



17/EN

WP 247

**Opinion 01/2017 on  
the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)**

**Adopted on 4 April 2017**

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO-59 05/035.

Website: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

**THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE  
PROCESSING OF PERSONAL DATA**

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

**HAS ADOPTED THE PRESENT OPINION:**

## SUMMARY

The Working Party welcomes the proposal from the European Commission from 10 January 2017 for an ePrivacy Regulation. The Working Party welcomes **the choice for a regulation** as the regulatory instrument. This ensures that rules are uniform across the entire EU, and provides clarity for supervisory authorities and organisations alike. It also helps ensuring consistency with the General Data Protection Regulation. Such consistency is further supported by the choice to make **the same authority responsible for monitoring compliance with GDPR** responsible for the enforcement of ePrivacy rules.

Simultaneously, the choice for (maintenance of) a **complementary legal instrument** is positive. The protection of confidential communication and terminal equipment has particular characteristics which are not addressed by the GDPR. Complementary provisions with respect to these kinds of services are therefore required to ensure adequate protection of the fundamental right to privacy and confidentiality of communications, including confidentiality of terminal equipment. In this regard, the Working Party strongly supports the **principled approach** chosen in the Proposed Regulation of **broad prohibitions and narrow exceptions**, and **the targeted application of the concept of consent**.

The Working Party welcomes the expansion of the scope of the Proposed Regulation to **include Over-The-Top (OTT) providers**, services that are functionally equivalent to more traditional communication means and therefore have a similar potential to impact on the privacy and right to secrecy of communications of people in the EU. It is also positive that the Proposed Regulation clearly covers **content and associated metadata** and recognises that **metadata may reveal very sensitive data**.

However, the Working Party also notes 4 points of **grave concern**. With regard to the **tracking of the location of terminal equipment; the conditions under which the analysis of content and metadata is allowed; the default settings of terminal equipment and software and with regard to tracking walls** the Proposed Regulation would lower the level of protection enjoyed under the GDPR. In this Opinion, the Working Party provides specific suggestions to ensure that the ePrivacy Regulation will guarantee the same, or a higher level of protection appropriate to the sensitive character of communications data (both content and metadata).

With regard to **WiFi-tracking**, depending on the circumstances and purposes of the data collection, such tracking under the GDPR is likely either to be subject to consent, or may only be performed if the personal data collected is anonymised. In the latter case, the following 4 conditions have to be complied with: the purpose of the data collection from terminal equipment is restricted to mere statistical counting, the tracking is limited in time and space to the extent strictly necessary for this purpose, the data will be deleted or anonymised immediately afterwards, and there are effective opt-out possibilities. The European Commission is invited to promote a technical standard for mobile devices to automatically signal an objection against such tracking.

With regard to the **analysis of content and metadata**, the starting point should be that it is prohibited to process communications data without the consent of all end-users (senders and recipients). To allow providers to provide services explicitly requested by the user, such as for

example search- and indexing functionality, or text-to-speech services, there should be a domestic exception for the processing of content and metadata for the purely personal purposes of the user him or herself.

With regard to **consent for tracking**, the Working Party calls for an explicit prohibition on tracking walls, that is, take it or leave it choices that force users to consent to tracking if they want to have access to the service.

Last but not least, the Working Party recommends that terminal equipment and software must **by default offer privacy protective settings**, and offer clear options to users to confirm or change these default settings during installation. The settings must be easily accessible during use. Users must be enabled to signal specific consent through their browser settings. Privacy preferences should not be limited to interference by third parties or be limited to cookies. The Working Party strongly recommends to make adherence to the Do Not Track standard mandatory.

The Working Party has also identified other points of concern, relating to for example the scope, the protection of terminal equipment and direct marketing. Last but not least, the Working Party has identified issues that deserve clarification, to better protect end-users, and to introduce more legal certainty for all stakeholders involved.

## TABLE OF CONTENTS

<b>1. INTRODUCTION .....</b>	<b>5</b>
<b>2. POSITIVE ASPECTS OF THE PROPOSED REGULATION .....</b>	<b>5</b>
<i>EU-wide harmonization, alignment of fines and exclusive enforcement by DPAs .....</i>	<i>5</i>
<i>Extension of the scope compared to the ePrivacy Directive .....</i>	<i>7</i>
<i>Targeted application of the concept of consent .....</i>	<i>8</i>
<b>3. POINTS OF GRAVE CONCERN .....</b>	<b>9</b>
<i>The protection under the GDPR is undermined by the Proposed Regulation .....</i>	<i>9</i>
<b>4. OTHER POINTS OF CONCERN .....</b>	<b>15</b>
<i>The territorial and substantive scope needs to be expanded .....</i>	<i>15</i>
<i>The protection of terminal equipment needs to be strengthened .....</i>	<i>16</i>
<i>Direct marketing .....</i>	<i>19</i>
<i>Timetable .....</i>	<i>21</i>
<i>Other concerns .....</i>	<i>22</i>
<b>5. SUGGESTIONS FOR CLARIFICATION TO ENSURE LEGAL CERTAINTY .....</b>	<b>24</b>
<i>Clarifications on the scope .....</i>	<i>24</i>
<i>Clarifications on the concept and application of consent .....</i>	<i>27</i>
<i>Clarifications on location and other metadata .....</i>	<i>28</i>
<i>Clarifications on unsolicited communications .....</i>	<i>30</i>
<i>Clarifications on the application of fundamental rights instruments .....</i>	<i>31</i>
<i>Other clarifications .....</i>	<i>31</i>

## 1. INTRODUCTION

1. The Article 29 Data Protection Working Party (Working Party or WP29) welcomes the Proposed Regulation of the European Commission (EC) for the ePrivacy Regulation (the Proposed Regulation, Proposed Regulation or ePrivacy Regulation)<sup>1</sup>, which is intended to replace the ePrivacy Directive (ePD).<sup>2</sup>
2. Many aspects of the Proposed Regulation are positive, and the European Commission has taken an important step with the introduction of the Proposed Regulation. The Proposed Regulation can, however, be further improved. This would not only serve to better protect end-users, but also introduce more legal certainty for all stakeholders involved.
3. The Working Party thus has several points of concern and recommendations for clarifications to be addressed by the European Parliament and the Council of Ministers in their debate on the Proposed Regulation. This opinion will first consider the positive aspects of the Proposed Regulation, and then highlight the issues of concern and points for clarification.

## 2. POSITIVE ASPECTS OF THE PROPOSED REGULATION

### *EU-WIDE HARMONIZATION, ALIGNMENT OF FINES AND EXCLUSIVE ENFORCEMENT BY DPAs*

4. The Working Party welcomes **the choice for a regulation as the regulatory instrument**. This ensures that rules are uniform across the entire EU (with certain exceptions, to be discussed below). This provides clarity for supervisory authorities and organisations alike. In addition, given the key role the General Data Protection Regulation (GDPR)<sup>3</sup> plays in the Proposed Regulation, this helps ensuring consistency across both instruments. Simultaneously, **the choice for (maintenance of) a complementary legal instrument** is positive. The protection of confidential communication and terminal equipment has particular characteristics which are not addressed by the GDPR. Complementary provisions with respect to these kinds of services are therefore required to ensure adequate protection of this fundamental

---

<sup>1</sup> 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), 2017/0003 (COD), url: [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=41241](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241).

<sup>2</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37-47, url: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058>.

<sup>3</sup> 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 119/1, 4.5.2016, p. 1-88, url: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.

right. In this context, the Working Party also **supports the principled approach chosen in the Proposed Regulation of broad prohibitions and narrow exceptions**, and believes that the introduction of open-ended exceptions along the lines of Article 6 GDPR, and in particular Art. 6(f) GDPR (legitimate interest ground), should be avoided.

5. The **enforcement of these rules by the same authority responsible for monitoring compliance with the GDPR** will further support consistency across the two instruments. Given the relationship between the protection of personal data and the protection of confidential communication and terminal equipment, it is useful that the enforcement of the provisions under the Proposed Regulation is entrusted to the same supervisory authority enforcing the GDPR (recital 38 and Art. 18 of the Proposed Regulation). In addition, jurisprudence from the Court of Justice of the European Union (CJEU)<sup>4</sup> confirms that it is essential that the supervisory authority is independent, as prescribed by Art. 7 of the Charter. On a practical note, however, this would lead to significant extra work for the DPAs, with no guarantee of fulfillment if no extra budget is obtained. The DPAs therefore welcome recital 38 of the Proposed Regulation, which highlights that each supervisory authority should be provided with the additional financial and human resources, premises and infrastructure necessary for the effective performance of the tasks under the new Regulation. It is also welcome that Article 18(2) provides the legal basis for co-operation between the supervisory authorities of the Proposed Regulation and the national regulatory authorities of the proposed Directive establishing the European Electronic Communications Code (“EECC”).<sup>5</sup>
6. Given the close relationship between the Proposed Regulation and the GDPR, **the alignment of fines under the Proposed Regulation with the GDPR** is also to be welcomed. The activities which fall within the scope of the Proposed Regulation are quite sensitive, involving *inter alia* the interference with confidential communications and terminal equipment. The level of fines should be commensurate to this sensitive context. This context is also the reason why harmonization across the EU is important, in order to provide the same high level of protection across the entire region. Art. 23 of the Proposed Regulation provides for effective fines for infringement of the regulation, similar to the level of fines set for violation of the rules from the GDPR, except on some points (see remark 38).
7. The **removal of specific data breach notification rules** from this legislation is also to be welcomed to prevent unnecessary overlap with the data breach requirements of the GDPR.

