EGTA FEEDBACK TO THE EDPB CONSULTATION ON DRAFT GUIDELINES 2/2023 ON TECHNICAL SCOPE OF ARTICLE 5(3) OF THE EPRIVACY DIRECTIVE

egta is the media trade body for television and radio advertising, representing over 170 companies in Europe and beyond. egta members come from both public and private sectors and cover respectively 75% and 50% of the total TV and radio ad spend in Europe, thus playing a fundamental role in the sustainable funding of the European audiovisual and radio industries.

- **Introduction**

We welcome the opportunity to provide feedback on the European Data Protection Board's (EDPB) draft Guideline 2/2023 on the Technical Scope of Article 5(3) of the ePrivacy Directive. We equally acknowledge the relevance of clarifying the application of the current rules to different technical solutions considering industry evolution and to ensure regulatory harmonisation.

However, we consider that the proposed approach would excessively limit interactions between a service provider and a user, or subscriber, forcing service providers to either obtain consent or rely on the "strictly necessary" exemption, even when these interactions do not have material privacy implications. It may also increase the volume of TV and radio operators' content that is behind paywalls. There is concern amongst egta member companies that operations essential to non-personalised advertising and contextual advertising would be affected by the guidelines. Non-personalised advertising is used by publishers to monetise their free content or services when they are accessed by users who have refused or withdrawn consent for read/write operations on their devices. This case is especially relevant for sales houses because this type of advertising is an alternative means of monetising content (although to a lesser extent) in the face of the drop in consent that are being experienced due to Cookie guidelines and the disappearance of third-party cookies. Finally, the proposal seems at odds with the many discussions on consent-fatigue, and the recent attempts by the European Commission to reframe cookie banners.

- **Our comments**

1- Gaining access

We challenge the notion of the terminal equipment being fully part of the user's private sphere, as well as the idea that it is "gaining access" even if information flows directly because of voluntary user action. As per the EDPB's draft, the proposed "Criterium 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 to receive back the targeted information.

We further note the EDPB's focus on the accessing entity's proactive approach to gain access to information. Yet, the use cases included in the draft guidelines refer to entities that are merely passives recipients of the information, following an active action initiated by the terminal equipment.

Such is the case when a terminal equipment sends a request for an IP address to the DHCP server to connect to the network. This request would equally trigger a provision of information by the terminal equipment to the DHCP server. While the server is not the entity actively taking steps to gain access to the information, article 5(3) would apply according to the guidelines proposed by the EDPB.

We believe that the Guidelines should exclude the passive receiving of information required for the transmission of communications, and therefore align with the ePrivacy Directive's first objective to protect the private sphere of users in the scenarios where there is active action to gain access to the user's terminal.

National Data Protection Authorities have rejected such an expansive interpretation of article 5(3). For example, 2021 guidance by the German Conference of Data Protection Authorities clearly states: "*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.*

In contrast, it is already considered access to information on the end user's terminal equipment if the properties of a terminal are actively read - for example, by means of JavaScript code - and transmitted to a server for the creation of a fingerprint."

This position was reiterated by the Local Supervisory Authority for the State of Baden-Württemberg in guidance from March 2022 where it was explicitly stressed that the German implementation of the cookie rule "*only covers 'access' to information if this is targeted. 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.*" Exemptions to article 5 (3) of the ePrivacy are also intended for measurement purposes. Both the French and Italian Data Protection Authorities in 2023 and 2021 respectively allow for the measurement of performance of websites and applications in such ways that does not pose any privacy risks, without requiring consent.

2- IP-based tracking

In the TV business, IP addresses are increasingly essential components of electronic communications. Such advertising solutions are important tools for publishers and their sales houses to maintain free access to their content on websites, mobile apps, and CTV.

While we acknowledge the point made in paragraph 3.3 of the proposed guidelines, we would like to stress that the reading of IP addresses can be done without including any tracking. Indeed, in the absence of user consent, the instant reading of the IP address for advertising purpose will not involve any tracking of profiling activity – both in the case of IPv4 and IPv6. In that sense, the relevant operators can offer advertising solutions that can technically exclude user profiling, IP achieved/storage, and user tracking.

Ensuring whether the IP address originates from the user's devices implies a technical and legal capacity to access information in advance. In this instance, access would still be necessary, regardless of any expression of user consent. While this may theoretically take place, the said information is only in the possession of internet providers, and out of reach of sales houses and their tools for practical and privacy reasons.

In addition, it should not be considered a viable solution to have the instant reading of IP address fall in scope of article 5 (3) of the ePrivacy Directive. The opposite would only lead to putting *spyware, web bugs, hidden identifiers and other similar devices* at the same level as IP address reading for advertising purposes that does not include any tracking: both of which are incomparable from a privacy perspective and not aligned with the objectives of the ePrivacy Directive as outlined in recital 24.

- **Conclusion**

Instead of adopting a broad view which considers terminal equipment as being part of the private sphere, and which would force Article 5(3) to apply to all routine, low-level exchanges of information across the internet (which are fundamental to its functioning), a more detailed analysis of the information disclosed under specific circumstances and the corresponding user controls could enhance the balance between functionality, transparency, and the right to privacy.

It is paramount to acknowledge that the purpose of the ePrivacy Directive is not to hinder internet activity but rather to reconcile the freedom to conduct business with the protection of the privacy of users of electronic communications services. The lack of progress in the trilogue negotiations on the ePrivacy Regulation does not justify attempting to expand the scope of the existing ePrivacy Directive via guidelines.