

#### 17.01.2024

**Timo Weigl** - Head of Communication & Public Affairs - weigl@bvdw.org **Daphne van Doorn** - Senior Public Affairs Manager - vanDoorn@bvdw.org

Position Paper on the Guidelines of the European Data Protection Board (EDPB) on the technical scope of Article 5 (3) of the ePrivacy Directive Communication (*ePrivacy Directive*)

### **Preliminary remarks**

The German Federal Association of the Digital Economy – BVDW (*Bundesverband Digitale Wirtschaft e. V.*) with EU transparency register number 479540331468, represents the interests of companies that operate digital business models or whose value creation is based on the use of digital technologies. The basis for this is the intelligent combination of data and creativity with a strong focus on ethical principles. With over 600 member companies – from large and small digital companies to agencies and publishers – the association represents the interests of the digital economy in society and the political arena. Its network of experts provides guidance on a key future field with facts, figures, and data.

The BVDW is pleased to have the opportunity to comment on the proposed guidelines of the *European Data Protection Board* (EDPB) on the technical scope of Art 5 (3) of the *ePrivacy Directive*. Many of our members are directly and indirectly affected by these guidelines. Therefore, the BVDW has already participated in many consultations at EU and national level on data protection regulations.

### **General**

In principle, we welcome the aim to clarify the applicability to new technologies and analyse current developments given the technology neutral nature of the ePrivacy Directive. However, while the EDPB outlines the emergence of new technologies as a driver and justification for this new effort, there is no reference to any new technologies or approaches in the draft guidelines. Everything mentioned (whether CPUs, IP addresses, URL parameters, etc.) is either a foundational internet/web technology for decades or has been common practice for many years. We have considerable doubts concerning the proposed EDPB Guidelines and their technical scope and will go into detail below.

### Responsibility

According to Art. 70 *General Data Protection Regulation* (GDPR), the EDPB is tasked, among other things, with issuing guidelines to promote the harmonised application of the GDPR. A guideline competence with direct reference to ePrivacy only arises from Art. 19 of the draft ePrivacy Regulation, which has neither been finalised nor adopted to date. A similar provision cannot be found in the ePrivacy Directive. We therefore question whether the chosen form of the guidelines is the correct one.



The EDPB does have some competence in relation to ePrivacy under Art. 15 (3) of the ePrivacy Directive, which provides that the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Art. 29 shall also perform the tasks laid down in Art. 30 of the 1995 Data Protection Directive in relation to matters covered by electronic data processing. According to Art. 94 (2) of the GDPR, references to the Working Party of Art. 29 are to be understood as references to the EDPB. However, this cannot unequivocally mean that the extended list of responsibilities assigned to the EDPB under the GDPR also applies to ePrivacy. Rather, the EDPB's competences in this regard must be limited to the competences that were previously transferred to the Art. 29 Working Party. This especially does not include the power to issue guidelines in relation to directives and in particular the ePrivacy Directive. Strictly speaking, the instrument of guidelines is currently only available to the EDPB for the interpretation of the GDPR.

The strong signal sent out by the wording "guidelines", which implies that national supervisory authorities must comply with them, is questionable when taking this into account. With regard to the ePrivacy Directive, which explicitly – and as is stated by the EDPB itself in the so-called guidelines – includes "information", i.e. data and data sets that contain more than just personal data, we hereby expressly question the competence of the EDPB with regard to issuing guidelines. We call for clarification by renaming it "Guidance" or "Recommendations".

We strongly disagree with the EDPB's statement at the beginning of the guidelines that ambiguities regarding the scope of Art. 5 (3) of the ePrivacy Directive have created incentives to implement alternative solutions for the tracking of internet users that have led to the circumvention of the legal obligations provided for in Article 5 (3) of the ePrivacy Directive. There can be no mentioning of circumvention. In the German market in particular, the data protection authorities not only act in a strict and differentiated manner, but the ePrivacy Directive was also last transposed into national law in 2021 with the TTDSG, the Telecommunications–Telemedia Data Protection Act (*Telekommunikation–Telemedien–Datenschutz–Gesetz*) and is therefore still highly up–to–date. For years, companies in the digital economy have been endeavouring to break new ground in alignment with data protection and ePrivacy rather than deliberately creating alternatives. This narrative, which discredits an entire industry, therefore meets our incomprehension. Such an insinuation must be removed from the so–called guidelines on the technical scope of Art. 5 (3) of the ePrivacy Directive.