---

<sup>4</sup> See e.g. ECJ 6 October 2015, C-362/14 (*Safe Harbour*), par. 41 and ECJ 21 December 2016, C-203/15 and C-698/15 (*Tele2/Watson*), par. 123.

<sup>5</sup> Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), 2016/0288 (COD), 12.10.2016, url: [http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM\\_2016\\_0590\\_FIN](http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN).

8. It is also **welcome that the focus is now on providing an equal level of protection to all end-users**, as the proposed Regulation has dispensed with the notion of differentiating between “subscribers” and other users of electronic communication services.

#### *EXTENSION OF THE SCOPE COMPARED TO THE EPRIVACY DIRECTIVE*

9. The Working Party welcomes **the expansion of the scope of the Proposed Regulation to include Over-The-Top (OTT) providers**, services that are functionally equivalent to more traditional communication means and therefore have a similar potential to impact on the privacy and right to secrecy of communications of EU citizens. The Working Party especially welcomes that all OTT-categories (OTT0, OTT1 and some OTT2)<sup>6</sup> now fall within the scope of the regulation as it does not only cover traditional communication means (OTT0), but also functionally equivalent services (OTT1) as mentioned in Art. 8(1)c of the Proposed Regulation. It also is positive that, in addition to the definitions under the EEC, some OTT2 are included when they provide ancillary interpersonal and interactive communication intrinsically linked to their service, such as in games, dating apps or review sites (Art. 4(2) Proposed Regulation). Similarly, **the clarification that the protection also covers machine-to-machine interaction** is also to be welcomed. Recital 12 makes it clear that devices that communicate with each other fall within the scope of protection afforded under the Proposed Regulation. This is desirable, as such communications often contain information protected under privacy rights. However, the applicability could be clarified (see remark 40h).
10. It is also positive that **the Proposed Regulation clearly covers content and associated metadata**. Recital 14 makes clear that the definition of Art. 4(3)(a) of “electronic communications data” is intended to be broad enough to cover *all* content as well as associated metadata, regardless of, for example, the means of conveyance of signals. However, the Working Party notes as a point of concern in remark 39 that this current definition of “electronic communications data” is still subject to debate. In line with this expansion of the scope, the Working Party finds **the recognition that metadata may reveal very sensitive data** (see par. 2.2 Explanatory Memorandum; recital 2) an essential addition. The Working Party welcomes the fact that the European Commission by doing so incorporates the considerations of the ECJ in *Digital Rights Ireland* and *Tele2/Watson*. The WP29 also appreciates the **acknowledgement that analysis of content is high-risk processing**. Recital 19 and Art. 6(3)(b) lay down the logical legal presumption that the scanning of content is high-risk processing under Art. 35 GDPR, and, apparently regardless of the existence of a residual high risk, always requires prior consultation with the (lead) Data Protection Authority. At the same time, the Working Party has concerns about the

---

<sup>6</sup> See for a further explanation of these terms BEREC, *Report on OTT Services*, BoR (16) 35, 29 January 2016, p. 15 and 16, url: [http://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/reports/5751-berec-report-on-ott-services](http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services). Please also note the comment in the report that the categories are intended as concepts to use in the debate about the review and are not intended as legal concepts.



scope of the definition of “metadata” and the fact that the analysis of metadata is not subject to the same mandatory DPIA requirement (see remarks 33 and 46).

11. The continued **recognition of the importance of anonymisation** is also to be welcomed. In the ePrivacy Directive, anonymisation measures already played a role in ensuring compatibility (for instance Art. 6(1) of the ePrivacy Directive which states that traffic data must be erased or made anonymous when they are no longer needed for the purpose of the transmission of a communication). In Artt. 6(2)(c) and 6(3)(b) of the Proposed Regulation, an exception to the processing prohibition of metadata and content is allowed on the basis of consent, provided that the purpose(s) concerned “*could not be fulfilled by processing information that is made anonymous*”. Requiring such privacy-protective measures in addition to asking for the consent of users protects these users from unwarranted processing. However, the Working Party simultaneously has a grave concern that adoption of such anonymisation techniques would not be required when tracking the location of users through their mobile equipment (see remark 17). In addition, even when anonymisation measures are to be applied, providers should always conduct a data protection impact assessment (DPIA) (see remarks 33 and 46), and the Working Party calls for an additional obligation to make public how the data are anonymised and aggregated (see remark 42b).
12. Another positive point is the **broad formulation of the protection of terminal equipment**. Recital 20 and Art. 8 define that the technologies used for accessing terminal equipment are not relevant: any interference with the terminal equipment, including the use of its processing capabilities, requires the consent of the end user (with certain exceptions). The EC has now helpfully confirmed that “device fingerprinting” falls under this provision. In addition, the Working Party welcomes that the failure of a third party to abide by the preferences expressed in an individual’s **browser settings are enforceable** as described in recital 22. This is helpful for those situations where a third party (e.g. an ad network) does not respect these settings. However, this should also be laid down in a relevant provision of the Proposed Regulation.
13. Lastly, the continued **inclusion of legal persons in the scope of the Proposed Regulation** is to be welcomed (see par. 2.2 Explanatory Memorandum; recitals 3, 33 and 42; Artt.1, 15 and 16(5)). This is already the case under the ePrivacy Directive, but as the data protection authorities will be tasked with enforcing the new rules, it is useful to specifically underline this. This allows the data protection authorities to take action in cases where legal persons are a victim of an infringement, for example when corporations receive spam or have their communications surreptitiously monitored. However, the Working Party also notes as points of concern that the application of consent to legal persons is not clear (see remark 41a) and it is not clear what is meant with “the legitimate interest” of legal persons in case of direct marketing (see remark 43c).

## TARGETED APPLICATION OF THE CONCEPT OF CONSENT

14. The Working Party welcomes another category of improvements related to the application and interpretation of the concept of consent. Firstly, **the clarification that internet access and (mobile) telephony are essential services and providers of these services cannot “force” their customers to consent to any data processing unnecessary for the provision of the essential service itself** is welcome. In recital 18, in particular, it is noted that basic broadband internet access and voice communications services are to be considered as essential services, which means, given the dependence of people on access to these services, that consent for the processing of their communications data for such additional purposes (e.g. processing for advertising or marketing purposes) cannot be valid. At the same time, the Working Party is concerned that this clarification is too limited. Services from certain OTT-providers may also be considered as essential services, and the ePrivacy Regulation should also specifically prohibit take-it-or-leave-it choices in other circumstances (see remark 20).
15. In addition, it is positive that **the consent requirement for the inclusion of personal data of natural persons in directories is harmonized**. Under Art. 15 of the Proposed Regulation, the processing of data in public directories is only allowed with the consent of natural persons and the possibility to object for legal persons. This is further elaborated in recital 31, which notes that this consent needs to be specific with regard to the specific categories of personal data to be included in the directory. However, the Working Party notes as a concern that the Proposed Regulation could be clearer that specific separate consent will be required for search and for reverse search (see remark 37).
16. **The new targeted exception for non-intrusive interference with terminal equipment** is also appreciated. The WP29 finds it helpful that the Proposed Regulation clarifies that the prohibition does not apply to measuring web traffic (under the narrow exception that such measurement is carried out by the provider of the information society service requested by the end-user, cf. Art. 8(1)(d) of the Proposed Regulation). See further recital 21. The Working Party, however, suggests to use a more technology neutral definition and to clarify the applicability of this exception (see remark 25).

### 3. POINTS OF GRAVE CONCERN

#### *THE PROTECTION UNDER THE GDPR IS UNDERMINED BY THE PROPOSED REGULATION*

As mentioned above, there are a number of key improvements in the Proposed Regulation. There are however, also points of concern, with different degrees of seriousness. In this section, the Working Party discusses the four issues about which it is **highly concerned**. These are provisions which **undermine the level of protection accorded by the GDPR**:

17. **The obligations in the Regulation for the tracking of the location of terminal equipment should comply with the GDPR-requirements.** Art. 8(2)(b) of the Proposed Regulation merely requires the display of a notice and the implementation of security measures in order for the collection of information emitted by terminal equipment. Art. 8(2)(b) further notes that the person responsible for this collection must indicate any measures end-users may take to minimize or stop the collection. In doing so, Art. 8(2)(b) gives the impression that organisations may collect information emitted by terminal equipment to track the physical movements of individuals (such as “WiFi-tracking” or “Bluetooth-tracking”) without the consent of the individual concerned. The party collecting these data could apparently comply by means of a notice informing users to switch off their devices, when they do not want to be tracked. Such an approach would be contrary to a basic goal of the telecommunications policy of the European Commission to provide high-speed mobile internet connectivity with strong privacy protections at a low cost to all Europeans, across borders.

In addition, the Proposed Regulation does not impose any clear limitations with regard to the scope of the data collection or subsequent processing activities. In this context, it should be noted that these MAC addresses are personal data, even after security measures such as hashing have been undertaken. By not imposing further requirements or limitations, the level of protection of these personal data under the Proposed Regulation is significantly lower than under the GDPR, under which such tracking would need to be fair and lawful, as well as transparent. Recital 25 further unhelpfully notes that some of the WiFi-tracking functionalities do not entail high privacy risks, while others – such as tracking individuals over time – do. While the Working Party appreciates the recognition that the latter has high privacy risks, it is not useful to already decide upfront that certain other functionalities do not, without further assessment of the circumstances and proportionality of the processing. Such assessment should be carried out taking into account the following conditions regarding non-anonymised Wifi-tracking.

