EPC European Publishers Council

EPC submission to the EDPB public consultation on Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive – 17 January 2024

About the European Publishers Council (Europ20300105)

The European Publishers Council (EPC) is a high-level group of Chairmen and CEOs of Europe's leading media groups representing companies which are active in news media, television, radio, digital marketplaces, journals, eLearning, databases and books.
EPC has been communicating with Europe's legislators since 1991 on issues that affect the health and viability of journalistically driven media and publishing companies in the European Union which uphold the freedom of expression, media diversity, and democratic debate.

www.epceurope.eu

Executive Summary

EPC supports the intent of EPDB to create more clarity on the scope and data protection requirements for online data collection through cookies, tracking and related techniques. However, the expansive interpretation of the Art 5(3) criteria of the ePrivacy Directive ("ePD") may imply that every request over the internet corresponds to gaining access to information and requires consent except for the narrowly defined and ancient Cookie Consent Exemptions[1].

We are highly concerned that Guidelines 2/2023 ("Guidelines"), if adopted in this form, will significantly threaten advertising revenues in our industry and harm media consumers because of consent fatigue, reduced access to editorial content, and more, not less, invasive data processing.

With the important caveat that the authority of EDPB beyond the scope of personal data is unclear, we provisionally recommend two actions. First, we encourage EDPB to redefine the notion of 'gaining access' (2.5) and 'storage' (2.6) more narrowly given the potential all-encompassing scope of ePrivacy as a consequence. Second, we would welcome more granularity, illustrated by examples, for each component of applicability. Third, we request

EPC
Chairman > Christian Van Thillo
chairman@epceurope.eu
Executive Director > Angela C. Mills Wade
angela.mills-wade@epceurope.eu
EPC > Avenue Des Arts 43, 5th floor, 1040, Brussels, Belgium | Tel +32 (0) 2231 12 99

an update to the Cookie Consent Exemption guidelines. A recent reading of the exemptions is equally critical as the technical scope.

Detailed comments on the Guidelines

Implication: The Guidelines affect every single online user interaction

The executive summary and introduction of the Guidelines suggest a narrow focus on regulatory coverage of "new tracking methods […] and […] new business models"[2]. However, the broad interpretation of 'gaining access' and 'storage' ('Technical Scope Components') arguably covers every request over the public internet and any storage on a terminal equipment.

This interpretation not only has far-reaching consequences, but also appears to go beyond the intention of the legislator. First, Art 5(3) refers to 'gaining of access' and not just 'access'. Recital 24 of the ePD describes active access in the sense that "spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal" similar to paragraph 31 of the Guidelines. Cookies indeed require an active step through the Set-Cookie header field in an HTTP response or Javascript (document.cookie). However, it is unclear why EDPB also considers information transmitted automatically as part of standard HTTP requests in scope of "gaining access" (paragraph 33), particularly when the receiving entity is different from the instructing entity. Second, the ePD does not signal that any storage, no matter how short or small, is in scope. In contrast, ePD recital 22 excludes "automatic, intermediate and transient storage" under specific conditions and ePD recital 25 only refers to a "cookie or similar device".

Let's consider the homepage of an online newspaper. When a user enters "news.com" in their browser, the browser will perform a Domain Name System (DNS) lookup to find the IP address associated with "news.com", which may have been cached already (see next section). The browser now sends an HTTP GET request to the server hosting "news.com". The server at "news.com" responds with HTML content for "news.com" along with CSS links for styling and JavaScript files for interactivity. As the browser renders the page, it may make additional HTTP requests to the home page server and other servers for additional images, recommended content, analytical functionality, advertisements, and other resources owned by the publisher. Each resource will receive information such as IP address, HTTP headers and the user agent by default as part of HTTP conventions, not because they are actively processed.

Consequence #1: Consent becomes the only legal basis for every non-exempted HTTP request

Article 5(3) of the ePrivacy Directive ('Article') establishes the need for consent for any access unless the 'Cookie Consent Exemption' applies. The following use cases illustrate

that the broad interpretation of the scope of ePrivacy creates uncertainty on the need for consent for widely accepted communications between a client and a server.

