DAGITAL LEGAL
Privacy & Technology Law Firm

Dagital Legal, s.r.o.
Law Firm
Nové Záhrady I/9
821 05 Bratislava
www.dagital.eu

+421 911 195 133
jakub.berthoty@dagital.eu

Comments to Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

To: European Data Protection Board
From: Dagital Legal, s.r.o., privacy & technology law firm
Date: 17th January 2024

1 Introduction

We very much welcome EDPB's Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive (the "**Guidelines**"). In fact, we believe that the interpretation of Article 5 (3) of ePrivacy Directive and its interplay with the GDPR is one of the most important topics to be dealt with by the EDPB. We would like to take this opportunity to comment on the Guidelines and address certain key points that in our view require revisiting. In Section 2 below, we summarize all our comments in an executive summary. All comments are in detail explained in Section 3 below.

2 Executive summary

The scope of Guidelines is not technical as is suggested. Guidelines dive deep into the legal regulation and overall applicability of Article 5 (3). While we agree with the list of use cases (which is most appreciated point of Guidelines), we do not agree with overall interpretation of key elements of Article 5 (3). We believe there is too much emphasis on telecommunication regulation in EDPB's interpretation of Article 5 (3). This unnecessarily complicates but also undermines the scope Article 5 (3).

Guidelines fail to confirm that Article 5 (3) has its own special applicability that is completely distinct to the general applicability of Article 1 the ePrivacy Directive (similarly as the unsolicited communications). Criterion C is not relevant to Article 5 (3) and needs to be removed from the Guidelines. Some further "TelCo" references in other criterions need to be polished in our view.

An important pre-requisite of Article 5 (3)'s application is missing in the Guidelines being the necessary interference with privacy on terminal device. This seemingly obvious requirement is far more important than might be assumed.

Lastly, we recommend universal and general guidelines on Article 5 (3) and its interplay with GDPR that the whole privacy & technology community has been waiting for since 2016.

3 Legal analysis

3.1 Scope of the Guidelines

We understand the Guidelines should only cover the technical scope of Article 5 (3) by listing some techniques of data collection concerning end devices. The Guidelines confirm this in the first paragraph on page 4: *"There is currently no comprehensive list of the technical operations*

covered by Article 5(3) ePD." If the aim is to comprehensively list technical operations covered by Article 5 (3), then there is no reason why Guidelines should not also mention some other commonly used techniques, such as SDK (especially in mobile applications), beacons or generally techniques that capture signals from a device. Some of these can be easily integrated into existing use cases – for example under IoT or Local processing – as these may be interlinked. However, just mentioning these techniques would help the practice a lot.

In relation to mobile applications and their operating systems, it would make sense to also mention that these tracking techniques might be subject to further conditions[1] under the respective operating systems' developer terms.

Although it is suggested that Guidelines concern only technical scope of Article 5 (3), in fact Guidelines discuss in detail key criteria for Article 5 (3) to apply. This is not technical scope but rather general applicability and general scope Article 5 (3). If the Guidelines discuss the general scope and legal theory around various definitions and terms used in first sentence of Article 5 (3) then we would recommend changing the title of Guidelines and covering all possible aspects of Article 5 (3), including the exemption of consents, application to legal persons, interplay with GDPR (Planet 49), information obligations (including under Article 13 and 14 GDPR) and relationship with the fundamental right to privacy.

In fact, we do not understand why such general guidelines are still missing at the EU level since April 2016, when the GDPR was adopted and the EDPB was established. There is nothing more pressing and important for privacy professionals, businesses, and supervisory authorities than the interplay between Article 5 (3) and the GDPR. This interplay is triggered by almost every data processing platform or technology including the whole advertising and privacy monetization industry affecting every European with smartphone and connection to internet.

3.2 Reference to "communication relay" and "conveyance of information"

In paragraph 15 on page 6 of the Guidelines, the EDPB notes:

"Whenever a device is not an endpoint of a communication and only conveys information without performing any modifications to that information, it would not be considered as the terminal equipment in that context. Hence, if a device solely acts as a communication relay, it should not be considered a terminal equipment under Article 5(3) ePD."

We would recommend removing this paragraph. Not because it would be incorrect to state that network equipment that serves as communication relay does not present a terminal equipment. Firstly, we do not see practical use or benefit of this paragraph. Who is asking this question in relation to Article 5(3): *"Is a telecommunication tower a terminal device?"*

Secondly, this paragraph introduces a new exemption to the regulation. It confirms the existence of some type of excluded[2] device that: (i) does not perform any modification to the collected information; and (ii) merely conveys the information elsewhere.