Depending on the circumstances and purposes of the data collection, the tracking under the GDPR is likely either to be subject to consent, or may only be performed if the personal data collected is anonymised. This anonymisation is preferably done immediately after collection. If immediate anonymisation is not possible in view of the purposes for which the data is collected, this data may be processed during a period in which it is not anonymised only under the following conditions; (i) the purpose of the data collection must be restricted to mere statistical counting (see the examples below), (ii) the tracking is limited in time and space to the extent strictly necessary for this purpose, (iii) the data is deleted or anonymised immediately afterwards and (iv) there must be an effective opt-out possibility. In all circumstances, controllers of course have to comply with the requirement to provide adequate information.

The Working Party is concerned that a potential offer of an individual opt-out per organisation that collects these data, would pose an unacceptable burden on citizens, given the increase in the deployment of such tracking technologies by both private and public sector organisations. Therefore the Working Party calls on the European

legislator to promote the development of technical standards for devices to automatically signal an objection against such tracking, and to ensure that adherence to such a signal is enforceable.

For example, consent under the GDPR would likely be required where a data controller collects and stores the indirectly identifiable (WiFi- or Bluetooth-) MAC addresses of devices, and calculates the location of the user, in order to track the user's location over time, for example across multiple stores. This is especially the case where such tracking takes place in public areas, where users have a legitimate expectation not to be identified or tracked yet where MAC addresses of passers-by are collected. Such consent may for example be obtained with the help of an app, that invites users to allow tracking of their location in specified areas in exchange for commercial offers, or by offering check-in points inside specific locations or through a consent module in WiFi hotspots.

Only in a limited number of circumstances might data controllers be allowed to process the information emitted by the terminal equipment for the purposes of tracking their physical movements without the consent of the individual concerned. For example, this could be the case when counting the amount of customers inside a specific location, or when collecting the emitted data at both sides of a security check point to display the waiting time. However, in both examples the data would have to be deleted or anonymised as soon as the statistical purpose can be fulfilled. That means that the MAC addresses of visitors' devices inside of a specific location, such as a store, have to be anonymised immediately upon the collection, without any permanent storage of the MAC addresses, and in such a way that re-identifiability is technically excluded. In the case of calculation of the waiting time, the MAC addresses would have to be deleted or anonymised as soon as the data are no longer relevant for calculating the waiting time (for example because the visitor has arrived at the other side of the security check or because he or she has left the queue). Additionally, the data controller would have to comply with data minimisation requirements (for example, not tracking 24/7 when the purpose is limited to shop opening hours and/or sampling at intervals). Data controllers must also take other mitigating measures to ensure that there is no or very little impact on the privacy rights of users for instance to protect the privacy of people living next to a collection point.

The choice in Art. 8(2) of the Proposed Regulation for a mere notice requirement is all the more remarkable given the conclusion in recital 20 that information related to the end-users' device may also be collected remotely for the purpose of identification and tracking, and that such processing – according to the Proposed Regulation – may seriously intrude upon the privacy of these end-users. In addition, the obligation does not go beyond the information obligation already foreseen by Artt. 13 and 14 GDPR. The serious privacy intrusion by the tracking is further compounded by the potential access of others to the collected data, such as the possibility for law enforcement to identify end-users based on the stored MAC address(es) broadcasted by their mobile devices.

**18. The conditions under which the analysis of content and metadata is allowed must be elaborated.**

In Article 6 of the Proposed Regulation, different levels of protection are accorded to metadata and content. The WP29 does not support this difference: both categories of data are highly sensitive. Metadata and content should therefore be accorded the same high level of protection. The starting point should thus be that it is prohibited to process metadata as well as content without the consent of all end-users (i.e. sender and recipient).

Depending on the purposes, however, certain processing may be allowed without consent, if strictly necessary for those purposes:

- Providers may process electronic communications data for the purposes mentioned in Artt. 6(1) (a) and (b), 6(2) (a) and (b) of the Proposed Regulation.<sup>7</sup>
- It should be clarified that certain spam detection/filtering and botnet mitigation techniques may also be considered strictly necessary for the detection or stopping of abusive use of electronic communications services (Art. 6(2) (b)). With regard to spam filtering, end-users receiving spam should be offered, where technically possible, granular opt-out choices.
- It should be clarified that the analysis of electronic communications data for customer service purposes may also fall under the “necessary for billing”-exception (cf. Art. 6(2) (b)). The relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law. The relevant data (such as URL's) may only be retained at the request of the end-user, and then only for a period strictly necessary to resolve a dispute over a bill (which means Art. 7(3) should thus be amended).
- It should be made possible to process electronic communications data for the purposes of providing services explicitly requested by an end-user, such as search or keyword indexing functionality, virtual assistants, text-to-speech engines and translation services. This requires the introduction of an exemption for the analysis of such data for purely individual (household) usage, as well as for individual work related usage.<sup>8</sup> This would thus be possible without the consent of all end-users, but may only take place with the consent of the end-user requesting the service. Such a specific consent would also preclude the provider from using these data for different purposes.

---

<sup>7</sup> With regard to the necessity to meet mandatory quality of service requirements, as outlined in Article 6(2) (a) of the Proposed Regulation, providers should take into account the conditions described in Regulation (EU) 15/2120 (the EECS), specifically Article 3 and recitals 10 and 13-15. Based on this provision, it may be required from providers to process communications data to detect and filter malware and spyware and they may be allowed to compress data.

<sup>8</sup> While Recital 13 of the Proposed Regulation explicitly excludes corporate networks from the scope of the Regulation, this new individual usage exception should also address the use of cloud services by employees for work-related usage such as searching in their e-mail.

This means that the analysis of content and/or metadata for all other purposes, such as analytics, profiling, behavioural advertising or other purposes for the (commercial) benefit of the provider, requires consent from all end-users whose data would be processed. As to those situations, the Proposed Regulation should explain that the mere act of sending an e-mail or other kind of personal communication from another service to an end-user that has personally consented to the processing of his or her content and metadata (for example in the course of signing up to a mailservice), does not constitute valid consent from the sender.

Lastly, 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

19. **Terminal equipment and software must *by default* discourage, prevent and prohibit unlawful interference with it and provide information about the options.** Though the Proposed Regulation obliges software providers permitting electronic communications to “offer the option” to prevent a limited form of interference with terminal equipment and, upon installation, obliges software providers to require from end-user to consent to a setting (Art. 10(1) and (2)), such a choice does not equal *privacy by default*. Besides, the “option” to prevent certain interference already currently exists, and to date this has not resulted in sufficiently addressing the problem of unwarranted tracking. This is exactly why, under the GDPR, a conscious policy choice has been made to introduce the principles of data protection and privacy by design and by default (Art. 25 GDPR). The Proposed Regulation undermines these principles with regard to communications- and device data. Meanwhile, the Radio Equipment Directive 2014/53/EU<sup>9</sup> (mentioned in recital 10) only provides for a very limited security obligation, requiring radio equipment to incorporate “safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected” (Art. 3(3)(e)). This cannot replace specific privacy by default settings under the Proposed Regulation. In this regard, it is also worthwhile to note that the e-Privacy Eurobarometer survey published in December 2016 notes that “[a]lmost seven in ten (69%) totally agree the default settings of their browser should stop their information from being shared”.<sup>10</sup> The Working Party has a separate concern with regard to browser settings and the definition of 'third parties'. See remark 24. Moreover, it should be kept in mind that this provision not only concerns browsers used on computers, but also extends to other types of software that permits communication (including operating systems, apps and software interfaces for Internet of Things-connected devices). In sum, terminal equipment and software must *by default* offer privacy protective settings, and guide users through configuration menu's to deviate from these default settings upon installation. These configuration menu's should always be easily accessible during use. The Working Party encourages the European legislature to clarify the scope of article 10 to this effect.

---

<sup>9</sup> Radio Equipment Directive 2014/53/EU.

<sup>10</sup> See Flash Eurobarometer 443, Report e-Privacy (published December 2016), p. 5.

20. **The ePrivacy Regulation should explicitly prohibit tracking walls**, i.e. the practice whereby access to a website or service is denied unless individuals agree to be tracked on other websites or services. As already noted in previous Working Party Opinions about the ePrivacy Directive<sup>11</sup>, such “take it or leave it” approaches are rarely legitimate.<sup>12</sup> When the use of processing and storage capabilities of terminal equipment or the collection of information from end-users’ terminal equipment enables the tracking of the activities of the user over time, or across several services (e.g., different websites or apps), such processing activities may seriously intrude upon the privacy of these users. Given the fundamental importance of internet in enabling the fundamental right of freedom of expression, including the right to access information, individuals’ ability to access content online should not be dependent on the acceptance of the tracking of activities across devices and websites/apps. The future ePrivacy regulation should therefore specify that access to content in for example websites and apps may not be made conditional on the acceptance of such intrusive processing activities, regardless of the tracking technology applied, such as cookies, device fingerprinting, injection of unique identifiers or other monitoring techniques. The necessity of this prohibition is underlined by the recent Eurobarometer survey on e-Privacy, which notes that “[a]lmost two thirds of respondents say it is unacceptable to have their online activities monitored in exchange for unrestricted access to a certain website (64%)”.

