**Response to the EDPB public consultation on Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive**

The undersigned associations representing the digital marketing and advertising ecosystem at EU-level and in various member states have taken note of the draft Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive (**ePD**), adopted by the European Data Protection Board (EDPB) on 14 November 2023. We are grateful for the opportunity to provide comments on the proposed guidelines.

## Executive summary

The proposed guidelines intend to clarify what is covered by the phrase '*to store information or to gain access to information stored in the terminal equipment of a subscriber or user*' in Article 5(3) ePD. The proposed guidelines come at a time when companies are increasingly using technologies other than cookies to deliver their services to users, in particular in new types of devices such as connected objects. It is clear from the text of the proposed guidelines that they may have stem from a desire by EDPB members to ensure that tracking techniques that make use of such technologies are subject to the same ePrivacy requirements as cookie-based tracking.

We believe in the technology-neutral principles of EU legislation on information and data, which allow it to remain up-to-date with technological advancement, to ensure a high level of data protection and to prevent circumvention. In that respect, we fully welcome regulators' initiatives intended to clarify in practice which requirements may apply to new technologies and allow companies to innovate with legal certainty.

Nonetheless, we are concerned that the proposed guidelines 2/2023 - which are intended to clarify the material scope of a directive that was transposed in national law with significant nuances across EU Member States - prescribe an expanded interpretation of how the ePD applies to existing technologies, in particular of the Transmission Control Protocol (TCP/IP). We contend that such interpretation is overbroad, technically unworkable, and misaligned with the objectives of the ePD, namely to regulate actual (active) access to information stored on users' devices, seen as part of the private sphere of the users (see in particular Recital 24 ePD). In particular, this interpretation extends beyond the specific tracking techniques the EDPB aims at providing guidance for, as it impacts operations and use cases that do not involve the tracking of users' activity.

**Areas of concern**

- The ePD has been transposed in national law with significant differences between member states - including as regards which authorities are charged with its regulatory tasks and how these authorities are interpreting and enforcing the ePD. Some of the regulatory authorities responsible for enforcing the ePD are not represented in the EDPB. This raises uncertainty regarding whether the proposed guidelines adequately capture the perspectives of authorities that are effectively assigned with the responsibility for enforcing national ePrivacy rules, and how such authorities will interpret the national ePrivacy rules in light of the proposed guidelines, particularly where such authorities have expressly taken differing approaches previously.
- The proposed guidelines create the potential for varied and conflicting interpretations across Europe, aggravating legal uncertainty and economic disparities for organisations operating in different jurisdictions:
    - The interpretation provided by the EDPB diverges from established positions issued by local regulators and that companies have heavily relied on to ensure compliance of their services;
    - The proposed guidelines are likely to cause confusion as to the application of consent requirements under the ePD due to the existing guidance over consent exemptions described in the WP29 Opinion or provided for by national regulators not aligning with the technologies and mechanisms now encompassed by the EDPB's interpretation.
- In their current form, the guidelines erode the distinction between operations that involve tracking of users and those inherently required for the technical delivery and management of non-personalised advertising and other similar non-intrusive, privacy-protective services. This disruptive shift would mean that a much greater number of operations would require consent under Article 5(3), and would have the combined effect of:
    - Worsening the so-called consent fatigue phenomenon;
    - Acting as a deterrent for companies to favour where possible privacy forward practices;
    - Decreasing the volume of online content and services provided for free to users.

**Key recommendations**

There are several areas in which we believe the proposed guidelines should be revised:

- The nature and content of the proposed guidelines should be reviewed to reflect the EDPB’s composition and competence over the ePD.
- The interpretations of the notions of “gaining of access” and “stored information” should exclude the passive receiving of information required for the transmission of communication or information that is stored only in transient, ephemeral manner in RAM or cache and align with the ePD’s primary objective of protecting the private sphere of users.

- The proposed guidelines should account for the interpretative guidance and recommendations that have already been issued by competent authorities over the technologies encompassed by the proposed guidelines.
- Rather than referring to Opinion 4/2012 of the Article 29 Working Party (WP29), it is essential for the proposed guidelines to concomitantly cover the situations in which an operation performed by means of the technologies newly addressed, may qualify for exemption from the consent requirement under Article 5(3).
- Finally, the proposed guidelines need to adequately consider that a broadening of the outdated text of the ePD in a way that disregards the flexibility afforded by the GDPR will have detrimental effects for companies operating in the online space.