The problem is that many spying or tracking devices would meet these criteria. What this exemption wrongfully implies is the following: *"Provided that you do not modify collected information, you can convey it somewhere else without triggering Article 5 (3)."* That is obviously not true and undermines the protection provided for by Article 5(3). It is irrelevant, whether the information is merely conveyed or if it is modified for Article 5(3) to apply.

3.3 Reference to the "communication"

In paragraph 19 on page 7 of the Guidelines, the EDPB notes:

[1] Without the need to elaborate on such contractual conditions.
[2] Excluded from scrutiny of Article 5(3).

*"The protection is guaranteed by the ePD to the **terminal equipment associated to the user or subscriber involved in the communication**, and it is not dependant on whether the electronic communication was initiated by the user or even on whether the user is aware of the **said communication**."*

We would recommend removing this paragraph. We do not understand what communication is meant here (and between whom). Simply because there does not need to be any communication at all for Article 5(3) to apply. For example, what communication is there when a website places a tracking cookie into a smartphone's memory and how is that communication relevant to the interference with user's privacy? Whether there is a communication between the user/subscriber and someone else is irrelevant for Article 5 (3) to apply.

3.4 Reference to the "electronic communications network" (Criterion C)

In Section 2.4 of the Guidelines, the EDPB explains one of four key elements for Article 5 (3) to apply. In paragraph 20 on page 7 of the Guidelines, the EDPB notes:

*"Another element to consider **in order to assess the applicability of Article 5(3) ePD is the notion of 'electronic communications network'**. In fact, the **situation regulated by the ePD is the one related to 'the provision of publicly available electronic communications services in public communications networks** in the Community'. It is therefore crucial to delimit the electronic communications network context in which Article 5(3) ePD applies."*

This is not true, and Criterion C is simply not relevant for Article 5 (3) to apply. We recommend that Criterion C is removed completely. In fact, the "electronic communications network" it is not even mentioned in the first sentence of Article 5 (3):

*"Member States shall ensure that the **storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user** is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing."*

The reference to "electronic communications network" was removed from the above sentence together with the opt-out regime in 2009 when the first sentence of Article 5 (3) read as follows:

*"Member States shall ensure that the **use of electronic communications networks** to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller."*

It is no longer relevant if the access is made by use of electronic communications networks or otherwise. Article 5 (3) simply protects the privacy of terminal equipment and only refers to: (i) storing of information on terminal device; or (ii) gaining access to information already stored on terminal device.

It is true that definition of the terminal device in Directive 2008/63/EC refers to the notion of public telecommunications network (and not electronic communication network). However, this definition only explains what is a terminal equipment. And it does so for the purposes of competition law. Thanks to this definition we know that Article 5 (3) protects privacy on smartphones, computers, laptops, tablets and similar devices that can be connected to the network in order to communicate. In other words, objects / devices that we need to focus on. But nothing more. It cannot be agreed that key criterion of Article 5 (3) to apply is "*the provision of publicly available electronic communications services in public communications networks*".

For example, who provides *publicly available electronic communications services in public communications networks* in the following use cases in Guidelines:

- URL and pixel tracking;
- Local processing;
- Tracking based on IP only;
- Intermittent and mediated Internet of Things (IoT) reporting;
- Unique Identifier?

The correct answer is: (i) no one; (ii) someone completely different to the person interfering with user's privacy; (iii) someone who has absolutely nothing to do with the above technical operations; or (iv) someone to whom Article 5 (3) does not apply at all in the given use case.

Where the reference to electronic communications network in Guidelines is particularly underming application of Article 5 (3) is paragraph 25 on page 8 of the Guidelines:

*"The **public availability** of the communication service over the communication network is necessary for the applicability of Article 5(3) ePD. It should be noted that the fact that the network is made available to a limited subset of the public (for example, subscribers, whether paying or not, subject to eligibility conditions) **does not make such a network private**."*

Whether or not network is private, or public might be relevant for the Code's applicability. However, the reference to a private network in which Article 5 (3) does not apply is particularly dangerous here and we do not understand what is meant by this paragraph. Is it suggested that when terminal device connects to private company intranet, Article 5 (3) does not apply?

Therefore, the context of "electronic communications network" and "electronic communication service" is simply not relevant for Article 5 (3) to apply and definitely isn't its key criterion. We would understand more if the reference here was made to the "information society service" in the context of the second sentence of Article 5 (3) but even that would be not relevant in all cases. The first sentence of Article 5 (3) simply does not need any service or network to apply, it just needs "entering" terminal equipment in a way that interferes with users or subscriber's privacy.

