ISTITUTO ITALIANO PER LA PRIVACY E LA VALORIZZAZIONE DEI DATI

Comments on the EDPB Guidelines on Anonymisation

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Guidelines 02/2026

15 October 2026

The Istituto Italiano per la Privacy e la Valorizzazione dei Dati (Italian Institute for Privacy and Data Valorisation) recommends five targeted changes to make successful anonymisation an outcome on which organisations can act. The same evidential standard should apply to commercial analytics, scientific research, and statutory data sharing.

The draft's contextual approach provides the right foundation.[1] Its practical value depends on specifying what an organisation must demonstrate and when the evidence is sufficient. That requires a test which both excludes purely hypothetical objections and examines the actual effect of safeguards: whether a relevant entity has a reasonably likely route from the information it can obtain to an identified or identifiable person.

Where legislation requires anonymisation before access, data utility must be pursued within that condition. Equally, useful information can be anonymous. Material facts equivalent to identifiability should receive equivalent treatment, whether sharing is voluntary or compulsory.

Our proposals address evidential sufficiency, residual identifying information, the contribution of safeguards, the distinction between outputs and inputs, and proportionate reassessment. They can be implemented through existing technical and accountability records, without additional assessment forms, certification schemes or general reporting obligations.

1 State when the evidence is sufficient

Priority amendments to paragraphs 21 to 33 and 48

The contextual approach requires a reasoned conclusion about realistic identification routes. It should not become an obligation to demonstrate the absence of every conceivable route. Paragraph 21's formulation "cannot be ruled out" needs to be read against the practical likelihood standard in paragraph 22. The final text should remove the possibility that uncertainty alone is treated as sufficient to defeat anonymity.[2]

We recommend an express statement that an assessment can conclude once the relevant perspectives and accessible information have been reasonably established and adequate evidence supports insignificant identification likelihood. The evidence may include the properties of the transformation, verified access limitations, and tests appropriate to the remaining routes. The absence of a successful attack is insufficient by itself. For lawful identification means, a completed attack is unnecessary where other evidence establishes a reasonably likely identification route. For prohibited means, we propose the actual-use threshold developed below, which concerns the conduct used to obtain or combine identifying information rather than proof of completed re-identification. This clarification concerns the substance of the assessment and should not alter statutory burdens of proof or supervisory powers.

The Austrian Datenschutzbehörde accepted anonymisation in an Article 17 complaint after examining the removal of links to the individual, including in logs and change history. An unspecified

---

1 European Data Protection Board, Guidelines 02/2026 on Anonymisation, version for public consultation, especially paragraphs 21 to 36, 48 and footnote 36, 51, 67 to 71, and 88 to 99. Official source

2 EDPB, Guidelines 02/2026 on Anonymisation, paragraphs 21–22. Official source

possibility of future reconstruction did not defeat that conclusion.[3] This individual erasure case illustrates acceptance of a substantiated result without a guarantee against every future technical possibility; it does not establish approval of a rich reusable dataset.

Give legal prohibitions substantive effect

The final Guidelines should give substantive effect to the legal barriers that prevent identification. Where an identification route depends on breaching a statutory prohibition applicable to the entity concerned, IIP recommends that prohibited means be taken into account only where there is evidence that they have actually been used in relation to the data and identification route under examination. The possibility that an actor might disregard the law should not, on its own, defeat an otherwise substantiated conclusion of anonymity. This requires a more precise evidential rule than the one currently proposed in paragraph 33.

The Court's recognition of legal prohibitions as a relevant constraint must retain practical significance. In Breyer, the Court explained that identification means need not be regarded as reasonably likely where a legal prohibition or practical impossibility makes the identification risk insignificant. The judgment also examined the existence of lawful channels through which additional identifying information could be obtained. That distinction gives legal accessibility an independent role in the assessment, alongside technical capability and the resources required for identification.[4]

In EDPS v SRB, the Court reaffirmed the relevance of legal prohibitions while requiring attention to the position of the relevant recipient and its actual means of identification. IIP proposes an actual-use threshold for prohibited means as a concrete way of giving effect to that recognition.[5]

Paragraph 33 already requires sufficient evidence of a concrete risk, rather than an unsupported allegation that unlawful conduct might occur. The difficulty lies in the breadth of the factors offered to establish that risk. Weak enforcement, possible economic gains, security vulnerabilities, and breaches in comparable circumstances can all inform a risk assessment, but they do not necessarily establish that a particular entity has obtained or used prohibited identification means in relation to the information concerned. Their inclusion therefore leaves considerable room for predictive judgments to displace the legal prohibition on which an organisation is otherwise entitled to rely.[6]

A clearer threshold would improve both legal certainty and the discipline of the assessment. An organisation can identify the prohibition that applies, establish which actors and conduct it covers, and explain which identification route it prevents. It cannot demonstrate that no person will ever find it advantageous to disregard that prohibition. If reliance also requires disproving every plausible incentive to offend, the legal barrier becomes conditional on predictions about future behaviour that are difficult to verify and even harder to apply consistently. The value attributed to the prohibition would then depend on an open-ended assessment of possible misconduct rather than on its application to the relevant processing context.