21. In summary, with regard to the four above mentioned points, **the Proposed Regulation should fulfill its promise to provide an equal or higher level of protection than the GDPR**. Recital 5 matter-of-factly notes that the Proposed Regulation does not lower the level of protection enjoyed under the GDPR. As the Proposed Regulation currently stands, however, this is incorrect, in particular with regard to the tracking of devices (remark 17) the missing principle of privacy by default (remark 19) and consent (remark 18). This is particularly relevant as it is noted in the same recital that the Proposed Regulation will be “*lex specialis* to the GDPR and will particularise and complement it as regards electronic communications data that qualify as personal data”. The Working Party suggests that, at the minimum, the text of the ePrivacy Regulation clarifies that

- (i) the prohibitions under the ePrivacy Regulation take precedence over permissions under the GDPR (e.g., the interference prohibition under Art. 5 of the ePrivacy Regulation takes precedence over the rights of electronic communications service providers to further process personal data under Art. 5(1)(b) and 6(4) GDPR);
- (ii) when the processing is allowed under any exception (including consent) to the prohibitions under the ePrivacy Regulation, this processing, where it concerns personal data, still needs to comply with all relevant provisions in the GDPR;

---

<sup>11</sup> See e.g. WP240 (ePrivacy review), p. 16; WP 208 (consent exemption), p. 5.

<sup>12</sup> This position is without prejudice to Article 7(4) of the GDPR, which may also preclude ‘take it or leave it choices’ in other situations where this is appropriate.

(iii) when the processing is allowed under any exception to the prohibitions under the ePrivacy Regulation, any other processing on the basis of the GDPR shall be prohibited, including processing for another purpose on the basis of Art. 6(4) GDPR. This would not prevent controllers from asking for additional consent for new processing operations. Neither would it prevent the legislators from providing additional, limited and specific exceptions in the ePrivacy Regulation, for example, to allow processing for scientific or statistical purposes under Art. 89 GDPR or to protect ‘vital interests’ of individuals pursuant to Art. 6(d) GDPR.

In addition, the ePrivacy Regulation should be interpreted in such a way as to ensure that it affords at least the same and where appropriate higher level of protection as under the GDPR

#### 4. OTHER POINTS OF CONCERN

In addition to the points mentioned above, the Article 29 Working Party is **concerned** about the following.

##### *THE TERRITORIAL AND SUBSTANTIVE SCOPE NEEDS TO BE EXPANDED*

22. **The term “metadata” is too narrowly defined.** This is now defined in Art. 4(c) as “data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content” (emphasis added). The use of the word “network” appears to suggest that only data generated in the course of the provision of services in the “lower” layer of the network would qualify as “metadata”. This could mean that data generated in the course of the provision of an OTT-service would be excluded from this scope. This would be undesirable, and probably also not intended given the intention to extend the scope of the Proposed Regulation to OTT-service providers. In order to address this, the definition of “electronic communications metadata” should be amended to include all data processed for the purposes of transmitting, distributing or exchanging electronic communications content.

23. In addition, a matter of concern is that **the territorial scope of the Proposed Regulation with regard to organisations without an establishment in the EU only addresses electronic communications service providers.** Under the Proposed Regulation, the provider of an electronic communications service not established in the EU shall designate in writing a representative in the Union (Art. 3(2)). It is also mentioned in recital 9 that the Regulation would apply to processing by electronic communications service providers without regard to the location of the processing. The Working Party welcomes this clarification. However, as the wording is restricted to providers of electronic communications services, it is uncertain to what extent this territorial scope applies to other types of parties (for instance parties interfering with or collecting information broadcasted by end-users’ terminal equipment cf. Art. 3(1) (c) jo. Art. 8 of the Proposed Regulation). Therefore, the Working Party suggests Artt. 3(2) and 3(5) be amended in order to include providers of publicly available directories, software providers permitting electronic communications and persons



sending direct marketing commercial communications or collecting (other) information related to or stored in end-users' terminal equipment, whenever their activities are targeted to users in the EU (cf. recital 8 of the Proposed Regulation).<sup>13</sup>

#### *THE PROTECTION OF TERMINAL EQUIPMENT NEEDS TO BE STRENGTHENED*

Another category of concerns has to do with insufficient protection of terminal equipment in the Proposed Regulation.

24. Firstly, **the Proposed Regulation incorrectly suggests that valid consent can be given through non-specific browser settings.** The Working Party recognizes the consideration that end-users are currently overloaded with requests to provide consent (recital 22). Browser (and comparable software) settings have a role to play in addressing this problem. However, as general browser settings are not intended to apply to the application of a tracking technology in one individual case, they are unsuitable for providing consent under Article 7 and recital 32 of the GDPR (as the consent is not informed and specific enough).

The end-user must be able to give separate consent per website or app for tracking for different purposes (such as social media sharing or advertising). A data controller responsible for several websites or apps may also ask for consent for all other sites of apps under his control, as long as this consent request is presented separately.

In addition, the controller has to comply with all other obligations related to consent, including the obligation to provide users with adequate information. For both browsers and data controllers this means it would be invalid if they would only offer an option 'to accept all cookies', since this would not enable users to provide the required granular consent. However, it should be possible for browsers to allow users to make an informed and conscious choice to accept all cookies, and thus prevent any future specific consent requests from websites they visit.

The Working Party strongly recommends that the ePrivacy Regulation makes it mandatory for browsers to implement technical mechanisms such as the Do Not Track standard to ensure that users are given genuine choice and control over the interference with their devices.<sup>14</sup>

More importantly even, the ePrivacy Regulation should ensure that both the choice with regard to storage of information in the device and a DNT signal from a browser is accepted as a legally binding indication of consent or refusal by all data controllers. This is without prejudice to further guidance from the Working Party on compliance of the DNT standard, inter alia with the principle of purpose limitation, when the standard will have been finalised (scheduled for the end of 2017).

---

<sup>13</sup> See Article 3(2) of the GDPR: "*This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*" This obligation could also include exceptions along the line set out in Art. 27(2) GDPR.

<sup>14</sup> See URL: <https://www.w3.org/TR/tracking-compliance/>. Paragraph 7 explains the exception model and the distinction between site-wide and web-wide exceptions. Paragraph 6 contains the machine readable information that data controllers may provide in terms of the information requirement for obtaining consent.

Implicit types of 'consent', such as a click on the website or scrolling of the page, cannot override choices with regard to storage and the DNT signal. An important benefit of the use of this standard is that it is not limited to the tracking technology of cookies, but also addresses other types of tracking, such as fingerprinting.

Making adherence to this standard legally mandatory will also solve another problem, with the current usage in Article 10 of the term 'third parties'. A web page or app generally contains many elements, both from the website itself, as well as external elements. And external code may also run in the context of the visited website, while it reports back to a third party server. A tracking cookie may be served by a first party when a user visits for example a social networking site. This social networking site could also be a third party when that user visits another website that contains interaction with that social networking site. In all of these cases, regardless whether it concerns 'access to' or 'storing' of information in the device of the end-user, this constitutes interference with the device, for which consent is required (unless one of the exceptions applies). In the DNT standard, this is addressed by using the terms 'site-wide' and 'internet-wide'. Therefore, to improve the legal certainty of all stakeholders, the reference in the ePrivacy Regulation to 'third parties' should be rephrased to cover all entities with which a device interacts (because they store or access information in the device).

In order to make the Do Not Track standard compatible with the high level of protection of confidentiality of communications and data protection accorded under the Charter, the ePrivacy Regulation should specify that requests for internet-wide tracking, as opposed to site-wide tracking, must be presented separately and users should be free to accept or deny such requests. Additionally, to protect users against frequent consent requests, the ePrivacy Regulation should ensure that a refusal to accept internet-wide tracking from a specific organisation (via the Do Not Track standard, or via a separate blacklist) blocks that organisation from making future consent requests, for at least 6 months. This rule does not preclude that organisation when directly visited by the user (i.e. as a first party) from asking for consent on its own website (i.e. a request for site-wide consent). In practice, this means that for example a videostreaming site that serves tracking cookies may ask for consent when that user visits the videostreaming site, but may not ask again for consent for a period of 6 months when that user has refused to consent, and visits other websites that contain videos served from the streaming website.

25. Additionally, **the exception for “web audience measurement” is imprecisely worded**. Art. 8(1) (d) of the Proposed Regulation provides for an exception for web audience measuring. The first point of concern is that this term is undefined and may be confused with user profiling. The definition should make clear that this exception cannot be used for any profiling purposes. The exception should only apply to usage analytics necessary for the analysis of the performance of the service requested by the user, but not to user analytics, (i.e. the analysis of the behaviour of identifiable users of a website, app or device). Therefore, the exception cannot be used in circumstances where the data can be linked to identifiable user data processed by the provider or other data controllers. In addition, its description suggests a very technology specific application. The term “web audience measuring” should therefore be redefined in a

technology neutral manner, in order to also include similar analytical usage information retrieved from apps, wearables and internet of things devices.

The Working Party suggests drawing inspiration from the Dutch exception, which applies if strictly necessary in order to obtain information about the technical quality or effectiveness of a delivered information society service, and has no or little impact on the privacy of the subscriber or end/user involved (cf. Art. 11.7a(3)(b) Dutch Telecommunications Act). This exception takes account of the fact that most of the data collected via web or app analytics are still personal data. This means that processing of this data is also subject to the GDPR. This for example implies that usage analytics could also be performed by an external organisation, but only if:

- (i) that organisation acts as data processor;
- (ii) a GDPR-compliant processor agreement is concluded;
- (iii) the analytics technology used prevents re-identification, including, among others, the anonymisation of IP-addresses from users;
- (iv) the specific cookie(s) or other data used for analytics can only be used for that specific site, app or wearable and cannot be linked to other identifiable data;
- (v) users have the right to opt out (see also remarks 17 and 50 in this Opinion).

