CEDPO Contribution on the EDPB Guidelines 02/2026 on Anonymisation

Public Consultation Response

30 October 2026

CEDPO welcomes the European Data Protection Board's Guidelines 02/2026 on Anonymisation. Clear and workable guidance can support effective protection of individuals, responsible use of anonymous information and a more consistent application of the GDPR across Europe.

CEDPO particularly welcomes the recognition that anonymity depends on the relevant perspective, that the likelihood of identification need not be zero and that the contextual approach reflects the legal standard. The distinction between record isolation and the identification of an individual is also a useful development. These elements provide a sound basis for assessments that are both protective and practical.

For Organisations and Data Protection Officers, the challenge is to translate this framework into a proportionate and documented assessment. CEDPO's comments focus on making the conclusions easier to apply, clarifying the evidence reasonably expected and promoting consistent supervisory practice. The objective should be to help organisations recognise both when anonymisation has succeeded and when personal data remain subject to the GDPR.

General remarks

The Guidelines expressly recognise that identification need not be theoretically impossible (paragraphs 8 and 22). They also explain that the simplified approach is voluntary, can produce false negatives and does not constitute an alternative legal standard (paragraphs 45 to 49). CEDPO supports these clarifications and recommends giving them greater prominence throughout the practical framework.

A defensible anonymisation assessment should address the relevant actors and the means reasonably likely to be used, rather than every conceivable identification scenario. This does not permit identifiable information to be treated as anonymous merely because the expected harm is low. Equally, the continuing application of the GDPR to pseudonymised information should not obscure the protective value of pseudonymisation and other measures that reduce risks without achieving anonymity.

1. Clarifying the conclusions of the assessment

The framework provides routes to a conclusion of anonymity, including where a criterion initially fails. Paragraphs 95 to 103 and Example 24 are important in this respect. The final Guidelines should make these routes easier to follow and use more consistent wording to describe successful outcomes: the Guidelines variously state that information can safely be considered anonymous, may be regarded as anonymous or can be presumed anonymous.

The EDPB should explain the practical significance of a positive, properly documented conclusion and distinguish it from an incomplete assessment. It should also clarify the circumstances requiring

reconsideration, without suggesting that a conclusion supported by the evidence remains indefinitely unresolved.

Footnote 36 usefully states that the simplified approach cannot definitively establish that information is personal data. This safeguard should appear in the main text. Where that approach does not establish anonymity, an organisation should be able to proceed to the contextual analysis and any further analysis required by section 3.5.3, or choose to handle the information conservatively as personal data.

The explanations of No Record Isolation and No Linkage should include prominent cross-references to the further analysis in paragraphs 98 to 103. Example 24 demonstrates why unique records do not necessarily identify individuals. The results table and Annex 1 should consistently convey these qualifications so that operational teams do not apply the criteria as standalone absolute requirements.

2. Defining relevant perspectives and chains of recipients

Paragraphs 9 and 11 to 15 provide useful guidance on relevant perspectives. CEDPO supports the distinction between an independent recipient and an entity processing on behalf of a controller. Anonymity for an independent recipient does not remove the originating controller's obligations concerning information that remains personal for it, as paragraph 37 also makes clear.

For public release, Example 1 correctly extends the assessment beyond the average reader. Further guidance should show how organisations can identify a reasonably foreseeable range of actors, accessible auxiliary information and credible chains of access without investigating every conceivable internet user. Example 22 usefully demonstrates that a reasoned assessment can exclude categories of actors whose access to the necessary combination of information is extremely unlikely. This reasoning could be developed for public releases, where access restrictions are absent.

Paragraph 21 warrants clarification. The reference to identification capabilities that "cannot be ruled out" could be read as requiring proof of their absence. The EDPB should explain how this wording operates consistently with the insignificant likelihood recognised in paragraph 22 and the assessment of the overall chain of means in paragraph 28. A merely hypothetical possibility should be distinguished from material uncertainty requiring further investigation.

A worked example involving an independent recipient and an onward recipient would help explain what the originating organisation should reasonably investigate and how reliable information from recipients can support its assessment. It should also show when a recipient's additional means affect the conclusion for earlier entities. The possibility that a later recipient will have GDPR obligations does not substitute for a sound assessment before disclosure.

3. Assessing unlawful means and the effectiveness of safeguards

CEDPO welcomes the general assumption in paragraph 32 that people will follow the law and the requirement in paragraph 33 for sufficient evidence of a concrete risk before that assumption is rebutted. Footnote 25 also confirms that the actors listed in paragraph 30 do not all need to be considered systematically. These qualifications should be brought into the main text to prevent the list from becoming a mandatory catalogue of potential threat actors.

Example 22 illustrates how the No Linkage criterion can be satisfied under the contextual approach, despite considering several possible access scenarios. It would be useful to clarify whether the inclusion of potential recipients following a hypothetical leak, despite strong security controls, reflects an additional precaution voluntarily adopted by the research institute or an expectation generally applicable to contextual

assessments. This clarification would help readers apply the example alongside paragraph 89, which recognises the effect of appropriate security controls on access.

Credible malicious access and accidental identification should not be excluded simply because they are unlawful or unintentional. Conversely, their abstract possibility should not automatically determine the outcome. Example 8 provides concrete reasons for considering unlawful access, including outdated security and previous incidents. A complementary example could show when effective controls and the absence of concrete contrary evidence justify excluding an access scenario.