#### Access

In 2022, the "Datenschutzkonferenz" (Data Protection Conference) published a new version of a guideline (DSK\_Telemedia) for "telemedia providers" (originally from 2021) in relation to the TTDSG and thus the ePrivacy Directive. The Data Protection Conference is an institution consisting of the independent data protection authorities of the federal and state governments of Germany. One of its tasks is to achieve a harmonised application of European and national data protection law and to jointly advocate its further development.



The position of the Data Protection Conference presented below contradicts the statements in the current EDSA Draft Guideline. As part of the orientation guide, it established the following:

"Access requires a targeted transmission of browser information that is not initiated by the end user. If only information, such as browser or header information, is processed, which is transmitted inevitably or due to (browser) settings of the end device when a telemedia service is called up, this is not to be regarded as "access to information that is already stored in the end device". Examples of this are:

- the public IP address of the end device,
- the address of the website accessed (URL),
- the user-agent-string with browser and operating system version and
- the set language."

It therefore requires specific access that is actively triggered by the telemedia provider in particular. Which is also logical and understandable given the choice of word *Access* in the regulation. After all, the obligations arising from Art. 5 (3) of the ePrivacy Directive should only apply to something that can be actively influenced/is actively requested. Both the IP address, as well as the user-agent are information that the browser automatically sends when a server request is made (e.g. to access websites), without the service provider being able to influence this. Just because there is an implicit instruction to the end device or terminal equipment to send information, this alone cannot be interpreted as "access" to the end device and even less so if this then means, conversely, that the scope of application of Art. 5 (3) cannot be interpreted so broadly.

Gaining access requires an action. The guidelines suggest that information sent by the terminal device (automatically and/or on the instructions of a third party) constitutes as "gaining access" by the recipient, even if the recipient has not taken any action to initiate the transmission of this information. Obtaining access requires an action by the recipient. Consequently, the mere passive receipt of data should not trigger Art. 5 (3). The EDPB should therefore urgently reconsider its statements in this regard. After all, we are not only asking ourselves the question of "whether", but ultimately also "how". Should companies be required by supervisory authorities to obtain consent for processing in these constructed access cases in the future through the application of these guidelines, it remains to be seen how this can be implemented in reality. It is difficult to imagine what exactly this information should look like. How is all this to be explained in a transparent manner and without constant repetition to users who, according to consumer protection authorities, are already completely overwhelmed by existing consent banners?

Additionally, the interpretation of access in relation to Internet-of-Things (IoT) devices is also questionably broad. If "access" to the information already exists as soon as a communication takes place in which the recorded information is transmitted to the manufacturer's or



operator's server (either directly by the device itself or via a relay, i.e. the user's smartphone), this is once again a case of passive access that cannot be influenced at all.

The fact that the EDPB considers the IP address – which is inherently part of the IP communication, and the URL requested by the device – as access to a terminal device, even if the server does not actually call this up from the device, means that the EDPB also includes passive processes, at least those that cannot be actively influenced. This would extend the scope of Art. 5 (3) in such a way that practically every communication process would have to be interpreted as access to a terminal device.

IP addresses are essential for routing data traffic over the internet, in particular from the client to the corresponding server and back to the client. If the guidelines would be interpreted in such a way that the mere reception of IP addresses would require consent in accordance with Art. 5 (3) of the ePrivacy Directive, then the very profane question arises as to how data traffic on the internet is supposed to function at all. This would mean that all internet communication would have to be assessed as absolutely necessary and subject to consent, which would lead to massive legal uncertainty and consent fatigue. This would not lead to any improvement in user privacy. From a technical point of view, IP addresses are not read from users' devices. They are absolutely necessary in order to direct data traffic via the internet. For precisely this reason, the guidance issued by the Data Protection Conference as the framework supervisory authority of Germany on the TTDSG confirms that non-transferable header information such as the public IP address of the end device do not fall within the scope of the TTDSG when it comes to storing and accessing information on users' end devices.

The EDPB confirms that this activity only falls under Art. 5 (3) if the IP address originates from the subscriber's or user's terminal equipment. This is usually not the case, but the EDPB gives some examples where this would apply: the static outgoing IPv4 address originating from a user's router, or IPv6 addresses (which are partly defined by the host). It should therefore be rejected that the IP address is generally considered as end device access. The IP address is necessary for the functioning of the internet and can hardly ever be traced back to an end device.