Even though consent would not be required if these conditions are met, data controllers must still provide adequate information to users, for example through the tracking status representation fields in the Do Not Track standard.<sup>15</sup>

26. The ePrivacy Regulation **should ensure narrow and precisely worded exceptions on consent requirements**. The wording of the exception to the consent requirement for interference with devices in Art 8(1)(c) is almost identical to the current wording in the ePrivacy Directive, Article 5(3), “*strictly necessary in order to provide an information society service explicitly requested by the subscriber or user*” but the critical word “strictly” is omitted, without any explanation. This is a concern for two reasons. Firstly, the provision in the ePrivacy Directive has already lead to ample discussion about its scope between supervisory authorities and organisations, and the deletion of the word 'strictly' will provide even less legal certainty. This is also a concern because the Working Party has already provided guidance on the interpretation of the term “strictly” in this context. The Working Party suggested the following clarification in the Opinion on the Cookie Consent Exemption (WP 194): “*A cookie is strictly necessary to provide a specific functionality to the user (or subscriber): if cookies are disabled, the functionality will not be available and this functionality has been explicitly requested by the user (or subscriber), as part of an information society service.*”<sup>16</sup>

Additionally, the Working Party clarified that:

---

<sup>15</sup> See: Tracking Preference Expression (DNT), Editor's draft 7 March 2016.

<sup>16</sup> Article 29 Working Party, WP 294, Opinion 04/2012 on Cookie Consent Exemption, adopted on 7 June 2012, url: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf).

*“third party” cookies are usually not “strictly necessary” to the user visiting a website since these cookies are usually related to a service that is distinct from the one that has been “explicitly requested” by the user.*<sup>17</sup>

The Working Party added that the use of social plugins aimed at non-users of a platform or website would equally not be considered strictly necessary.

Moreover, while Article 6(1) (b) of the Proposed Regulation allows the processing of electronic communications data if “necessary” for security purposes, recital 49 of the GDPR requires this to be strictly necessary. The omission of the word “strictly” might not have been intentional, since recital 21 of the Proposed Regulation does mention that consent for interference should not be requested where “strictly” necessary. Nevertheless, the Proposed Regulation provides an opportunity to further clarify that the necessity-test in the context of this regulation should be interpreted narrowly with regard to all exceptions. The Working Party therefore suggests that with regard to all exceptions in Artt. 6 and 8(1) of the Proposed Regulation the word “strictly” should be added before “necessary”.

On the other hand, the ePrivacy Regulation should explicitly allow for interference with equipment in order to install security updates. Sending security updates via the internet is the preferred method for installing security updates on most end-user devices. Installing updates is considered an interference with terminal equipment. There is a legitimate interest in ensuring that the security of these devices remains up-to-date. A provider of security patches should in general therefore be able to install the strictly necessary security updates without consent from the end-user. It is, however, uncertain whether this interference can profit from the “information society”-exception to the interference prohibition (Art. 8(1) (c)). It should be clarified that the installing of security updates is allowed under this exception, but only to the extent that (i) the security updates are discretely packaged and do not in any way change the functionality of the software on the equipment (including the interaction with other software or settings chosen by the user), (ii) the end-user is informed in advance each time an update is being installed, and (iii) the end-user has the possibility to turn off the automatic installation of these updates.

## *DIRECT MARKETING*

Another category of concerns relates to the insufficient protection against direct marketing.

27. Firstly, a matter of concern is that **the scope of direct marketing is too limited**. In Art. 4(3) (f) of the Proposed Regulation, “direct marketing communications” are defined as “any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services”. The use of the word “sent” implies the use of technological communication means that necessarily involve the conveyance of a communication, whereas most advertising on the web (through social media platforms or on websites) would not involve “sending”

---

<sup>17</sup> Ibid.

advertisements in the strict sense. This is further underlined by the examples which follow in this definition (SMS, email) and in recital 33. These all refer to quite traditional forms of marketing communication, and even then the use of – quite traditional – calling systems arguably does not fall within the scope. The Article and recital should be amended to include all advertising *sent, directed or presented* to one or more identified or identifiable end-users. In addition, it should further be ensured that behavioural advertisements (based on the profiles of end-users) are also considered direct marketing communications directed at “one or more identified or identifiable end-users” (as such advertisements are targeted to specific, identifiable users).

Further, under the proposed scope of “direct marketing communications”, the protection of Art. 16(1) would be limited to messages containing advertising material, and would not protect individuals from other messages sent, directed or presented for marketing purposes (such as lead-generation messages seeking consent, promotion of political views or voting preferences, promotion of charities or other non-profit organisations or general branding of an organisation). Moreover, fax machines are still in use as a direct marketing method, although they are not mentioned in the definition. Article 4(3)(f) should therefore include any form of advertising, canvassing or promotion, also for non-profit organisations, and should explicitly include fax machines alongside email and SMS (see also the suggestion for clarification in remark 43(a)). Lastly, recital 32 states that direct marketing includes messages sent by political parties to promote their parties. This should be updated to include politicians and candidates for election who are promoting their candidacy.

28. Secondly, **the withdrawal of consent for direct marketing is not free of charge, nor as easy as to give consent.** The option to withdraw consent under the Proposed Regulation needs to be clarified to ensure consistency and improve protection of recipients. Art. 16(6) of the Proposed Regulation currently provides that recipients of direct marketing must be informed about “the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner, to receive further marketing communications” (emphasis added). This is confirmed in recital 34. It follows from recital 70 of the GDPR, however, that data subjects under the GDPR should not only have the right to object to processing for the purposes of direct marketing in an easy manner, but also to do so “free of charge”. This term is also 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.

Art. 7(3) GDPR provides that it shall be as easy to withdraw as to give consent and that individuals should be able to withdraw consent at any time. Additionally, in its Opinion 04/2010 on FEDMA (WP174), the Working Party already recognised the importance of offering “a simple effective, free of charge, direct and easily accessible method of unsubscribing” from direct marketing.<sup>18</sup> This standard for withdrawing

---

18 Article 29 Working Party, WP174, Opinion 04/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing, adopted 13 July 2010, url: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_en.pdf).

consent should be incorporated in the rules for direct marketing in the Proposed Regulation. The same goes for the requirement of Art. 7(3) of the GDPR that it should be as easy to withdraw as to give consent at any time.

29. Related to this, **the way to withdraw consent or opt-out from direct marketing calls should be clarified**. Based on Article 16(4) of the Proposed Regulation, Member States may choose an opt-out regime for voice to voice marketing calls. The ePrivacy Regulation should specify the arrangements for the withdrawal of consent and for the opt-out for marketing calls. Recital 36 specifies that Member States *should be able to* establish and/or maintain national opt-out systems. Based on this provision, Member States thus could even allow a situation where a user would have to opt-out with individual communication providers. Such an implementation fails to protect users against the nuisance of unwarranted communication<sup>19</sup> or provide a GDPR-compliant mechanism to withdraw consent easily and at any time. Therefore the Regulation should specify that each Member State *must* create a national Do Not Call register. Additionally, the Regulation should specify that recipients of voice-to-voice calls should be given two options to withdraw their consent: for future calls from that company or organisation and the possibility during these calls to register in a national Do Not Call register.
30. Another point of concern is that **the use of false identities when sending direct marketing communications is not explicitly prohibited**. 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 Art. 16(4), 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.
31. This point relates to another concern: **the prefix-requirement for direct marketing calls is presented as an alternative to the contact line identification requirement**. Under Art.16(3), direct marketing calls are allowed if the caller either (i) presents the identity of a line on which the natural or legal person placing the call can be contacted (Art. 16(3)(a)) or (ii) uses a specific code/prefix to identify it as a marketing call (Art. 16(3)(b)). Although the Working Party welcomes the obligation at Art. 16(3) (b) to use a prefix, it believes that this requirement does not address the same issue addressed by the contact line identification obligation at Art. 16(3) (a). Whereas the prefix-requirement is intended to enable the recipient to identify a call as a marketing call upfront (and to implement measures to block these calls), the contact line identification requirement is intended to provide recipients (and supervisory authorities) with means to identify and contact the instigator of the marketing. This is particularly relevant for automated calls, where there is a strong imbalance between the possibilities of the marketer to send nuisance calls and the possibilities of the

---

<sup>19</sup> For example, in the UK, telecom operator BT recorded 31 million nuisance calls in one week. See: <http://www.bbc.com/news/business-38635921>.

recipient to avoid these calls. The requirements must thus not be alternatives, but be complementary to each other.

#### *TIMETABLE*

32. The Article 29 Working Party commends the European Commission for acknowledging the need for the Proposed Regulation to enter into force alongside the GDPR in May 2018, in order to avoid inconsistencies between the two legislative acts. However, it is still of concern that this is an ambitious timescale which also requires the draft EECC to be finalised. WP29 therefore requests that all stakeholders in the legislative process commit to the deadline of May 2018.

#### *OTHER CONCERNS*

This section discusses a number of additional concerns.

