Piltz Legal

Position Paper

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

Date: 17 January 2024

Piltz Rechtsanwälte
PartGmbB
Südwestkorso 3
12161 Berlin

Telefon: +49 30 814 53 50 00
Telefax: +49 30 814 53 50 09
E-Mail: info@piltz.legal
Web: www.piltz.legal

Partner:
Dr. Carlo Piltz,
Prof. Dr. Burghard Piltz
AG Charlottenburg,
PR-Nr.: 1593 B

Bankverbindung:
UniCredit Bank AG (HypoVereinsbank)
IBAN DE59 1002 0890 0034 3795 80
BIC HYVEDEMM488
Steuernummer: 1120/472/01963

Piltz Legal

Table of content

Piltz Legal

A. Brief overview of the current view of the EDPB (paragraph 3.1. URL tracking)

The EDPB guidelines 2/2023 on Technical Scope of Art. 5 (3) of ePrivacy Directive (in the following "ePD") address the scope of application of this provision. To eliminate ambiguities and prevent new technologies from circumventing the ePD's protective purpose, the EDPB considers it necessary to clearly define the scope of application in light of new technical developments in tracking. Therefore, the EDPB assumes a broad scope of application of Art. 5 (3) epD and, in particular, defines the legal elements so broadly that they can no longer be reconciled with the wording and the objectives pursued by the provision. The terms "*gaining access*" and "*storage of information*" are used inconsistently, leading to a result with regard to URL tracking that does not comply with the legal requirements of the ePD. This poses a risk for the e-commerce sector and new digital business models that should not be underestimated, as the growing regulatory burden resulting from an unlimited scope of application of Art. 5 (3) ePD will have an inhibiting effect on innovative business models. Finally, the broad interpretation of Art. 5 (3) ePD also runs counter to the interests of users, as less invasive tracking methods are now also included in the scope of Art. 5 (3) ePD and website or App operators consequently no longer have any incentive to use alternatives to cookie tracking.

B. Legal aspects of the terms of Art. 5 (3) ePD

According to Art. 5 (3) ePD the storage of or gaining access to information in the terminal equipment of a user is only allowed if the user consents unless the storage or access serves only for carrying out or facilitating the transmission of a communication over an electronic communications network or is strictly necessary to provide an information society service explicitly requested by the user. The regulation is technology-neutral and applies regardless of the method used to access the terminal equipment, so that, for example, not only cookies are covered by the regulation.[1]

C. Our legal assessment

We assume that the guidelines of the EDPB do not correspond with the legal requirements and the objectives of Art. 5 (3) ePD. The EDPB's view is incompatible with the provision's wording, and it allows the scope of application of Art. 5 (3) ePD to expand beyond its intended limits. This is especially relevant to the view of the EDPB on URL tracking, which in fact, due to its technical design, does not involve storing or accessing

[1] Conference of Independent Federal and State Data Protection Supervisory Authorities: Guidance from the supervisory authorities for telemedia providers (OH Telemedien 2021) Version 1.1. from December 2022, p. 8 margin no 18, which is accessible under: https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf.

information on the user's terminal equipment. As a result, and contrary to the view expressed by the EDPB, URL tracking does not fall within the scope of Art. 5 (3) ePD.

D. Legal arguments

I. Gaining access

The wording of Art. 5 (3) ePD clearly states that the provision only applies if, among other things, information is accessed on the user's terminal device.[2] The EDPB's guidelines already deviate from the legal requirements at this point. In the opinion of the EDPB, Art. 5 (3) ePD should already apply "*whenever the accessing entity wishes to gain access to information stored in the terminal equipment and actively takes steps towards that end*".[3] This interpretation is contra legem and contradicts the clear wording of the provision which clearly refers to the activity of "accessing" or "storing" the information. Mere preparatory acts like "wishing" to gaining access, however, are not covered. The purpose of Art. 5 (3) ePD is to protect the private sphere of users of electronic communication networks, which includes their terminal equipment and any information stored on it, as stated in Recital 24 ePD. However, this protective purpose and objective is not yet affected if the accessing entity merely has intentions, e.g. if a company plans to use cookies. Based on the view of the EDPB, already during the planning phase of an App or a website, the entity would probably have to obtain consent, although no accessing of information or storing of information took place. On top of that the EDPB does not clearly describe what is meant by "*actively takes steps*". In practice, such an approach bears a high legal risk and legal uncertainty, as it is now hardly possible to determine with certainty when access to information in the terminal equipment has taken place and Art. 5 (3) ePD actually applies.

