Public Comments on EDPB Guidelines 02/2026 on Anonymisation

Version 1.0, adopted 7 July 2026 for public consultation

Submitted to: European Data Protection Board (EDPB), Public Consultation on Guidelines 02/2026 on Anonymisation
Submitted by: Jewel Darlington, Chief AI Governance Officer & Founder
Organisation: Solutions by Jewel (SBJ), United States
Contact: governance@solutionsbyjewel.com | solutionsbyjewel.com
Date: 16 October 2026

1. Introduction and Summary

Solutions by Jewel (SBJ) is an AI governance advisory firm serving mid-market and enterprise organisations. SBJ welcomes the EDPB's draft Guidelines 02/2026 on Anonymisation and the structured framework they provide: the applicable-perspective analysis in Section 2.2, the three criteria in Section 3.4, and the choice between the contextual and simplified approaches in Section 3.2.

These comments address one question the draft opens and leaves for practice to settle: how an organisation demonstrates that a conclusion of anonymity remains valid after the initial assessment, as the data, the processing context, the access conditions and the capabilities of AI systems change. The draft already establishes the premise. Paragraph 35 states that "the likelihood of re-identification typically increases over time due to advances in the technology" and that it is good practice "to periodically reassess the likelihood of re-identification." Paragraph 88 recognises that "the capabilities of different entities may vary over time" and recommends "adequate safety margins ensuring that the assessment remains robust as the entities' capabilities evolve." Paragraph 41 calls for "adequate documentation of the anonymisation processing."

The draft does not specify what triggers a reassessment beyond technological advances, the increased availability of additional information, changes in entity capabilities and security incidents; how often periodic reassessment should occur; or what the documentation in paragraph 41 should contain. SBJ offers five recommendations to close those points:

- **SBJ-ANON-01.** Set out a non-exhaustive list of material changes that should prompt reassessment (paras 35, 42, 88; footnote 3).
- **SBJ-ANON-02.** Specify minimum contents for anonymisation documentation (para 41).
- **SBJ-ANON-03.** Ask controllers to record the safety margins and assumptions each conclusion depends on, so reassessment can test them (paras 29(e), 32–34, 88, 90).
- **SBJ-ANON-04.** Treat changes to query, prompting and AI-model access as reassessment triggers (paras 77, 82, 92–93).
- **SBJ-ANON-05.** State what follows when reassessment finds that data is no longer anonymous (paras 35, 42).

2. Comments

SBJ-ANON-01: Material changes that should prompt reassessment

Relevant text: Paragraph 35; paragraph 42; paragraph 88; footnote 3.

The draft identifies the forces that erode anonymity over time: advances in technology and "the increased availability of additional information" (para 35), changes in entity capabilities (para 88), and security incidents (para 42). It describes reassessment as periodic good practice, without a frequency. An organisation applying the guidelines therefore has no reference point for deciding when a past conclusion needs to be tested again, and supervisory authorities have no common reference point for evaluating that decision.

Event-based triggers give the periodic expectation a practical form. Each of the following changes alters one or more factors listed in paragraph 29, and each is observable by the controller when it occurs:

- **Release model or recipients.** A move from restricted to public release, a new category of recipient, or onward sharing by a recipient (paras 89–90).
- **Additional information.** Publication or leak of a dataset that shares attributes with the given data, which bears directly on the No Linkage criterion (paras 29(c), 65).
- **Processing context.** Combination of the given data with other datasets, a new purpose, or new attributes added to records (paras 29(a)–(b), 56).
- **Access conditions.** Removal or weakening of a technical, organisational or contractual measure the assessment relied on, or evidence that such a measure is not being respected (paras 32–34, 90).
- **AI-system capability.** Availability of AI tools, including agentic AI, that materially reduce the time or cost of linkage or inference, which paragraph 92 anticipates (paras 29(d)–(e), 92–93).
- **Security incident.** As already addressed in paragraph 42.

SBJ also recommends that a trigger event apply to assessments carried out under Opinion 05/2014. Footnote 3 provides that such assessments need not be repeated on publication of the new guidelines. A material change after publication is a separate matter, and the guidelines would benefit from stating that legacy assessments enter the same reassessment cycle when one occurs.