33. Firstly, the WP29 is concerned about **the suggestion that non-targeted data retention measures are acceptable**. The Explanatory Memorandum notes that under the Proposed Regulation, Member States remain free to keep or create national data retention frameworks that provide, *inter alia*, for targeted retention measures (par. 1.3). After the *Tele2/Watson*-decision<sup>20</sup>, it is clear that retention frameworks providing for anything other than targeted retention are not allowed under the Charter (and even then are subject to important conditions such as oversight), and that generalised access to metadata will have to be seen as infringing the essence of Art. 7 in the same manner as generalised access to the content of electronic communication is (cf. CJEU, Schrems, and recital 94). The phrasing of this sentence thus suggests a certain room for Member States in respect to data retention measures which does not exist. Related to this, **metadata is not accorded a sufficient level of protection** in the Proposed Regulation. As noted in remark 10, the Article 29 Working Party welcomes the recognition that metadata may reveal very sensitive data. However, metadata in the Proposed Regulation do not receive the protection which should follow from this recognition. Given the sensitivity of metadata, in particular, prior to an analysis under Art. 6(2) (c), a DPIA should be conducted (see also remark 46).
34. Secondly, **the Proposed Regulation would undesirably broaden the possibilities to retain data**. Article 11 of the Proposed Regulation refers to Article 23(1)(a)-(e) of the GDPR in describing the purposes for which Member States may restrict the obligations and rights provided for in Articles 5 to 8 of the Regulation. The GDPR does not foresee such restrictions with regard to special categories of data, in line with the high risks for data subjects. While Art. 15 of the ePrivacy Directive currently allows for a similar restriction, the purposes are more limited. The new Proposed Regulation would make new restrictions possible for the purposes of “the execution of criminal penalties, including the safeguarding against and the prevention of threats

---

<sup>20</sup> ECLI:EU:C:2016:970, URL: <http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203>.

to public security” (Art. 23(1)(d) GDPR) and “other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security” (Art. 23(1)(e) GDPR). These purposes are not only new compared to the ePrivacy Directive, the last purpose of Art. 23(1) (d) and the entire purpose of Art 23(1) (e) are worded extremely broadly. It is therefore suggested to delete the reference to Art. 23(1) (a)-(e) GDPR and instead mention only the purposes currently mentioned in Art. 15 of the ePrivacy Directive.

35. **The obligation to inform users about security risks has a minimalistic scope.** The Working Party welcomes the fact that service providers must inform users about security risks and measures to address these risks, such as encryption (Art. 17 and recital 37). The title of the provision, however, reads: “Information about detected security risks”. The fact that the title speaks of detected risks suggests that this provision only relates to (potential) security breaches, while the wording of the provision and the recital points more towards general education of end-users. As an example, if a service provider detects that a user’s device is infected with malware and has become part of a bot-net, this provision seems to put a direct obligation on the provider to inform the user about the resulting risks. However, the scope of this provision could be clarified, and should not be limited to this specific scenario. The provision should at least cover detected security risks in all equipment provided to the end-user by the provider as part of the subscription, such as for example routers and mobile devices and include education about the risks of changing settings that have been set to privacy protective according to the principle of privacy by design.

The Working Party recommends that the scope be extended to include software providers permitting electronic communications (cf. recital 8) and possibly also to a new category: providers of technology essential to secure communications, which are not service providers (e.g. providers of encryption technology). In case of this latter expansion, care should be taken that this obligation does not overlap with the security breach notification obligations in other instruments such as the NIS Directive<sup>21</sup> and other legal instruments regarding certificate providers. As the latter category of technology providers usually do not have direct contact with end-users, it also has to be explained how they can comply with their information obligation under this provision.

36. The Working Party welcomes the provisions of Articles 2 and 13 which will apply to number-based interpersonal communications services. However, it is not immediately apparent why a **similar level of privacy protection should not also be available to functionally-equivalent OTT call services.**

---

<sup>21</sup> 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.1-30, url: [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.194.01.0001.01.ENG](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG)



37. The Working Party is also concerned about the **lack of clarity over granular consent for reverse search in directories**. Art. 15(2) of the Proposed Regulation requires providers to obtain consent from end-users before enabling search functions related to data (see also recital 31). The Working Party welcomes the harmonisation of the consent requirement with regard to inclusion in directories, but regrets the lack of granularity with regard to different kinds of searches. The current ePD allows Member States to require a separate consent requirement for reverse search, based on Article 12(3). This Article states that “*Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers*”. Based on this provision, in many Member States a separate consent is required for reverse search functionalities, taking into account the different levels of identifiability and thus intrusiveness of the two functionalities.
38. On a more formal point, **the level of fines is not harmonised for all infringements of the Regulation**. In the Proposed Regulation, Member States shall lay down the rules on penalties for infringements of Articles 23(4), 23(6) and 24 of the Proposed Regulation). It is more consistent to arrange for this also in the ePrivacy Regulation itself.
39. And lastly, **the Proposed Regulation relies on definitions which can become “moving targets”**. For a number of its key concepts, the Proposed Regulation refers to a different legal instrument which is currently in draft form: the proposed EECC (see for example Art. 4(1) (b)). Two important examples of this are the definition of “end-user”, which currently includes natural and legal persons, and the definitions of “electronic communications service” and “interpersonal communications service” which are reflected in the Proposed Regulation at Art. 4(1) (b) and, the case of the latter, further particularised at Art 4(2) to include service types specifically excluded in the EECC.<sup>22</sup> This Opinion is based on the definitions as they currently stand, however it is quite likely that the proposed EECC and/or its key concepts will change. This would have immediate implications for the ePrivacy Regulation as well. Ideally, all terms that originate from the EECC should be independently defined in the ePrivacy Regulation; or, as a minimum, the Proposed Regulation should include clarification where there are any terms whose definitions deviate from those contained within the EECC (e.g. the aforementioned inclusion of “ancillary services” in the definition of “interpersonal communications service”). However, if this is not possible the Working Party would like to suggest to all parties involved in the legislative process ensure that both the Proposed Regulation and the EECC are discussed and voted on simultaneously, in order to allow stakeholders to correctly assess the scope and implications of the new instruments.

---

<sup>22</sup> For example, Art. 4(2) of the Proposed Regulation says that an interpersonal communications service “shall include services which enable interpersonal and interactive communications merely as a minor ancillary feature that is intrinsically linked to another service” whereas Art. 2(5) of the EECC specifically excludes such services from that definition. (The EECC includes “interpersonal communications service” within the wider category of “electronic communications service” at Art. 2(4).)

## 5. SUGGESTIONS FOR CLARIFICATION TO ENSURE LEGAL CERTAINTY

In addition to the points discussed above, the Working Party also wishes to highlight some provisions in the Proposed Regulation that would benefit from clarification. Such clarifications are considered necessary to improve the legal certainty of all stakeholders that there will be a uniform understanding and application of the ePrivacy Regulation throughout the EU.

### *CLARIFICATIONS ON THE SCOPE*

40. With regard to the scope of the Proposed Regulation, WP29 suggests the following clarifications:

- a. **The term “end-user” should include all individual users.** Art. 2(14) of the EEC Directive defines “end-user” as a user not providing public communications networks or publicly available electronic communications services. It should be clarified that individuals who contribute to networks – for example to mesh networks with their WiFi-router – are not excluded from the scope of protection of the Proposed Regulation.
- b. **It should be clarified that the territorial scope extends to all end-users in the Union.** Art.3(1)(a) provides that the Proposed Regulation applies to the provision of electronic communications services to end-users “in the Union”, whereas Art. 3(1)(c) provides that it applies to the protection of terminal equipment of end-users “located in the Union” (emphasis added). This differs in the various translations. The German translation does not contain this distinction, while others, such as the French, Spanish and Dutch do. It is clear from recital 9 that the territorial scope is intended to be broad, without regard to whether the services are provided from outside the Union, or whether the processing takes place in the Union. It is therefore suggested to remove the term “located” in Art. 3(1)(c) in order to underline this broad scope.
- c. **The Proposed Regulation only seems to protect confidential communications in transit, not when stored.** The current approach in the Proposed Regulation is to focus on the protection of the transmission of communications. See for instance recital 15, which states 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. The scope of this protection is based on a conceptual framework of communications which is outdated. 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 a mail would mostly involve reflecting this in the database of the provider, rather than actually sending communications between two parties. The argument that this would already be covered by the GDPR is unconvincing: the whole intent of the Proposed Regulation is to protect all

confidential communication, regardless of the technical means of such communication. It is possible that this is a mere drafting error, as the prohibition in Article 5 relates to “storing” and “processing”.