1) EDPB competence to issue guidelines relating to the ePD

Member States have chosen different ways of allocating the task of enforcing national ePrivacy rules, and some of them have conferred such competence to a body or authority other than the data protection authority[1]. These other bodies or authorities are not represented in the EDPB, and it is therefore unclear how the proposed guidelines can represent their views. Moreover, some EDPB members are not tasked with enforcement of national ePrivacy rules, which raises questions as to whether they took part in any discussions or might otherwise have influenced guidelines that relate to areas of law falling outside of their formal remits.

As the EDPB rightly points out: "*unless national law gives them such competence, data protection authorities cannot enforce the provisions (of national law implementing) the ePrivacy Directive as such when exercising their competences under the GDPR.*"[2] Additionally, the proposed guidelines make no distinction between personal and non-personal data, even though non-personal data clearly falls outside the material scope of the GDPR and therefore is not in the remit of the EDPB's competences under the GDPR.

In its current form and taking into account the procedure that led to its adoption, it is unclear how and whether the considerations laid out in the proposed guidelines should be abided by any body or authority other than data protection authorities, or even considered in relation to operations that do not trigger the material scope of the GDPR.

Moreover, the proposed guidelines aim to bring clarifications to the notions of "terminal equipment" and "electronic communication network". Both notions are defined in separate legal instruments from the ePD, namely Article 1 of Commission Directive 2008/63/ EC and Article 2 of Directive 2018/1972 establishing the European Electronic Communications Code. The adoption of guidelines and common approaches to the definition of both notions is therefore the responsibility of the competent telecommunications national regulatory authorities and the Body of European Regulators for Electronic Communications (BEREC). Again, these other bodies or

[1] https://digital-strategy.ec.europa.eu/en/library/list-personal-data-protection-competent-authorities
[2] https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

authorities are not represented in the EDPB, and it is therefore unclear how the proposed guidelines can represent their views.

There is a need for clear and consistent interpretation on the boundaries of the EDPB competences, tasks and powers, to ensure improved legal certainty in the EU. We would urge the EDPB to re-draft and change the nature of the document to reflect such boundaries.

For instance, we consider that recommendations or a simple public statement may be a more appropriate format, in line with the EDPB's composition and competence. If the legal form of "guidelines" is important to the EDPB, it could adopt guidelines specifically within the material scope of the GDPR, describing how the EDPB interprets the practical implications of GDPR obligations for entities that process personal data by way of such technologies.

2) <u>EDPB interpretation of the notion of "gaining of access"</u>

The application of Article 5(3) ePD is triggered by two scenarios: (i) "the storing of information [...] in the terminal equipment of a subscriber or user" and (ii) "the gaining of access to information already stored, in the terminal equipment of a subscriber or user". We have focused below on that second scenario, i.e. "gaining of access".

In its proposed guidelines, the EDPB states that this "gaining of access" scenario is one where "*the accessing entity wishes to gain access to information stored in the terminal equipment and actively takes steps towards that end*" (paragraph 31).
However, those "active steps" to "gain access" are interpreted very expansively, as the EDPB considers the following points:

- "*the fact that the receiving entity might not be the entity instructing the sending of information does not preclude the application of Article 5(3) ePD*", and "*one entity may have used protocols that imply the proactive sending of information by the terminal equipment which may be processed by the receiving entity*";
- "*Network communication usually relies on a layered model that necessitates the use of identifiers to allow for a proper establishment and carrying out of the communication. The communication of those identifiers to remote actors is instructed through software following agreed upon communication protocols*", with IP addresses being an example;
- The use of "established protocols" is elsewhere described (in the section about "storage") as being covered by Article 5(3) ePD, "*regardless of who created or installed the protocols or software on the terminal equipment*".

