Published on *The National Law Review* https://natlawreview.com

EU Regulators Confirm That Cookie Consent Rules Apply to Much Broader Range of Tracking Technologies

Article By:

Rosa Barcelo

Anna Ciesielska

Matúš Huba

Simon Mortier

Article 5(3) of the EU ePrivacy Directive (ePD) requires consent for tracking cookies (unless exceptions apply). Although this rule is best known as the reason behind ‘cookie’ banners, it is technology neutral and applies to other tracking technologies as well.

- At the end of 2023, the European Data Protection Board (EDPB) issued draft Guidelines explaining how the rule applies to a broad variety of tracking solutions, ranging from tracking URLs/pixels and IoT devices reporting, to other unique identifiers, e.g., obtained from hashed email addresses (‘Guidelines’). If a technology is subject to the consent requirement, this has significant implications for all stakeholders involved, ranging from the AdTech industry/advertisers, which heavily rely on such technologies, to every website (publisher) and B2C/B2B companies using them. Guidelines also analyze key elements of the rule, such as the notions of ‘terminal equipment’, ‘gaining access’, and ‘storing’.
- The EDPB findings present a mixed bag, with some outcomes expected (e.g., prior consent requirement for pixels tracking email opens) and others, less so (e.g., storage through “caching on the client-side software” alone triggers the rule).
  After the EDPB considers the comments submitted in a public consultation, it will adopt the Guidelines in their final form.

IN DEPTH

This article analyzes the key elements when applying Article 5(3) ePD, differentiating between novel and previously established conclusions (e.g., from the past guidance) (‘*Key Elements for Applicability of Article 5(3) ePD*‘). Subsequently, it discusses specific use cases where consent pursuant to Article 5(3) ePD will be necessary (‘*Selected Use Cases*‘). It concludes by suggesting actions companies and organizations may consider while awaiting the final version of the Guidelines and potential future enforcement.

Key Elements When Applying Article 5(3) ePD

Under Article 5(3) ePD, anyone storing information or gaining access to information already stored in the terminal equipment of a subscriber or user is allowed to do so only if the subscriber or user has consented, unless an exception applies. This OTS focuses on the following four of the key elements analyzed by the EDPB:

A. Information – This term includes any information, whether it constitutes personal data or not. This aligns with past guidance and has been confirmed by the Court of Justice of the European Union in the Planet49 case. The rule aims to protect the private sphere of users, regardless of the nature of the data. The interpretation of this element is undisputed.

B. Gaining Access to Information Already Stored – This typically involves the accessing entity proactively sending instructions to the terminal equipment to retrieve information. Examples include cookies where the accessing entity instructs the browser on the terminal equipment to transmit information (e.g., the originating website) to a server. Another case is when software distributed on a user’s terminal equipment actively calls an application programming interface (API) to send data back to the server. An example is the use of JavaScript code, instructing the browser to send information. The EDPB explains that the entity instructing the terminal to send back the targeted data and the entity receiving information might not be the same. These are new clarifications which were not specifically provided by regulators in the past.

C. Storing Information/Storage – Refers to placing information on the user’s terminal equipment. A typical example is the storage of cookies. The EDPB provides new clarifications on the term ‘storing’ by including storage resulting from a third-party instructing software on the user’s equipment to generate specific information (e.g., through various protocols and customized software) or to provide pre-existing information. Furthermore, there is no defined time limit for how long information must be on the equipment to be considered as ‘stored’. Storage, even if brief, can occur in different parts of a device (e.g., Central Processing Unit (CPU) cache, or Random-Access Memory (RAM)).

D. Terminal Equipment – Defined in Directive 2008/63/EC as equipment directly or indirectly connected to the interface of a public telecommunications network for sending, processing, or receiving information. The connection can be made via wire, optical fiber, or electromagnetically, and is considered indirect if equipment is placed between the terminal equipment and the network interface. Examples provided by the EDPB include smartphones, laptops, connected cars, connected TVs, and smart glasses.