An interpretation based on the wording and the objectives of the provision is also supported by the fact that Recital 24 mentions spyware and web bugs, hidden identifiers and other similar devices that access the user's terminal device without the user's knowledge as examples of interference in the scope of protection of Art. 5 (3) ePD. In this respect, it is clear that preparatory acts are not covered but Art. 5 (3) ePD addresses the activity of accessing or storing.

---

[2] European Data Protection Board, Guidelines 2/2023 on Technical Scope of Art. 5 (3) of ePrivacy Directive, adopted on 14 November 2023, p. 8 margin no 31, which is accessible under: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en.

[3] European Data Protection Board, Guidelines 2/2023 on Technical Scope of Art. 5 (3) of ePrivacy Directive, adopted on 14 November 2023, p. 8 margin no 31.

According to the ECJ's settled case-law, in interpreting a provision of EU law, it is necessary to consider not only its wording, by reference to its usual meaning in everyday language, but also the context in which it occurs and the objectives pursued by the rules of which it is part.[4]

The history of the legislative process is a further argument for the fact that the objectives pursued by the ePD refer to an "intrusion" into the terminal equipment – which clearly refers to the activity as such.

The LIBE Committee in Parliament proposed for the first time that that Member States shall prohibit the use of electronic networks to store information or to gain access to information stored in the terminal equipment of a user without prior consent.[5] The committee justified this amendment by stating that intrusion into the terminal equipment to gain access to information or to store hidden information or to trace the user's activities constitutes a serious violation of the private sphere.[6] Therefore, the private sphere should be protected from the outside. The opposite direction and thus the sending of information from the terminal device, however, should not fall within the scope of the provision, as the wording explicitly mentions "*intrusion into the terminal device*".

The amendments of the Council of the European Union also support such an interpretation. In particular, secret access, for example by spyware, should be prohibited, while the use of cookies should be permitted under certain conditions.[7]

II. Sending of specific instructions to the terminal equipment

The EDPB also holds the view that the proactively sending of specific instructions to the user's terminal equipment in order to receive back targeted information is also covered by Art. 5 (3) eDP. It appears to fall under the term "gaining of access" (margin no 31), however, it remains unclear what exactly can be considered as "sending of specific instructions" since in margin no 35 it is described as storing information.

---

[4] ECJ, judgement of May 4, 2023, Case C-487/21, ECLI:EU:C:2023:369 margin no 19.

[5] See Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, which is accessible under: https://www.europarl.europa.eu/doceo/document/A-5-2001-0374_EN.html.

[6] See Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, which is accessible under: https://www.europarl.europa.eu/doceo/document/A-5-2001-0374_EN.html.

[7] See Council of the European Union, Interinstitutional File: 2000/0189 (COD), Report from Coreper on 28th November 2001 regarding the Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, p. 5, which is accessible under: https://data.consilium.europa.eu/doc/document/ST-14629-2001-INIT/en/pdf.

The use of the term "*sending of specific instructions*" is therefore more diffuse than clear and leads to legal uncertainty. The EDPB should explicitly only refer to the two alternative actvities mentioned in Art. 5 (3) ePD – accessing or storing of information. If the EDPB wishes to also cover the "*sending of specific instructions*" it must be made clear 1) why this sending of instructions shoud be covered by Art. 5 (3) ePD, 2) what these "*instructions*" mean and 3) under what alternative of the two requirements in Art. 5 (3) ePD this activity falls.

Consequently, the EDPB should clarify this term and provide examples to illustrate its meaning. However, it should be noted that the "*sending of specific instructions to the user's terminal equipment*" is not used in Art. 5 (3) eDP and therefore cannot be a point of reference for its scope of application.

III. The receiving entity

The fact that the EDPB already includes the recipient of information under the scope of Art. 5 (3) ePD is also problematic, even if the recipient has not accessed the user's terminal device at all. The EDPB extends the legal obligations under Art. 5 (3) ePD to an entity which does not fulfill the requirements set up in Art. 5 (3) ePD.

This interpretation also contradicts the protective purpose and the objectives of the provision. After all, it is primarily the integrity of the terminal equipment and the information it contains that is protected. Accordingly, a recipient who has not accessed this terminal equipment cannot fall within the scope of the provision, as it does not fulfill the requirements of Art. 5 (3) ePD at all – if an entity does not access or store information an a user's terminal equipment, the application of Art. 5 (3) ePD to this entity is clearly out of scope of this provision.

If following the EDPB's view, a company that receives data from a user's terminal equipment at the user's request could, for example, be obliged to obtain consent in accordance with Art. 5 (3) ePD. In practice, this would lead to unacceptable conditions, as it is simply impossible for the receiving company to obtain consent from the user in advance that meets the requirements of Art. 7 GDPR if they have no way of knowing which users might send information to them at what time and why – the view of the EDPB would lead to extending legal obligations to entites which will factually not be able to fulfill these obligations.

