Position Paper

15. January 2024

Bitkom Position Paper on the EDPB Consultation Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

Summary

The European Data Protection Board (EDPB) has issued Guidelines focusing on the technical scope delineated in Article 5(3) of the ePrivacy Directive (ePD). These guidelines serve the purpose of clarifying the Directive's application in various technical realms, particularly considering recent advancements in technology and emerging tracking methodologies.

This position paper aims to contribute to the public consultation on behalf of Bitkom. It examines the guidelines, explores their ramifications, and presents suggestions within the digital sphere. We appreciate this opportunity to participate in this consultation and look forward to future chances to provide our expertise in open discussions.

Bitkom welcomes the EDPB’s initiative to seek clear understanding of what is covered by Article 5(3) of the ePD. While regulatory guidance can play a helpful role in providing greater clarity for both individuals and businesses involved in tracking methods, there are significant concerns and challenges which must be resolved in relation to these Guidelines. These include the potential broadening of the ePD's scope and a lack of alignment with established regulatory principles, and industry practice.

An overly broad interpretation of Art 5(3) risks slowing the adoption of privacy enhancing technologies as an alternative to existing techniques. The Guidelines also have the potential to bring a greater number of activities within scope of the consent requirement, including, non-personalized content such as contextual advertising (targeted to the contents of a page rather than the identity or characteristics of users). The broad approach sought to be adopted by the EDPB interpretation will not protect against harm to customers’ privacy. Instead, it disincentivizes privacy enhancing

technologies, because potentially even those technologies are subject to regulation. In short, it risks exacerbating customers' consent fatigue, since the loading of every webpage, including webpages populated with non-personalized content, may require consent.

Furthermore, the directive's scope broadening lacks to discuss and address the legal terms of Art 5(3) sentence 2 ePD "sole purpose of carrying out the transmission of a communication" and "provide the service (…) explicitly requested by the subscriber or user" from the perspective of new technologies.

Lastly, we are concerned about the limited involvement of stakeholders and citizens during the guideline's development process. Inclusive participation is essential to ensure that diverse perspectives are considered from the outset. This emphasises the requirement for a more comprehensive and collaborative approach in regulatory decision-making processes.

Jurisdictional Concerns Surrounding EDPB Competence

Recent guidelines and decisions issued by the EDPB have sparked considerable debates regarding their legality and intrinsic nature. Regardless of the course of action chosen, guidelines raise pertinent questions about their compatibility within the existing legal framework. This complex situation necessitates careful examination, especially defining where the EDPB's authority lies, especially in areas where its members might not have direct power.

Instruments aimed at wielding authority over regulatory bodies have predominantly concentrated on executing ePD implementations at the local level rather than prioritizing data protection. In Opinion 05/2019, the EDPB clarified that a data protection authority lacks the legal basis to enforce the ePD without explicit authorization. Delegation of competence to an authority by national law must delineate specific tasks and powers.

The general competence of the EDPB in ePrivacy, established by Art 15(3) ePD, draws from the tasks assigned to the WP29 under Art 30 of the 1995 Data Protection Directive. However, mere reliance on GDPR tasks for ePD enforcement isn't automatically permissible. Instead, ePrivacy responsibilities should be confined to those previously granted to the WP29.

Even where these concerns do not arise in certain jurisdictions, the EDPB's interpretation is inconsistent with the guidance issued by some of the national authorities. For example, the EDPB's view that "access" can include passive receipt of information differs from the guidance previously issued by Datenschutzkonferenz (DSK) of Germany.

It is furthermore noticeable that the recent maneuvers in the guidelines seem to align its definitions with a possibly forthcoming ePrivacy Regulation. This proactive stance by the EDPB, although commendable in seeking alignment, raises crucial concerns about the timeline and procedural legitimacy of these definitions. The current absence of a negotiated and enacted Regulation prompts reflections on the EDPB's prerogative in pre-empting forthcoming legislation. While acknowledging the EDPB's pivotal role in ensuring data protection, it's imperative to underscore the mandate's adherence to the existing directive rather than anticipatory actions, as delineated by their role.

Key elements for the application of Article 5(3)

Within the sphere of the published guidelines, notions such as "terminal equipment", "gaining access", “storage” and "stored information" have been reinterpreted by the EDPB compared to past regulatory positions. The altered stances raise considerable concerns, particularly the departure from explicit language of legislative texts.

The Guidelines are clear in extending the scope of applicability of Art.5(3), but do not clarify how the requirements of Art.5(3) can be met in practice. For example, it does not provide information on how consent requirements will be fulfilled where the instructing entity and the entity receiving information from terminal equipment are not the same, or where multiple users/subscribers use the same terminal equipment. (such as public networked computers at a library). In this sense, assuming this interpretation of Art.5(3) can be accepted at all, the Guidelines raise more questions and offer little by way of suggesting potential solutions.