For this reason, the proposed rule should require evidence of actual use of the prohibited means. That requirement should concern the conduct through which the legal barrier was crossed. It should not require a final judicial finding of unlawfulness or proof that every step of re-identification has

---

3 Austrian Datenschutzbehörde, decision DSB-D123.270/0009-DSB/2018, 5 December 2018, sections C.2 and D.2–D.3. The official register records the decision as final. The complaint concerned erasure under Article 17 through removal of the link to an individual. Official source

4 Court of Justice, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, 19 October 2016, ECLI:EU:C:2016:779, paragraphs 45 to 49, especially paragraph 46 on legal prohibitions and paragraphs 47 to 49 on lawful channels for obtaining additional identifying information. Official source

5 Court of Justice, EDPS v Single Resolution Board, C-413/23 P, 4 September 2025, ECLI:EU:C:2025:645, paragraphs 77 to 88, especially paragraph 82. The actual-use threshold proposed here is an IIP recommendation for the final Guidelines, not an express holding of the Court. Official source

6 EDPB, Guidelines 02/2026 on Anonymisation, paragraphs 32–33. Official source

already succeeded. Evidence that a protected lookup table has been unlawfully obtained, that access credentials have actually been misused to retrieve identifying information, or that an unlawful combination of datasets has taken place may establish the relevant conduct. The subsequent question is whether that conduct has made individuals identifiable from the perspective under examination. An unsuccessful attempt may warrant investigation and remediation without, by itself, establishing that anonymity has been lost.

The distinction matters because identifiability and completed identification remain different questions. Once actual unlawful use has made the necessary additional information available to an actor, the assessment should examine that actor's resulting capacity to identify individuals. It need not wait for evidence that names have been assigned to particular records. Equally, the mere absence of a detected attack cannot establish anonymity where the information already accessible to a recipient supports identification. The proposed threshold concerns reliance on prohibited means; it does not replace the assessment of other identification routes.

The final text should also distinguish a legal barrier to obtaining identifying information from a restriction on the purposes for which already identifiable information may be processed. An entity cannot treat a record as anonymous merely because it is prohibited from using the identity that the record already reveals. Nor can a general prohibition on unlawful processing neutralise an identification route supported by information already available to that entity. Reliance must concern a specific statutory barrier affecting the means needed for identification. Lawful channels for obtaining additional information, and other reasonably available identification routes, would continue to require assessment without proof of their actual use.

This proposal would preserve the preventive character of applicable security obligations. Article 32 GDPR requires controllers and processors to address risks to personal data, including risks of unlawful access and disclosure. Those duties apply before a breach occurs. A controller retaining personal source records or identifying keys must therefore address vulnerabilities, unauthorised access, and foreseeable misuse within the scope of those obligations.[7]

A requirement to strengthen the protection of those records should not, however, automatically determine the classification of every output disclosed to an independent recipient. The assessment should identify the information and capabilities available in each setting.

Consider an analytics recipient whose access to a dataset has been assessed and whose available information does not otherwise enable identification. Additional information necessary for attribution is held separately, and obtaining it would require conduct prohibited by law. The hypothetical possibility that an employee might unlawfully disclose that information should not, under the proposed rule, be sufficient to invalidate the recipient's anonymity assessment. If evidence subsequently establishes that the information has in fact been disclosed, the recipient's position must be reassessed against the access thereby created. This approach gives the actual event a clear consequence while avoiding an assumption that every conceivable future breach has already occurred.

The consequences of actual unlawful use should remain connected to the facts established. The reassessment should identify the information affected, the entities that obtained additional capabilities, any onward disclosures, and the period during which those capabilities existed. An unlawful act affecting one recipient should not automatically invalidate anonymity for recipients whose circumstances remain materially different. Where the event exposes a wider weakness or creates broader access, the reassessment must extend to those consequences. Its scope should follow the evidence.