Put together, we understand that in the eyes of the EDPB, there is "gaining of access" as soon as one protocol that involves the automatic transmission of information (even if that transmission is automatic and inherent to the architecture of the internet, e.g. in the IP headers within the IP layer of the TCP/IP) to a third party's online resource, simply because one instructing party "created or installed" a (generic) protocol on the terminal equipment (e.g. a link or URL) despite the receiving third party not being able to influence this.

We contend that such interpretation cannot have been the intention of the EU legislator, who chose the words "gaining of access". The word "access" necessarily implies some form of active movement by the party doing the "accessing", as opposed to e.g. the verb "to receive" (where a recipient can "receive" things passively). The active nature of "access" is confirmed by the text of Recital 24 ePD, which describes only the act of "*enter[ing] the user's terminal without their knowledge*" ("enter" implying active movement also). Nowhere does the ePD use broader, passive words to describe the gaining of access (for instance, it could have used the word "receive" or could have included an example about remote monitoring of server logs).

An example of an unintended consequence of this excessive interpretation of "access" is a lack of clarity about who should support which obligations or even how they might be workable. The EDPB introduces the idea of an "instructing party" in the proposed guidelines that would be the entity that instructs the sending of information, while the "receiving party" would then be the entity that receives such information, automatically or not. According to the proposed guidelines, "the receiving entity might not be the entity instructing the sending of information". Yet in the case of information that is transmitted automatically and thus purely received by the receiving party, the receiving party is not in a position to seek consent prior to receiving the information and it would be illogical for the "instructing" party to seek consent on behalf of the receiving party, given that the instructing party might be the device manufacturer, operating system developer or web browser developer - a third party without any knowledge of the identity of the relevant receiving party.

In addition, the aforementioned Recital 24 ePD emphasises the fact that the information whose access or storage is regulated is "part of the private sphere of the users". This express statement by the authors of the ePD is fundamentally incompatible with EDPB's attempt to broaden the scope of the ePD to cover information that has already left the private sphere of the users by virtue of its automatic transmission through the TCP/IP. Indeed, in a similar fashion, reference to "*information on the user's terminal device*" shows the intention of the ePD to cover specific information that is stored on and present within a user's terminal equipment; not to extent it to information which forms an inherent part of a transmission itself rather than the user's terminal equipment.

Moreover, TCP/IP is a generic protocol that was introduced in 1974, i.e. nearly 50 years ago - well before HTTP cookies were formally standardised in 1997. While the ePD makes multiple mentions of so-called cookies, it does not mention TCP/IP anywhere, which is evidence that its inclusion in the scope of the directive was never intended.

This is also supported by Opinion 9/2014 of the WP29 relating to the application of the ePD to device fingerprinting, contrary to the assertion made in paragraph 2 of the proposed guidelines that this same Opinion "*has already clarified that fingerprinting falls within the technical scope of Article 5(3) ePD*". In fact, Opinion 9/2014 of the WP29 only confirms that "*in a number of circumstances, the technology leads to the gaining of access to, or storing of, information on the*

*user's terminal device*" and recognises that a device fingerprint may be constructed from "*information elements [that] did not require the storage of, or access to, information*".

The EDPB's justification for attempting to extend the scope of Article 5(3) to apply to TCP/IP is that "*the abuse of those mechanisms (for example in the context of fingerprinting or the tracking of resource identifiers) [which] can lead to the application of Article 5(3) ePD*." (paragraph 42). This does not follow. Most obviously, the drafting of Article 5(3) is clear that its application is not dependent upon the intention underlying the storage or access of information on users' devices. If, as the EDPB suggests, Article 5(3) can apply to information transmitted from a user's device under the TCP/IP protocol, it will necessarily apply to all such TCP/IP transmissions regardless of what the recipient chooses to do with the information. The drafting of the ePD does not offer any mechanism to distinguish between "abusive" and "non-abusive" use cases. This would have severe consequences for the functioning of the internet, as all TCP/IP requests would be in scope of Article 5(3) and would therefore require consent unless strictly necessary.

Alternatively, if the EDPB intends to adopt this significantly broader interpretation of the technical scope of Article 5(3), we consider that it would be prudent for it to clearly define what amounts to an "abuse" of the TCP/IP mechanisms and expressly extend the "strictly necessary" exemption to include "non-abusive" use cases. Furthermore, the EDPB does not indicate why it does not consider such alleged "abuse" to already be covered by the GDPR rules on profiling (Article 4(4) GDPR and Recital 24), which already provide supervisory authorities with means of regulating various kinds of "tracking" or "fingerprinting" for profiling purposes.

