Position Paper

EDPB Guidelines 02/2026 on Anonymisation: Numeum calls for operational, risk-basedand workable guidance

Numeum response to the public consultation, September 2026

Executive summary

Numeum, the French trade association for the digital sector, represents 2,500 technology companies, from innovative SMEs to large international players, covering the full digital value chain, including AI, cloud services, data management, cybersecurity, and digital infrastructures. Our members are directly affected by the way the notion of anonymous data is defined, since it determines which processing activities fall within the scope of the GDPR and which data can be safely put to use.

Numeum welcomes the EDPB decision to update the 2014 doctrine on anonymisation in the light of CJEU case law. Two clarifications are particularly valuable and should be preserved: the recognition that identifiability is relative and assessed from the perspective of each relevant entity, and the confirmation that anonymity does not require a zero risk of re-identification but a risk that is insignificant in reality.

The draft nonetheless remains a long and largely theoretical document which, in several places, sets expectations that cannot be met in practice. The strategic stakes are significant: the notion of anonymous data circulates across the wider digital acquis, and any uncertainty introduced here will propagate to other instruments and weigh directly on AI development in Europe. Numeum therefore calls on the EDPB to convert these principles into operational, auditable and risk-based standards.

Anonymisation and pseudonymisation are distinct concepts, but they are closely related in the way they bear on data protection, and joint guidance, or guidance released in tandem, would have been preferable. Since the EDPB has chosen otherwise, it should at least anticipate the crossover between the two sets of Guidelines. Numeum considers that the finalisation of both sets of Guidelines should be paused, which would also allow the EDPB to take account of recent case law and of the ongoing Digital Omnibus negotiations.

Numeum therefore calls on the EDPB to:

- Deliver legal certainty and actionable guidance
- Calibrate the assessment of re-identification risk
- Recognise the technical state-of-the-art
- Clarify the legal test and its wider articulation
- Pause the finalisation of both sets of Guidelines

1) Provide guidance organisations can act upon

➢ Provide positive use cases and auditable standards

The draft almost exclusively describes situations where anonymisation fails and provides no roadmap for success. Instead of what now stands as abstract legal analysis, organisations need operational deliverables. The Guidelines should be drafted as a compliance framework that engineering and product teams can build against, supported by a cumulative approach combining technical and organisational measures, including audits.

The Guidelines also start from scratch instead of building on existing international standards. ISO standards addressing re-identification risk already exist and could provide a structured methodology combining legal principles with practical implementation.

Recommendation: The EDPB should include concrete examples of successful anonymisation in standard business operations, and complement the Guidelines with checklists, controls and auditable methodologies. The Guidelines should build on existing methodological work rather than developing an approach in isolation, drawing on European standardisation work and on guidance already issued by national authorities, and taking international standards into account where they are consistent with the GDPR standard as interpreted by the CJEU.

➢ Provide guidance that organisations can act upon

The draft is a long and legalistic document that does not, in its current form, provide the legal certainty organisations need. This is a concern of principle as much as of practice: the less clearly the boundaries of anonymity are defined, the broader the scope the regulator retains to determine the limits of its own intervention. This contradicts commitments made in the Helsinki Statement to provide concise guidance that is accessible and practical, including for SMEs.

Recommendation: The Guidelines should explain how they implement the Helsinki Statement and should be complemented by a concise operational version accessible to organisations of all sizes and risk profiles.

➢ Reflect stakeholder input and publish the outcome of the consultation

The Guidelines make no reference to the multistakeholder workshop of 12 December 2025, nor to the resulting report published on 18 February 2026. This gives the impression that they were prepared in isolation from stakeholder input. Other authorities, however, have published detailed consultation reports explaining which points were retained and which were set aside. The Guidelines would benefit from offering the same level of transparency.

Recommendation: The Guidelines should set out why certain points raised were retained and others disregarded. The EDPB should also publish a substantive summary of the consultation responses received, going beyond the report on the stakeholder event published in February 2026.