- d. **All public wireless internet hotspots should fall within the scope.** As the use of wireless hotspots is common, it is only logical that there should be no doubt as to whether the confidentiality of communication conveyed via such hotspots is protected. The attempt in the Regulation to clarify this fails, however, as the scope is only extended to networks provided to an “undefined group of end-users” (recital 13). The terms “undefined group of end-users” and “closed group of end-users” need to be defined. In particular, it should be clarified that secure wireless networks (i.e. with a password) also fall within the scope, if this password is provided to a theoretically indefinite group of users whose identity cannot be determined in advance (e.g. customers of a cafe, visitors to an airport). The underlying principle in this context is that, in line with the WP29’s prior opinion on the review of the ePD, *“only services which occur in an official or employment situation solely for work-related or official purposes, or technical communication between non-public bodies or public bodies solely in order to control work or business processes, as well as use of services for exclusively domestic purposes, may be exempted from the ePrivacy instrument.”* (p. 8).
- e. **Data collected in the course of offering digital broadcasting services should be covered by the Proposed Regulation.** Given the sensitive nature of viewing behavior, since it reveals personal interests and characteristics of the viewers, the ePrivacy Regulation should specify (perhaps by way of a recital), that the exclusion of services providing “content transmitted using electronic communications networks” from the definition of “electronic communications service” does not mean that service providers who offer both ECS and content services are outside the scope of the provisions of the ePrivacy Regulation which targets the providers of ECS. This is particularly relevant as the provision of services providing “content transmitted using electronic communications networks” is excluded from the definition of “electronic communications service” under the proposed EECC (Art. 2(4)).
- f. **Communications data generally are personal data.** It is noted in recital 4 that communications data may include personal data. However, most communications data are personal data,<sup>23</sup> and for a large part data of a rather intimate and sensitive nature, so this should be amended to state that these generally are personal data
- g. **Confidential communication includes in-platform messages.** Recital 1 explains that the principle of confidentiality applies to ‘current and future means of communication’. This recital continues with a list of examples of such means, including ‘personal messaging provided through social media’. This is probably intended to include private messages between users of a

---

<sup>23</sup> See for example CJEU 6 November 2003, C-101/01, par. 24 (with regard to a telephone number), CJEU 19 October 2016, C-582/14 (*Breyer*), par. 49 (with regard to dynamic IP-addresses) and CJEU 8 April 2014, C-239/12 and C-594/12 (*Digital Rights Ireland*), par. 26-27 (with regard to the sensitivity of metadata).

social network (e.g. Facebook, or Twitter) or messages posted on a timeline which are accessible to a finite number of persons, but the wording is not clear enough.

h. **How the ePrivacy Regulation applies to machine-to-machine interaction.**

As mentioned in paragraph 9, the Working Party welcomes the expansion of protection to machine-to-machine interaction. However, this is only mentioned in Recital 12 and not in a corresponding Article. This protection is desirable, as such communications often contain information protected under privacy rights. On the other hand, a narrow category of pure machine-to-machine communication should be exempted if they have no impact on either privacy or the confidentiality of communications, such as for example the cases where such communication is performed in execution of a transmission protocol between network elements (e.g. servers, switches,) to inform each other on their status of activity.

One particular context in which the application of the ePrivacy Regulation requires clarification is the area of Intelligent Transport Systems. It is envisaged that vehicles will continuously transmit data containing a unique identifier, via radio. Without the additional protection in the ePrivacy Regulation regarding communications data, this could lead to continuous tracking of the driving habits, itineraries and speed of the drivers. Article 2(1) of the EECS, however, contains a new and expanded definition of communications networks. They include transmission systems that do not have a centralised administration capacity and that allow for the conveyance of signals by radio. Recital 14 of the ePrivacy Regulation specifies that such data are electronic communications data. Based on Article 5 of the Proposed Regulation, any kind of interception, monitoring or storing of these communications data is prohibited, unless one of the exceptions applies. Still, there is an interest in processing this data allowing objects such as self-driving cars and devices to warn each other about their vicinity or other risks. The question then is what exception would apply in this case. Consent from end-users is not a feasible exception because it may become necessary to always be able to process these data. Providers should therefore be able to rely on a specific exception, allowing objects such as self-driving cars and devices to warn each other about their vicinity or other risks.

*CLARIFICATIONS ON THE CONCEPT AND APPLICATION OF CONSENT*

41. Regarding the concept and application of consent in the current Proposed Regulation, the WP29 suggests the following clarifications:

- a. **How the concept of consent is to be applied in the context of legal persons.** Recital 3 notes that the Regulation should ensure that provisions of the GDPR also apply to end-users who are legal persons. This, according to the recital, includes the definition of consent under the GDPR (see also recital 18). As noted in remark 13, the Working Party welcomes the explicit inclusion in the scope of the Regulation of legal persons. The practical application of this principle, however, is not clear. The definition of consent

under the GDPR requires it to be “informed” and the indication of the data subject’s wishes must be “by a statement or by a clear affirmative action” (Art. 4(11) GDPR). It needs to be clarified when a legal person can in fact be considered to be “informed” and when there is such an expression of will by a legal person.

- b. In this context, it is worthwhile to note that the employer can under most circumstances not give consent on behalf of its employees because, where an employer requires consent from an employee, and, given the unequal balance of power, there is a real or potential relevant prejudice that arises from not consenting, such consent is not valid because it is not freely given.<sup>24</sup> With regard to **companies issuing devices or equipment to individuals, the Proposed Regulation does not contain a (suitable) exception** to the interference prohibition. One example is where an employer wants to update a company-issued phone. A second example is where an employer offers employees lease cars, and for administrative purposes lets a third party collect location data via the onboard unit of a car. In both cases, the employer has an interest in interfering with these devices.

This interference cannot be considered necessary for the provision of an information society service (Art. 8(1) (c)) or necessary for web audience measuring (Art. 8(1) (d)). This could be solved by creating a new exception, to include a situation where (i) the employer provides certain equipment in the context of an employment relationship, (ii) the employee is the user of this equipment, and (iii) the interference is strictly necessary for the functioning of the equipment by the employee (which implies the application of the principles of proportionality and subsidiarity with regard to the collection of data). Only if those conditions are fulfilled, should it be possible for the employer to interfere with the end-users device.

- c. **Improving controls to stop automatic call forwarding.** Article 14 provides an important control for end-users to stop automatic call forwarding by a third-party. This protection can be further improved by also requiring the end-user’s consent to initiate the call forwarding in the first place.

#### *CLARIFICATIONS ON LOCATION AND OTHER METADATA*

- 42. The Working Party suggests clarifying the following with regard to location data and other metadata:

- a. The meaning of **“location data generated other than in the context of providing electronic communications services” in recital 17 should be clarified.** It is unclear whether this relates to location data collected through, for example, apps that use the data from the GPS-functionality in smart devices, and/or generate location data based on nearby WiFi-routers, and/or location data collected with on-board navigation assistants and/or other ways

---

<sup>24</sup> See Opinion 15/2011 on the definition of consent (WP 187), Opinion 8/2001 on the processing of personal data in the employment context (WP48) and the new Opinion on Data Processing at Work (adopted simultaneously with this Opinion).

of generating location data. This lack of clarity creates legal uncertainty as to the scope of the obligation. In any case, location data of the terminal device of a natural person is personal data and thus the processing of those data is subject to the obligations from the GDPR.

- b. It should be clarified that **most legitimate processing of location data and other metadata does not require a unique identifier**. Recital 17 mentions heatmaps as an example of commercial usages of electronic communications metadata by providers of electronic communications services. However, to create a basic heatmap, no unique identifiers are necessary, mere statistical counting will suffice. Another example mentioned in the recital, the usage of - and pressure on - infrastructure can also be counted by certain measuring points, for example by creating aggregate statistics on the use of traffic towers to provide an indication of the pressure at a location at a certain point in time, without needing to also know the identity of the persons connected.

Additionally, the recital mentions as an example displaying the traffic movements in certain directions during a certain period of time, where a unique identifier would be necessary to link the positions of individuals at certain time intervals. With this example, the recital seems to legitimise further processing of these data to support “big data” analytics. The only condition under the Proposed Regulation for this type of processing, is the obligation to conduct a Data Protection Impact Assessment, if the processing is *likely to result in a high risk to the rights and freedoms of natural persons*. This condition is insufficient. It also is contrary to the obligation in Art. 6 that this type of processing may only be performed with the consent of users, and only if the data cannot be anonymised, that is, without any unique identifiers. Users often cannot refuse the collection of their geolocation data by the providers of electronic communication services, where such collection is technically necessary to convey the communication to the user or where such processing is necessary to deliver the requested (for example navigation) service. In previous Opinions, the Working Party has concluded that such location data from smart devices are personal data of a sensitive nature, and that the benefits of analysing these data do not prevail over the rights of users to protection of the confidentiality of their communications metadata, nor do they prevail over their general rights to data protection under the GDPR. Therefore, the recital must at the very least specify that providers must comply with the obligations from Art 25 GDPR in case of further processing of the location data or other metadata. This entails at least the following measures must be taken

- (i) the use of temporary pseudonyms;
- (ii) deletion of any reverse look-up table between these pseudonyms and the original identifying data;
- (iii) aggregation to a level where individual users can no longer be identified through their particular itineraries, and;
- (iv) the deletion of outliers with regard to which identification would still be possible (all of these measures need to be applied together).

Finally, the ePrivacy Regulation must oblige parties that are involved in the processing of location and other metadata to make public their methods of

anonymisation and further aggregation, without prejudice to secrecy safeguarded by law. This would enable both the supervisory authorities and the public at large to easily verify whether the chosen method is adequate.

