Advertising
Information
Group

SUMMARY

1. The Advertising Information Group (AIG) (transparency number: 11220347045-31) welcomes the opportunity to respond to the European Data Protection Board's (EDPB) Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive adopted in November 2023.

2. Whilst we wholeheartedly support and respect Article 7 (Respect for private and family life) and Article 8 (Protection of personal data) of the Charter of Fundamental Rights, we strongly believe there must be an equitable balance between confidentiality of private communications and the sustainability and freedoms of industry.

3. We challenge the notion of the terminal equipment being fully part of the user's private sphere; and the idea that it is somehow "gaining access" even if information flows directly because of voluntary user action.

4. The guidelines appear to affect other parts of the ePrivacy Directive. In particular, it renders a marketers' use of the soft opt-in under Article 13(2) meaningless.

5. It is not clear whether the EDPB has considered its competence properly to issue such guidelines especially when EDPB members may not have direct jurisdiction over the local implementation of the ePrivacy Directive.

6. The broader notion of information must be subjected to the same level of protections to personal data is untenable, especially when considering that non-personal data is not within the scope of GDPR.

7. Rather than taking a blanket view of terminal equipment being part of the private sphere, a more granular examination of what information gets revealed under what circumstances and user controls over that may serve better to balance functionality, transparency, and respect for privacy.

DETAIL

8. The Advertising information Group (AIG) (transparency number: 11220347045-31) welcomes the opportunity to comment on the European Data Protection Board's (EDPB) Guidelines 2/2023 on the Technical Scope of Art. 5(3) of ePrivacy Directive (ePD) adopted in November 2023.

9. AIG is an informal network of European advertising and media associations that brings together various parts of the advertising industry, and this submission comments on points contained in the proposal that are relevant to the advertising industry.

10. Advertising and marketing are essential for the financing of free media, culture and sport. Targeted, data-driven advertising and marketing carries benefits for advertisers, service providers and users alike. Firstly, it facilitates users to see more timely and relevant ads, which leads to a better and more personalised user experience whilst at the same time optimising consumer engagement with brands. Secondly, users who agree to providing (pseudonymised) data get access to quality content in exchange.

11. Given that trilogue negotiations on the draft e-Privacy Regulation have stalled, we recognise the need to conduct a technical analysis on the scope of application of Article 5(3) ePD to ensure it remains fit for purpose and relevant given recent technological changes. Hence it is our sincere hope that an amicable solution can be found that

addresses the challenges of the digital economy, ensures fair competition and the long-term sustainability of all economic players, and respects the privacy of citizens.

12. Whilst we wholeheartedly support and respect Article 7 (Respect for private and family life) and Article 8 (Protection of personal data) of the Charter of Fundamental Rights, there must be an equitable balance between confidentiality of private communications and the sustainability and freedoms of industry.

13. Specifically, Article 11(2) of the Charter of Fundamental Rights protects media freedom and pluralism – this has been interpreted to also provide protection against legislative measures jeopardising the financing conditions of the media. In addition, Article 16 also protects the right to conduct a business. Many businesses and charities rely on email marketing to promote goods, services and other activities. It is vital to marketers to understand the effectiveness of their email campaigns and how their customers interact with them.

14. We would also like to respectfully point out that one of the key aims set out in Article 1 of the ePD is not only to protect privacy and confidentiality but "to ensure the free movement of such data and of electronic communication equipment and services in the Community".

15. It is on this basis we have six key concerns:

    - That the EDPB guidelines pushes for a maximalist interpretation of "gaining access" to information stored on the terminal equipment without proper consideration of the evidence.
    - The EDPB guidelines do not present a convincing case to demonstrate how the private sphere extends to information which is essentially voluntarily requested by the user's terminal equipment and does not identify the user.
    - The notion of storage seems to be incorrectly applied to URL or pixel tracking which are set dynamically. They do not "store" information in the way that a cookie is written to the terminal equipment.
    - The marketers' use of the soft opt-in under Article 13(2) ePD is rendered meaningless under these guidelines.
    - It is unclear whether the EDPB has the competence to issue such guidelines especially when its members may not have direct jurisdiction over the local implementation of the ePD.
    - It is difficult to reconcile the idea that all information must be protected to the same standard as personal data, especially when GDPR does not apply to non-personal data.