---

[7] Regulation (EU) 2016/679, Article 32(1) and (2), concerning preventive security measures and risks including unlawful access to, or disclosure of, personal data. Official source

The temporal implications also require care. A later unlawful act should not, merely because it occurred, establish that an earlier assessment was defective. Conversely, later discovery may reveal that prohibited means had already been used when that assessment was made, or that relevant identifying information was already available. The assessment must therefore distinguish the time at which the facts changed from the time at which those facts became known. This preserves the possibility of correcting an earlier conclusion where the evidence warrants it, without treating every subsequent incident as retrospective proof that anonymisation had never been achieved.

Organisations should document the statutory prohibition relied upon, its application to the relevant entity and conduct, the identification route it constrains, and any evidence of actual circumvention material to that route. They should also assess alternative means of identification and maintain arrangements for responding to relevant changes. The proposed rule would not alter supervisory powers or statutory burdens of proof. It would specify the substantive evidence needed to displace reliance on a legal barrier, while preserving scrutiny of the remaining factual assumptions.

Paragraph 33 and Example 8 should be revised consistently with this approach. Vulnerabilities and incidents involving other systems can justify preventive security measures and further investigation. Under the proposed threshold, they should not independently establish that prohibited identification means have been used in the case under examination. Where actual unlawful use is established, the resulting access and identification capabilities should be assessed promptly, and the affected processing brought into compliance where necessary.

Add after paragraph 22 and cross refer to it in paragraph 21

An assessment may conclude that information is anonymous where adequate evidence supports insignificant identification likelihood from the relevant perspectives. It need not exclude purely hypothetical means or chains of access. The evidence must address identification routes reasonably supported by the circumstances; absence of a demonstrated attack alone is insufficient. A materially different conclusion should identify the relevant means, information or circumstance that the assessment does not cover or has evaluated incorrectly. For lawful identification means, this does not require a completed re-identification attack. Where reliance on a statutory prohibition is material, the actual-use rule in paragraph 33 should apply. Statutory burdens of proof remain unchanged.

Replace paragraph 33 and align Example 8 accordingly

Where an assessment relies on a statutory prohibition applicable to the relevant entity and identification route, prohibited means should be taken into account only where there is evidence that they have actually been used in relation to the data concerned. A prediction that an entity might disregard the prohibition should not, by itself, displace reliance on that legal barrier. Factors such as possible economic incentives, enforcement limitations, security vulnerabilities, or unlawful conduct in other circumstances should not independently establish actual use in the case under examination.

Evidence of actual use does not require a final judicial determination or proof of completed re-identification. It must establish that prohibited conduct relevant to the identification route has occurred. The assessment should then determine whether that conduct has made the necessary information or capabilities available to the relevant entity and whether individuals are consequently identifiable.

Reassessment should address the affected information, entities, identification routes, and processing operations, including any consequences for onward recipients. A finding concerning one entity should extend to others only where the evidence supports that conclusion. The assessment should distinguish when the relevant circumstances changed from when the change

became known. Subsequent unlawful conduct does not, by itself, establish that an earlier assessment was defective.

This rule concerns reliance on statutory barriers to identification. It does not exclude the assessment of lawful or otherwise available identification routes, make already identifiable information anonymous, or displace applicable security obligations, statutory burdens of proof, supervisory powers, or liability for unlawful conduct.

The clarification in footnote 36 that the simplified approach cannot conclusively establish a violation should also appear in paragraph 48 itself. An optional conservative screening method should not become the practical default against which every successful contextual assessment must defend itself.

2 Examine the residual information that can actually identify someone

Priority amendment to paragraph 51 and the application of the three criteria

The assessment must cover all information reasonably available to the relevant recipient for identification. A threshold applied to selected quasi-identifiers cannot establish what happens when the remaining content, event sequences and accessible auxiliary information are combined. Conversely, the mere existence of a rich or unusual record does not establish that it can be attributed to a person.

The Italian Garante's decision of 23 September 2026 concerning IQVIA examines longitudinal clinical information outside the selected quasi-identifiers. Its alternative compliance route in paragraphs 145 to 149 requires upstream anonymisation and assessment of residual variables against the recipient's capacity to observe or measure them. Where those variables can contribute to identification, paragraph 148 provides for their inclusion in protected attribute combinations, distributed computation preventing acquisition of the complete original data in clear text, or removal.[8]

The CNIL identified the same assessment defect in Cegedim Santé: an analysis combining only birth year, sex and whether the patient had children omitted much of the clinical and longitudinal information available. It therefore did not reliably establish anonymity.[9] The Conseil d'État upheld the sanctions on 13 February 2026, accepting the concrete assessment of identification through reasonably available means.[10]

In its separate French IQVIA decision of 26 May 2026, the CNIL examined a further route: combining coded longitudinal records with information readily available online about treatment, timing and location.[11] This illustrates why removing direct identifiers or protecting a coding key leaves a separate question about identification through content.