2) Calibrate the assessment of re-identification risk

➢ Scale the threat model to the sharing environment

The Guidelines currently state, in paragraph 29, that all objective factors influencing the availability of re-identification means should be considered. Paragraph 30 lists the entities to be considered, including rogue employees, cybercriminals, unethical companies, and domestic and foreign intelligence agencies. Taken together, these provisions describe a test that cannot realistically be performed. Malicious actors exist in every sector and every context, hence paragraph 30 could apply to virtually any dataset. Referencing national and foreign intelligence agencies seems particularly excessive. Having a clear vision of these organisations' technological capacities and therefore their capability to reidentify data is by nature extremely difficult. Since the risk that these organisations have unknown reidentification methods will never be zero, the provision could support an interpretation under which no data is ever anonymous.

The practical effect runs counter to the objective of legal certainty. Organisations will qualify all data as personal just in case, diverting compliance resources away from the processing activities that genuinely present risks to individuals.

Recommendation: The EDPB should focus on what is reasonably likely in a specific processing context, rather than on abstract risks that are conceivable but remote. It should also clarify whether previous breaches are relevant to a current assessment, and under what conditions of comparability. More specifically, the Guidelines should adopt a proportionate framework centred on the foreseeability of re-identification, scaled to the nature and openness of the sharing environment. Assuming that a trusted recipient will act as a malicious attacker in voluntary, controlled B2B settings between vetted partners using secure infrastructure is a disproportionate baseline. Where data is broadly disseminated or shared under mandatory frameworks, the attack surface expands and the assessment should reflect that. The Guidelines should distinguish explicitly between exceptional and ordinary scenarios. Besides, if the current approach is retained, the Guidelines should explain how organisations are expected to conduct this assessment in practice. This should include reference to the motivated intruder test and set out the methodology supervisory authorities apply themselves.

➢ Align paragraphs 31 to 33 with paragraph 22 and with CJEU case law

Paragraph 22 recognises that anonymity does not require the likelihood of re-identification to be zero, but only that it be insignificant in reality. Paragraphs 31 to 33

substantially narrow that opening. Paragraph 31 sets aside the argument that an entity has no motivation to re-identify, on the grounds that identification may occur by accident or negligence, or because an entity is compelled by outside circumstances to identify an individual. These are precisely the residual and unpredictable scenarios that can never be entirely excluded, and which are the reason why a zero-risk standard is unattainable in the first place. Relying on them to discount an otherwise relevant factor therefore reintroduces, in substance, the requirement that paragraph 22 expressly disclaims. Paragraph 32 then confines the CJEU holding on legally prohibited means to actors effectively constrained by the rule of law, going beyond what the case law provides. Paragraph 33 allows the assumption of compliance with the law to be rebutted wherever a concrete risk of unlawful means is evidenced, so that no assessment can ever be regarded as settled. Taken together, these paragraphs withdraw much of the flexibility paragraph 22 appears to grant.

Recommendation: Paragraphs 31 to 33 should be redrafted for consistency with paragraph 22 and with settled CJEU case law[1], under which means prohibited by law need not be considered where the likelihood of their use is insignificant.

- **Revisit the treatment of mixed datasets and the precautionary default**

Paragraph 36 states that when a dataset contains both anonymous and personal data, it must be treated as personal data entirely. Treating an entire dataset as personal because a small number of records may be identifiable also disregards the realities of data management. The Guidelines fail to consider the techniques a controller may use to isolate a single record in order to preserve the remainder of the set. Such an extensive approach is not grounded in the GDPR and disregards the EU principle of proportionality. Paragraph 48 compounds this by introducing a precautionary standard under which data is subjected to the GDPR in case of doubt, which likewise goes beyond the risk-based approach of the Regulation.

Recommendation: Paragraph 36 should replace blanket dataset-wide qualification with a contextual assessment. Controllers should be permitted to evaluate whether identifiable records can be effectively segregated, and whether the presence of residual identifiable records realistically increases the identifiability of the remainder of the dataset. The last sentence of paragraph 48 should be deleted, as no greater caution than strictly necessary is required by the GDPR.

- **Clarify the triggers for reassessment**

Numeum shares the view that re-identification risk evolves over time. However, the obligation set out in paragraph 35 is open-ended and creates a risk of permanent reassessment without a defined framework. The Guidelines also appear to create a

[1] Breyer c. Bundesrepublik Deutschland (C-582/14), § 46.

separate accountability pathway for anonymisation, whereas the risks involved are the same as those already addressed through existing controller obligations.

