Asylum Research&Global Assistance

Anonymisation and reidentification risk

Response to EDPB Guidelines 02/2026

European Data Protection Board

21 October 2026 | France

ARGA — Asylum Research & Global Assistance welcomes guidance that makes anonymisation assessments explainable and reviewable. Our perspective is the protection of people whose identification can expose them to serious consequences and whose access to correction or redress may be limited. We propose practical additions to the consultation draft while preserving the GDPR test of identifiability.

1 Document the context of the assessment

The final guidance should provide a short assessment template stating the dataset and version, intended recipients, release environment, relevant actors, reasonably available auxiliary information, likely means of identification and review horizon. An anonymity claim should identify the perspective and circumstances to which it applies. A result established for restricted access should not be carried over automatically to unrestricted publication.

The analysis should consider realistic cooperation between recipients or other actors where relevant, without assuming an omnipotent adversary with unlimited resources. Conversely, contractual prohibitions should not be treated as conclusive where practical access, incentives or weak enforcement make identification reasonably likely. The record should show why assumptions about access and capabilities are credible.

We support the distinction between anonymisation and pseudonymisation. Replacing direct identifiers, hashing a field or calling data “synthetic” does not by itself establish anonymity. Data-processing steps undertaken to achieve anonymisation remain subject to the applicable GDPR requirements while personal data are being processed.

2 Explain the three criteria and their limits

Paragraphs 52–53 and section 3.5.3 should be accompanied by a worked decision record showing how the three criteria — No Record Isolation, No Linkage and No Inference — feed into the overall assessment. The guidance should make clear both the significance of satisfying all three and the need for further analysis when a criterion is not met. Failure of a screening criterion should not be reduced to an unexplained automatic verdict.

We recommend examples involving small populations, longitudinal records and unstructured narratives. Removing a name may leave a distinctive combination of location, dates, family circumstances or procedural events. An assessment limited to individual database columns can miss the identifying effect of the combined record or of linked releases.

Tests should report the attack or inference attempted, auxiliary data used, success definition, false positives, uncertainty and limits of the evaluation. A low average success rate may conceal a readily identifiable subgroup. No single numerical threshold should be presented as a universal safe harbour across datasets, recipients and release conditions.

3 Protect people during reidentification testing

Reidentification testing should not create an avoidable new disclosure. We recommend controlled environments, authorised access, minimisation of test outputs, separation of identifiers where appropriate and documented deletion or restricted retention of test material. External evaluators should be bound by suitable confidentiality and security arrangements.

The likelihood of identification and the severity of its consequences should be recorded separately. Vulnerability does not replace or redefine the legal test of identifiability. It should nevertheless inform the safeguards, release design and scrutiny of assumptions. For sensitive narratives, aggregate publication or controlled access may be preferable to releasing granular records.

The final guidance should include a decision point for uncertainty. Where the evidence does not substantiate anonymity in the planned context, the organisation should continue to apply the relevant personal-data protections or change the release design. An unresolved assessment should not be converted into an anonymity claim merely because further testing is inconvenient.

4 Treat anonymity as a maintained conclusion

We recommend explicit review triggers: new auxiliary datasets, changes in access conditions or recipients, improved identification techniques, additional releases that can be combined, and credible reports of identification. The initial decision should name a review owner and record the rationale for the review interval. Periodic reassessment should be proportionate and should not imply that every previous assessment is automatically invalid.

A response plan should describe how to investigate a credible reidentification report, preserve necessary evidence, contain further access where possible and reassess the processing under the applicable law. If public release cannot be reversed, that limitation should be acknowledged before publication and reflected in the initial decision.

We also recommend separate assessment of source data, transformed data and any model produced from them. A conclusion that a released table is anonymous does not establish that a model trained on identifiable source material is anonymous. Testing and documentation should identify the particular artefact and use context to which the conclusion applies.

5 Retain accountability and access to remedy

The draft should retain the distinction between anonymisation for a recipient and the obligations of a controller that collected identifiable data. Later anonymisation must not be used to retroactively erase transparency obligations that arose at collection. Retention of original identifiable data should be justified separately; anonymising one copy does not resolve the storage limitation assessment for all other copies.

ARGA proposes a proportionate evidence package comprising the assessment record, test results, access controls, residual uncertainties and review triggers. In cases presenting substantial consequences for individuals, independent scrutiny may be appropriate. It should test the stated assumptions and methods, not merely certify that a checklist exists.

A public explanation can describe the purpose, techniques, release context and limitations without disclosing an attack recipe or personal information. A confidential channel should allow people and qualified researchers to report credible weaknesses. The objective is an anonymity claim that remains defensible in practice and can be challenged responsibly.

References

[1] EDPB Guidelines 02/2026, consultation draft, version 1.0, adopted 7 July 2026. Principal references: paragraphs 3, 6–14 and 52–53; sections 2.4, 2.5 and 3.5.3. Official source

[2] Regulation (EU) 2016/679, in particular Recital 26 and Articles 4, 5, 13, 14, 24, 25 and 32. Official source