The proposed guidelines also add to the confusion with the consideration paragraph 55 that Article 5(3) only applies to the gaining of access to IP addresses that originates from users' terminal equipment, and that it is for the receiving entity to ascertain such origin. An entity operating web servers has no legal nor technical means to identify whether the network makes use of several layers of Network Address Translations (NAT) - unless such entity provides otherwise ISP services and has assigned the IP address in question. This means that the proposed guidelines introduce a two-tier system by which a handful of companies would actually be in a position to demonstrate and benefit from the inapplicability of Article 5(3) to certain operations.

3) EDPB interpretation of the notion of "stored information" and "storage"

Article 5(3) ePD applies effectively to (i) "the storing of information [...] in the terminal equipment of a subscriber or user" or (ii) the gaining of access to information "already stored, in the terminal equipment of a subscriber or user".

As indicated above, the proposed guidelines misrepresent those two requirements by stating that there is no upper or lower limit in the ePD regarding either (i) the length of time that information must persist on a storage medium to be counted as stored or (ii) the amount of information to be stored. While the ePD does not contain an exact threshold in relation to information's retention

period, the word "already" introduces a notion of time which is completely ignored from the proposed guidelines. This approach is particularly problematic as the EDPB suggests as a result that any information "stored" in random-access memory (RAM) or in the cache of the central processor unit (CPU) is covered by Article 5(3) ePD.

Indeed, any operation over a communication network requires ephemeral storage in order to execute the intended computation. Such a temporary form of data storage is used for short-lived and transient workloads in the processing of instantaneous calculations, and the information does not persist for later retrieval.

For example, a website may include a Javascript code that carries out a calculation on the device in order to highlight a text element once the mouse hovers over it. The browser will as a result interpret the Javascript code by parsing and then executing it line by line using ephemeral storage (runtime environment). The process itself by which the execution of the code is carried out should not be viewed as "storing of information", since it does not persist for later retrieval, nor should it be viewed as gaining access to information "already stored", since the processing happens on the fly.

Such novel interpretation would also raise serious issues in terms of scope, in particular due to the proposed guidelines not specifying the scope of consent exemptions. For instance, any use of technologies such as Cascading Style Sheets (CSS) and Javascript to adapt and improve the visual layout of an online service (as per the example above or according to the device capabilities) would henceforth be considered in scope of Article 5(3) ePD and subject to user's consent in the absence of any updated EDPB guidance covering on the granular basis the various operations that are covered by the two exemption provided by the ePD.

In addition, the proposed guidelines create a confusion between access to information already stored on the terminal equipment and the data being inputted on websites by the users. The EDPB appears to consider "unique identifiers" or "persistent identifiers", "usually derived from persistent personal data (name and surname, email, phone number, etc.)" and on websites, generally "obtained in the context of authentication or the subscription to newsletters", can fall within the scope of Article 5(3) ePD, "as this information is stored temporarily on the terminal before being collected".

This position is not supported by the text of Article 5(3) ePD, which refers only to access to information already stored on the terminal equipment, and not to information entered by the user on a website. The potential temporary storage of information on the device does not imply that access to the information is achieved via this storage (in addition to the question of temporality already developed above). By opening the way to such an interpretation, expressed in a particularly lacunar way at the end of a short use case, the proposed guidelines lead to significant confusion between the scope of the ePD and that of the GDPR. This is a major topic that deserves, at the very least, to be addressed in a more nuanced way, taking into account the different scenarios.

Finally, the proposed guidelines 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) which creates confusion as regards the practical application of the notion of storage.

We wish to stress that the choice of words "already stored" by the legislator should not be disregarded, as it implicitly excludes instantaneous execution of code. This position is reinforced by the text of Recital 25 of the ePD which focuses on cookies, a clear example of actual storage - whereby the instructing entity actively selects which information should be stored and for how long (by specifying a time of expiry or by indicating that it should only remain active during the user's browser session).

