Unlocking ePrivacy further to Recent EDPB Guidelines on Article 5(3) of ePrivacy Directive

Pursuant to Article 5(3) of ePrivacy Directive ("**ePD**"), storing or accessing information on a user's or subscriber's device is permitted only with his/her consent or when necessary for the specific purposes set out in the same provision of ePD.

On 7th October 2024, the European Data Protection Board ("**EDPB**") adopted *Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive* (the "**Guidelines**"). The Guidelines aim to resolve issues and clarify ambiguities relating to the application of article 5(3) ePD and in particular, but not only, to emerging tracking tools.

To this end, the Guidelines:

- ✓ **clarify the key elements** for Article 5(3) ePD applicability, including '*information*', '*terminal equipment of a subscriber or user*', and '*gaining access*' and '*storage of information and stored information*'; and
- ✓ **address and provide a selection of common use cases** that may fall under the scope of Article 5(3) ePD.

Key Elements for Article 5(3) ePD to Apply

The EDPB explains the three key elements that determine the applicability of Article 5(3), as follows:

(i) the scope of '**information**' covers both personal and non-personal data stored or accessed on a user device;

(ii) the notion of '**terminal equipment of a subscriber or user**' refers to any device directly or indirectly connected to a public network: from phones through IoT devices; and

(iii) '**gaining access**' and '**storage of information and stored information**' includes access or storage of any information on a user's or subscriber's device by the business organization or an agent acting on its behalf; storing or gaining access to information can involve independent operations and be performed by independent organizations.

Use Cases of Article 5(3) ePD Applicability: EDPB Selected Illustrative Examples

According to the Guidelines:

(a) User's consent under Article 5(3) ePD is required in respect of **URL and pixel tracking** because tracking pixels or tagged URLs generates information about user actions that are then accessed by the host server.

(b) **Local processing** may fall within the scope of Article 5(3) ePD if the processed information is made available to a third-party by, for example, sending it back over the network to a server. Local-only data usage without external communication is generally exempt.

(c) **Internet protocol (IP)-based tracking** triggers the application of Article 5(3) ePD unless the organization can ensure that the IP address does not originate from the terminal equipment of a user or subscriber.

(d) Article 5(3) would apply to **IoT devices** if the relevant 'gaining of access' is made through instruction of the code on the IoT device to send the dynamically stored data to a remote server.
(e) Consent is required when **unique identifiers** are stored or accessed on a user's device. The rational is that the organization collecting unique identifiers on websites or mobile applications is actually instructing the browser to send that information and, in this manner, a 'gaining of access' occurs.

These are only a few of the examples given by the EDPB to illustrate the technical scope of applicability of Article 5(3) ePD.

The Guidelines show once again how important to the businesses is to make diligent assessment of the concepts of '*information'*, '*terminal equipment of a subscriber or user'*, and '*gaining access*' and '*storage of information'* in each specific use case of ePD to stay compliant and competitive.