The effect of the Guidelines is also that, consent will be required for a significant range of scenarios. If the Guidelines are strictly applied, users/subscribers will receive consent request for each such transmission now in scope, resulting in them receiving an overwhelming number of consent requests, to a level they likely have never expected. This also conflicts with the underlying objective and principle of the European Commission's cookies pledging principle, supported by the EDPB, which was a proposal driven to reduce fatigue of the users.

Notion of “Terminal Equipment of a Subscriber or User”

In the evolving landscape of technological advancements, the definitions and categorizations of terminal equipment encounter challenges in harmonizing definitions, particularly concerning IoT devices and their interconnections. The ambiguity in defining terminal equipment under the ePD leads to complexities in its application and enforcement, warranting a precise re-evaluation and definitions to mitigate confusion and streamline compliance measures.

Paragraphs 15 and 16 introduce discrepancies – while one exempts communication relays from this definition, the other broadens it to encompass hardware combinations like smartphones or IoT devices. The document's complexity heightens in paragraph 60, where IoT devices connected through relays blur the scope of Article 5(3) ePD. Data transmission outside public networks might fall beyond its jurisdiction, yet once relayed to a server, it's considered stored by a terminal, invoking Article 5(3) ePD. Adding to this confusion, the guidelines deviate from Directive 1999/5/EC's definition, expanding coverage beyond terminal equipment enabling communication. This shift amplifies ambiguity, complicating the identification of terminal equipment. A clearer, consistent definition within the ePD is crucial to mitigate confusion, ensuring a unified framework for compliance and enforcement.

Although the technical and legal challenge with multiple users or subscribers of a terminal equipment is mentioned (Paragraph 18), there is no real discussion of a technical solution on the bases of the law text of Art 5(3) ePD (“subscriber or user concerned has given his or her consent”). The clear legal definitions of a “subscriber” (Art 2 lit k Framework-Directive 2002/21/EC) and “user” (Art 2 lit a ePD) and the clear wording of “subscriber or user” in the whole Art 5(3) ePD do not lead to the result that these roles have to be seen quite similar to the term “data subject” (Art 4 Nr 1 GDPR) as EDPD and many national data protection authorities want to interpret legally. So, a specific legal and technical analysis would have to be made, who has the power to decide in situation with with multiple users or subscribers about a “gaining access” or a “storage” in connection with a terminal equipment. Legal certainty is also required for whom the service fulfilment has to take place (“subscriber or user”), that the exemption of Art 5(3) sentence 2 ePD is applicable. While the term “user” (Art 2 lit a ePD) can only be a natural person, a “subscriber” (Art 2 lit k Framework-Directive 2002/21/EC) can also be a legal person (e.g. a company as “subscriber” of the terminal equipment of its employees). According to the clear law text of Art 5(3) ePD, consent or the service fulfillment is necessary only from a “subscriber or user” before “gaining access” or “storage”.

Notion of “gaining access”

The interpretation of "access" under the ePD has undergone significant expansion, posing challenges in distinguishing between active and passive engagement. Previously, "gaining access" in the ePD primarily focused on intentional actions to retrieve or acquire information stored in terminal equipment. However, the EDPB's widened interpretation broadens this definition to encompass passive access, extending it to instances where information is transmitted or received without active solicitation. While the Guidelines clarify that storage and access do not need to be cumulatively present for Art. 5(3) to apply, it does not clarify the respective roles and obligations between the entity “gaining access” vs the entity “storing information”. This may lead to scenarios where both entities are expected (or feel they need) to comply with transparency and consent requirements, exacerbating the user's consent fatigue and creating additional, duplicative barriers in a user's journey.

This reinterpretation carries implications for data transmission via communication protocols. For fingerprinting, the lack of distinguishing between active and passive in Opinion 9/2014 of the Article 29 WP, prevents the necessary technical assessment of Art. 5(3) ePD. While active fingerprinting uses technologies such as JavaScript that actively read information from the terminal equipment, passive fingerprinting only uses the information available on the server that was automatically transmitted as common connection data. In addition, the Baden-Württemberg data protection authority is of the opinion that passive fingerprinting at best falls within the scope of the GDPR (↗LfDI BW, section 3.1).

Paragraph 55 introduces further confusion. It discusses the concept of an IP address "originating" from the user's terminal equipment, contributing to the intricacies of this widened interpretation and its practical applications in legal contexts. Notably, if the serving of non-personalized ads falls outside the "strictly necessary" exemption, obtaining consent for delivering any non-personalized ad on a website could become mandatory.