4) Contradictions with national interpretations

Importantly, the proposed guidelines contradict interpretative guidance and recommendations on the concept of "gaining access" that have been issued by local regulators and that companies have made significant investments to comply with. This is completely ignored by the proposed guidelines, and antinomic to the EDPB's Statement on cooperation on the elaboration of guidelines "*Guidelines and Recommendations of the EDPB reflect the common position and understanding which authorities agree to apply in a consistent way*"[3]. It seems likely that the proposed guidelines go well beyond reflecting Data Protection Authorities' common position and understanding, as they reach surprising and disruptive conclusions that have never been considered before.

- On 20 December 2021, the Datenschutzkonferenz (German conference of data protection authorities) published guidance for "telemedia providers" in relation to the German implementation of the cookie rule[4], in which it stated the following (machine translation): "*An 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 that is transmitted inevitably or due to (browser) settings of the end device when calling up a telemedia service, this is not to be considered "access to information already stored in the end device. Examples of this are:*
• *the public IP address of the terminal device,*
• *the address of the called website (URL),*
• *the user agent string with browser and operating system version and*
• *the set language*."

This position was also confirmed by the local supervisory authority for the State of Baden-Württemberg in later guidance in March 2022[5], stating explicitly that (machine translation) "*[the German implementation of the cookie rule] only covers "access" to information if this is targeted.*

[3] https://edpb.europa.eu/news/news/2021/edpb-statement-edpb-cooperation-elaboration-guidelines_en
[4] https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf
[5] https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/03/FAQ-Tracking-online.pdf

*Both IP address and user agent are information that the browser automatically sends when a website is called up, without the provider of the [digital] service being able to influence this*".

- On 22 January 2021, the CNIL (French Supervisory Authority) joined an online conference[6] organised by national trade associations to provide clarifications over the French implementation of the ePrivacy rules, in which CNIL representatives stated that the use of TCP/IP is specifically not in scope of the ePD - provided that no cookie is passed in the http request. They further stated that the automatic receiving of the IP address does not constitute a "gaining of access" to users' devices.

These interpretations of which the proposed guidelines take no account and appear to invalidate, have led organisations to invest significant time and resources to ensure compliance of their services accordingly. The EDPB's proposed guidance would render this privacy-enhancing work obsolete and demonstrate to businesses that investment in user privacy is at risk of being wasted because of inconsistent regulatory guidance.

For example over the past decade, several analytics solutions[7] have been developed to allow the measurement of performance of websites and applications in a manner that does not pose any privacy risks while providing accurate measurements and not necessitating consent, precisely because authorities had not previously considered TCP/IP to be covered by the ePD. Yet by changing the meaning of "access", the EDPB would require these solutions to change their approach, and might significantly affect their legitimate business.

5) Lack of further guidance on consent exemptions

In its proposed guidelines, the EDPB explicitly states that "*[t]hese Guidelines do not intend to address the circumstances under which a processing operation may fall within the exemptions from the consent requirement provided for by the ePD*". Putting aside the various concerns with the proposed extension of the scope of Art. 5(3), the omission of any guidance as to which use cases might qualify for the necessity exemption will undercut any legal certainty that the EDPB wishes the proposed guidelines to provide.

Firstly, Opinion 4/2012 on Cookie Consent Exemption of the WP29[8] (to which the proposed guidelines refer in their very first paragraph) was never formally endorsed by the EDPB, and in fact it has even been disavowed by authorities[9] that adopted diverging guidance over the past decade (see in particular the WP29 position on first-party analytics).

[6] https://www.dailymotion.com/embed/video/k1CBd9Y3iOEm6wwCvb1

[7] For example, the CNIL, the Garante and the AEPD most recently have laid out practical requirements for audience measurement solutions to be exempted from the consent requirement of the ePD (https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies-solutions-pour-les-outils-de-mesure-daudience, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876 and https://www.aepd.es/guias/guia-cookies-analiticas-externas.pdf)

[8] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

[9] See footnote n°7

Secondly, Opinion 4/2012 explicitly states that it "explains how the revised Article 5.3 impacts on the usage of cookies but the term should not be regarded as excluding similar technologies". But all of the use cases it develops are firmly based on the premise of information being created and read on a device using a technology such as a cookie and completely ignore the TCP/IP mechanism. The reasoning in the WP29 Opinion therefore does not transpose well to this new interpretation and cannot be easily used to understand which use cases would not require consent under the revised ePD scope, because cookies and similar technologies share certain technical characteristics that are not shared by the TCP/IP mechanism. This is all the more critical due to the TCP/IP mechanism being the primary protocol that can be used by businesses to interconnect network devices on the internet and supporting a variety of use cases that are, by their technical nature, best suited to be covered by the two exemptions provided by the ePD.

