, pages 28-33 of WP29 Opinion 3/2013 on purpose limitation (WP203), adopted on 2 April 2013.

[44] Joined cases C-293/12 and C-594/12 *Digital Rights Ireland*, EU:C:2014:238.

[45] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.5.2006, p. 54.

[46] Joined cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson*, EU:C:2016:970.

[47] See, by analogy, C-275/06 *Promusicae v* Telefónica de España SAU, EU:C:2007:454, Opinion of AG Kokott, paras. 86-88.

[48] See also EDPS, Assessing the necessity of measures that limit the fundamental rights to the protection of personal data: A "Toolkit", 11 April 2011, available at https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

[49] See also para 11 of the Opinion of the European Academy for Freedom of lnformation and Data Protection (EAID), 21 March 2017, available at www.eaid-berlin.de/wp-content/uploads/2017/04/EAID_Opinion_E-Privacy-Regulation.pdf (EAID Opinion).

[50] See, e.g. EDPS Opinion on the Commission proposals for a Regulation of the European Parliament and of the Council on insider dealing and market manipulation, and for a Directive of the European Parliament and of the Council on criminal sanctions for insider dealing and market manipulation, adopted on 10 February 2012 (2012/C 177/01), Section 2.3.2, in particular, paras 27 and 28, available at https://edps.europa.eu/sites/edp/files/publication/12-02-10_market_manipulation_en.pdf.

[51] See Article 48 GDPR *'Transfers of disclosures not authorised by Union law'.*

[52] See EDPS Preliminary Opinion, Section X.3, p. 21.

[53] Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code, COM (2016) 590 final/2, 2016/0288(COD) of 12.10.2016.

[54] These comments are following up on previous comments made by the EDPS on the subject as early as 2008 and 2009. In particular, on the occasion of the last, 2009 review of the ePrivacy Directive, the EDPS issued two Opinions at two different stages of the legislative procedure. In his first Opinion, the EDPS argued that *'the rising importance of the mixed (private/public) and private networks in everyday life, with the risk to personal data and privacy increasing accordingly, justifies the need to apply to such services the same set of rules that apply to public electronic communication services. To this end, the EDPS considers that the Directive should be amended to broaden its scope to include such type of private services'.*

In his second Opinion, issued at a later stage when specific amendments were discussed during the legislative procedure, the EDPS suggested including under the scope of application of the ePrivacy Directive at least *'the processing of personal data in connection with the provision of publicly available electronic communications services in public* ***or publicly accessible private*** *communications networks in the Community'* (emphasis added).

For further details, see Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on

privacy and electronic communications), issued on 10 April 2008 (2008/C 181/01), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf See in particular, paras 22-24. See also Second Opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), issued on 9 January 2009 (2009/C 128/04), available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_EN.pdf See, in particular, paras 60-72, including the quoted text in para 66.

[55] EDPS, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 14 March 2017.

[56] See also *'EDRi's Position on the proposal of an ePrivacy Regulation'* (Position paper, 9 March 2017).

[57] See WP29 Opinion 1/2017, para 40(g).

[58] Article 2(4) of the EECC Proposal defines '*electronic communications services'* by referring, among others, to *'interpersonal communications services'*, which are, in turn, defined in Article 2(5) of the EECC Proposal.

[59] See also Annex, Section 18 discussing concerns regarding the scope of protection against unsolicited communications.

[60] See also para 2, second sentence, of the EAID Opinion.

[61] For justification and a more detailed overview, see WP29 Opinion 1/2017, para 18 and 26.

[62] WP29 Opinion 2/2006 on privacy issues related to the provision of email screening services (WP118) adopted on 21 February 2006.

[63] For the technological background, please refer to the OSI model https://en.wikipedia.org/wiki/OSI_model and the Internet protocol suite https://en.wikipedia.org/wiki/Internet_protocol_suite.

[64] *'We kill people based on metadata'* was a statement made by former CIA and NSA Director Michael Hayden at John Hopkins University in April 2014. See: Pomerantz, J., Metadata, United States of America: MIT Press 2015, p. 118. The speech at John Hopkins University is available at: https://www.youtube.com/watch?v=kV2HDM86XgI with Mr Hayden's quote at 17:59 minutes.

[65] Metadata had been used during the criminal investigation, resulting in the apprehension of the accused assassins of former Prime Minister Rafiq Hariri. *'Of the 10 mobile phones used in connection with these 10 cellular telephone cards, 5 have been traced to a store in Tripoli.*' United Nations Security Council, Report of the International Independent Investigation Commission established pursuant to Security Council resolution 1595 (2005), S2005/662, Beirut: 19 October 2005, nr. 151, p. 147, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/563/67/PDF/N0556367.pdf?OpenElement.

[66] De Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013), *Unique in the Crowd: The privacy bounds of human mobility*, Nature SRep, 3, available at: http://www.nature.com/articles/srep01376 showed that four spatio-temporal points are enough to uniquely identify 95% of the individuals.

[67] New York Times Editorial Board, Surveillance: *A Threat to Democracy*, 11 June 2013, available at: http://www.nytimes.com/2013/06/12/opinion/surveillance-a-threat-to-democracy.html?hp.

[68] See WP29 Opinion 1/2017, para 18, as well as paras 10, 33 and 46 on metadata.

[69] EDPS Preliminary Opinion, pages 16 and 17.

[70] It should be clear in the legislative text that when an organization uses analytics services from a third party, which are setting their own cookies, these cannot be considered as first party cookies.

[71] WP29 Opinion 04/2012 on the Cookie Consent Exemption (WP194), available at: http://ec.europa.eu/justice/data-protection/article-29/documentationopinion-recommendation/files/2012/wp194_en.pdf.

[72] For further recommendations, see also WP29 Opinion 1/2017, pages 18-19, para 25.

[73] See also para 7 of the EAID Opinion.

[74] Recital 32 referring to messages promoting political parties or calling for support of a non-profit organisation's purposes is welcome but not sufficient to provide legal certainty comprehensively and for all relevant situations. As this is an area where freedom of expression and right to privacy may need to be carefully balanced, further guidance would be particularly helpful.

[75] See also WP29 Opinion 1/2017, para 43(c).

[76] Article 7(3) GDPR requires, among others, that it shall be as easy to withdraw as to give consent and that individuals should be able to withdraw consent at any time.

[77] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, OJ L 153, 22.5.2014, p. 62.

[78] Directive (EU) 2016/1148 of the European Parliament and of the Council 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.

[79] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73

[80] That said, the GDPR and the ePrivacy Regulation should be aligned to ensure consistency. For example, the EDPS recommends a cross-reference to the security obligations in the GDPR (including data protection impact assessments and accountability).

[81] See question 21 of the public consultation questionnaire.

[82] EDPS Preliminary Opinion, p. 19; Opinion 3/2016 of the WP29, p. 19.

[83] See https://en.wikipedia.org/wiki/Backdoor_(computing).

[84] See para 38 of WP29 Opinion 1/2017.