New technical details include:

- Any combination of hardware pieces can collectively constitute terminal equipment.
- The specific way in which a device (such as a computer or a smartphone) connects to its

storage system, whether it’s built-in, external (e.g., connected via USB), or accessed over a network, does not matter as long as the storage system works as effectively as if it were directly part of the device.

- The consent rule aims to cover endpoint devices. A device which only acts as a communication relay (i.e., conveys information without modification) would not be considered terminal equipment subject to the rule. However, if an endpoint device is only connected to public communication network using a relay device, EDPB notes that such information stored on the relay device should nevertheless be subject to the consent rule.
- The Guidelines interpret the old ‘cookie’ consent rule broadly. Technologies fall within its scope even if they merely instruct the terminal equipment (directly or through any technology) to produce/export information, and the recipient of such information does not actually access it on the device.

Selected Use Cases

The draft Guidelines present a non-exhaustive list of tracking technologies (beyond cookies) that require prior consent, including:

1. Tracking Pixels with Identifiers: Commonly referred to as marketing pixels/web beacons, these are embedded in emails or websites via small code snippets and typically include identifiers. They enable pixel’s host to receive information about the user. For instance, conveying details about when and how they opened an email or interacted with a website. The EDPB notes that tracking pixels are covered under Article 5(3) ePD as they constitute ‘gaining access’ to such information. While the inclusion of tracking pixels is not new, as noted by several data protection authorities, the EDPB provides a more detailed technical explanation for this inclusion.

2. Tracking Uniform Resource Locators (URLs): These are unique hyperlinks embedded with an identifier. They are typically shared/ included in social media accounts, blog posts, emails, newsletters, and advertisement. When the user clicks on them, the destination website collects certain information about the user (e.g., the website where the user clicked on the URL, or the search engine they used, and the search terms used). They are used to measure success of advertising campaigns, or to know from which websites users are coming from. Data protection authorities had not prominently asserted that tracking URLs fall under Article 5(3) ePD’s scope until now. The EDPB clarifies that tracking URLs involve both storing information in the user’s terminal equipment (within the caching mechanism) and ‘gaining access’ to the data transmitted to the URL host.

3. Tracking Based on IP Addresses Only: This use case revolves around tracking technologies instructing the terminal equipment to disclose its IP address for cross-domain tracking. The EDPB explains that the transmission of the IP address, which originates from the terminal equipment (alone or together with other related identifiers in the communications protocol) to a third party is categorized as ‘gaining access’ to information stored in the terminal equipment.

4. Unique Identifiers: Also called persistent identifiers, these are generated from personal data hashed within the user’s terminal equipment (e.g., email addresses), which are then shared between various stakeholders to identify the individual (e.g., to serve them an ad). The EDPB considers that instructing the browser to forward this information to a third party constitutes ‘gaining access’ to the data in the terminal equipment.

5. Intermittent and Mediated Internet of Things (IoT) Reporting: This pertains to IoT devices transmitting information to a third party over time, such as a smart home device sending data to a service provider. The information may be processed locally before transmission. The EDPB views the act of sending data to a remote server upon instruction (e.g., from the service provider) as 'gaining access'.

What Does This Mean for Your Company or Organization?

The Guidelines are currently still in a draft form.

Although their content may still undergo changes, they provide an insight into the EDPB's perspective on more modern non-cookie-based tracking technologies and inclination to interpret the scope of application of Article 5(3) ePD broadly. Therefore, despite some uncertainty regarding the final version of the Guidelines, we recommend companies and organizations to:

- Evaluate the range of tracking technologies, beyond cookies, they currently use.
- Determine if they need additional consent mechanisms/their ability to collect required consents.
- Assess whether they need to improve disclosures in their current website/app cookie/privacy notices.
- Stay informed about ongoing developments in this field, including those at the national level.

National Law Review, Volume XIV, Number 19

Source URL:https://natlawreview.com/article/eu-regulators-confirm-cookie-consent-rules-apply-much-broader-range-tracking