"Gaining Access" and the notion of storage

16. Article 5(3) of the ePD concerns itself with "*the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user*". We would argue that the key word here is "access" which implies an active action to obtain information rather being the passive recipient of information.

17. The EDPB guidelines also refer to "*the accessing entity to proactively send specific instructions to the terminal equipment in order to receive back the targeted information*" but does not consider that in some instances it is the terminal equipment that initiates the process.

18. We outline the following examples to illustrate these points:

- HTTP header requests
  HTTP header requests containing information like the user agent string and accepted encoding methods that are automatically sent with each website request. It is important to highlight here that it is the user's terminal equipment that initiates the HTTP header request to the web server to obtain information such as HTML files. Information is transmitted automatically by the user accessing the page. There is no proactive instruction by the server to the terminal equipment to provide information – the transmission is initiated by the terminal equipment, based on world wide web protocols. Nor is there an instruction to store this information either.

- IP addresses
  IP addresses are fundamental to how terminal equipment connect to networks. The terminal equipment, in this case the DCHP client, on connecting to the network will try to discover DHCP server to request an IP address. In the process of address allocation, the terminal equipment 's MAC address is revealed to assign it an IP address. This is to differentiate it from other terminal equipment that might be connected to the network, and for the terminal equipment to know that the message from the DCHP server is intended for it.

- URL tracking
  URL tracking involves clicking on a link embedded in a website or email. It requires the affirmative action of the user to click on the link and does not convey any personal information. Tracking links also work by redirecting clicks from the original link to a tracking link that contains additional parameters. When a user clicks on the tracking link, the tracking software records the information about the click, such as the source, location, and campaign.

  The core of URL tracking is appending a tracking token or ID to a URL link. When a user clicks on that tracked link, the tracking ID gets sent to the domain that is being linked to. UTM codes are also known as UTM parameters — or tracking tags, are typically used to by marketers to track the metrics and performance of a specific marketing campaign. A UTM (Urchin Tracking Module) code is a snippet of text added to the end of a URL. UTM codes can contain up to five parameters: campaign, source, medium, content, and term.

  Consider the following example URL which utilises UTM codes:

  http://anexampleurl.com?utm_campaign=blog_post &utm_medium=social&utm_source=facebook

  Breaking this example into to its constituent parameters reveals the following information:

Parameter	Explanation
http://anexampleurl.com:	This is the base URL.
?	This signals that a string of UTM parameters will follow.
utm_campaign=blog_post	This is the first UTM parameter, which shows that the visitor engaged with a blog post.
&:	This symbol separates UTM parameters.
utm_medium=social:	This is the second parameter, which shows that the visitor was referred by social channels.
&:	This symbol separates UTM parameters.
utm_source=facebook:	This is the last parameter, signalling that the visitor came from Facebook.

  In other words, URL tracking just captures the click event with a referrer token. It does not automatically collect identifying information about the specific user who clicked the link. The token itself typically has no intrinsic meaning about the user. The target website that loads still only sees the request coming from the user's terminal equipment, with no additional user details. Information like IP address may get logged as with any website request, but URL tracking itself does not facilitate transmitting additional user identity or attributes.

- Email pixels

  Tracking pixels collect information on what type of terminal equipment was used to open the email; when the email was opened; how long the message opened for; how many times the message was re-opened; and whether any links within the message were clicked on.

  Tracking pixels do not collect sensitive information, they are not saved to the terminal equipment and do not collect any information outside of the engagement with the email they were embedded in. If the user was already on an email list, then the company or organisation already has their name and email address. In this instance, the tracking pixel helps the company see which emails that user was interacting with and how they were interacting with it.

19. These examples challenge the notion of the terminal equipment being fully part of the user's private sphere and the idea that it is somehow "gaining access" even if information flows directly because of voluntary user action.