Thirdly, because the ePD has been transposed in national law with significant levels of variations, the use cases locally covered by consent exemptions diverge significantly from one Member State to another and do not take good account of the technical scenarios and mechanisms which would be newly covered as a result of the EDPB's novel interpretation. For instance, while certain regulators provide exemptions for using technologies such as cookies for the management of advertising spaces[10] (such as the AEPD and Traficom, the Finnish competent authority over ePrivacy rules), others have specifically excluded their use (such as the CNIL)[11]. Similarly, the CNIL has started consulting with companies and other stakeholders to elaborate a comprehensive doctrine on both the scope and use of tracking pixels subject to consent, as well as those exempt from it[12].

By not providing guidance on exemptions in the light of the EDPB's novel interpretation of the scope of the ePD, the EDPB is effectively creating room for further divergent interpretations

[10] https://www.aepd.es/documento/guia-cookies.pdf "*Also belonging to this category, due to their technical nature, are those cookies that allow the management, in the most efficient way possible, of the advertising spaces that, as another element of design or "layout" of the service offered the user, the editor has included in a web page, application or platform based on criteria such as the edited content, without collecting information from users for other purposes, such as personalising that advertising content or other content."* and https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Sanoma%20Media%20Finland%20Oy.pdf *"According to Traficom's assessment, the purpose of the non-personalized distribution cookie on the front page is to enable a specific advertisement to be shown to Helsingin Sanomat readers once a day." and "Traficom considers that the non-personalized distribution cookie of the front page in question is necessary in the sense of Section 205 subsection 2 of the SVPL to provide a service explicitly requested by the subscriber or user".*

[11] For instance, in its cookie recommendation of 9/17/2020 (https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf), the CNIL included capping among advertising operations that have to be explained in relation to the purpose of "advertising" that is subject to consent (see point 15). See also point 55 of its "TikTok" deliberation (https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046977994/).
In addition, the CNIL specifically stated that capping cookies are not exempt, in its summary of the public consultation on its draft guidelines on cookies (https://www.cnil.fr/sites/cnil/files/atoms/files/synthese-contributions-cookies-et-autres-traceurs.pdf).

[12] https://www.fnps.fr/2023/10/24/lancement-de-trois-ateliers-de-concertation-par-la-cnil-sur-les-pixels-de-suivi-dans-les-emailing/

across Europe and economic inequalities between organisations operating in various jurisdictions, because the exemptions described in the WP29 Opinion do not match the technologies newly covered as a result of the EDPB's new interpretation.

6) Consequences

We would like to draw particular attention to the role of TCP/IP which is strictly necessary for routing traffic on the internet and inter alia:

- Displaying (non-targeted) advertisements on Internet content and service websites;
- Logging that an ad was delivered to count ad impressions in order to charge the advertiser accordingly;
- Detecting invalid or fraudulent traffic.

The majority of publishers rely on a third-party ad server to perform the operations listed above - integrated online platforms being the notable exception. This means that delivering an ad file to an IP address through TCP/IP constitutes a separate operation (i.e. a separate HTTP request) from delivering the content of the webpage hosted on the publisher's servers. TCP/IP is also used to log that an ad was delivered to count ad impressions in order to charge the advertiser according to the number of ads that were served or used to detect invalid or fraudulent traffic (e.g. internet bots that have datacenter IP addresses).