IV. URL tracking

1. Storage on the terminal equipment

a) View of the EDPB

According to the EDPB, the use of tracking links constitutes a storage on the communication network of the user's terminal equipment, at least through the caching mechanism of the client-side software. As a result, Art. 5 (3) ePD shall be applicable for URL tracking.

b) Our legal opinion

This view is not acceptable. URL tracking does not technically differ from using a regular URL. When a user enters a regular URL in their browser, by default, various requests are made to the browser as part of providing the desired website. Once the user enters a URL into the browser, the browser must locate the server of the requested domain. This is achieved through a DNS lookup. The browser caches the DNS information for a brief period to verify if the IP is already in the cache.

In the opinion of the German data protection authorities, only web storage objects, such as the use of cookies or browser fingerprinting, constitute the storage of information that leads to the reading of information on the end devices.[8] However, the intermediate storage of URL information as part of the cache for loading the website cannot fall under this term, as the protective purpose of Art. 5 (3) ePD is not affected at all. This is because this storage is technically necessary in order to load the website. The same applies to the sub-tag of the URL (identifier). This URL sub-tag does not store information on the terminal equipment to read other data from it. Instead, it functions as an identifier. For instance, an online platform may use it to direct the user to different web shops. The identifier allows a web shop to determine if the user was referred from a specific online platform, which is a common e-commerce business model for remunerating the platform. This process does not involve extracting any information from the user's device.

2. Gaining access to information stored in the terminal equipment

[8] Conference of Independent Federal and State Data Protection Supervisory Authorities: Guidance from the supervisory authorities for telemedia providers (OH Telemedien 2021) Version 1.1. from December 2022, p. 8 margin no 19 et seq.

a) **View of the EDPB**

The EDPB describes URL tracking as follows[9]: When the user clicks on the URL the targeted website loads the requested resource and collects an identifier. This identifier is initially stored in the user's terminal equipment and retrieved again later.[10] This procedure is commonly used by websites to identify the origin of their inbound source of traffic. The inclusion of the tracking link in the content sent to the user should be considered as an instruction to the terminal equipment to return the identifier.[11] Consequently, the collection of the identifier provided by the tracking URL constitutes a "*gaining of access*" within the meaning of Art. 5 (3) ePD.

b) **Our legal opinion**

However, this view of the EDPB is not in line with the intention of the legislator and does not accurately represent the technical circumstances of URL tracking.

aa) **Description of URL tracking**

The purpose of URL tracking can be described as follows: The owner of the requested URL (e.g. owner of a web shop) merely receives the information that a user (who may not be identifiable at all) was redirected to the target URL via a specific website (e.g. online platform) so that the web shop owner can remunerate the online platform for the traffic generated. From a technical perspective the URL (universal resource locator) consists of several parts (inter alia the scheme with the used protocol, the domain name as well as the specific path to specify the resource that a user wants to load). The identifier also becomes a part of the URL and is visible there. It can be regarded as a hint for the owner of the targeted website from which original website the user was sent. As a result, neither a storage nor an access to the user's terminal equipment takes place. Regarding the functioning of a URL, the web server does not initiate the storage of information on the user's end device, nor does it instruct the end device to send information back. Instead, the information contained in the URL is sent automatically, e.g. when the user clicks on a link.

[9] European Data Protection Board, Guidelines 2/2023 on Technical Scope of Art. 5 (3) of ePrivacy Directive, adopted on 14 November 2023, p. 11 margin no 48 et seq.
[10] European Data Protection Board, Guidelines 2/2023 on Technical Scope of Art. 5 (3) of ePrivacy Directive, adopted on 14 November 2023, p. 11 margin no 48 et seq.
[11] European Data Protection Board, Guidelines 2/2023 on Technical Scope of Art. 5 (3) of ePrivacy Directive, adopted on 14 November 2023, p. 11 margin no 51.

Following the EDPB's view and its technical representations that the identifier in the URL falls under the scope of Art. 5 (3) ePD, this would have the consequence that in principle almost any information of a URL could be considered as an "identifier" and clicking a URL would fall within the scope of the provision. As a result, consent would have to be obtained before each click on a URL in accordance with Art. 5 (3) ePD. This contradicts the protective purpose of this provision and the practical question will arise, how this can be implemented by obliged entities.

bb) **URL tracking does not fall under Art. 5 (3) ePD**

In fact, the URL tracking approach does not affect the user's private sphere. This also corresponds to the ECJ case law cited by the EDPB[12], which is based on the protective purpose of Art. 5 (3) ePD (see also Recital 24 ePD) and thus on the fact that the user needs to be protected against hidden identifiers being stored on his terminal device without his knowledge in order to gain access to information from the terminal device and thus from his private sphere.