20. The view above is not unique given that German data protection authorities take a similar position. On 20 December 2021, the Datenschutzkonferenz (German conference of data protection supervisors) published guidance[1] for "telemedia providers" which stated (page 8):

> *"Ein Zugriff setzt eine gezielte und nicht durch die Endnutzer:innen veranlasste Übermittlung der Browser-Informationen voraus. Werden ausschließlich Informationen, wie Browser- oder Header-Informationen, verarbeitet, die zwangsläufig oder aufgrund von (Browser-)Einstellungen des Endgerätes beim Aufruf eines Telemediendienstes übermittelt werden, ist dies nicht als „Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind", zu werten. Beispiele dafür sind:*
>
> - *die öffentliche IP-Adresse der Endeinrichtung,*
> - *die Adresse der aufgerufenen Website (URL),*
> - *der User-Agent-String mit Browser- und Betriebssystem-Version und*
> - *die eingestellte Sprache."*

21. A machine translation of the above text provides 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 that is transmitted inevitably or due to (browser) settings of the end device when a telemedia service is accessed, this is not considered "access to information that is already stored in the end device". Examples of this are:*
>
> - *the public IP address of the terminal device,*
> - *the address of the website accessed (URL)*
> - *the user agent string with browser and operating system version and*
> - *the language set."*

22. Furthermore, in these guidelines the German authorities contrasted these examples with the execution of JavaScript code to read and transmit the properties of the terminal equipment to a server to create a fingerprint.

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

23. This creates an important distinction between a) the implementation of communication technology protocols, which necessitates the exchange of information, and b) the interception of information and or the unwitting or surreptitious divulgence of information.

24. However, taking a maximalist interpretation of gaining access could mean that every communication over the internet is somehow "gaining access" to information and is therefore within scope of Article 5(3) of the ePD.

Interplay between Article 5(3) and Article13(2) of the ePD

25. One of the unintended consequences of the guidelines is its impact on other provisions within the ePD. Article 13 (2), for example, 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, of course, must always have the possibility to opt-out.

26. Given that email pixels are embedded in those emails, application of the draft guidelines would in effect mean that marketers would still be obliged to obtain a separate consent, even when relying on the soft opt-in, to use email pixels and measure the effectiveness of their email campaigns with existing customers.

27. Hence, this would make marketers' use of the soft opt-in under Article 13(2) ePD meaningless. We would argue that this creates an imbalance between the right to privacy and the right to conduct a business guaranteed under the EU Charter of Fundamental Rights.

Competence of the EDPB

28. Many Member States have multiple supervisory authorities with competences related to the provisions adopted under the ePD[2]. This is not unusual given that Article 15(a) of the ePD explicitly provides that more than one national body may be competent to enforce its provisions. What this means in practice though is that EDPB members do not have direct jurisdiction in every Member State over the local implementation and enforcement of the ePD. Hence this raises an important question whether these guidelines could be applied consistently across Member States given that:

    - Local ePD regulators have differing enforcement powers and, in several cases, the ePD is supervised by multiple regulatory authorities.
    - The EDPB has no legal authority over non-EDPB members.

29. The second point is even more pertinent given that the EDPB clarified in its own Opinion 5/2019[3] that "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."

30. Therefore, it is not entirely clear on what legal basis these guidelines are based on. Without this clarity it is only likely to create further uncertainty around the proper legal interpretation and application of the ePD.

[2] ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation – Final Report. European Commission. https://digital-strategy.ec.europa.eu/en/library/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data

[3] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. EDPB. Adopted on 12 March 2019. https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

CONCLUSION

31. The EDPB guidelines also explains that the notion of information is applies much broader than the notion of personal and is within scope of the ePD. This is without dispute, but guidelines seem to imply that this broader notion of information must be subjected to the same level of protections to personal data is untenable, especially when considering that non-personal data is not within the scope of GDPR.

32. Rather than taking a blanket view of terminal equipment being part of the private sphere, a more granular examination of what information gets revealed under what circumstances and user controls over that may serve better to balance functionality, transparency, and respect for privacy. In any case, such interpretations should also consider the effect it may have on other provisions contained within the ePD.

33. Finally, there are lingering questions over the legality of these guidelines and whether they could be applied consistently across every Member State. Without addressing these fundamental questions upfront, it only serves to throw up more legal uncertainty around the proper interpretation and application of the ePD.

Advertising Information Group

27 December 2023