3.5 Insufficient reference to interference with privacy

Article 5 (3) cannot be triggered without some form of interference with the fundamental human right it serves to protect. The respect for private and family life and communication (in the context of the terminal device) can only by interfered by 3rd parties and not by user himself. Guidelines indirectly confirm this on several occasions, but do not regard this a key criterion. Yet, if this basic prerequisite of Article 5 (3)'s application is not met, many practical use cases that should not fall under Article 5 (3) will.

For example, a vehicle dashcam locally stores a video recording on a driver's smartphone's memory without anyone else having access to such recording. Information has been clearly stored on user's terminal device. The reason why Article 5 (3) does not apply to such use case is that there is no interference with privacy as the storing has been done by the user himself. The driver (the protected person) is accessing his own private sphere, and no 3rd party is interfering with his privacy.

Another example could be a simple taking of a picture on a smartphone. Again, the file with the photo is stored on smartphone's memory would grammatically trigger Article 5 (3). But the Article 5 (3) does not apply, because such action is done by user himself and therefore, there is no interference with his privacy by 3rd party. In other words, entering the perimeter of terminal device is in many ways the same as entering someone's house.

Different situation would be, if the user instructs a 3rd party to interfere with his privacy on terminal device. For example, the user would back-up his photo stored locally on his smartphone on a 3rd party cloud storage. By doing so, 3rd party would technically access information on the terminal device within the meaning of Article 5 (3). Article 5 (3) would be triggered and such interference could be legitimate in the same way as "necessary cookies" provided that further conditions are met (such as to inform user).

3.6 Unexplained reference to protection of legal persons

It is true that Article 5 (3) protects legal persons too. Guidelines confirm this in paragraphs 17 and 28 but not explain. According to Article 1 (2), provisions of ePrivacy Directive: *"provide for protection of the legitimate interests of* ***subscribers who are legal persons****."* Article 5 (3) refers to "*subscriber or user concerned"* who gives his or her consent.

The term "subscriber" is not defined in ePrivacy Directive nor in the Code, despite being regularly used therein. In the context of electronic communication services, it generally refers to anyone who has subscribed to such service. This reference makes little sense for the purposes of Article 5 (3). The term "user" is defined in Article 2 of ePrivacy Directive and only encompasses a natural person (i.e. individual). Therefore, to sum up, for the purposes of Article 5 (3):

- legal person can only be a subscriber which is not a defined term;
- such legal person is a different person to individual user using the terminal device;
- such legal person can allow interference only with its own privacy on terminal device (but not with user's privacy on the same terminal device).

Practically, this situation can occur when legal person subscriber owns terminal device used by individual user. It goes beyond the legal regulation to analyse what the relationship between such legal person and individual might be. However, nature of such relationship determines the expectation of individual's privacy on such terminal device alongside the legal person's expectation of privacy. For example, it can be completely prohibited by employer to use such device for private purposes. On the other hand, private use of device might be the sole purpose using a rented device. Also, one device can be legitimately or illegitimately used by multiple users. An adult user might unlock the device that can be controlled by a child user. Unlocked device can be stolen and used illegally by a different user in complete technical control over the device. This complexity and unpredictability only confirm it is impossible for 3rd party providers to determine and analyse such relationships or even realise such situations might exist.

A simple solution to this exact problem was suggested by one of the proposals for ePrivacy regulation:

"*As far as the controller is not able to identify a data subject, the technical protocol showing that consent was given from the terminal equipment shall be sufficient to demonstrate the consent of the end-user according Article 8 (1) (b).*"

We believe this is the only possible approach that solves the above problem. We should be able to assume – to some reasonable degree – that whoever controls the terminal device is authorised to allow interference with both user's and subscriber's privacy. If we cannot assume this, every cookie stored on company-owned computer or smartphone with user's permission is insufficient, because the company did not consent.

We remain at your disposal should you wish to discuss the above.

Yours sincerely,
Dagital Legal, s.r.o.
Jakub Berthoty

Annex No. 1
Definitons

The following terms or references used in this memorandum have the following meaning:

“**Article 5 (3)**” means Article 5 (3) of the ePrivacy Directive, as amended;

“**Code**” means Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), Text with EEA relevance;

“**EDPB**” means European Data Protection Board;

“**Directive 2008/63/EC**” means Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version);

“**ePrivacy Directive**” and “**ePD**” means 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);

“**ePrivacy regulation**” means Proposal for a regulation of the European parliament and 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);

“**Framework Directive**” means Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive);

“**Guidelines**” means EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive Adopted on 14 November 2023;

“**GDPR**” means means 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);

“**Planet 49**” means Judgement of the Court of Justice of 1 October 2019, Planet 49, Case C-673/17, ECLI:EU:C:2019:801;

“**SDK**” means Software development kit;

“**WP29**” means “article 29 working party” what is EU Commission's advisory body on data protection established under Article 29 of Directive 95/46/EC.