Paragraphs 34 and 90 recognise that contractual, technical and organisational measures can affect the assessment. Further guidance should explain how their combined effectiveness can be evidenced, including enforceability, access restrictions, monitoring and limits on onward disclosure. Contractual restrictions should neither establish anonymity on their own nor be discounted merely because they could theoretically be breached.

4. Providing proportionate evidence and complete worked examples

The Guidelines contain useful positive and qualified examples, particularly Examples 13, 14, 20, 22 and 24. Their practical value would be strengthened by complete examples following one dataset through its transformation, all three criteria, any necessary further analysis and the final documented conclusion. CEDPO recommends examples covering published aggregate statistics and a controlled research environment.

Each example should identify the relevant perspectives, realistically accessible auxiliary information, validation performed, limitations and review triggers. It should show how additional measures change the outcome without suggesting that a particular technique or access arrangement always produces anonymous information. Examples should also distinguish anonymised outputs from retained source data and other copies.

Building on paragraph 41 and Annex 1, a short, adaptable documentation model could record the intended use, relevant actors and chains of means, transformations, safeguards, evidence, reasons for the conclusion and review arrangements. It should allow reuse of an assessment for genuinely comparable situations, subject to checking material differences.

The depth of investigation and testing should reflect the complexity of the data and the release context, while applying the same legal standard. The EDPB should explain when validated methods and reasoned analysis may suffice and when specialist testing is warranted. Organisations should not be expected to investigate every conceivable technique or independently reproduce all research on re-identification. Paragraphs 92 and 93 should support a case-specific assessment of time, cost and accessible resources rather than a general presumption that these factors can never be prohibitive.

5. Explaining inference and the reliability of identification

CEDPO supports the distinction in paragraphs 67 to 71 between specific and meaningful inference and the application of general population knowledge to an individual. Examples 13 and 14 help prevent the conclusion that any prediction about a person makes the underlying dataset personal data. This distinction should remain clear when applying paragraph 82 to AI models and synthetic data.

Further illustrations should explain the evidence needed to assess precision, reliability and confidence under paragraph 87. Example 20 usefully distinguishes a credible identification result from an inference whose correct subject cannot be established. Quantitative measures and qualitative reasoning should inform the legal assessment without introducing a universal numerical threshold. Identification should not be reduced to discovering a name, nor should uniqueness of a record alone be equated with identification of a person.

6. Clarifying the treatment of mixed datasets

Paragraph 36 appropriately distinguishes the status of particular records from the dataset as a whole and recognises separate treatment of its constituent parts. CEDPO supports the protection of individuals whose records remain identifiable. A low average identification likelihood across a dataset should not conceal a material identification possibility affecting particular individuals.

The Guidelines could nevertheless explain more practically when anonymous and personal components can be treated separately, what evidence supports that separation and how subsequent linkage or combined use affects the conclusion. This would help organisations isolate, suppress or further transform problematic records. The presence of personal data in a dataset should not be described as automatically changing the legal nature of every other record, while the processing of inseparable mixed components remains subject to the GDPR as explained in paragraph 36.

7. Making reassessment proportionate and actionable

CEDPO supports the recommendation in paragraph 35 to reassess anonymity as relevant circumstances change. Footnote 3's clarification that previous assessments under Opinion 05/2014 do not require a new assessment merely because these Guidelines are published should be included in the main text.

Practical review triggers could include material changes in recipients or access arrangements, a release enabling new linkage, credible evidence of re-identification, newly accessible auxiliary data or a relevant technical development. Periodic review should reflect the use context and reasonably foreseeable developments. The safety margins recommended in paragraph 88 would benefit from examples and a stated assessment horizon, avoiding an expectation of protection against indefinitely speculative future capabilities.

The EDPB should distinguish a later change in circumstances from evidence that the original assessment was unsound. Guidance should explain appropriate steps when anonymity can no longer be supported, including reassessing further processing and disclosure, applying additional measures and considering any incident obligations under paragraph 42. Public releases merit particular attention because retrieving all copies may be impossible.

8. Supporting DPOs and consistent supervisory expectations

Anonymisation assessment requires appropriate legal, technical, statistical and operational input. The controller remains responsible for the decision and its supporting evidence. The DPO advises and monitors compliance within their statutory role and should not be expected to certify anonymity personally or replace the expertise needed to validate a technical method.

CEDPO recommends guidance on allocating responsibilities, involving the DPO in good time, recording material reservations and documenting the controller's reasons where it departs from the DPO's advice. Documentation should support the substance of the assessment without disproportionate formality.

Common supervisory expectations concerning relevant perspectives, evidence and review would help DPOs advise consistently across Europe. Shared examples and a common documentation model should support this harmonisation while accommodating different sectors, organisational resources and release contexts.

Closing observations

The Guidelines provide a valuable basis for contextual anonymisation assessments. CEDPO encourages the EDPB to preserve that approach throughout the practical framework, clarify the targeted issues identified above and provide tools that help organisations demonstrate successful anonymisation. These adjustments would strengthen protection for individuals while supporting proportionate implementation and greater consistency across Europe.