amazon EU SARL

COMMENTS ON THE EDPB GUIDELINES 02/2026 ON ANONYMISATION

Amazon welcomes the opportunity to contribute to the public consultation on the EDPB's draft Guidelines 02/2026 on Anonymisation. We appreciate the EDPB's effort to update the framework established by the Article 29 Working Party's Opinion 05/2014, reflecting developments in CJEU case law (notably EDPS v SRB, C-413/23 P) and the evolving technological landscape.

As a technology company that processes data, including personal data, at scale, Amazon invests significantly in anonymisation and privacy-enhancing technologies. This enables us to develop and improve services, conduct research, and generate insights while protecting individuals' personal data. We have a direct interest in a framework that sets clear, workable standards and gives organisations confidence that properly anonymised data will be recognised as such.

We believe the Draft Guidelines strike a broadly positive balance. In particular, we support the contextual approach, which recognises that anonymity may vary from one entity to another depending on their respective means and capabilities, consistent with CJEU jurisprudence and the practical reality of modern data ecosystems. We also welcome the practical orientation of the Guidelines, including the focus on how to conduct a re-identification risk assessment in practice and the worked examples illustrating the application of the three criteria. We encourage the EDPB to maintain and further develop this operational dimension in the final text.

We set out below areas where the final Guidelines could, in our view, be further strengthened.

1. The re-identification risk assessment: ensuring a realistic and proportionate framework

The Draft Guidelines establish a comprehensive and well-structured framework for assessing re-identification risk. We believe some further refinement could help ensure the framework remains fully workable in practice and produces assessments that consistently reflect real-world conditions. In particular:

- The contextual approach represents a significant and positive step forward. To maximise its effectiveness, it would be helpful for the Guidelines to ensure that this approach remains firmly tied to a practical, risk-based assessment. The evaluation of whether means are reasonably likely to be used to re-identify an individual should be anchored in the realistic probability of re-identification occurring (including the consideration of factors like valid and reliable internal segregation measures, regardless of company structure), rather than relying on abstract organisational considerations that may not reflect genuine risk.

- Scope of "relevant entities" (para. 30). We appreciate the Guidelines' thorough approach to identifying whose perspective should inform the re-identification assessment, including adversarial actors such as cybercriminals or rogue employees. We think the final Guidelines would benefit from clearer guidance on how controllers should prioritize and scope this analysis in practice. In particular, it would be helpful to build on the existing acknowledgement (fn. 25) that not all perspectives need to be considered systematically in every case, and to provide criteria for when adversarial scenarios can reasonably be set aside, for example where appropriate security measures make unauthorized access unlikely. By way of illustration, in the scenario considered in Example 8, the media company's outdated security leads to a negative anonymity assessment because unauthorised third parties could likely access the data. It follows, however, that if the media company adequately upgrades its network security such that unauthorised third-party access becomes unlikely, the re-identification risk from those unintended recipients could fall below the "insignificant" threshold and the anonymity test could yield a positive outcome. This would help controllers focus their assessment on realistic scenarios, in line with the "means reasonably likely to be used" standard.

- We understand the Guidelines' caution against over-reliance on motivation or contractual prohibitions as standalone factors. We think it would be more in line with the contextual approach and the "means reasonably likely to be used" standard to consider these elements as part of the overall assessment rather than exclude them entirely. For instance, motivation, when weighed alongside capability, cost, and time, informs a reasonableness analysis. Equally, we believe the final Guidelines would benefit

from recognizing that contractual prohibitions, when supported by verifiable compliance mechanisms (e.g., technical controls, penalties), meaningfully reduce re-identification likelihood and could be considered a relevant factor within the holistic assessment the Guidelines themselves advocate.

- We also note that the Guidelines' treatment of the No Inference criterion would benefit from additional practical guidance. As analytical techniques and AI capabilities advance, guidance on how controllers should calibrate the "means reasonably likely to be used" test in relation to AI-based re-identification techniques would be valuable, for example to distinguish between capabilities that are realistically deployable in a given context and those that remain theoretical. Examples illustrating these boundaries would assist controllers in applying these standards consistently and proportionately. We would also welcome further guidance on how the No Inference criterion applies where the inference is not drawn from an individual's own data but from general, population-level, or publicly available information, even when these are applied to a specific individual.

2. Operationalizing the “insignificant” risk standard and practical examples

We welcome the Guidelines’ principled position that re-identification risk need not be zero, only “insignificant in reality” (para. 22). To ensure this proportionate standard is applied consistently, we think the final Guidelines would benefit from clearer operational benchmarks. Currently, the absence of quantitative or qualitative guidance on what “insignificant” means in practice creates a risk of divergent interpretation across Member States and leaves controllers without the tools to demonstrate compliance. While the Guidelines currently include helpful, worked examples illustrating where anonymisation techniques fall short of establishing that data is no longer personal data, we encourage the EDPB to complement these with examples showing where anonymisation succeeds, demonstrating configurations, techniques, or contextual factors that meet the “insignificant risk” standard across common use cases such as research data sharing, aggregated analytics, etc.. Balanced examples would provide real operational value: they would give controllers a practical reference point for what “good” looks like and encourage investment in privacy-enhancing technologies. Such examples need not establish rigid technical mandates; rather, they would signal that good-faith implementation of recognised privacy-enhancing techniques is positively valued by the EDPB, providing organisations with concrete reference points to work towards. Similarly, the Guidelines' requirement that controllers periodically reassess anonymisation effectiveness (para. 35) would benefit from indicative criteria, whether event-driven, time-based, or a combination, for when reassessment is warranted. Practical guidance on how to calibrate the "adequate safety margins" referenced in paragraph 88, particularly in light of foreseeable AI developments, would help ensure this obligation is applied consistently.

***

We appreciate the EDPB’s work on these Guidelines and the opportunity to contribute to this consultation. We remain committed to responsible data practices and to the development of a framework that enables innovation while upholding the highest standards of privacy protection. We would welcome the opportunity to discuss these points further with the EDPB.