## PREISKEL 🗞 CO

Preiskel & Co LLP 4 King's Bench Walk Temple London EC4Y 7DL United Kingdom

t +44 20 7332 5640 e info@preiskel.com www.preiskel.com

**European Data Protection Board** 

Rue Wiertz 60 B-1047 Brussels Belgium

For the attention of: Anu Talus, Aleid Wolfsen, Irene Loizidou Nicolaidou

By email only

Our Ref: TC/ADM838 9<sup>th</sup> January 2024

Dear Sirs,

#### Re: Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

We write on behalf of Movement for an Open Web ("MOW"), a not-for-profit organisation campaigning to secure a free and open internet. MOW represents a consortium of players in digital markets affected by large platforms' abuse of dominance, enabling them to benefit from anonymity and whistle-blower protections when helping authorities with their enquiries.

MOW submits that the new guidelines introduced by the EDPB to broaden the scope of the ePrivacy Directive, particularly Article 5(3) which governs tracking techniques, represent an unnecessary and alarming shift away from previous interpretations.

Principally, there are two issues with the EDPB's proposed guidelines:

- 1. The EDPB adopts the false assumption that *all* match keys (both identity-linked and deidentified) and *all* information (both sensitive and innocuous) linked to these match keys pose equal risk to specific individuals. This is a marked shift from the well-established 'in whose hands test'<sup>1</sup>, which correctly exempts anonymous and deidentified data when protected by organisational safeguards. Basing policy on such assumptions thus gives rise to concerns over regulatory overreach.
- 2. The EDPB's exemption of local processing from the scope of Article 5(3), whilst capturing server-side processing, is based on a clear fallacy that risk to individuals is based on *where* data is processed, rather than *what* data is processed. There is a misconception that local processing is inherently safer as consumers understand what data is being processed and to whom it is going. Yet, there is no evidence that the harms envisaged by server-side processing could not be inflicted using the same processing running locally.

<sup>&</sup>lt;sup>1</sup> ICO, Chapter 1 Anonymisation Introduction (May 2021), page 9:

<sup>&</sup>quot;the same information can be personal data to one organisation, but anonymous information in the hands of another organisation."

https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf

These issues are discussed as follows.

# 1. Lack of distinction between sensitive, identity-linked data and innocuous, deidentified data

The EDPB's position includes a new interpretation of the ePrivacy Directive, suggesting that the "cookie rule" should apply to a wider range of activities involving a user's terminal equipment, including the processing capabilities of such equipment. The guidelines note that the scope of Art 5(3) extends to capture any "information" rather than just "personal data". Moreover, Paragraph 9 explicitly states that:

"[T]he definition of the term 'information' should not be limited the property of being related to an identifiable natural person."<sup>2</sup>

This is an unnecessary shift away from previous interpretations that incentivised businesses to adopt important safeguards by exempting both innocuous and deidentified data from the scope of regulation. Data protection laws around the globe rely on reasonable safeguards given the likelihood and severity of risk associated with the processing of different forms of data.<sup>3</sup> Data protection laws are not written to restrict interoperability or distort competition but incentivise the use of appropriate safeguards, such as the use of deidentified match keys and aggregate data instead of identity-linked information whenever possible.

Exempting innocuous, deidentified data from Article 5(3)'s remit aligns with and substantiates wellestablished international standards. Incorporation of data protection guidance from the UK's Information Commissioner's Office, the "in whose hands rule," may also help protect consumers' continued access to innovation supplied by competition. The rule was affirmed in the landmark 'SRB' case<sup>4</sup>, which highlighted that risk is situationally dependent rather than inherent in technology. Thus, data in the hands of one organisation may be linked to the identity of a specific individual, while in the hands of another organisation relying on the appropriate organisational measures, such information is deidentified.

Moreover, the Digital Markets Act's key policy objective is to promote a pluralistic and decentralised web, eliminating the barriers to entry erected by the major platforms. It explicitly highlights the need to establish:

"[A] targeted set of harmonised legal obligations...to ensure contestable and fair digital markets featuring the presence of gatekeepers within the internal market to the benefit of the Union's economy **as a whole** and ultimately of the Union's consumers."<sup>5</sup>

It is strikingly clear that non-identity-linked deidentified data appropriately mitigates risks to individuals, and without adequate exemption, smaller consumer-facing businesses that depend on a competitive marketplace of independent business-facing solution providers (i.e., "third parties") will no

<sup>&</sup>lt;sup>2</sup> See P5, <u>edpb\_guidelines\_202302\_technical\_scope\_art\_53\_eprivacydirective\_en.pdf (europa.eu)</u>

<sup>&</sup>lt;sup>3</sup> GDPR, Art. 32: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk...." <sup>4</sup> See Case T-557/20, SRB v EDPS at EUR-Lex - 62020TJ0557 - EN - EUR-Lex (europa.eu)

<sup>&</sup>lt;sup>5</sup> See Paragraph 8, Digital Markets Act (2022)

longer be able to compete with larger, vertically-integrated rivals. This anticompetitive distinction has the knock-on effect of reducing choice for consumers served by those business. As such, without appropriately exempting innocuous, deidentified data, Article 5(3) ePD will only reinforce centralisation and the position of the major platforms – contrary to the Digital Markets Act's principal policy objective.

### 2. Exemption of local processing, whilst continuing to regulate remote processing

The proposed EDPB guidelines explicitly differentiate between local and remote processing. Paragraph 43 stipulates:

"The use of such information by an application would not be subject to Article 5(3) ePD as long as the information does not leave the device, but when this information or any derivation of this information is accessed through the communication network, Article 5(3) ePD may apply".

This targeting of remote processing, whilst exempting local processing, stems from the misconception that local processing is a safer and a more transparent method. It is predicated on the assumption that, as local processing happens on consumers' own devices, an individual would have more knowledge about the software code and data processing occurring. This is simply untrue, as the vast majority of consumers have little to no visibility or understanding of operating system or browser code that runs on their devices. Moreover, it would be counter to public policy to allow consumer software operating system and browser manufacturers to pass significant processing costs onto unaware consumers via local processing used for their own business-facing purposes.

The EDPB's position exempts local processing, despite there being no evidence that the harms envisaged by server-side processing could not be inflicted using the same processing running locally. Instead of differentiating between local processing and remote cloud processing, the EDPB must focus on *what* data is being processed, rather than *how*.

### Conclusion

Without addressing the aforementioned issues, the EDPB's guidelines are at risk of regulatory overreach, placing excessively onerous compliance obligations on smaller, independent stakeholders. The remedy is clear: focus on regulating only sensitive, identity-linked information whilst exempting deidentified data, rather than making artificial distinctions between local and remote processing that benefits internet gatekeepers in contravention of new protections for interoperability via the Digital Markets Act.

Yours faithfully,

Perto & lo

Preiskel & Co LLP