The German Data Protection Conference suggests that transmitting basic HTTP header and related connection data doesn't align with the German interpretation of Art. 5(3) ePD (↗DSK, OH Telemedien 2021, V.1.1, Recital 21). According to their view, automatic transmission of this ordinary connection data via the HTTP header shouldn't be considered "access" under the directive. We further conclude that passive fingerprinting and using pixels without actively accessing information from the technical equipment should not be interpreted as “access”. Instead, such processes might fall under GDPR if involving personal data processing, ensuring no gap in protection under the ePD while maintaining its technical considerations.

The EDPB's expanded interpretation potentially categorizes all internet communications as instances of "access", but some minimal invasive tracking technologies are technically the same as the retrieval of other web content, such as images, fonts or CSS files from a terminal’s perspective. The following processing on the server are not part of the ePD’s scope. This has significant implications for compliance and enforcement. We believe that this will have a negative impact on the user experience of EU-based individuals, and on organisation’s ability to innovate and offer better tailored services to individuals in Europe.

This broad interpretation also seems disproportionate given the objective of the ePD. It arguably does not align with the spirit of Recital 24 of the ePD which suggests that ePD's objective (or at least the requirement for users' consent under Art.5(3)) is to protect the users' terminal equipment from active intrusion that occurs without their knowledge, that seriously intrudes upon their privacy).

Notion of “Stored Information” and “Storage”

The EDPB’s position regarding information stored in terminal equipment under the ePD encompasses a broad spectrum, extending beyond traditional definitions. However, a closer examination reveals nuanced complexities in understanding the notion of "stored information" and its interpretation within the regulatory context.

First, the document conflates the two concepts of "stored information" and "storage". This approach leads to two problems: (1) it is confusing because the two are very different: as the guidance states, stored information may have been placed on the terminal equipment by the subscriber or by the user or by the equipment manufacturer, but neither of these acts of "storage" would trigger an ePrivacy consent; and (2) it means that the section on "gaining access" contains no discussion of what the recipient must gain access to – which is a worrying omission. It would be clearer to address the concept of "information already stored" in the section on obtaining access, to make it clear that the consent requirement for access applies only to "information already stored".

Second, the expanded interpretation by the EDPB redefines stored information, now encompassing both physically stored and ephemeral data generated or processed on the terminal equipment. This includes the storage and processing capabilities of terminal equipment, challenging traditional legislative boundaries and emphasizing the need for clarity in distinguishing between transient data processing and stored information under the ePD. This widened interpretation carries practical implications, especially regarding compliance measures such as consent and technical exceptions. It introduces complexity, particularly when dealing with data processed but not physically stored. For instance, in the realm of network communication, data writing is integral for the creation or reception of messages. A website logging a subscriber's or user's activity on a specific page necessitates the writing of that log. However, this ephemeral storage falls beyond the scope of Art 5(3) ePD.

Therefore, and finally, technical caching of information and its utilisation in RAM or the CPU should not fall within the scope of Art. 5(3) ePD. A synchronization with conclusions of Art 4 – Art 5 DSA (EU) 2022/2065 (ex Art 12 – Art 13 E-Commerce Directive 2000/31/EC) of the Digital Services Act (no responsibility for "mere conduit" and "caching") could help. Such activities do not constitute "storage" within the meaning of the directive, while the EDPB seems to anticipate a possible forthcoming regulation. An interpretation of Art. 5(3) ePD that even considers the temporary or fleeting technical caching of information or the use of RAM and CPU as "storage" within the meaning of the directive would disregard the wording of the law, render its scope of application limitless and make practical implementation impossible. In the case of storage on the terminal equipment that requires consent, such as a marketing cookie, this is aggravated by the fact that the broad interpretation of the scope of application, including processing operations in RAM and CPU, would make it practically impossible to implement the information obligation of Art. 5(3) ePD. This applies in particular to the duration of storage, which is part of the mandatory information according to the case law of the ECJ (ECJ, judgement of 01 October 2019 - C-673/17, para. 81). Here, too, the data controller under Art. 5(3) ePD has no way of predicting the processes in the RAM or CPU or providing information about their specific activities. This creates significant confusion as regards practical application, extent of compliance/enforcement and how the requirement of consent will be dealt with in practice, in particular without further guidance on if/how the ePD's exemptions apply to these scenarios.

The Guidelines also do not shed any light on storage in the context of terminal equipment powered by cloud-based technologies (e.g., devices without significant RAM/CPU that rely on cloud-based systems).

