European Data Protection Board

Rue Wiertz 60

B-1047 Brussels

Belgium

Subject: Joint Comments on the Draft Guidelines 2/2023 on the Technical Scope of Article 5(3) of the ePrivacy Directive

Dear Members of the European Data Protection Board,

We are writing to submit our joint comments regarding the draft Guidelines 2/2023 on the Technical Scope of Article 5(3) of the ePrivacy Directive. As legal professionals with a dedicated interest in data protection and privacy law, we have thoroughly reviewed the guidelines and wish to express several collective concerns and suggestions.

Interpretation of 'Storage':

The classification of CPU and RAM as storage mediums raises significant concerns. These components are primarily designed for ephemeral processing and temporary data handling, not long-term storage. It is our opinion that this sort of interpretation stretches the scope of Article 5(3) beyond the directive's original wording and intent.

The current draft guidelines appear to be drafted with the approach that since the concepts of "storage" or "storage medium" have not been specifically defined under the ePrivacy Directive, the EDPB takes the liberty to interpret them in the broadest possible manner and without regard to the purpose components like CPU and RAM truly serve.

We call for a more balanced approach where the purpose of non-defined terms is not to extend them without careful consideration of the impact. We understand that the EDPB has rather decided that the broadest possible interpretation is justified in favor of the right to data protection and privacy. In this light, the approach seems inherently principle-based rather than pragmatic.

Concept of 'Gaining Access':

As with the interpretation of the concept of storage, the EDBP appears to be equally aggressive on its reading of the "gaining access" part of Article 5(3).

We note that "gaining access" implies an active effort in trying to access the terminal equipment and the information stored on it. However, the EDPB looks be interpreting the concept as covering any passive reception of information from the terminal equipment, as long as there is any sort of technical instruction towards the terminal equipment.

We do not believe that such reading of the word "gaining" access aligns with the legislator's intent. Further, such interpretation would cover scenarios where seeking consent would be either impossible or excessively difficult.

Again, the EDPB seems to be taking a very principled approach that would have significant implications on the legal obligations of multiple actors, without carefully reasoning how such a broader reading is legally justified.

Definition of 'Information':

The guidelines' approach to “information” inadequately differentiates it from “traffic data”, as delineated in the ePD. An IP address, for instance, is categorized as traffic data, not information.

The practice of including identifiers in a URL should not be construed as instructing terminal equipment to send back targeted information. Many such identifiers serve legitimate, non-invasive functions, like traffic source categorization.

Implications for the Data Act

We would like to draw your attention the recently introduced Data Act.

Recital 36 of the Data Act acknowledges that IoT devices, or connected products as they are defined in the Act, can be qualified as terminal equipment under the ePrivacy Directive.

Given the considerably broad interpretation that the EDPB is now looking to introduce, especially in respect of the concept of storage, these guidelines imply significant risks on data sharing under the Data Act, even when the data is non-personal.

We would like to point out the fact that it is very common for IoT devices to not have any screens or other user interfaces through which a consent could be sought in a manner that could satisfy the requirements for the consent as they are provided under Article 7 of the GDPR.

Also, the supply chains in IoT hardware (and hardware in general) function in a manner where there often is no direct line of communication between the user of the terminal equipment and the manufacturer or other data holder that intends to collect data from the connected product under the Data Act. Therefore, the possibilities for seeking an ePD/GDPR-compliant consent would often be nearly or completely impossible.

Further, Article 4(13) Data Act provides that the basis for the collection of non-personal data should be a contract between the data holder and the user, and not a consent.

In essence, it is our opinion that the currently suggested, very broad interpretation of Article 5(3) would significantly hamper EU-wide data sharing, including sharing non-personal data. Not only is that a problem from the free movement perspective, it also conflicts with one of the main goals of the Data Act itself, the intention to facilitate and encourage data sharing in the internal market.

As broader point, it is our opinion that the EDPB should put greater emphasis on evaluating how their interpretations on different issues may coincide with or impact other EU laws. Application and interpretation of data protection and privacy laws affect multiple areas.

Final conclusions

The interpretations in the guidelines often disregard the legislator's intent, practical implications, or compatibility with other regulations. In addition, they fail to recognize the other express aim of the ePD, namely the ensuring of free movement of data in its scope and of electronic communication equipment and services in the EU.

This approach could result in almost every internet communication being subject to the ePD, leading to significant uncertainty and practical issues, especially in scenarios where user consent is unfeasible, such as certain IoT environments.

The guidelines fail to strike a balance between privacy rights and other fundamental freedoms, like the freedom to conduct business or the freedom of information.

The overly broad interpretation of Article 5(3) risks encompassing standard practices that neither constitute individual tracking nor pose significant privacy threats.

In conclusion, we urge the EDPB to reevaluate and amend the guidelines to ensure they more accurately reflect the ePrivacy Directive's language and objectives. A balanced approach that respects privacy protections while acknowledging other fundamental rights and the practicalities of the digital world is essential.

Finally, as a practical remark, we want to draw the EDPB’s attention to the fact the EDPB website, where this file was uploaded, makes use of CAPTCHA. To our understanding, based in the draft guideline at issue, using CAPTCHA without consent does not comply with the article 5(3) of the ePD. Yet, EDPB itself is making use of it, without consent.

Thank you for considering our joint comments on this crucial topic. We look forward to the final version of the guidelines, hoping they will present a more balanced and precise interpretation of the ePrivacy Directive.

Sincerely,

Otto Lindholm

Attorney

Janne Valo

Data Protection Lawyer