The EDPB's understanding of the private sphere, in particular of the term "information" within the meaning of Art. 5 (3) ePD, is not correct. Recital 24 ePD states that the "terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms" and consequently are also protected by Art. 7 of the EU Charter of Fundamental Rights. According to this provision, every person has the right to respect for their private and family life, their home and their communications. The concept of private life covers all activities and aspects of the private sphere, including the intimate sphere, in which the protection of privacy can reasonably be expected due to the circumstances. Furthermore, activities and aspects of the social sphere are covered that have a particular personal reference, whether in general or for the person concerned.[13] However, the procedure of URL tracking in fact does not constitute access to information in the terminal equipment and does not involve information or data with regard to the private sphere or with any personal reference. Consequently, there is no interference in Art. 5 (3) ePD. Even assuming that the identifier would access the end device, this access would not affect any private information. The protective purpose would not be affected, which would therefore not open up the scope of application of Art. 5 (3) eDP, even assuming the opinion of the EDPB.

---

[12] ECJ, judgement of October 1, 2019, Case C-673/17, ECLI:EU:C:2019:801, margin no 70; European Data Protection Board, Guidelines 2/2023 on Technical Scope of Art. 5 (3) of ePrivacy Directive, adopted on 14 November 2023, p. 5 margin no 10.

[13] *Jarass*, in: Jarass, EU Charter of Fundamental Rights, 4. Ed. 2021, Art. 7 CFR margin no 13.

In the opinion of the German supervisory authorities, access to information in the end device requires a targeted transmission of browser information that is not initiated by the end user, which is why a URL that is inevitably transmitted when a telemedia service is called up cannot be regarded as access to information that is already stored in the end device.[14] In contrast, the active reading of attributes of a terminal device for the subsequent creation of a fingerprint should constitute access to information on users' terminal equipment.

Furthermore, it must be taken into account that an URL does not jeopardize the integrity of the user's terminal equipment and does not affect the user's private sphere. The aim of the URL tracking is also not to collect information about the user, but rather regarding traffic that an online platform for example has forwarded to a web shop. Moreover, the URL is not saved at the instruction of the online platform or the web shop, but is triggered solely by the user's click on the website link. In addition, tracking parameters in the URL are also visible to the user, as these parameters are appended to the target URL. In this respect, this does not constitute a secret process, which also speaks against an interference on the scope of protection of Art. 5 (3) ePD.

V. Application of guidelines to supervisory authorities not being part of the EDPB

Due to the legal nature of the ePD requiring a national implementation act, Member States must entitle national authorities with the task of enforcing national ePrivacy rules. The EDPB has stated accordingly that member states have chosen "*different ways of allocating the task of enforcing national ePrivacy rules to one or more entities*".[15] Therefore, national authorities may be responsible for enforcing ePrivacy rules although they are not responsible for enforcing data protection laws and the GDPR. As a corollary, the EDPB Guidelines 2/2023 should not have any binding effect on those authorities that are not data protection authorities and are therefore not represented in the EDPB. This is because, as an umbrella organization, it should only represent national data protection authorities and the EDPS.[16]

---

[14] Conference of Independent Federal and State Data Protection Supervisory Authorities: Guidance from the supervisory authorities for telemedia providers (OH Telemedien 2021) Version 1.1. from December 2022, p. 9 margin no 21.

[15] European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, p. 18 margin no 58, accessible under: https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

[16] See website of the European Data Protection Board, accessible under: https://edpb.europa.eu/about-edpb/who-we-are/edpb-chairmanship_en.

E. Practical considerations

European online platforms and web shops have been striving for years to implement the requirements of the ePD in practice and to protect the rights of users. In view of increasing regulation in the area of tracking, these companies are reaching their limits in implementing the requirements. Not only growing legal uncertainty due to numerous case law and regulatory decisions on the design of cookie banners and cookie management platforms are challenging these companies. In addition, further legal requirements are putting European companies at a disadvantage in global competition, benefiting in particular the digital monopolists from the USA, whose practices have a much more invasive impact on the rights of European users. The new EDPB guidelines exacerbate this situation, as they now also subject link tracking as an alternative to the use of cookies to the scope of the ePD. For users in particular, there is no better protection of their rights, as the resulting legal uncertainty does not contribute to this.