### **Storage**

According to the EDPB, it should be sufficient for information to be stored, even temporarily, in order to fall within the scope of Art. 5 (3) of the ePrivacy Directive. This is not clear to us. The EDPB refers to RAM and CPU cache and thus appears to include not only the use of the storage capacities of end devices, but also the use of the processing functions of end devices in the scope of application. RAM only stores short–term data that is currently being used by a device. This is de facto a transiently process. The data is constantly and quickly replaced by other data. RAM is only used for information that is utilised by the device. CPU cache memory is similar, as it is also a temporary "storage" for data and instructions that the CPU may need to access quickly. RAM is intended for currently used data, while the CPU cache is intended for frequently used data.



We strongly doubt that such processing-related situations of short-term storage should be covered by Art. 5 (3) ePrivacy Directive. This is because it would mean that no use of RAM or CPU cache is permitted unless the user has given consent to this use of RAM or CPU cache, or the use of RAM, or CPU cache is strictly necessary for the provision of a service explicitly requested by the user, or the use of RAM or CPU cache is for the sole purpose of transmitting a message over an electronic communications network.

The same applies to the temporary storage of Unique Identifiers, which are derived from information provided by the user (e.g. hashed emails or telephone numbers) and are intended to represent stored information on the user's devices according to the EDSA. Almost any communication over a network requires data to be written by the sending or receiving party simply to construct or receive the communication. For example, a website may receive network log data about a user's activity on a particular page of its website. In order to be sent, this log must first be written. However, this fleeting storage should not fall within the scope of Art. 5 (3). The guidelines state that there is no lower limit for the duration of storage or the amount of information to be stored. However, if Art. 5 (3) ePrivacy Directive also covers caching mechanisms, the transmission of a URL or any other transmission of data between two endpoints, this can either lead to an unmanageable number of consents or to the exceptions having to be interpreted very broadly just to make the internet work.

The guidelines also confuse and interchangeably use the terms "stored information" and "storage". This is confusing as these two terms are very different in meaning. As stated in the guidelines, stored information may have been placed on the device by the user or by the device manufacturer, but none of this "storage" would trigger ePrivacy consent. The "obtaining access" section contains no discussion of what the recipient must obtain access to. It would be clearer to address the concept of "information already stored" in the access section to clarify that the consent requirement for access only applies to "information already stored". The guidelines also lack a separate discussion of the concept of "already stored information". The use of the term "already" in the Guidelines clearly implies the passage of time, so that storage and access cannot be essentially simultaneous. We also note that the Guidelines refer to "stored information", although this is not the term used in Art. 5 (3) ePrivacy Directive.

### **Conclusion**

Rethinking new technologies, regulating tracking and monitoring are noble goals that we are happy to support, as long as they are carefully developed and accompanied by the necessary detailed consideration of the regulated technical processes.

The use cases presented by the EDPB mostly lack clarity as to whether and under what circumstances they actually fall within the scope of Art. 5 (3) of the ePrivacy Directive. The EDPB's explanations, some of which are very broad and open to interpretation, give the impression that all server–side processing is to be included into the scope of application. This would apply to all processing operations, even outside a terminal device and all network communication in which a terminal device participates.



There are also inconsistencies in the use of definitions in the guidelines. Such as in the case of terminal equipment. The guidelines do not make a clear statement about what constitutes a terminal equipment. The EDPB relies on the definition used in Directive 2008/63/EC, while the ePrivacy Directive refers to the definition in Directive 1999/5/EC (confirmed by the amending Directive 2009/136/EC). The key element of the legal definition is that the devices must "enable communication". The definition used in the Guidelines extends the scope of Art. 5 (3) ePrivacy Directive to devices that should not fall under the definition given in the Directive.

The exorbitant expansion of the scope of application could have a significant impact on a large number of digital service providers. The inclusion of tracking URLs in the scope of Art. 5 (3) could also have a significant impact on the operators of affiliate networks and companies that rely on such systems to collect sales data or generate revenue in the first place.

Extending the technical scope of Art. 5 (3) of the ePrivacy Directive to include the delivery of all types of non-personalised advertising would not only lead to an economically undesirable disaster, but would also mean that access to information would only be possible via paywalls. Publishers and other members of the digital economy and industry would have no other choice. We cannot imagine that this is the intended purpose of these Guidelines.

An overly broad interpretation of Art. 5 (3) ePrivacy Directive also harbours the risk that the introduction of technologies to improve data protection as an alternative to existing, more privacy-intrusive technologies could be slowed down. The Guidelines could lead to a greater number of activities being subject to the consent requirement (e.g. including activities necessary for the provision of contextual advertising, which explicitly forego the recognition of devices or people). If consent is required regardless of the type of information accessed or its purpose, and is always required, there is less incentive to use these alternative techniques.

These Guidelines urgently need to be reconsidered and revised in terms of form and content.