Criteo's Comments on the EDPB Draft guidelines 02/2026 on Anonymisation adopted on 07 July 2026

We welcome the EDPB's release of draft guidelines on anonymisation (the "Guidelines"). Anonymisation is an important concept as it enables to define the limits of the GDPR. It helps to delineate personal data that is fully subject to the GDPR's obligations and anonymous data that is not subject to the GDPR.

Clear and practical guidelines on anonymisation can provide enhanced legal certainty which brings benefits for organisations and data subjects:

- **Better allocation of resources to implement the GDPR**: Organisations avoid wasting resources to implement the GDPR obligations to data[1] even when they are unsure whether data qualifies as personal data or anonymous. These resources can be better allocated to data processing activities that may convey risks to individuals.

- **More trust to innovate with data**: organisations have a clear indication of which data can be more widely shared, reused and repurposed including for AI training. Consequently, organisations can invest more in robust processes to protect personal data and implement data subject rights.

General comments:

- **The Guidelines do not make any reference to the Helsinki statement** to explain how they enable to implement its principles. The EDPB should better explain how the Guidelines enable a fundamental rights approach to innovation, facilitate GDPR compliance especially for SMEs, foster competitiveness, empower responsible innovation, enhance consistency and promote cross-regulatory cooperation.

- **The Guidelines do not align with the Helsinki's statement to provide concise guidance that is accessible, easy to understand, and practical for SMEs**. The 34-page legalistic document provides a few examples but overall is not concrete enough to be understood easily by organisations of all sizes and all risk profiles. As requested by a Cross-Industry Joint Letter of 19 November 2025, calling for clear and practical guidance following the CJEU SRB case, the Guidelines should include operational and auditable standards with a list of positive tasks, controls, checklist and how-tos. This would make the Guidelines more workable in practice for organizations and would facilitate the effective anonymisation of data.

- **The Guidelines do not reference the multistakeholder workshop** held on12 December 2025 to collect stakeholders' input on anonymisation and pseudonymization, nor does it reference the corresponding report published on 18 February 2026 that summarises the main ideas and issues raised by participants. This event was intended to inform and support the EDPB's ongoing work on these topics, and particularly the Guidelines on anonymisation.

[1] e.g. DPIAs, records of processing activities, contractual negotiations with business partners, safeguards in case of transfer of personal data.

The Guidelines should not be drafted in isolation of these important exchanges with the relevant stakeholders. The Guidelines should at minimum explain why some points raised during the discussions have been selected and why some have been disregarded.

- **The Guidelines fail to rely on concrete empirical evidence** and reference purely hypothetical use cases. They also tend to describe what does not work for effective anonymisation rather than providing a toolbox of measures and safeguards that enables to achieve anonymisation in practice. The EDPB should consider the report From pseudonymous to anonymous data that compiles five concrete, real-world and industry-driven use-cases on data pseudonymisation and anonymisation provided by leading EU companies across sectors[2].

- **The Guidelines seem to reinvent the wheel.** They fail to rely on existing European and international standards (such as ENISA, ISO or OECD[3]) or guidance from other DPAs. These references could help developing structured methodologies across sectors and borders that combine legal principles and practical implementation.

- **The Guidelines adopt a precautionary approach** by recommending taking a maximalist interpretation of the GDPR or to always applying the GDPR in case of doubt, which is not grounded in law and even contradicts the GDPR's risk-based approach.

- **The Guidelines fail to acknowledge the relevance of the concept of anonymization across the EU digital rulebook:** GDPR, DMA, DGA, Data Act, AI Act for instance. The Guidelines need to ensure that the anonymisation standard of the EDPB also works under these regulatory regimes. For example, the DMA references anonymisation as compliance measure[4] and the Data Act defines non-personal data as data other than personal data.[5] There is no indication whether the Guidelines are being reviewed by other relevant regulators to ensure workability and consistency across all digital areas and different policy objectives.

We welcome the following:

- The Guidelines acknowledge the relative notion of personal data in line with the CJEU longstanding case law, including the SRB case.

- The Guidelines provide for a test methodology according to which if one of the criteria fails, it is still possible to conduct further analysis to assess whether the data can still qualify as anonymous data.

---

[2] The report shows that: (1) The threshold for pseudonymised data to actually qualify as anonymous is in practice very high; (2) Achieving anonymisation requires layered safeguards, combining technical, organisational and contractual measures; (3) Identifying recurring patterns and effective safeguards can support the definition of clear, operational criteria to determine when pseudonymised data becomes anonymous.

[3] See for instance https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases; ISO/IEC 27559:2022 - Privacy enhancing data de-identification framework; ISO/IEC 20889:2018 - Privacy enhancing data de-identification terminology and classification of techniques; ; OECD Global Repository for Privacy Enhancing Technologies

[4] See Article 6(11) of the DMA.

[5] See Article 2(4) of the Data Act.

- The Guidelines clarify that the CJUE standard of "*not being ruled out that the receiving entity has the means to identify the individual*" is not to be understood as a risk zero standard – which is impossible to implement in practice – but means that the risk needs to be insignificant in reality as it would involve disproportionate efforts to identify the individual or would be legally prohibited. (see paragraphs 21 and 22)

Unfortunately, many of these positive points fail to be implemented in the examples provided.

We respectfully ask the EDPB to reconsider the following:

- The Guidelines do not clarify anonymisation **in relation to other key concepts** such as pseudonymised data, deidentified data, non-personal data, synthetic data or other Privacy Enhancing Technologies (PETs). This could be done by the insertion of a glossary as annex of the Guidelines.

