

**DMA France** is the leading professional association for data marketing industry in France. DMA France's mission is to federate, promote and enhance the value of the Data and Marketing industry in France in order to encourage their development. DMA France is member of FEDMA, the Federation of European Data and Marketing.

DMA France welcomes the EDPB consultation process on the draft guidelines and the opportunity to provide comments.

## **EXECUTIVE SUMMARY**

- DMA France is concerned that not all national supervisory authorities responsible for the implementation and enforcement of the ePrivacy Directive are members of the EDPB. It is thus unclear to what extent these authorities were involved in the drafting of the Guidelines and to what extent they will implement them.
- The Guidelines refer to the harm posed by alternative tracking solutions. It would be fundamental to provide an analysis and measurement over the harm or potential harm to users' privacy deriving from such solutions.
- DMA France questions the EDPB's broad interpretation over the notion of "gaining access" which would also cover the passive receiving of information required for the transmission of communications, thus applying to any basic Internet protocol.
- The broad interpretation provided by the Guidelines over the notion of "gaining access" would exacerbate "consent fatigue" with no additional value to the data subject's privacy. The Guidelines should rather or additionally provide guidance over the exemptions to the consent requirement and the conditions for further processing after the storing or gaining access to data.
- DMA France also contests the inclusion of email pixels in the scope of the Guidelines as they do not technically involve any "entering in the user's terminal" or "information storage" or "gaining access to information" in the user's terminal equipment, whereas only HTTP requests are performed.
- This inclusion of email pixels in the scope of the Guidelines, if not accompanied by a functional or technical exemption of consent, would also adversely affect marketers' reliance on (i) the soft opt-in principle as per Article 13(2) ePD as well as (ii) the opt-out regime for direct marketing in Business-to-Business relations in those Member States, including France, which opted for this system as per 13(3) ePD.

## AREAS OF CONCERNS

The responsibility to oversee the implementation and enforcement of the ePrivacy Directive does not always fall on the national Data Protection Authorities (DPAs). Some Member States have entrusted this responsibility to their national telecommunications supervisory authority. As these national bodies are not part of the EDPB, it is unclear to what extent they might have been involved in the drafting of these Guidelines, and it also raises the question of whether they could endorse them (especially if they did not have any say over them).

We also urge the EDPB to clarify the concerns over the use of alternative tracking solutions mentioned throughout the draft Guidelines, especially on paragraph 3, which would be the drivers of these Guidelines. Given the significant implications of the EDPB's interpretation of Article 5(3) ePD, it is fundamental that these Guidelines are based on actual and measurable evidence about the harm or potential harm to users' privacy stemming from the alternative solutions for tracking internet users.

In this regard, we overall regret that the EDPB's interpretation over Article 5(3) ePD, especially the notion of "gaining access", seems to unnecessarily expand the scope of the Article and the consent requirement to the implementation of any Internet protocol as well as non-privacy intrusive practices. We would like to remind that the ePrivacy Directive was not adopted to impede the activity of the actors of the Internet, but to conciliate their freedom to conduct a business with the protection of the privacy of users of telecommunications services. Instead, the proposed extension of the scope of Article 5(3) ePD does not only seem to override a competence which should only belong to the EU legislators, but it would also make consent meaningless vis-à-vis the users' increasing "consent fatigue" by adopting a draconian legalist approach. We would therefore like to remind the EDPB **that [the ePrivacy Directive's REFIT evaluation](#) explicitly stated that adopting a consent rule that is over-inclusive is neither effective nor efficient**, as it results in covering non-privacy intrusive practices. It would have been more beneficial to focus or accompany these Guidelines with an analysis over (i) the extent of the Directive's exemptions to the consent requirement and their application in the context of the evolving data-driven technology landscape, as well as (ii) the GDPR's rules and legal bases on further processing (Article 6(4) GDPR) after the storing or gaining access to data.

In particular, we believe that the draft Guidelines raise significant concerns both from a technical and legal perspective regarding the application of Article 5(3) of ePD. While the EDPB's broad interpretation of the notion of "gaining access" risks applying to any internet communication, the inclusion of email pixels in the scope of Art. 5(3) ePD does not only seem unjustified from a technical point of view, but it also creates legal uncertainty with other provisions of the Directive.

