To EDPB
Public consultation of draft guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive
Public consultation reference: 2/2023

Comments of DMA Finland, ASML (Data and Marketing Association Finland)

1. EDPB's lack of legal competence to issue guidance on ePD

1.1 EDPB's Compliance with Fundamental EU Law

- EU institutions are bound by fundamental democratic principles, being essential EU law enshrined in the Treaties (TEU & TFEU). Going beyond legal authority undermines the democratic legitimacy of EDPB.
- Article 5 TEU protects the principles of conferral, subsidiarity and legal basis.
- If an institution exceeds its legal powers and issues guidance without a clear legal basis, it violates the fundamental principle of legal basis.
- EU institutions can act only within the limits of the competences conferred upon it. Any action or guidance outside these limits would breach the principle of conferral.
- Additionally, in accordance with the legal certainty principle, entities and individuals can rely on clear and predictable legal rules. Actions beyond legal authority create uncertainty and can undermine the principle of legal certainty.
- The competence of the EDPB should definitely and precisely be expressed already in the opinion version of each set of guidelines.

1.2 EDPB's legal competences are stipulated in the GDPR

- GDPR explicitly grants the EDPB the competence to ensure the consistent application of the GDPR, as outlined in Article 70(1) of the GDPR. This pivotal role involves the issuance of guidelines to facilitate the uniform interpretation and application of the GDPR across EU.
- On page 6 of the draft guidelines 2/2023, the EDPB refers to GDPR Article 70 as the legal basis. This is, regrettably, an inaccuracy. The EDPB possesses independent legal personality and was expressly established by the GDPR. Any legal basis for guidelines issuance must be firmly rooted in the provisions of the GDPR. The competence has not been extended to apply to ePD by any legal act.
- Under ePD each Member State designates its own national supervisory authority responsible for enforcing the ePrivacy rules within its jurisdiction.

1.3 EDPB's Jurisdictional Overreach: A Critical Assessment of Guideline Issuance Beyond Legal Authority

- To conclude, EDPB has legal competence to assess and guide aspects related to the processing of personal data within the limits set by the GDPR. EDPB has gone beyond its authority trying to issue such guidelines. Unlike national data protection authorities, which, as EDPB members, are bound by the interpretations of the EDPB, national authorities within ePD are not subject to the same constraints.
- Matters on which the EDPB has expressed guidance fall within the jurisdiction of the Member States' national supervisory authority.

2. Analysis & Use cases

EDPB misinterprets and overinterprets Article 5(3) regarding 'storing of information, or the gaining of access to information already stored', to the extent that the draft includes activities that do not meet the requirement of 'storing/gaining access to information stored'. Including IP addresses, URLs, user agent strings, email pixels, and IoT reporting. EDPB is broadening ePD 5(3) to cover almost all basic internet communication protocols which do not fall under the definition of 'storing/gaining access to information stored'. This a fundamental issue.

2.1 Unique Identifiers

- Considering Unique Identifiers within the scope of ePD 5(3) is an inaccuracy.
- Unique Identifiers can be considered personal data, hence do not fall within the scope of ePD

2.2 Email tracking

- Requesting separate consent for email tracking is complicating legitimate interest-based customer marketing.
- The control of email pixel loading depends on the recipient's email system. Businesses cannot influence how this operates.
- There’s no element of “storing of information…in the terminal equipment of a subscriber or user” when using email pixels.

2.3 IP Tracking

- IP addresses are also used in logging, serving various purposes beyond what is 'strictly necessary' from an ePD perspective.
- It remains unclear whether logging would require consent in the future, but the demand to seek consent whenever the source of the IP address cannot be confirmed as a device seems unreasonable. This requirement should be reconsidered from a practical implementation perspective.
- Logs are utilized e.g. for cybersecurity and resolving error situations.

2.4 IoT reporting

- It is evident that IoT sensors typically store and transmit data to systems that collect and utilize them. The presented opinions and justifications seem generally acceptable. However, in section 59, the argument is made that an independently networked IoT device is considered an end device. This assertion is problematic or unfamiliar, as these devices rarely involve the direct use by a natural person, especially for monitoring purposes. Monitoring may occur, for example, in the case of a locatable IoT device.
- Should be emphasized that these technologies are not inherently tracking technologies unless explicitly employed for such purposes.
- How does this relate to the Data Act, especially in situations where the data from the device is not personal data but still requires user consent, particularly when the user is a business?

2.5 Other

- When consent requirements are expanded and tightened, the outcome may be gatekeeper platforms developing 'privacy-friendly' solutions, where sharing data with third parties ceases, and users avoid endless consent requests by providing them directly to the platform. This results in an increased accumulation of data on the platform itself. Whether this is the optimal regulatory outcome from a privacy perspective will likely be analyzed by competition authorities in the end.
- Use cases para. 41 problematic: the most commonly used identifier is the IP address. The listing of routing protocols here is an overinterpretation, as these are typically employed and have identifiers set by network intermediary, transmission, and routing devices for messages transmitted, rather than by end-user devices.
- Para. 53: too broad and unclear. According to this interpretation, almost any information generated would meet the requirements of tracking technology under ePD.