Applicability of Exemptions

Whilst significantly expanding the scope of applicability of Art.5(3) of ePD and highlighting specific use cases, the Guidelines are silent on exemptions.

There is no indication of how the existing exemptions would apply to scenarios that are now in scope (e.g., in respect of information that is generated/stored by default in the terminal equipment and are transient in nature, such as RAM or CPU cache). We would need the EDPB to clarify this. Similarly, to how the Guidelines explained how Art.5(3) applies to each use case, we would expect the EDPB to explain if/how exemptions would apply to each use case (tracker by tracker).

There is also no indication of additional exemptions being introduced. Noting that tracking based on IP address is a specific use case highlighted by the EDPB as coming under the scope of Art.5(3), query whether exceptions should be made where such use of IP address is necessary for legal compliance. For example, use of IP addresses may be necessary to ensure that particular content is shown only to the user in a licensed territory or filter content that are deemed illegal or inappropriate in a specific territory.

Use cases

The guidance contains a description of various "use cases", but in some cases without sufficient clarity as to whether, and under what circumstances, these are actually in scope of Art 5(3) ePD. It would be helpful for the guidance to include more concrete analysis, applying the facts to the language of Art 5(3) ePD. By way of specific examples where more clarity is needed:

- **Unique identifier**: Caching of entries in form fields that have not yet been submitted is one of the usual functions of a web browser, for example, in order to enable basic functionality. Here too, extending the scope of application of Art. 5 (3) ePD to such caching would make the scope of application limitless. The guidance should clarify that unique identifiers are only in scope when the unique ID is stored and/or subsequently accessed from the user's terminal equipment (as with a cookie ID). Furthermore, identifiers such as those commonly used for authentication, subscription, purchases and similar uses cases – on both websites and applications, would be in scope, according to the EDPB Guidelines. It is unclear why authentication is used as an example when it is typically exempt under GDPR DPA guidance.

- **Tracking based on IP only**: IP addresses are sent automatically by virtue of the way in which communication is made over the internet. The EDPB's position appears to be that the developer/implementer of a communication protocol can be the instructing party and therefore the collection/receipt of IP addresses will be in scope (even if not stored on a user's device). This is another example which illustrates that an individual's day-to-day access to webpages will come under the scope of Art.5(3), which seems disproportionate.
  IP addresses are not technically "read" on user's devices and cannot be used as a tracker due to their non-persistent nature. Art.5(3) states it shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network. This should not apply to use of IP address.
  The Guidelines state that, unless the entity can ensure that the IP address does not originate from the terminal equipment of a user/subscriber, it must take all the steps pursuant to Art.5(3). This places a disproportionate burden on businesses to carry out an assessment to identify the origin of a particular IP address. Such blanket approach based solely on whether a transmission has occurred is not

proportionate or practical, and also discriminates certain technologies used.
It would be helpful for the guidance to clarify that other uses of IP address in isolation, for purposes which are not tracking, would be out of scope.

- **URL tracking**: In URL tracking, parameters are used in the URL to provide information about content that is clicked and the origin of that content (marketing from a brand about one of its products on sale) The EDPB's view would mean the reading of the URL being requested by the device is still “access” or “storage” even if the server is not querying the device – this illustrates a significant widening of the scope of what Art.5(3) captures, extending to automatic/consequential transmission of information which occurs simply by the virtue of how the internet functions; day-to-day visiting of a webpage by a user (even if there are no ads at all) could come under scope. This goes beyond what is required, and what was originally intended, by the ePD.

- **Pixel tracking and passive fingerprinting**: In Pixel tracking, a 1x1 graphic operates by being loaded when a user accesses content to aid in analytics. Using pixels without other technologies, that would actively access information on the terminal equipment, only the information available on the server that was automatically transmitted as normal connection data is used (e.g. in case of passive fingerprinting). Summarized, there isn’t an actively access of terminal’s information, so that this process shouldn’t be in the scope of the ePD. The guidance also assumes that these activities are in-scope, “at the very least” through the caching mechanism on the client-side software. This suggests the EDPB considers there may be other means by which these practices may be in scope of Art 5(3) ePD, which it would be helpful to specify here.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Tabea Wilke | Head of Data Protection and Security
T 030 27576-161 | t.wilke@bitkom.org

Responsible Bitkom committee
Working Group Data Privacy

This publication is intended to provide general, non-binding information. The contents reflect the view within Bitkom at the time of publication. Although the information has been prepared with the utmost care, no claims can be made as to its factual accuracy, completeness and/or currency; in particular, this publication cannot take the specific circumstances of individual cases into account. Utilising this information is therefore sole responsibility of the reader. Any liability is excluded. All rights, including the reproduction of extracts, are held by Bitkom.