



## **Comment on the European Data Protection Board's Draft Guidelines 2/2023 on the Technical Scope of Art. 5(3) of ePrivacy Directive, published November 16, 2023**

### **1. About GetYourGuide**

GetYourGuide Deutschland GmbH ("GetYourGuide" or "we") operates an online platform that allows customers to view and book various travel services including tours, attractions, and other touristic activities.

We appreciate the opportunity to respond to the public consultation of the EDPB on its draft Guidelines 2/2023 on the Technical Scope of Article 5(3) of the ePrivacy Directive ("EDPB Guidelines"). While we recognise the EDPB's efforts to provide guidance on the scope of Article 5(3), we have substantial concerns that we believe may benefit from further consideration by the EDPB.

### **2. Main Concern**

In the EDPB Guidelines, the EDPB addresses the applicability of Article 5(3) to different technical solutions. According to these guidelines, URL tracking would fall within the scope of Article 5(3) and, therefore, require consent collection. We believe that imposing such a requirement is counterproductive for both users and businesses. It risks degrading the user experience and makes one of the most transparent and fair advertising methods - affiliate marketing via partner websites - nearly impossible. To avoid this outcome, we highly recommend:

- Narrowing the definition of "gaining access" to exclude automatic data transmissions
- Excluding temporarily stored data from the scope of "stored information"

Most digital businesses rely on the use of URL tracking, especially when managing partner attribution within affiliate marketing programs. Up until now, tracking URLs have not required user consent as they primarily identify the source website, not the individual user. The purpose of URL tracking is not to monitor user behaviour, but rather to monitor the performance of the contract with the affiliate partner and to count the total number of referrals.

With the EDPB's interpretation that tracking URLs fall in the scope of Article 5(3), obtaining user consent each time such a URL is used on a website or embedded in an email would be required. The practical implementation of such a consent mechanism would not be feasible. Consequently, it could potentially jeopardise a straightforward advertising model that, compared to others, is fully transparent to the user, whose intention and interest in the advertised content are made clear by their action to actively click on the URL. It should also be noted that, if consent is requested too frequently for routine and low-risk interactions like URL tracking, this could diminish the significance of consent for more invasive forms of data collection, thus inadvertently weakening the privacy protections the ePrivacy Directive aims to strengthen. This would not only affect the user experience but also undermine the ePrivacy Directive's goal of protecting user privacy without limiting the functionality of digital services.

### **3. Specific recommendations on the EDPB Guidelines**

In order to address the practical concern mentioned above, we ask the EDPB to make following adjustments:

#### **3.1 Narrowing the definition of "gaining access" to exclude automatic data transmissions**

The EDPB Guidelines suggest a broad interpretation of the term "gaining access". In particular, the Guidelines clarify that "gaining access" to information is not limited to scenarios where an entity takes active steps to retrieve stored information from a user's terminal equipment. It also applies to cases where information is automatically transmitted to the entity as a result of a user accessing a service.<sup>1</sup> The consequence of this interpretation is that almost every data transmittal - active or passive - would fall within the scope of Article 5(3). This includes, for example, the automatic transmission of information that occurs when a tracking pixel or URL is loaded, as well as the browser or header information that is inevitably transmitted when accessing a website. This, however, does not appear to have been the intent of the EU legislator when drafting the ePrivacy Directive. According to Recital 24 of the ePrivacy Directive, the objective of the Directive is to safeguard users' terminal equipment against intrusions by harmful technologies that may attempt to "enter" the device. Apart from the word "entering" clearly having an active connotation, the original legislative intent was focused on the protection against unwanted and potentially malicious interference, rather than covering automatic data transmissions that occur in the context of routine use of internet services or standard marketing practices.

As a German company, we are particularly mindful of the previous stance taken by various German data protection authorities. These authorities have clarified that the processing of information that is automatically transmitted from a user's device, is not considered as "access" within the meaning of the ePrivacy Directive.<sup>2</sup> The EDPB's broader interpretation, represents a significant shift from this position, which creates legal uncertainty especially for German companies.

#### **3.2 Excluding temporarily stored data from the scope of "stored information"**

The EDPB Guidelines note that the ePrivacy Directive does not distinguish between the duration or type of storage medium used for retaining information, thereby encompassing a wide array of data storage scenarios under the term "stored." The EDPB considers information as "stored" regardless of whether it is held temporarily or long-term on various storage media, such as a device's hard drive, SSD, RAM, or CPU cache. This understanding implies that transient data, commonly found in RAM or CPU cache, qualifies as "stored information" and consequently, falls within the scope of Article 5(3) of the ePrivacy Directive.<sup>3</sup>

---

<sup>1</sup> Paragraph 31-33 of the EDPB Guidelines

<sup>2</sup> Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 20. Dezember 2021, page 8; FAQ der Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg: Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps, page 14

<sup>3</sup> Paragraph 36- 37 of the EDPB Guidelines

However, this expansive interpretation by the EDPB raises concerns as it contradicts the actual language of Article 5(3). Article 5(3) specifically refers to “gaining of access to information already stored”. The use of the term “already” indicates that the ePrivacy Directive is referring to information that is, in effect, retained for some period and not information only existing for immediate processing. It should also be noted that Recital 25 of the ePrivacy Directive explicitly mentions cookies as an example of actual storage, which, along with Recital 24, suggests that the legislator primarily intended to address concerns around more persistent forms of data retention that have a greater potential for impacting user privacy. Furthermore, stating that “transitional storage” within a cache constitutes “storing” of information in the sense of Art. 5(3)<sup>4</sup>, has implications for a wide range of common internet functions that rely on some level of caching for efficiency and user experience e.g. URL tracking. This interpretation clearly expands the scope of the ePrivacy Directive far beyond its original intent and practical application.

We appreciate your consideration of our comments on the Draft Guidelines 2/2023 and look forward to engaging in a constructive dialogue that advances a regulatory framework beneficial to all stakeholders—users, service providers, and regulators.

---

<sup>4</sup> Paragraph 50 of the EDPB Guidelines