## RECOMMENDATIONS

In light of the above, DMA France therefore recommends to:

- 1) exclude from the draft notion of "gaining access" passive receiving of information resulting from exchanges of information initiated by the user's terminal equipment;
- 2) exclude email pixels from the scope of Article 5(3) of the ePrivacy Directive;
- 3) clarify the Guidelines' interplay with Article 13(2) and Article 13(3) of the ePrivacy Directive.

**1. Exclude from the draft notion of “gaining access” passive receiving of information resulting from exchanges of information initiated by the user’s terminal equipment**

We believe that draft Guidelines’ interpretation of the notion of “gaining access” is excessively broad. As per the EDPB’s draft, the proposed “Criterion D” would trigger the application of Art. 5(3) ePD whenever the accessing entity wishes to gain access to information stored in the terminal equipment and actively takes steps towards that end, implying that the accessing entity proactively sends specific instructions to the terminal equipment in order to receive back the targeted information.

Considering any basic internet protocol as an instruction given to the user’s device, with this extension of the scope of Article 5(3) ePD to IP addresses in particular, is a factor of legal uncertainty as it would constitute significant change in the way the ePrivacy Directive will be applied and implemented that was not originally envisaged.

Despite the EDPB’s focus on the “pro/active” approach by the external entity to gain access to information, the draft Guidelines also include use cases where this entity is merely a passive recipient of such information following an active action initiated by the terminal equipment. This would be the case, for example, of a terminal equipment sending a request for an IP address to the DHCP server to connect to the network. Such request would also trigger a provision of information by the terminal equipment to the DHCP server: though the server is not the entity “actively” taking steps to gain access to the information, Art.5(3) would apply according to the draft Guidelines.

Under the current draft Guidelines, even simple Internet browsing by a user would constantly trigger the application of Article 5(3) ePD for the display of any website page or email, since the loading of any online resource would involve HTTP requests instructed by the terminal equipment. The EDPB’s broad interpretation of “gaining access” would thus mean that every communication over the internet is somehow “gaining access” to information within scope of Art 5(3) ePD as a result of the implementation of basic internet protocols which necessarily require an exchange of information. In doing so, the draft Guidelines’ interpretation also captures technologies and basic technical operations which are not necessarily related to marketing or advertising purposes as it could be the case of cookies, nor to the interception of information. This broad interpretation by the EDPB of this notion of access would imply that all communications on the Internet involve access to the user’s terminal and fall within the scope of Article 5(3) ePD due to the implementation of any Internet protocol that requires an exchange of information.

We therefore argue that the proposed notion of “gaining access” constitutes a stretching of the material scope of the ePrivacy Directive which would apply to use cases going beyond the concept of “tracking technologies”. The current lack of progress in the trilogues of the ePrivacy Regulation cannot justify a change in the scope of the Directive through guidelines: any deviation from the material scope of the ePD can only be the result of the EU ordinary legislative procedure.

As a result of extending the scope of the Directive, it is therefore unclear how a consent requirement for non-intrusive technical operations which do not necessarily involve the processing of personal data would bring a better protection of privacy to the user. This also seems detrimental to the user’s online experience as they will be asked to engage with additional consent requests, likely exacerbating the so-called “consent fatigue”. In this context, we would like to remind the EDPB that the European Commission is working on an initiative of voluntary commitments, named “Cookie Pledge”, to address, among others, “consent fatigue” and simplify the information that users must process in order to provide informed consent. Despite its title, the initiative will not only be applicable to the use of cookies, but to all forms of online technologies whose use requires prior consent. However, though the

EDPB expressed support to the Cookie Pledge's objective, the new interpretation put forward in the draft Guidelines would result in a massive increase of consent requests for the users, along with a surge in the amount of information that users should process. As such, even if companies wished to sign the Commission's Pledge, it is unclear how they could ensure informed consent while explaining in clear and concise language the purpose of extremely technical processing as well as the nature of the data they wish to process.