Proposed text (addition after paragraph 35):

> "In addition to periodic reassessment at an interval the controller determines and documents, the EDPB recommends reassessment whenever a material change occurs in the factors listed in paragraph 29. Material changes include, among others: a change in the release model or recipients of the data; the publication or availability of additional information sharing attributes with the given data; the combination of the given data with other data or its use for a new purpose; the removal or weakening of a measure relied on to limit access; the availability of tools, including AI tools, that materially reduce the time or cost of re-identification; and a security incident as described in paragraph 42. This applies equally to assessments made under Opinion 05/2014."

SBJ reference. SBJ applies the same principle to AI authorization. Control AC-01 (Authorization Invalidation Trigger Semantics) of the SBJ AI Governance Architecture V2.0 provides that a material change to a condition supporting an authorization triggers reassessment, narrowing, suspension or revocation, and the Architecture requires that when a material change affects the conditions or evidence supporting an assurance claim, the continuing validity of that claim be reassessed. Its adversarial finding ATC1-001 treats material changes in how outputs are consumed, acted on or automated as a change in exposure, even where the underlying system is unchanged. The release-model and processing-context triggers above follow the same reasoning for anonymised data (solutionsbyjewel.com/ai-governance/architecture/).

SBJ-ANON-02: Minimum contents of anonymisation documentation

Relevant text: Paragraph 41; Sections 2.2, 3.2, 3.3 and 3.4.

Paragraph 41 provides that controllers "should ensure adequate documentation of the anonymisation processing" and that "this documentation should then be retained after the completion of the anonymisation process." It does not state what adequate documentation contains. The guidelines themselves supply the structure such documentation would follow, since each step of the analysis produces a determination that a later reviewer, including a supervisory authority, would need to see.

Proposed text (addition to paragraph 41):

> "Adequate documentation should, at a minimum, record: (a) the applicable perspective or perspectives and the relevant entities considered (Section 2.2); (b) the approach used, whether contextual, simplified or combined, and the reasons for that choice (Section 3.2); (c) the data mapping carried out (paragraph 51); (d) the outcome for each of the three criteria, the techniques tested and the evidence relied on (Sections 3.4 and 3.5); (e) the assumptions and safety margins on which the conclusion depends (paragraph 88); (f) the reassessment interval and the events that will prompt earlier reassessment; (g) the person or function that approved the conclusion; and (h) the date of the assessment and a record of any subsequent reassessments and their outcomes."

Element (g) matters for accountability under Article 5(2) GDPR. A conclusion of anonymity determines whether the GDPR applies to subsequent processing, and the record should show who was authorised to reach that conclusion.

SBJ reference. The SBJ AI Decision Record v2.0 (solutionsbyjewel.com/ai-decision-record-template) is one illustrative implementation of these elements for consequential AI decisions. It records the decision and the information that influenced it, the accountable owner and human reviewer, the evidence and its location, and a review section completed at each scheduled or triggered review, with fields for Reassessment Trigger, Reassessment Date, Material Change, Continued Authorization and Owner Sign-Off. The elements proposed above can be met in any format the controller chooses.

SBJ-ANON-03: Recording the assumptions each conclusion depends on

Relevant text: Paragraph 29(e); paragraphs 32–34; paragraph 88; paragraph 90.

Under the contextual approach, a conclusion of anonymity rests on assumptions about the world outside the dataset: the capabilities of each relevant entity, the technology available to them, and the effectiveness of legal, organisational and contractual limits on access. The draft treats these with care. Paragraph 29(e) requires account of "reasonably foreseeable technological developments"; paragraphs 32 to 34 limit the weight of legal and contractual prohibitions; paragraph 90 states that technical, organisational and contractual measures "are not by themselves sufficient"; and paragraph 88 recommends safety margins.

A reassessment can only test an assumption that was written down. SBJ recommends that the guidelines ask controllers to state, for each criterion relied on, the capability assumed of each relevant entity, the measures assumed to limit access and how their observance is monitored, and the safety margin applied. When a trigger under SBJ-ANON-01 occurs, the controller can then check the specific assumptions it affects, and the reassessment becomes proportionate to the change.

Proposed text (addition to paragraph 88):

> "The safety margins adopted, and the assumptions about entity capabilities and access limitations on which the assessment relies, should be stated explicitly in the documentation referred to in paragraph 41, so that any reassessment can determine whether they continue to hold."