#### *CLARIFICATIONS ON UNSOLICITED COMMUNICATIONS*

43. The Working Party suggests clarifying the following with regard to unsolicited communications:

- a. **The wording of the prohibition on direct marketing without consent.** Art. 16(1) of the Proposed Regulation now notes that electronic communications services “may” be used for the purposes of sending direct marketing (with consent), but does not contain an explicit prohibition on sending (directing or presenting) direct marketing without consent. This contrasts with the approach in the other provisions, where first a prohibition is formulated, and this is then followed-up with certain specific exceptions. The current wording suggests a more lenient approach (which presumably is not intended). The Working Party suggests a slightly amended wording of the current Art 13(1) of the ePrivacy Directive: “The use by natural or legal persons of electronic communications services, including voice-to-voice calls, automated calling and communication systems, including semi-automated systems that connect the called person to an individual, faxes, electronic mail or other use of electronic communication services for the purposes of presenting direct marketing communications to end-users may be allowed only in respect of end-users who have given their prior consent.”
- b. **The scope of the provisions on marketing communications and calls to existing contacts.** Article 16(2) provides that where a person obtains electronic mail contact details from an existing customer, it may use those details for further direct marketing of its own products and services if a clear, free and easy opportunity to object is given at the time of collection and in each message. This is currently limited to commercial contacts obtained “in the context of the sale of a product or service” and for further commercial marketing of its own similar products or services. Given that the direct marketing provisions apply equally to non-commercial promotional activities (e.g. of charities or political parties), this provision should be amended to apply equally to non-commercial organisations to contact previous supporters when promoting their own similar aims or ideals, and the same right to object should apply to direct marketing calls. Additionally, a time limit should be set to the validity of 'existing customer contacts' in electronic communications for a commercial, charitable or political purpose, and this time limit should also apply to direct marketing calls. Where Member States have chosen for a system of objection against voice to voice marketing calls, the presence of an 'existing customer contact' relation overrides registration in a Do Not Call register. In those circumstances, end-users have no effective possibility to prevent nuisance calls from companies or organisations they have once had contact with, but no longer wish to engage with. Therefore, as a rule of thumb, the Regulation should specify a validity of this 'existing customer'

exception, for example one or two years, in relation to the legitimate expectations of the concerned end-users.

- c. **The application of the direct marketing rules to legal persons.** Art. 16(5) of the Proposed Regulation provides that Member States shall ensure the legitimate interest of end-users that are legal persons with regard to unsolicited communications are sufficiently protected. Art. 13(5) of the current ePrivacy Directive describes the legitimate interests of subscribers other than natural persons. It is unclear what the implications of this change in wording are. It should be clarified in the recitals that this change does not reflect the intention to provide a lower level of protection. In relation to this, the prohibition on direct marketing without consent relates to “end-users who are natural persons that have given their consent” (emphasis added). It should be clarified that this includes natural persons *working for* legal persons. On the other hand, consent would not be required to approach legal persons through generic contact details they have made public for this purpose (such as 'info@companyname.eu').
- d. **The application of the direct marketing rules to those acting in a (political) representative capacity:** Article 16 as drafted may prevent some communications sent to elected representatives outlining commercial concerns or interests. It should be clarified that the Regulation does not prevent such communications.

#### *CLARIFICATIONS ON THE APPLICATION OF FUNDAMENTAL RIGHTS INSTRUMENTS*

- 44. **The application of the Charter and the ECHR to national data retention laws** should be further clarified. Recital 26 provides that any measures of Member States to safeguard the public interest, such as lawful interception measures, need to be in accordance with the Charter (in addition to the ECHR). This is desirable, as it is in line with the reasoning in *Tele2/Watson* that any national exceptions to EU law data processing protections are subject to the Charter (and infringements through national laws can thus be brought before the EU Court of Justice). Art. 11 of the Proposed Regulation, however, merely notes that restrictions of the scope of Art. 5-8 of the Proposed Regulation must respect the essence of fundamental rights and freedoms and be a necessary and proportionate measure. An explicit reference to the Charter and the ECHR should also be included here.
- 45. **That the confidentiality of communications is also protected under Art. 8 ECHR.** In paragraph 1.1 of the Memorandum and in recital 1, it is explained that the Proposed Regulation implements Art. 7 of the Charter. This is repeated in recital 19. The fundamental right to confidential communications is, however, not only protected in this provision, but also under Art. 8 ECHR. Inclusion of an explicit reference in an Article of the Proposed Regulation would further confirm that any relevant jurisprudence of the European Court of Human Rights will also have to be taken into account when assessing the (final) regulation. This reference is, by the way, already included in recital 20 (relating to terminal equipment) and 26 (relating to lawful interception) and further supported by the considerations in par. 2.1 of the



Memorandum (on the relationship between the Charter and the ECHR in the context of legal persons), but not in any of the relevant Articles, such as Article 11(1).

#### OTHER CLARIFICATIONS

46. It should be clarified that **the obligations under the GDPR, such as with regard to the data breach regime and DPIA's, remain applicable**, when parties process personal data in the context of electronic communications data. As it is mentioned in recital 5 that the Proposed Regulation is *lex specialis* to the GDPR and that processing of electronic communications data should only be permitted in accordance with the Proposed Regulation, it could be questioned whether certain obligations under the GDPR also apply in the context of the Proposed Regulation. This is especially the case where the Proposed Regulation could be interpreted to arrange for a certain obligation, while the GDPR also covers this. Indicative examples include:

- (i) the Proposed Regulation obliges a certain notification of “detected” security risks (Art. 17) (see also remark 35) but the GDPR contains a data breach notification regime (Art. 33 and 34);
- (ii) The Proposed Regulation mentions that the performance of a DPIA and consultation with the supervisory authority in line with the GDPR is obligatory under certain circumstances (recitals 17 and 19 and Art. 6(3)(b)), while the GDPR already lays down when a DPIA has to be performed and when consultation is required (Art. 35 and 36) and;
- (iii) It is not spelled out that if one complies with the necessary conditions of an exception to the processing prohibition under Art. 5 of the Proposed Regulation, one still has to comply with all relevant obligations under the GDPR where it concerns the processing of personal data and any other processing under the GDPR is prohibited. It should be clarified that the compatibility test laid down in Art. 6(4) GDPR therefore does not apply.
- (iv) The proposed ePrivacy Regulation does not provide for certification mechanisms similar to articles 42 and 43 of the GDPR. As the scope of article 42 GDPR is, strictly speaking, limited to the establishment of data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance with the GDPR, it should be considered whether a comparable provision should not be introduced to allow the certification of processing operations, standards, products or services for their compliance with the ePrivacy regulation.

In order to ensure that this lack of clarity is not used as an argument to lower the level of protection under the Proposed Regulation, it should be made clear that in all these cases, controllers also need to comply with the GDPR.

47. Furthermore, it should be clarified that **the requirement for consent withdrawal also applies in the context of interference with terminal equipment**. Art. 8(1) (b) of the Proposed Regulation provides for the possibility to interfere with the end-users’ terminal equipment with consent. Art. 9(3) requires that end-users are given the possibility to withdraw their consent at any time, but this only applies to consent for the analysis of metadata and content. It should be clarified that this obligation extends to the interference with terminal equipment.

48. Related to this, it should be clarified that **the reminder of the possibility to withdraw consent also applies to consent through browser settings**. Art. 9(3) requires that end-users are at periodic intervals of 6 months reminded of the possibility to withdraw their consent at any time. While the Working Party believes that general settings of browsers and other software, including operating systems, apps and software interfaces for Internet of Things-connected devices (i.e. not on the basis of specific granular controls) cannot be a valid measure for providing consent, as general settings are not appropriate to give specific consent to specific scenarios (see remark 24), default settings should be user-friendly (see remark 19). *If* this remains in the Proposed Regulation, settings must be granular enough to control all data processing the user is consenting to and cover every functionality of the equipment that might lead to data processing. Additionally, the end-user should at least at periodic intervals (of 6 months) be reminded of the possibility to change these settings.
49. It is welcome that the Proposed Regulation requires software already placed on the market to inform the end-user about its privacy settings options (Art. 10). **However, it is unclear how this can be applied effectively to legacy products** and others which are no longer supported. Additionally, further clarification should be provided as to how this obligation will apply to open source software which is developed in an open and decentralised manner.
50. It should be clarified that **the offering of the possibility to block (third party) cookies under Art. 10 of the Proposed Regulation takes precedence over the exception for web audience measuring** under Art. 8(1) (d). Or in other words: even though a website may employ analytics for web audience measuring under Art. 8(1) (d), users still should have the right to block these tracking technologies in their browser.
51. The **definition of (semi-)automated calling and communications systems should be clarified**. The definition of this term, at Art. 4(3) (h) of the Proposed Regulation contains a reference to the term itself in the second part of the sentence (“including calls made using automated calling and communication systems which connect the called person to an individual”). It is suggested to delete this last sentence from the definition, and change the definition in 4(3) (g) to include calls made with the help of semi-automated communication systems, such as for example automatic dialers, which connect the called person to an individual.
52. The **information that is “part of the subscription to a service” should be clarified**. In recital 14, it is mentioned that electronic communications metadata “may include information that is part of the subscription to the service when such information is processed for the purposes of transmitting, distributing or exchanging electronic communications content”. It is unclear what is intended with this wording.
53. **The applicability of the consistency and co-operation mechanisms** should be clarified. In recital 38 it is noted that the Proposed Regulation relies on the consistency mechanism of the GDPR. In addition, Art. 18(1) provides that Chapter VI and VII of the GDPR shall apply *mutatis mutandis*. In Art. 19, it is further noted that

the European Data Protection Board (“EDPB”) shall exercise the tasks laid down in Art. 70 of the GDPR. Although the application of these provisions is relatively clear, it cannot be excluded that questions of interpretation will arise with regard to the key concepts of the consistency and co-operation mechanisms under GDPR. For example, the lead authority mechanism applies in those cases where there is “cross-border processing” (Art. 56(1) GDPR): it is uncertain how this applies in the case of the interference of terminal equipment or analysis of content or metadata under the Proposed Regulation. It is therefore advisable to clarify the application of these key concepts in a recital and underline that any remaining questions concerning the applicability of these chapters of the GDPR in the context of the Proposed Regulation will be resolved by interpreting the provisions of these chapters in line with their intention. In addition, it is advisable to clarify that Art. 70 applies *mutatis mutandis* to the EPDB in the context of the Proposed Regulation (this is now missing from the recital).

\* \* \*