## **2. Exclude email pixels from the scope of Article 5(3) of the ePrivacy Directive**

The draft Guidelines also take the view that email pixels are subject to Art. 5(3) of the ePrivacy Directive on the basis that they store and gain access to information on the user's terminal equipment. We would however like to nuance this opinion in light of arguments above on the broad notion of "gaining access" and the technical nature of email pixels. We also feel it's important to reiterate some of the points highlighted in the note sent to EDPB by DMA France and GESTE on April 24, 2023.

It is important to remind that recital 24 of the ePrivacy Directive states that the technologies covered by article 5(3) are technologies that enter the user's terminal equipment 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.

E-mail pixels are usually a 1px-by-1px transparent image, but they can also be any image included into the header, body, or footer of an email. When an email is opened, all integrated images are usually loaded, sending a request to the server (HTTP request). Through this basic HTTP request, it is possible to infer that an interaction has occurred with the email. It is this HTTP request (informing of the call of the image) that allows to measure the receipt/opening of the email and not the image itself, which is the same for all recipients.

Though email pixels could be considered at first sight similar to tracking cookies, they do not technically involve any "entering in the user's terminal" or "information storage" or "gaining access to information" in the user's terminal equipment, whereas only HTTP requests are performed.

When using email pixels, the gathering of information is carried out solely on the basis of the message sent to the server when the HTTP request is executed, and not with the information stored or already existing in the user's terminal equipment. Insofar as no "entering in the terminal", "information storage" or "gaining access to information" operation is carried out through the use of this technology, it cannot therefore be included in the scope of Article 5(3) of the ePrivacy Directive.

In this regard, it is important to point out that email pixels only report information of received and opened emails. This valuable information is used worldwide by all stakeholders (including DPAs) to conduct their emailing activities and to manage their communication policies, including by limiting the sending of emails to individuals who are interested by them and avoiding burdening the ones who are not. It is for instance considered a good practice by mailbox service providers not to send emails to individuals who are not reading them.

We point out that the argument that the information is stored in the user's terminal equipment when the images/pixels are loaded into the user's browser/message reader is not reflected in the draft ePrivacy Regulation currently under negotiations between the EU co-legislators. As mentioned in our introductory remarks, the Directive's REFIT underlined that adopting a consent rule that is over-

inclusive is neither effective nor efficient, as it results in covering non-privacy intrusive practices. We believe that this is the case of email pixels given their very limited and legitimate purpose.

We would also like to add that not applying Article 5(3) of the ePrivacy Directive to email pixels would not entail that the use of such means would remain uncontrolled. It would still be secured by the requirements of the GDPR, with the same objective of protecting the privacy of individuals, whenever there is a processing of personal data collected from the HTTP request triggered by the loading of the email pixels.

### **3. Clarify the Guidelines' interplay with Article 13(2) and Article 13(3) of the ePrivacy Directive**

The extension of the application of Article 5(3) ePD raises another significant question in regard to another provision of the ePrivacy Directive. Article 13(2) ePD enables a natural or legal person who “obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service” to use these electronic contact details for “direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object”.

In other words, this provision allows marketers to rely on the so-called soft opt-in to send direct marketing emails to existing customers without having to ask for their consent for sending each new email, though customers must always have the possibility to opt-out. As email pixels are embedded in those emails, the application of the draft Guidelines would still impose on marketers the obligation to obtain a separate consent, even when relying on the soft opt-in, in order to use email pixels and measure the effectiveness of their email campaigns with existing customers. This would make marketers' use of the soft opt-in under Article 13(2) ePD meaningless.

In parallel, Article 13(3) ePD enables Member States to determine the direct-marketing regime in Business-to-Business (B2B) relationships. In those countries, including France, where marketers can reach out to another legal person on the basis of opt-out, the extension of the consent requirement to email pixels would prevent marketers from measuring the performance of their B2B campaigns unless they switch to an opt-in system, making the Article 13(3) ePD meaningless.

We therefore stress the need to exclude email pixels from the scope of Article 5(3) ePD, or at least, to carve out an exemption to the consent requirement to ensure consistency with Article 13(2) ePD and Article 13(3) ePD.