Under the proposed guidelines, these operations would fall within the scope of Art.5(3) ePD. It is worth stressing in this respect that the delivery of non-targeted advertising is leveraged by publishers to monetise their free content or services when they are accessed by users who have refused or withdrawn consent to read and write operations on their devices. In fact, authorities and privacy campaigners regularly promote contextual advertising as, in their view, a better option than targeted advertising from the perspective of user privacy - yet the proposed guidelines would necessarily discourage businesses from devoting resources to this form of advertising that is already less remunerative if it is subject to the same obligations as targeted advertising.

To date, there is no EDPB position recognising that such operations associated with the technical delivery and management of advertising are strictly necessary for the provision of the service explicitly requested by the user, namely the provision of the website or app (which would not exist without some form of funding or monetisation). Authorities' views on what is "strictly necessary" tend to focus purely on the actual delivery of the service from the perspective of the end-user, not the surrounding context without which the service would not even exist. In such a context, the revised scope of Art. 5(3) ePD introduced by the proposed guidelines would make such operations regarding contextual advertising subject to consent.

## Conclusions

We encourage the EDPB to observe the ePD's first objective to limit "*spyware, web bugs, hidden identifiers and other similar devices*" from entering a user's device "*in order to gain access to information, to store hidden information or to trace the activities of the user*" without their knowledge and therefore seriously intruding on the privacy of affected users (Recital 24 ePD). The amendments that were made in 2009 to the ePD confirmed the intent of the EU legislator to prioritise the serious threat to the privacy of users from such spywares and viruses (Directive 2009/136, Recital 65 and 66).

As mentioned above, the use cases primarily targeted by the EDPB in the proposed guidelines necessarily trigger the material scope of the GDPR and as a result are already subject to its obligations (Article 4(4) GDPR and Recital 24). Supervisory Authorities can already assess compliance of these use cases with the stringent requirements of the GDPR, including the appropriateness of the legal basis chosen by companies for such processing.

Such an excessively broad and unfit interpretation of the notions of "gaining of access" and "storage of information" is therefore not justified to ensure a high-level of protection of users' privacy, since it eliminates all distinction between operations that involve tracing users' activities and operations that are reasonably expected from users, such as the technical delivery of ads or fraud prevention, and instead broadly moves all information that originates through, or is interacted by, a user's terminal equipment, or any communication related thereto, into the scope ePD.

On the contrary, it removes the flexibility provided by the GDPR to justify where reliance on consent may not be preferable and renders the other relevant legal grounds in Article 6(1) GDPR inapplicable. This does not reflect the appropriate balance between the right to data protection and the freedom to conduct business, and ultimately undermines the warning function of consent. Users cannot make informed decisions on whether to give or withhold consent if service providers are required to request their consent for a whole range of practices, some of which are completely innocuous. In particular, it will inevitably lead to a disproportionate increase of the information and consent choices provided to users and exacerbate the so-called consent fatigue phenomenon that is already regularly called out in the online space. In that regard, the proposed guidelines and their timing do not appear consistent with the current cookie pledge initiative of DG Justice whereby companies are requested to make strong commitments that are intended to reduce consent fatigue.

The proposed guidelines as currently drafted will also create negative repercussions and legal uncertainty for companies operating in the online space, that will be decentivized from investing in privacy forward practices that ultimately benefit users and may lead to more content and services being placed behind paywalls. We urge the EDPB to revisit its position and appreciate the fact that there are real-life technical and business considerations that ought to be taken into account when prescribing any new rules affecting the digital advertising supply chain. In particular, the absence of any guidance relating to the two exemptions provided by the ePD in line with the

novel positions taken by the EDPB entails significant risks of discrepancies in their application by organisations, and therefore defeats the purpose of the proposed guidelines to remove ambiguities related to the material scope of Article 5(3) of the ePD.

Finally, we have previously been calling on lawmakers to understand the interplay between the ePD and the GDPR and focus on aligning the two rather than deviating from the principles adopted with the GDPR. The ePD was adopted more than 20 years ago in 2002, and the few amendments adopted in 2009 have not rectified the obsolescence of the text. The ePD does not reflect the significant evolutions of the technological landscape, and also lacks cohesion with the GDPR adopted in 2016. While the negotiations over the future ePrivacy regulation have not made significant progress over the past few years, this does not give the EDPB mandate to expand the scope of the ePD by means of soft law guidelines that further undermine its consistency with the GDPR and disregard the particularities of its transpositions in national law.

