POSITION PAPER

VAUNET
Verband Privater Medien

Opinion on the European Data Protection Board's (EDPB) Guidelines 2/2023 on the Technical Scope of Art. 5 (3) of the ePrivacy Directive

17. January 2024

1. Preliminary remarks

VAUNET - German Media Association would like to thank you for the opportunity to comment on the European Data Protection Board's (EDPB) Guidelines 2/2023 regarding the technical scope of Art. 5 (3) of the ePrivacy Directive (ePD).

VAUNET is the German umbrella association for private media providers. It represents over 160 companies that provide private journalistic and editorial radio, television, and online media. Its members enrich Germany's and Europe's media landscape through diversity, creativity, and innovation.

VAUNET supports the EDPB's approach of using the guidelines to contribute to a clear and thus legally certain interpretation of the scope of application of Art. 5 (3) ePD. At the same time, VAUNET fully shares the concern to protect the privacy of users and the confidentiality of private communications.

However, private media providers are particularly dependent on the successful utilisation of their offerings while at the same time being able to refinance them efficiently. The use of innovative data-based advertising technology is essential for this. When interpreting Art. 5 (3) ePD, the freedom of conduct a business must therefore be given sufficient consideration. Barriers to the use of advertising technologies and the communication of content arising from the interpretation of Art. 5 (3) ePD always have a direct negative impact on the diversity of opinion and media.

Against this background, VAUNET notes with concern the EDPB's interpretation of the terms "*gaining access to*" and "*stored information*", which are relevant to Art. 5 (3) ePD.

Due to its breadth, it harbours the risk of making any interaction in the online environment in principle subject to consent, contrary to the wording and the purpose of Art. 5 (3) ePD. This leads to innovation-inhibiting hurdles for the data protection-compliant distribution of audio-visual media content that are almost impossible to overcome in practice.

VAUNET therefore suggests **abandoning the broad interpretation** of the terms "*gaining access to*" and "*stored information*". In particular, the statements in points 2.5 and 2.6 of the guidelines should be deleted or adapted.

Having said this, VAUNET comments as follows:

2. EDPB Interpretation leads to contradictory results in practice

According to the guidelines, the scope of Art. 5 (3) ePD should not only cover access to information stored in the terminal equipment (such as cookies) (para. 31 and 32 guidelines).

Rather, it should be sufficient for "*access to information*" if information is sent from a terminal equipment to a recipient outside the terminal equipment (para. 33 of the guidelines). The mere fact that there is a technical instruction to send information from the terminal equipment opens the scope of application of Art. 5 (3) ePD.

At the same time, according to the guidelines it is irrelevant who stored the information or initialised the sending of the information. This also applies to the duration of the storage of information in the terminal equipment. Consequently, volatile storage processes (e.g. in RAM and CPU) are also covered (para. 37 guidelines).

VAUNET rejects this interpretation as too broad. It harbours the risk that, in practice, all electronic communication falls under the scope of Art. 5 (3) ePD and is therefore in principle subject to consent or justification. In the diction of the EDPB, generic, protocol-based communication instructions, through which user terminals send information to enable communication in the first place, would be covered by Art. 5 (3) ePD.

In practice, this leads to considerable contradictions.

For example, regarding internet communication, it would have to be assumed that every visit to a website or a video or audio contribution is "*gaining access*" within the meaning of Art. 5 (3) ePD, as IP addresses are sent by the terminal equipment via the HTTP header request.

The same could also be assumed for the broadcasting-specific distribution of audio-visual media content via HbbTV standard, as information is exchanged between the end device (e.g. smart TV or set-top box) and the provider based on the Application Information Table (AIT).

In both cases, however, there is no "*access to information in the end device*" in the literal sense and therefore no access to the user's privacy if the interpretation is done technically and realistically correct: In the case of online communication, information that is absolutely necessary for the communication process is sent automatically based on the HTTP protocol. When using the HbbTV signal, it is the user who initialises the transmission of information from their end device by pressing the so-called "Red Button" on the remote control.

3. Data protection requirements cannot be realised and inhibit innovation

In addition, the interpretation of the EDPB in practice leads to almost insurmountable hurdles for the data protection-compliant distribution of media content.

Firstly, media providers that offer video and/or audio content on websites would have to prove the existence of GDPR-compliant consent ***for each individual*** connection process with the

interpretation of the EDPB (unless they can demonstrate that the use of the information was strictly necessary to provide an information society service expressly requested by the user).

As a result, many new content banners can be expected to appear alongside the existing content banners. A result that is obviously undesirable from both the provider's and the user's perspective, even taking into account the considerable disadvantages of browser default settings. The guidelines are thus in contrast to the ongoing discussion about the prevention of cookie fatigue.

