Response to the public consultation on Guidelines 02/2026 on Anonymisation

Submitted by: Maja Kurek, AIGP, CIPM, CIPP/E · RuleBridge Advisory
Contact: Zagreb, Croatia · office@rulebridge.eu · rulebridge.eu

Scope and principal recommendation

An anonymity conclusion should travel with the limits of the assessment that supports it. A dataset may remain unchanged while a new recipient, access permission or processing relationship changes the applicable analysis. The organisational problem is that the decision changing those facts is often made outside the team that performed the assessment.

This response proposes targeted additions on scope, reassessment, interim handling and communication to recipients, together with a note for Annex 1. It preserves the draft's distinction between simplified and contextual approaches and its analysis of the applicable perspective. Paragraph references are to the version adopted for public consultation on 7 July 2026 [1]. The proposals concern implementation; they do not introduce an additional test of anonymity or an assessed anonymisation technique.

1. Record which data, processing and perspective the conclusion covers

Suggested placement: addition to paragraph 41; cross-references to paragraphs 9 and 13–15.

A statement that data is anonymous can be separated from the reasoning that supported it. Procurement may apply it to a replacement service, or a recipient may read it as covering a new disclosure. Paragraph 41's documentation expectation would be more useful if it expressly included the assessment's scope and material assumptions.

Proposed wording

> Documentation should identify the given data and relevant version, the date and scope of the assessment, the applicable perspective or perspectives, and the material assumptions supporting its conclusion. These should include the relevant entities or categories of entities, the reasons for excluding others, relevant additional information and access constraints, the techniques and capabilities considered, any relied-upon safety margin, and the intended processing or release arrangement. The record should allow a later decision-maker to determine whether a proposed use remains within the assessment's scope.
>
> The applicable perspective should be determined before relying on the conclusion. In particular, where an entity processes information on behalf of a controller for whom it is personal data, paragraph 15 requires reference to the controller's perspective. Separate legal personality or the recipient's lack of direct identifiers does not, by itself, justify an independent anonymity conclusion for that processing.

The record need not identify every hypothetical actor or reproduce confidential technical analysis. It should preserve the assumptions that matter to subsequent decisions. Information remaining personal for the disclosing controller is not made anonymous for that controller simply because an independent recipient cannot identify the individuals. The respective obligations remain those described in paragraphs 14–15 and 37.

2. Identify authorised changes as well as incidents, and connect them to review

Suggested placement: after paragraph 42; cross-references to paragraphs 29, 35 and 88.

A security incident is one trigger, not the whole category. Authorised changes can also affect the analysis: appointing another provider, granting support staff access to a second service, changing a recipient's role, combining datasets or releasing more detailed outputs. The fact that a change is permitted does not establish that the previous anonymity conclusion covers it. Nor does every change necessarily undermine the conclusion.

Proposed wording

> Entities relying on an anonymity assessment should identify events capable of materially affecting its assumptions, alongside proportionate periodic review. Relevant events may include changes in recipients or processing relationships, access or onward disclosure, reasonably available additional information, released detail, identification capabilities or the effectiveness of a relied-upon restriction. Such events may be authorised operational changes as well as security incidents or external developments.
>
> For material dependencies, the entity should identify the function able to observe or control the change and a route to the function responsible for reassessment. Decisions on provider replacement, permissions or release should have access to the relevant limits of the earlier conclusion. The arrangement should remain workable when personnel or suppliers change. Roles may be combined where appropriate; a separate committee or register is not required.
>
> Before relying on the earlier conclusion for changed processing, the entity should determine whether the change affects that conclusion and revisit the affected analysis, including consequential dependencies. Unaffected reasoning may be retained where its continued applicability is supported. A record should state what was reconsidered, what remained applicable and why.

For example, the team controlling access can report that a previously separate dataset is now available; the technical assessor then examines its relevance. The access team should not be expected to perform a re-identification assessment, and the assessor should not be assumed to see every permission change. Their information route is the missing operational connection.

Review should also work from a changed dependency back to the uses relying on it. If several releases depend on the same access restriction or provider arrangement, checking only the newest release may leave earlier reliance unexamined. This is not a requirement to repeat every assessment: it is a way to identify which conclusions the changed premise may affect.

3. Define protective handling without making review itself a legal status change

Suggested placement: implementation clarification after paragraph 35, linked to paragraphs 41–42.

Paragraph 35 explains that information can become personal when identification is no longer insignificantly likely. That consequence follows from the relevant facts, not from the date an internal reviewer finishes a report. Conversely, opening a routine review does not make otherwise anonymous data personal. Paragraph 36's treatment of mixed datasets does not establish such a general presumption [2].

A useful clarification should address material uncertainty in a defined processing context, without either creating a grace period for obligations or treating every scheduled review as a reason to suspend all uses.

Proposed wording

> Where credible new information leaves a material doubt about whether the earlier anonymity conclusion remains applicable, the entity should promptly assess the affected data, perspective and processing. It should not authorise a new release or expanded use solely on that unresolved conclusion. For ongoing processing, it should determine what protective handling is necessary while the question is resolved, such as restricting the affected activity or managing it on a personal-data basis with the required legal grounds and safeguards. Applying protective controls is not itself a lawful basis for processing.
>
> The interim decision should identify its scope, responsible function, outstanding question and next action with a defined timeframe. It must not postpone obligations that already apply to personal data. Where the requirements for the affected processing cannot be met, that processing must not proceed. Neither commencement nor completion of the internal review determines the legal status of the information. Unaffected processing may continue on the earlier assessment where its applicability remains supported.