SBJ reference. Control AC-05 (Evidence Sufficiency as an Authorization Condition) of the SBJ AI Governance Architecture V2.0 holds that evidence must be sufficient for the specific decision it supports, with the burden scaling to the consequence of that decision, and adopts the principle that "evidence existence does not establish evidence sufficiency." Recorded assumptions and margins are what allow a reviewer to judge whether the evidence behind an anonymity conclusion remains sufficient after a change.

SBJ-ANON-04: Query, prompting and AI-model access as reassessment triggers

Relevant text: Paragraph 77; paragraph 82; paragraphs 92–93.

The draft recognises that inferences can be drawn "by querying (or, in the case of AI models, prompting) the given data" (para 82), refers to attacks on "supposedly-anonymous AI models" (para 77), and anticipates that "developments in AI, and especially agentic AI, will likely further reduce the time and costs necessary" for re-identification (para 92). Where anonymised data is made available through a query interface, or used to train or fine-tune an AI model that others can prompt, the conditions of that access shape the No Inference analysis: who may query, how many queries are permitted, what outputs are returned, whether queries are logged, and whether the model can call external tools or retrieve additional information.

These conditions change frequently in practice: an interface opens to new users, rate limits are raised, a model is retrained or fine-tuned, or tool and retrieval capabilities are added. Each such change can make an inference feasible that was not feasible when the assessment was made. SBJ recommends that the guidelines identify these changes expressly as reassessment triggers and add an example, alongside Examples 18 and 19, showing how a controller reassesses the No Inference criterion when access to a query interface or AI model is widened.

Proposed text (addition after paragraph 82):

> "Where given data is made available through a query interface or is used to train or adapt an AI model that other entities can prompt, the assessment should take into account the conditions of that access. A material change to those conditions, including wider access, higher query volumes, retraining or adaptation of the model, or the addition of tool use or retrieval of additional information, should prompt reassessment of the No Inference criterion."

SBJ reference. Control AC-04 (Execution Identity and Material Version Binding) of the SBJ AI Governance Architecture V2.0 ties consequential actions to the specific execution instance and the material model or configuration version. Applied here, binding an anonymity assessment to the model version and access configuration it evaluated makes a later retraining, adaptation or change of access visible as a trigger.

SBJ-ANON-05: What follows when reassessment finds data is no longer anonymous

Relevant text: Paragraph 35; paragraph 42.

Paragraph 42 addresses one outcome of reassessment: after a security incident, the affected entity "should then determine its role with respect to the processing and whether it needs to fulfil any obligations under Article 33 and 34 GDPR." In its review of the draft, SBJ did not identify

equivalent guidance for reassessments prompted by the other causes the draft recognises, such as technological advances under paragraph 35. Organisations will reach that outcome, and consistent handling across controllers would benefit data subjects and supervisory authorities alike.

Proposed text (addition after paragraph 42):

> "Where a reassessment, for whatever reason, concludes that data previously assessed as anonymous is personal data from one or more perspectives, the entities concerned should treat it as personal data from those perspectives from that point, determine their role and the legal basis for any continued processing, consider whether further release or sharing should be suspended, consider informing recipients to whom the data was disclosed, and record the finding and the actions taken in the documentation referred to in paragraph 41."

SBJ reference. The SBJ AI Governance Architecture (V1.0 and V2.0) includes Adverse Evidence Preservation: evidence associated with failures, interventions and findings that cut against a prior result is retained. A reassessment that reverses an anonymity conclusion is such a finding, and preserving it alongside the original assessment gives supervisory authorities a complete record.

3. SBJ Resources Referenced

- SBJ AI Governance Architecture V2.0: solutionsbyjewel.com/ai-governance/architecture/
- SBJ AI Governance Architecture V1.0: solutionsbyjewel.com/sbj-ai-governance-architecture-v1
- SBJ AI Decision Record v2.0: solutionsbyjewel.com/ai-decision-record-template

These resources are cited as illustrative implementations. The recommendations in this submission stand on the text of the draft guidelines and do not depend on their adoption.

4. Conclusion

The draft guidelines establish that anonymity depends on context and that context changes. The five recommendations above give that principle an operational form: defined events that prompt reassessment, documentation that records what each conclusion depends on and who approved it, explicit treatment of AI query and prompting access, and a consistent response when a reassessment changes the result. SBJ appreciates the opportunity to comment and consents to the publication of this submission.

Respectfully submitted,

/s/ Jewel Darlington
Jewel Darlington
Chief AI Governance Officer & Founder
Solutions by Jewel
governance@solutionsbyjewel.com