- **Untargeted advertising**

Publishers embed scripts or iFrames from their ad server on web pages as a placeholder for ads. As the browser renders the page, it sends a request to the ad server including the IP address, user agent (browser and operating system information) and the URL of the news website. Just as any other element on the page, this server exchange occurs regardless of the use of cookies. In response, the ad server needs the IP address at a minimum to respond to the homepage request with a creative. By extending the notion of gaining access to "instruct[ing] the terminal equipment to proactively send information on each subsequent HTTP (Hypertext Transfer Protocol) call", the Guidelines create ambiguity around embedded HTML components on a page adjacent to the main content.

- **Tag management**

Tag managers allow publishers to manage logic for snippets of code (e.g., tracking pixels) dynamically on websites. Modern tag managers[3] often load scripts asynchronously in the background to avoid blocking the page rendering. Loaded scripts don't run immediately. They are just available for the tag manager to execute based on specific triggers or conditions such as consent choices. This approach improves the responsiveness of the page, avoids loading scripts too often, and supports resolving dependencies between scripts. The Guidelines discuss scripts explicitly in the context of 'gaining access'. However, they are not strictly needed for transmission (failure of Criterion A) and are not requested by the user who may not have expressed consent choices yet (failure of Criterion B). Therefore, users will need to give a separate consent to accept the storage of scripts before interacting with the consent management platform. Alternatively, publishers need to slow down loading times significantly by waiting until users make consent choices or stored choices are retrieved.

- **Caching**

Caching stores data (e.g., images and layout components of a site) in a temporary storage area of the browser to make future access to that data faster and more efficient. While caching occurs across several components of client-server communication, browser or application caching specifically may require consent under the Guidelines. The Guidelines refer to "caching mechanism of the client-side software" in the context of 'Storage' and 'URL and pixel tracking'. However, caching is only a 'facilitation' (failure of Criterion A) of a transmission and may not be required for a service requested by the user (failure of Criterion B). If Guidelines are applied broadly in this sense, user experiences may degrade significantly (e.g., lower responsiveness and higher bandwidth costs) without very limited impact on privacy protection.

- **Automatic software updates**

A smartphone checking for operating system updates may send data about the current OS version, device model, and potentially retrieve information on the smartphone from previous checks. If these checks are automatic, as ENISA[4] and most security agencies recommend, consent is arguably needed. Indeed, the request involves a query that goes beyond mere transmission (failure of Criterion A) and the user has not explicitly requested the check (failure of Criterion B).

If EDPB does not consider consent a requirement for the use cases discussed, we encourage EDPB to provide additional guidance and examples around the notion of "strictly necessary in order to provide an information society service explicitly requested by the subscriber or user".

On a final note, technological adaptations related to these examples would require significant workload for the entire industry (e.g., full redesign of tag management software).

Consequence #2: Publishers can no longer monetise their content through advertising

The immediate repercussion of consequence #1 is that media consumers will always be able to opt out of seeing any advertisement as well as any other experience that users have not explicitly requested (e.g., a list of popular articles based on the number page reads). The advertisement is not essential for the transmission as it can collapse without a response (failure of Criterion A) and the user does not explicitly request ads when clicking a link or entering a URL (failure of Criterion B).

Publishers today use contextual advertising and technical ad delivery[5] as a fallback for users who opt out of personalised advertising. Even authorities and legislators themselves often offer contextual advertising as a more privacy friendly and less intrusive monetisation option for behavioural advertising. An additional consent for the fallback effectively eliminates that option.

Consequence #3: Users will have less access to free editorial content

Publishers already face fundamental pressures on historical revenue models such as the decline of print subscription, an advertising market which is very challenging, distorted by the dominance of gatekeeping platforms which take the lion's share of digital advertising revenues, and the continued rise of ad blocking. The increasingly strict interpretation of consent requirements (e.g., 'reject all' button on the first layer) have further reduced the addressable audience for legitimate personalised advertising for publishers.