- The Guidelines miss the opportunity to consider that proper anonymisation works for **data deletion** obligations (paragraph 10) and contributes to storage limitation. If once anonymous, the data falls outside of the scope of the GDPR, it should be considered that the original personal data has been properly deleted.

- In paragraph 29, the Guidelines require that to assess whether an entity is likely to use certain means to identify an individual, **all objective factors** that might influence the availability of such means should be considered. This seems to veer again towards an objective approach of the notion of personal data not aligned with the CJEU standard and appears to be a standard impossible to reach.

- The Guidelines provide that **unauthorised and malicious actors, rogue employees, or unethical companies** should be included in the list of entities to consider as able to identify the individual (paragraph 30). Such condition does not seem realistic as malicious and unethical actors potentially operate in all industries and contexts. This condition is impossible to assess realistically. On this point, the Guidelines raise the level of legal uncertainty instead of bringing legal clarity destined to help organisations; To be on the safe side, they will continue to consider all data as personal data to avoid any future misalignment with the data protection authorities.

- If the EDPB keeps this condition, it should explain clearly how this assessment must be done in practice and provide concrete use cases when data passes muster this requirement. It could also reference available resources on how to conduct a "**motivated intruder test**" to help organisations determine whether data is likely to result in the identification of a person. It should also agree on a common methodology used by the DPAs when they conduct their own assessment. This would raise the level of legal certainty by aligning risk assessments methodologies between organisations and DPAs.[6]

[6] See the ICO guidance on anonymisation explaining how the test works, providing official links and confirming that the ICO and the UK courts rely on this test https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/how-do-we-ensure-anonymisation-is-effective/#applythemotivatedintrudertest

- Similarly, paragraphs 32 and 33 should be redrafted to comply with the CJUE case law according to which **means do not need to be considered if they are prohibited by law**. As currently drafted, these paragraphs create more legal uncertainty for organisations.

- Paragraph 31 on **lack of motivation** should be reviewed to consider the EPDB acknowledgment that risk zero is not achievable and that an insignificant residual risk can remain. The examples provided by the EDPB in this paragraph are exactly these edge cases that make risk zero impossible: an accident or an entity exceptionally forced outside of reasonable circumstances to identify and individual.

- Paragraph 36 needs to be reconsidered. There are no legal grounds to consider that a **mixed data set containing both personal and anonymous data** should always be treated as personal data. This interpretation goes beyond the law. The assessment in each case must be left to the organisation. Ideally, the Guidelines should help organisations identify personal and non-personal data in mixed data sets.

- The last sentence of paragraph 48 introduces a **precautionary standard** that is not required by the GDPR and that goes beyond the risk-based approach of the GDPR. No more cautious approach is required than strictly necessary. Subjecting data to the GDPR "in case of doubt" goes against providing the legal certainty organisations are asking for and reinforces the waste in resources. The Guidelines encourage organisations to apply the list of obligations of the GDPR to data where it may not be in fact necessary to do so.

- The Guidelines consider that **being able to single out an individual** and treat him/her differently amounts to identification. We disagree with this assessment and consider on the opposite that being able to single out an individual and treat him/her differently does not amount to direct or indirect identification. The "**no record isolation" criteria** (a natural person can be identified of identifiable if it can be distinguished from others in a context in a way that makes it possible to treat them differently) should only contribute to the possibility that data may be personal, but may not, in of itself constitute a criteria for the party that does not hold the reasonable means to identify this individual. Saying otherwise would not be aligned with the SRB ruling. In addition, subjecting this data to the regime of the GDPR would not really add value for individuals as anti-discrimination laws already regulate situations where individuals, regardless of whether they are directly or indirectly identified or identifiable, are treated differently (Paragraph19).

- The Guidelines' structure should be reviewed to clarify the test to be conducted and their concrete consequences to enable that **identifiability is assessed concretely and not merely presumed.**

    - Paragraphs 6 and 18 set up two separate tests: does the data relate to a person? and is that person identified or identifiable? Paragraph 18 says plainly that relating to someone is "not enough" to make them identifiable. Differential treatment belongs to the first test (the "effect" limb at paragraph 16(c)), which asks whether processing is liable to affect a person's rights because they could be treated differently as a result.
    - Paragraph 19 then folds that first test into the second: it defines identification itself as distinguishing an individual to treat them differently. Example 6 applies this: a

third-party using fingerprint-derived pseudonyms to distinguish and treat individuals differently is said to render them identifiable from that party's perspective, with no inquiry into whether the third party can ever put a name to any of them[7].

- The following developments then become irrelevant. The "means reasonably likely to be used" test at paragraphs 26 to 35, and the three-criteria framework built to test No Record Isolation, No Linkage and No Inference, all become redundant, because paragraph 19 has already decided the outcome for any data used to single someone out. It also undercuts the Guideline's own standard two paragraphs earlier, at paragraph 22, that the likelihood of identification need not be zero, only insignificant in reality: a test that returns "identified" the moment singling out is possible leaves no room for that assessment to ever run.
- On this logic, any service built on distinguishing one user from another is personal data, regardless of whether anyone involved can retrieve a name. That is a conclusion the Guidelines reach by assumption at paragraph 19, not by applying the contextual, risk-based test of the SRB CJEU case.

[7] As the EDPB explains in the Guidelines (see paragraph 3), if one of the criteria fails, it is still possible to conduct further analysis to assess whether the data can still qualify as anonymous data. See example 24 for an opposite outcome.