Contribution to the EDPB Public Consultation

Guidelines 02/2026 on Anonymisation

Submitted by **La Minute Data** October 2026

1. Purpose and scope of this contribution

La Minute Data welcomes the EDPB Guidelines 02/2026 on Anonymisation and their contextual approach to identifiability. This contribution focuses on a narrow operational issue concerning the effectiveness over time of an anonymisation assessment where that assessment materially depends on the accessibility, from the relevant perspective, of additional information held by another relevant entity or on contextual elements under another relevant entity's control.

The purpose of this contribution is not to suggest a general monitoring or notification obligation between entities. Rather, it proposes a limited clarification of paragraph 35 concerning how the reassessment already contemplated by the Guidelines can operate effectively where relevant external factors underlying the initial assessment may subsequently change.

2. Paragraph 35 read together with paragraphs 34, 42, 47, 51 and 88-90

Paragraph 35 expressly recognises that the likelihood of re-identification may increase over time, notably because of developments in re-identification technologies and techniques and the increased availability of additional information. It accordingly recommends, wherever possible and as appropriate, that entities processing anonymised data periodically reassess the likelihood of re-identification.[1]

This temporal dimension should be read together with paragraph 34, which recognises that contractual terms may affect which means are reasonably likely to be used, while noting that such measures may be revised or disregarded and should be reliable, verifiable and enforceable.[2]

Paragraph 42 also recognises, in the specific context of a security incident, that an incident may lead to reassessment where the assessment relied on certain information remaining confidential and that confidentiality is affected.[3]

This temporal dimension should also be read in light of paragraph 47. The Guidelines acknowledge that the contextual approach may be complex where it is difficult to account for, or even know about, all relevant contextual elements, and that this may create a risk of false positives where an assessor is unaware of means reasonably likely to be used by another entity.[4]

Paragraph 51 further recommends, as an early step in the assessment, mapping the data together with additional information that may aid re-identification and that is either held by other relevant entities or accessible to them through means reasonably likely to be used.[5]

The Guidelines also address the evolution of relevant entities' capabilities under the contextual approach. Paragraph 88 recognises that those capabilities may vary over time and gives the example of a data leak making previously unavailable datasets accessible. It therefore recommends incorporating, as much as possible, adequate safety margins so that the assessment remains robust as entities' capabilities evolve. Paragraphs 89 and 90 further emphasise the accessibility of data and additional information and the need to assess access restrictions holistically in light of the capabilities of the different relevant entities and the surrounding contextual elements.[6]

Taken together, these provisions already recognise the contextual and evolving nature of anonymisation assessments, the distribution of relevant information and means across different entities, the importance of anticipating changes in their capabilities, and the need for reassessment over time.

3. Practical difficulty: reassessment where relevant external factors may change

The practical issue arises where an anonymisation assessment supports a conclusion of anonymity at the time it is carried out but materially depends on factors relating to another relevant entity. These may include additional information held by that entity, restrictions affecting access to such information, or other contextual elements that contribute to keeping the likelihood of re-identification insignificant.

---

1 European Data Protection Board, Guidelines 02/2026 on Anonymisation, Version 1.0, adopted on 7 July 2026 for public consultation, para. 35.

2 Ibid., para. 34.

3 Ibid., para. 42.

4 Ibid., para. 47.

5 Ibid., para. 51.

6 Ibid., paras. 88-90. Paragraph 88 concerns evolving capabilities and adequate safety margins; paragraphs 89-90 concern the accessibility of data and restrictions on access.

At the time of the initial assessment, such factors should be considered as part of the contextual analysis insofar as they are known or can reasonably be identified. Paragraph 51, in particular, recommends mapping additional information that may aid re-identification and that is either held by other relevant entities or accessible to them through means reasonably likely to be used.

Paragraphs 88-90 also provide an important safeguard. By recommending adequate safety margins and a holistic assessment of access restrictions and evolving capabilities, the Guidelines seek to make contextual assessments sufficiently robust as relevant entities' capabilities evolve over time. Adequate safety margins can improve the robustness of an assessment against such changes. They do not, however, by themselves resolve the separate question of whether a material change to an external factor can become known to the entity relying on the assessment.

A distinct residual difficulty may therefore arise where a factor on which the assessment materially depends subsequently changes without the entity relying on the assessment necessarily becoming aware of that change. The Guidelines already recognise both that contextual elements may be difficult to know and that the likelihood of re-identification may evolve over time.