Secondly, media providers would have to obtain the necessary consent ***before*** accessing or sending the information in question. However, this is not possible in internet communication, as consent would have to be requested before the data exchange that makes communication possible (HTTP header request) is established. According to the guidelines, it remains unclear how providers could fulfil these requirements at all.

Thirdly, website operators would have to obtain consent for processing operations that were ***not*** initialised ***by them*** but are carried out based on general communication standards (and therefore on the basis of third parties). This also leads to unresolvable frictions under data protection law regarding the responsibility under GDPR.

VAUNET therefore suggests that the above-mentioned aspects be considered to a greater extent than when drawing up the guidelines and to consider that excessively high data protection hurdles inhibit innovation. This also applies in particular to the ongoing development of privacy-friendly advertising technologies if the legal interpretation leads to a requirement for consent per se due to its breadth.

4. Legal concerns against a broad interpretation

The broad interpretation of "*gaining access to information*" also raises legal concerns.

Firstly, the interpretation is not compatible with the wording of Art. 5 para. 3 sentence 1 ePD. This expressly refers to "*access to information*". According to common usage, "*access to*" presupposes an active action by the person accessing the information. If the European legislator had also wanted to include the passive receipt of information in the scope of application, it could and should have included "*receipt of*" or "*delivery of information*".

Secondly, the meaning and purpose of Art. 5 (3) ePD, which can be seen from recital 24, speaks against the interpretation given. Recital 24 of the ePD reads:

> *"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.* ***So called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge*** *in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these*

users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned." **(Emphasis added by the author)**

Art. 5 (3) ePD is therefore essentially intended to protect against the "entry" ("to enter") of harmful technology on a terminal equipment and thus into the privacy of the user. The object of protection is therefore the integrity of the end device, which is not affected by the proactive and voluntary sending of information from the end device.

Systematic reasons also oppose the interpretation. The broad interpretation would in fact also cover "*traffic data*" regarding the exchange of information for the establishment of communication. However, "*traffic data*" is explicitly addressed and conclusively regulated in Art. 5 **(1) and (2)** ePD. From this follows that "*traffic data*" is not also covered by Art. 5 (3) ePD.

Just as the broad interpretation of the term "*gaining access to*" therefore has no legal basis, there is also no such basis for the extension of the term "*stored information*" to merely ephemeral storage processes. The term "***stored*** *information*" clearly contains a temporal element. Stored information must ***already*** exist on the end device for it to be accessible. Logically, this does not include storage that is only created because of a processing operation and only for its duration.

The above considerations are also confirmed by the German data protection authorities. They published guidance for "Telemedia providers" via the Data Protection Conference (DSK) on 20 December 2021[1]. It follows from these that browser or header information that is transmitted inevitably or due to the settings of the end device when a Telemedia service is accessed should not be regarded as "access to information that is already stored in an terminal equipment".

5. Disproportionate consequences for media freedom to be feared

The reservation of consent and justification resulting from the guidelines also constitutes a disproportionate interference with the freedom of expression and information protected under Art. 11 of the Charter of Fundamental Rights of the European Union (CFR), which must be considered when interpreting Art. 5 (3) ePD.

According to Art. 11 (2) CFR, the freedom and pluralism of the media shall be respected. In addition, the right to freedom of expression must be upheld, which includes the right to receive and impart information and ideas without interference by public authorities.

The broad interpretation of Art. 5 (3) ePD for electronic communications is diametrically opposed to this if - as explained above - it must be assumed that the dissemination of private audio-visual media content, e.g. on the Internet, is generally made dependent on the user's consent to each individual connection process.

In addition, the interpretation creates a possibility for the authorities to control the question of which audio and video content on a website, for example, is still "*strictly necessary*" within the

[1] Cf. www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

meaning of the exception to the consent requirement provided for in Art. 5 para. 3 sentence 2 ePD, which jeopardizes media freedom. There is no question that official assessments of this kind can jeopardize the free dissemination of media content and opinions in the long term.

Finally, the interpretation of the EDPB should take greater account of the fact that data-based advertising and marketing are essential for financing free media and media diversity as well as media freedom in Europe. This applies even more as the refinancing of private media is facing considerable challenges. This is not only due to changes in user habits, but in particular due to competition from globally active big tech platforms, which dominate the online advertising environment and claim the majority of advertising revenues for themselves. An interpretation which, in this market situation, as in the present case, creates further and innovation-inhibiting hurdles for the distribution of electronic media and the display of data-based advertising should be critically scrutinised and analysed for its media compatibility.