Consent for advertising of any nature may push publishers further towards subscription only models and "consent or pay[6]" models. However, many consumers are unable or not willing to purchase multiple publisher subscriptions in the face of 'subscription fatigue' as

we explained to the EDPB in our open letter of 11 December about the consent or pay models.

Guidelines and rulings by several DPAs on publishers[7] as well as rulings on Meta[8] confirm the validity of this model under certain conditions. The DMA (Recitals 36 and 37 DMA) also leaves room for a paid option for users declining consent under article 5(2) of the DMA. These Guidelines therefore conflict with recent decisions on the validity of monetising content through advertising while respecting fundamental rights of data privacy but also of access to information via a pluralistic press. An independent press is vital to democracy, providing critical oversight and authoritative information to the public. Financial instability in news media publishing risks eroding this democratic cornerstone, highlighting the need for data privacy policies that support, not undermine, the press's sustainability.

Consequence #4: Users have less agency over data protection

Consent gives users the benefit but also the burden of opt-in choices. EPC reminds the EDPB of the efforts by the European Commission ('EC') in the Cookie Pledge initiative. In the discussion paper on cookies, the EC frames the notion of 'consent fatigue' observing that "[m]any people are tired of having to engage constantly with complex cookie banners […] and as a result they may simply give up trying to express their real privacy preferences". EDPB has also acknowledged this phenomenon in guidelines 05/2022.

In sum, the sheer volume of consent requests already far exceeds human limits to attention for meaningful judgements. This leads to heuristics such as blindly accepting or refusing any consent choice. In the spirit of combatting consent fatigue, we invite EDPB to revisit the Cookie Consent Exemption guidelines for analytical and advertising related exemptions (e.g., technical ad delivery, impression-based measurement signals). More exemptions support aligning ePrivacy to GDPR legal bases other than consent and allow users to focus choices on more invasive data processing activities.

Consequence #5: Controllers have fewer incentives to invest in privacy-enhancing techniques for online personalised experiences

The demise of third-party cookies has accelerated the development of privacy-by-design alternatives to cookie-based tracking. Most initiatives include privacy-enhancing components such as federated learning, secure multi-party computation, and differential privacy. Google's privacy sandbox is the most notable example. However, these new approaches to profiling, selecting, and measuring ads trade off granularity with privacy. When pressed for consent in every advertising scenario, publishers and advertisers are indirectly incentivised to adopt more invasive approaches that stay at the individual level to retain granularity (e.g., universal ID solutions in combination with pixel tracking).

References:

[1] 'Wp194_en.Pdf' <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf> accessed 7 December 2023.

[2] As alluded to in the introductory remarks of the Guidelines: "due to the new advances in technologies further guidance is needed with respect to the tracking techniques currently observed. The technical landscape has been evolving during the last decade, with the increasing use of identifiers embedded in operating systems, as well as the creation of new tools allowing the storage of information in terminals."

[3] Popular tools are Google Tag Manager, Tealium, and Adobe Launch.

[4] 'Software Patches' (*ENISA*) <https://www.enisa.europa.eu/securesme/cyber-tips/enhance-processes/software-patches>

[5] Defined in the IAB TCF as "Certain information (like an IP address or device capabilities) is used to ensure the technical compatibility of the content or advertising, and to facilitate the transmission of the content or ad to your device."

[6] Consumers are offered a choice between consenting to personalised advertising or accessing the service for a fee without personalised advertising.

[7] CNIL, Cookie walls : la CNIL publie des premiers critères d'évaluation, <https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation>; DSB, decision 2023-0.174.027, <https://noyb.eu/sites/default/files/2023-04/Standard_Bescheid_geschw%C3%A4rzt.pdf>; Il Garante privacy apre istruttorie su uso dei cookie wall' <https://www.gpdp.it:443/web/guest/home/docweb/-/docweb-display/docweb/9816536>; Datasylnet Norway, Decision 20/02136-18, <https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine---grindr-llc.pdf>; Datasylnet Denmark, Brug af cookie walls, <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/feb/brug-af-cookie-walls>

[8] C-252/21 Meta Platforms and Others, ECLI:EU:C:2023:537, para. 150.