

## ACT COMMENTS ON EDPB DRAFT GUIDELINES ON THE TECHNICAL SCOPE OF ARTICLE 5(3) OF THE EPRIVACY DIRECTIVE

**Impact on privacy preserving technologies.** Audiovisual services rely on a number of privacy preserving technologies to avoid encroaching unnecessarily on users' privacy. However, some of the concepts outlined in the guidance could undermine the ability to rely on these privacy preserving technologies (ie. URL tracking or pixels). This could lead to more reliance on cookies, going against on-going policy objectives of the European Union, such as reducing cookie banner fatigue.

**Risk and explainability.** The draft guidance could essentially make consent required for a wide variety of innocuous and non-intrusive processes where there are minimal risks for end-users privacy. However, due to the extreme technical nature of these processes, obtaining valid GDPR consent is just not possible (eg. via cookie banner-like solutions). The extended scope therefore puts into question the very existence of these processes.

**EDPB competence.** In some European territories, Data Protection Authorities (DPAs) do not have jurisdiction or competence for interpreting and enforcing the national measures implementing the ePrivacy Directive (ePD). For instance, telecom authorities are sometimes responsible. As far as we are aware, only GDPR supervisory authorities were involved in the drafting of this guidance, which could prove problematic with its application if the non-DPA regulators do not share the EDPB's expansive interpretation of the ePrivacy Directive.

**Notion of 'gaining of access'.** The wide interpretation of this concept set out in the draft guidelines implies that the mere usage of specific protocols (eg. HTTP) are akin to instructing a user's terminal equipment to send information. This is not in line with the general understanding of the term "gaining of access" among service providers and even DPAs, at least in a number of member states<sup>1</sup> and could have far-reaching consequences such as leading to worsening consent fatigue undoing some of the ambitions set out by the cookie pledge. The expansive notions also prescribe a novel interpretation of existing technologies, in particular of the Transmission Control Protocol (TCP).

**Notion of 'terminal equipment'.** The guidance for the "notion of terminal equipment" is unclear. For instance, it is unclear from §15 and §16 whether - in an environment including a router, a set-top box and a connected TV environment - all of the devices are individually terminal equipment or whether they collectively constitute terminal equipment. This may have implications with regard to who may have to collect consent.

**Notions of 'Stored Information' and 'Storage'.** According to the guidance, accessing information ephemerally stored in RAM or even CPU cache would fall within the scope of art. 5(3). This could imply that merely interacting with terminal equipment would require user consent unless it is necessary for the provision of a service, which appears to go beyond the intent of the legislators. For example, following the reasoning in §61-63 of the guidance, a user's voluntary submission of a review by clicking a star rating could constitute "storage" subject to art. 5(3) because their clicking on the star rating triggers an event and thereby causes information to be stored in RAM and cache. The effect is to expand the scope of art. 5(3) to include low level technical interactions, but without a corresponding expansion of the exemptions to maintain balance.

**URL tracking use case.** The use of URL tracking allows for tracking without relying on personal data. As such, it is largely considered a privacy enhancing technology. However, the guidelines seem to imply that consent would be necessary in this context. This could be difficult to roll out in practice and would

---

<sup>1</sup> See for instance: [Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 20. Dezember 2021](#)

undermine its use. Ultimately, this could lead to even more reliance on less privacy preserving technologies such as cookies. Increasing cookie banner fatigue in the process.

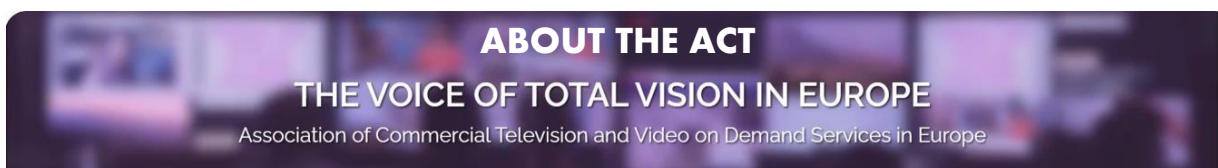
**Pixel tracking use case.** Pixel tracking is used in a wide variety of contexts, ranging from advertising (eg. to calculate impressions) to the distribution of audiovisual services, for instance to authenticate users. Whilst we assume that the use of pixels for the latter would be exempted from the technical scope of art. 5(3), this is not explicit in the guidelines and could create significant issues to the proper functioning of our services. In these situations, the transfer of data is necessary to allow access and is only used for this purpose. A clarification would be welcome in this regard.

**Contextual advertising use case.** Delivering a non-targeted ad-file to an IP address through TCP constitutes a separate operation than delivering the content of the webpage hosted on the publisher's servers making this operation fall in scope of art. 5(3). This is significant because publishers use non-targeted ads to generate revenue from users who have declined or withdrawn consent for certain operations on their devices. Despite authorities and privacy advocates endorsing contextual advertising as a preferable option to targeted advertising, the guidelines could discourage businesses from investing in this less lucrative form of advertising if subjected to the same obligations as targeted advertising.

#### Missing guidance on exemptions

The EDPB's failure to offer guidance on exemptions following its novel interpretation of the ePD's scope is seen as potentially leading to varied interpretations across European jurisdictions. For instance, while certain regulators provide exemptions for using technologies such as cookies for the management of advertising spaces (such as the AEPD and Traficom), others have specifically excluded their use (CNIL). Additionally, the 'strictly necessary' exemption in art. 5(3) is limited to 'information society services', the EDPB's view that TCP or information simply inputted into a website by a user is in-scope of art. 5(3) will lead to unfair, distortive and inconsistent outcomes and increased complexity for organisations grappling with ePD compliance. As the term 'information society service' does not include, for example: (i) broadcast services including those delivered over the internet or (ii) offline services and websites which only provide information about them, this could mean that individuals would need to provide ePD consent simply to use those services or sites, even in the absence of any cookies or tracking technologies.

---END---



*ACT members are at the heart of Europe's media landscape; embracing the digital environment and continuously providing new services, formats and content to meet the growing European demand for quality content on various distribution models. ACT member companies finance, produce, promote and distribute content and services benefiting millions of Europeans across all platforms. At ACT we believe that the healthy and sustainable commercial broadcasting & VoD sector has an important role to play in Europe's economy, society and cultures.*