This is a proposed protective handling rule, not a third category between personal and anonymous data. It also distinguishes a review deadline from permission to continue: repeatedly extending the deadline cannot establish the missing basis for reliance. The recommendation does not displace any applicable incident response or notification obligations.

4. Communicate changed assumptions to recipients that relied on them

Suggested placement: addition to paragraph 41; linked to paragraphs 12, 21 and 35.

A relevant finding may arrive after data has been supplied. Recipients can continue to rely on a report whose assumptions the assessing entity no longer supports. The useful communication is not an unqualified announcement that the data has changed status for everyone. It is a scoped update identifying the changed facts, the conclusion affected and the implications that recipients need to examine from the applicable perspective.

Proposed wording

> Where data is supplied with information on an anonymity assessment, the release arrangement should provide a proportionate means for material changes to that information to reach known recipients that may rely on it. Updates should identify the affected data or release, the assumption or conclusion no longer supported, any relevant interim limitation, and an appropriate contact for follow-up. They should provide enough information to support action without unnecessarily disclosing personal data or confidential analysis.
>
> Recipients should assess the relevance of the update to their processing and applicable perspective, including the consequences of onward disclosure. A changed conclusion for one entity should not be assumed to apply identically to all others. If an assessment supported public release to unknown recipients, the entity should consider a version-linked public correction or advisory and other proportionate communication measures, while recognising that these cannot be relied upon to reach every copy, recall released data or restore the earlier conditions. Those limitations should inform the original release assessment.

The scope and limits of any continuing communication arrangement should be clear at release. This recommendation does not require identification of everyone who accesses a public dataset; it addresses communications on which reliance actually depends. Any applicable legal duties, including breach notifications where their conditions are met, remain separate; a public advisory is not a substitute for them.

5. Add a scope-and-review note to Annex 1

Suggested placement: beside the flowchart outcomes, complementing the existing note referring to paragraph 21.

Annex 1 already warns about transfers to an entity that may be able to identify individuals. An additional note should address the later use of the conclusion, not duplicate that warning or introduce another decision box.

Proposed note

> Record the applicable perspective, processing scope and material assumptions of the conclusion. Before applying it to changed processing, consider whether a relevant change affects those assumptions and revisit the affected analysis, including consequential dependencies. Retain unaffected reasoning where it remains applicable. A review does not itself determine that information is personal or anonymous.

A conservative simplified assessment may remain applicable across a wider range of changes than a context-dependent assessment. Review effort should reflect actual dependencies, not apply an identical checklist to both. Consistently with footnote 3 to paragraph 2, publication of the final Guidelines should not itself require repetition of an assessment that was valid under Opinion 05/2014; relevant changed facts are a different matter.

Illustrative example: unchanged data, a different recipient

A company makes transformed records available to an independent research organisation for that organisation's own benchmarking research. The recipient determines its own purposes and essential means; it does not conduct the research on the company's instructions. The company retains identifying information. An assessment supports anonymity from the research recipient's perspective, while the records remain personal data for the company.

For the next release, the company proposes a different independent research recipient. That recipient already has authorised access, through another activity, to additional information that could be relevant to identification. The transformed records are unchanged, and there has been no security incident.

The release decision should not copy the earlier conclusion under the new recipient's name. It should establish whether the additional information affects the means reasonably likely to be used for identification, including relevant routes through other entities. The review might support the same conclusion, require different protections or find that anonymity cannot be relied upon. The authorisation to access the additional information, and a contractual promise not to identify individuals, do not settle that assessment on their own.

The assessment record makes the relevant assumptions available to the function deciding the release. That function can hold the proposed disclosure while obtaining the necessary analysis, without reopening unrelated uses whose conditions remain supported. If the proposed recipient instead processes the records on the company's behalf, paragraph 15 supplies a different starting point: the company's perspective applies. Calling that recipient an independent business does not change the role analysis.

This is a hypothetical example, not a finding about a particular organisation or evidence that any stated transformation achieves anonymity.

Closing recommendation

The draft's contextual analysis should remain attached to the organisational decisions that can change its premises. A scoped record, a working route from change to reassessment, proportionate interim handling and targeted communication to recipients would make that possible without treating anonymity as a certificate, review as a legal switch, or every operational change as a complete restart.

About the contributor

Maja Kurek, AIGP, CIPM, CIPP/E, is Founder and Principal of RuleBridge Advisory, an independent AI governance practice in Zagreb, Croatia. The practice advises on the operator and deployer side of AI arrangements — organisational AI governance, human oversight and decision accountability, and external AI relationships spanning vendors, platforms, models and external contributor networks. She brings close to a decade of operational experience across Google, Photomath and Uber, including responsibility for the human layer of an AI-powered learning product at the scale of a 10,000-strong external expert network, with its admission, access, cross-border payment, data protection and offboarding processes, data and access controls, programmes adapting platform operations to changing national regulation, and governance-sensitive provider transitions. This contribution is made through RuleBridge Advisory, which provides advisory services in related areas. It does not represent any former employer or client.

Notes and sources

[1] European Data Protection Board, Guidelines 02/2026 on Anonymisation, version 1.0, adopted for public consultation on 7 July 2026; especially paragraph 2 (footnote 3), paragraphs 9, 13–15, 20–22, 29, 34–42, 45–49, 88–93 and Annex 1. https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202602_anonymisation_v1_en_0.pdf

[2] Regulation (EU) 2016/679 (GDPR), Article 4(1) and Recital 26; Articles 5, 6 and 9 apply where information is personal data and the processing falls within the Regulation. The interim handling proposed here does not replace that legal assessment. https://eur-lex.europa.eu/eli/reg/2016/679/oj