## List of signatories

IAB Europe: IAB Europe is the European-level association for the digital marketing and advertising ecosystem. Through its membership of national IABs and media, technology and marketing companies, its mission is to lead political representation and promote industry collaboration to deliver frameworks, standards and industry programmes that enable business to thrive in the European market.

Alliance Digitale: Alliance Digitale is the leading professional association for digital marketing players in France. It was formed in 2022 from the merger of IAB France and the Mobile Marketing Association France. Alliance Digitale's main mission is to structure the development of the digital marketing industry and promote innovative, responsible and interoperable solutions by defining industry standards and best practices. The association is also a privileged interlocutor for public authorities, the media and other professional organisations in matters of digital regulation and the promotion of an open Internet. The association brings together the vast majority of digital marketing players in France, representing more than 250 companies (Brands, Media, Agencies, Tech).

IAB Italia: IAB Italia is the Italian chapter of the Interactive Advertising Bureau, the leading association of digital marketing and advertising. Since 25 years it has significantly contributed to the diffusion of digital culture and to the acceleration of market growth in Italy through the development of ethical and sustainable communication.
IAB Italia pursues its mission through the realisation of vertical events, special projects, training activities and with IAB Forum, the largest Italian event dedicated to marketing and digital innovation on the most relevant issues for the industry, involving top national and international speakers. The Association has more than two hundred members, among the main Italian and international operators active in the interactive advertising market.

IAB Spain: IAB Spain undertakes a comprehensive mission as a forum for meeting and representing the digital advertising industry in Spain. Since its inception in 2001, IAB Spain has played a crucial role in the promotion and development of digital advertising. IAB Spain's mission unfolds on various strategic fronts: With the aim of contributing to the proper regulation of the sector, by contributing, assisting, and fostering conversations with public administrations. Furthermore, IAB Spain proactively works on creating industry standards, with the goal of establishing guidelines and best practices that promotes the sustainable and ethical growth of digital marketing, advertising and therefore promoting innovation and positivities for the society. Members of IAB Spain encompass a wide range of stakeholders in the digital advertising ecosystem, including digital and audiovisual publishers, platforms, media agencies, marketing and advertising agencies, advertisers, consulting firms, technology providers, advertising networks, and others, such as eCommerce and research institutes.

IAB Polska: IAB Polska is a Polish advertising industry organisation that unites and represents entities of the interactive industry. IAB Poland members include more than 200 companies, including the biggest web portals, global media groups, interactive agencies, media houses and technology providers. In 2012 the organisation received the MIXX Awards Europe, honouring the best IAB bureau in Europe.
The mission of IAB Poland is to support development of the Internet industry and take regulatory actions to enhance the competitiveness of the market, conducting research projects, leading educational programs and providing legal protection.

IAB Sweden: IAB Sweden is the leading association for interactive advertising and digital marketing in Sweden. By gathering stakeholders throughout the nations digital marketing ecosystem, IAB Sweden advances the progression of a well-functioning and sustainable industry. The fundamental mission of IAB Sweden is to unite, educate and promote the market for digital and interactive advertising in Sweden.

SPIR: For over 20 years, the Association for Internet Progress (SPIR) represents the most important players of the Czech Internet economy from among media publishers, media agencies and technology companies with an annual turnover of more than 37 billion Czech crowns (1,5 billion EUR). The services offered by SPIR members are used by over 90% of the population of the Czech Republic. Member companies pay 3 billion Czech crowns (120 million EUR) a year in taxes and other fees to the state budget and employ 7,500 people throughout the Czech Republic. SPIR operates the only official measurement of Czech Internet traffic NetMonitor, monitoring of Internet advertising AdMonitoring and provides expert analyses of the development of the Czech Internet market.

VIA Nederland: VIA is the industry association that looks, thinks and works more broadly. We believe that connection is the engine of progress. By bringing together a wide variety of persons and disciplines, an environment is created in which people, companies and the marketing profession can continue to grow. By working together intensively and by sharing knowledge and experiences we seek to predict and interpret developments and trends in the market and where possible determine or influence standardisation, legislation and (self-)regulation.