Recommendation: The Guidelines should identify clear triggers for reassessment, such as a security incident, a documented evolution in the state-of-the-art, or a defined periodicity, aligned with existing controller accountability measures, rather than an undefined continuous obligation.

3) Recognise the technical state-of-the-art

➢ Provide concrete guidance on Privacy Enhancing Technologies

The Guidelines do not address the rapid evolution of Privacy Enhancing Technologies, nor do they clarify the relationship between anonymisation and adjacent concepts such as pseudonymised data, de-identified data, non-personal data and synthetic data. What organisations need is not an exhaustive list of approved techniques, but concrete examples of what works and what does not. The current level of abstraction, however, is too high to guide implementation.

The treatment of noise addition and distortion techniques deserves particular attention. These methods involve a trade-off between the degree of distortion applied and the residual utility of the data, and properly calibrated differential privacy should be recognised as a protective measure rather than treated as a residual risk. Here too, the assessment should focus on what is reasonably likely, namely the likelihood of re-identification where differential privacy is in place, taking account of the privacy parameters, the threat model, the assumptions made about auxiliary data and the evidence retained by the controller.

Recommendation: The EDPB should add a non-exhaustive annex addressing state-of-the-art Privacy Enhancing Technologies, including Trusted Execution Environments, secure multi-party computation, differential privacy and advanced cryptographic protocols, illustrated by concrete examples of effective and ineffective implementations, and expanding on the role these technologies may play in supporting an anonymisation assessment. Given the pace of innovation in Privacy Enhancing Technologies and in their validation, the EDPB should make clear that the examples given are a snapshot in time rather than a closed list. This list should be updated regularly to take into account technological developments. The annex should be coupled together with a glossary clarifying the relationship between anonymisation and neighbouring concepts.

4) Clarify the legal test and its wider articulation

➢ Clarify the relationship between singling out and identification

The Guidelines set out two successive questions: whether the information relates to a person, and whether that person is identified or identifiable. Under paragraph 16, information relates to a person where, among other things, its processing makes it concretely possible to treat that person differently from others. Paragraph 19 then defines identification as distinguishing an individual in a way that makes it possible to treat them differently.

Both questions, therefore, turn on the same element. As a result, any record that can be singled out is treated as relating to an identified person, without any need to ask whether an entity actually holds means reasonably likely to be used to identify them. The means test and the three criteria framework, which occupy the bulk of the Guidelines, then have nothing left to determine, since the outcome is settled as soon as a record can be isolated.

Recommendation: Paragraph 19 should be revised so that the possibility of singling out contributes to, but does not by itself establish, identification for an entity that does not hold means reasonably likely to be used to identify the individual. Differential treatment of individuals is already addressed by anti-discrimination law.

➢ Ensure coherence with the wider digital acquis and with erasure obligations

The Guidelines do not address the relevance of anonymisation under other digital frameworks, including the DMA, the DGA, the Data Act and the AI Act, nor whether the definition has been reviewed for workability across these regimes. This matters beyond the GDPR: these Guidelines shape the contours of several other instruments, and any uncertainty they create will propagate across the wider framework and weigh directly on AI development.

Recommendation: The EDPB should confirm the cross-regulatory workability of its definition, in coordination with the other regulators concerned.

Paragraph 10 further leaves open whether anonymisation contributes to storage limitation. Where data is properly anonymised and falls outside the scope of the GDPR, the original personal data should be considered to have been erased for the purposes of storage limitation, and the Guidelines should say so.

➢ Ensure coherence with the Digital Omnibus

The Guidelines are being finalised in parallel with the negotiations on the Digital Omnibus, which would address the definition of personal data at legislative level.

Recommendation: The EDPB should ensure that these Guidelines remain sufficiently flexible and risk-based so as not to contradict the outcome of the Digital Omnibus negotiations and should commit to reviewing them once the co-legislators reach political agreement.

Conclusion

Numeum supports the EDPB objective of clarifying when data can be considered anonymous, and the draft contains clarifications that European companies have been waiting for. These should be preserved.

However, to deliver on that objective the Guidelines must move from abstract legal analysis to operational standards that organisations can implement and auditors can verify, and must calibrate their expectations to what is technically achievable today. Given the influence this definition will have across the wider digital framework, the cost of leaving it abstract extends well beyond the GDPR. Numeum stands ready to contribute technical input and concrete examples, and to engage constructively with the EDPB.