The issue is therefore not whether the Guidelines address changing capabilities or contemplate reassessment. Rather, where the assessment remains materially dependent on an external factor despite the precautions built into the initial analysis, the effectiveness of reassessment may also depend on whether relevant changes can become known to the entity relying on that assessment. A limited clarification on this point could strengthen the practical operation of paragraph 35 where relevant factors are distributed across entities.[7]

4. Operational illustrations

A recent practical assessment of a generative AI architecture operating under a Zero Data Retention ("ZDR") arrangement illustrates one aspect of this issue. In that use case, an organisation removes direct identifiers before prompts are transmitted to an AI provider, while the provider is expected to enforce zero retention through technical controls at infrastructure level.

The report notes that the organisation cannot itself inspect the provider's infrastructure and that this part of the assessment therefore rests on the provider continuing to honour that condition. It further identifies audit rights or independent attestation as possible means of verifying that system or contractual changes have not altered the relevant retention safeguards.

The relevance of this example is not the particular conclusion reached as to anonymity, but the fact that an assessment concerning another entity's perspective may depend on a technical condition whose continued application is not directly observable by the entity carrying out or relying on that assessment.[8]

An audience-measurement use case illustrates two related but distinct aspects of the same practical difficulty. The platform receives only aggregated reports, while the provider retains the underlying raw signals, panel roster, identifier mappings and processing logic.

First, the report notes that the provider deletes or anonymises its raw data according to its own retention schedule, while the platform has no visibility into that schedule and may not be informed when the underlying situation changes. This illustrates the potential information asymmetry surrounding changes occurring at another entity.

Second, the report concludes that the assessment of thin demographic breakdowns depends on the provider suppressing cells below a minimum size and being able to demonstrate that safeguard on request. This separately illustrates how an assessment may depend on a safeguard implemented and controlled by another entity.[9]

These examples illustrate why, in multi-entity settings, the effectiveness of reassessment may depend on whether relevant changes to external factors can become known to the entity relying on the assessment.

> *These examples are used to illustrate operational dependency and information asymmetry; they are not intended to suggest that every change to an external factor alters the legal status of the data.*

7 This contribution assumes that the initial assessment has already accounted for the relevant perspectives and possible chains of means in accordance with paragraphs 20-21 and 28-29 of the Guidelines. Those paragraphs recognise that information and means may be distributed across entities, that transfers may affect the status of the data from the relevant perspectives, and that possible chains of means must be taken into account in the initial assessment.

8 Rob van Eijk and Benjamin de Vanssay, From Pseudonymised to Anonymous Data: A Practical Assessment Framework under the SRB Ruling, Applied to Real Use Cases Provided by European Companies, Joint Policy Report, June 2026, Use Case 1, pp. 12-13.

9 Ibid., Use Case 4, pp. 26-27.

5. Proposed clarification to paragraph 35

Against that background, La Minute Data suggests the following limited clarification to paragraph 35:

> **"Where an assessment materially depends on the accessibility, from the relevant perspective, of additional information held by another relevant entity or on contextual elements under another relevant entity's control, the entity relying on the assessment should, where appropriate, consider how relevant changes to those factors could become known and whether such changes warrant reassessment."**

The proposed wording builds on concepts already present in the Guidelines. Paragraph 47 recognises that relevant contextual elements may be difficult to know, while paragraph 51 addresses additional information held by other relevant entities. Paragraph 88 recognises that relevant entities' capabilities may evolve over time, while paragraphs 89-90 address the accessibility of data and additional information and the assessment of restrictions on access.

The proposed clarification would complement, rather than replace, the adequate safety margins recommended in paragraph 88. Safety margins seek to improve the robustness of the assessment as relevant entities' capabilities evolve; the proposed wording addresses the separate question of how a relevant change to an external factor on which the assessment materially depends could become known.

The appropriate means are deliberately left unspecified. The proposal does not prescribe continuous monitoring, notification, audit or any other particular verification mechanism, nor does it suggest that every external change warrants reassessment. It would not alter the substantive standard for anonymisation.

6. Conclusion

The proposed clarification would preserve the substantive anonymisation standard and the contextual approach established by the Guidelines. It would provide limited operational support for the reassessment contemplated by paragraph 35 in multi-entity settings where relevant external factors may change over time.

References

European Data Protection Board, *Guidelines 02/2026 on Anonymisation*, Version 1.0, adopted on 7 July 2026 for public consultation.

Rob van Eijk and Benjamin de Vanssay, *From Pseudonymised to Anonymous Data: A Practical Assessment Framework under the SRB Ruling, Applied to Real Use Cases Provided by European Companies*, Joint Policy Report, June 2026.