---

[8] Garante per la protezione dei dati personali, decision concerning IQVIA Solutions Italy S.r.l., 23 September 2026, register No 710, web document No 10302112, especially paragraphs 89 to 100 and 145 to 149. The distributed-computation option forms part of a conditional compliance route. Official source

[9] CNIL, decision SAN-2024-013 concerning Cegedim Santé, 5 September 2024, especially paragraphs 48, 75 to 85 and 88. Paragraph 81 addresses omitted variables; paragraph 85 distinguishes breach risk from data classification. The decision does not determine whether the subsequently modified processing is anonymous. Official source

[10] Conseil d'État, GERS, GERS as successor to Santestat, and Cegedim Santé, joined cases Nos 498628, 498629 and 498749, 13 February 2026, ECLI:FR:CECHR:2026:498628.20260213, especially paragraphs 9 to 12 and 26. Judicial confirmation of the CNIL sanctions, including SAN-2024-013. Official source

[11] CNIL, decision SAN-2026-008 concerning IQVIA Operations France, 26 May 2026, especially paragraphs 88 to 92, 104 to 112. The decision considers the controller's role from collection, identification through external information, and the distinction between contractual undertakings and statutory prohibitions. Official source

These decisions support examining the information that completes a realistic identification route. They do not establish that every rich dataset is personal, a universal numerical threshold or approval of the architectures proposed below. The Italian decision's prescribed threshold and upstream responsibilities remain specific to its compliance route.

For a release of event data, the question may therefore concern the combination of content, sequence, and timing with a recipient's independently available observations. If that combination supports reliable attribution, expanding a cohort measured only on location and device type does not answer the identified problem. If attribution instead depends on auxiliary information that the relevant entity cannot reasonably obtain, the assessment should explain that limitation and give it effect. Neither conclusion requires exhaustive enumeration of every mathematical combination of attributes.

Add after paragraph 51

> The assessment should consider residual information outside the attributes covered by a technical metric where, alone or in combination, it supports a plausible identification route from a relevant perspective. It should examine whether the entity can observe, measure, or otherwise obtain the corresponding information and associate it with a person. Where such a route exists, the measures should address the information or access that enables it. This may be achieved through appropriate transformation, restrictions on intelligible access or output, or removal. Exhaustive enumeration of hypothetical attribute combinations is not required.

Technical validation should follow the same logic. A test should distinguish uniqueness, reliable attribution and specific inference; identify the auxiliary information used; and explain false matches and any materially exposed subset. An average success rate cannot resolve a credible route affecting that subset. Existing test results and technical guarantees should be reusable where their assumptions cover the actual release, avoiding repeated empirical testing of a question already adequately answered.

3 Require safeguards to address the identification route relied upon

Priority amendment to paragraph 34

EDPS v SRB makes the recipient's actual position decisive, including its ability to overcome the measures or identify by other reasonably available means. It also preserves the source controller's applicable obligations.[12] A contextual assessment should therefore explain what each safeguard prevents the relevant entity from doing.

Technical transformation can reduce the identifying information disclosed. A restriction on access or combination can affect whether additional information is reasonably obtainable or usable. These contributions may work together but should remain distinguishable in the reasoning. A contract that restricts access to a separately held key addresses a different factual problem from a promise not to identify using information already intelligible and attributable to a person.

The CNIL's French IQVIA decision distinguishes a contractual undertaking from a statutory prohibition on identification.[13] Its Cegedim Santé decision also distinguishes protection against a data breach from anonymity of the data held by the organisation.[14] Together, these findings support

---

12 Court of Justice, EDPS v Single Resolution Board, C-413/23 P, 4 September 2025, ECLI:EU:C:2025:645, paragraphs 77, 82 to 88 and 102 to 111. The judgment concerns Regulation 2018/1725 and informs the equivalent GDPR concept. See GDPR Article 4(1) and Recital 26. Official source

13 CNIL, IQVIA Operations France, SAN-2026-008, 26 May 2026, paragraphs 109–112 (contractual undertakings and statutory prohibitions). Official source

14 CNIL, Cegedim Santé, SAN-2024-013, 5 September 2024, paragraph 85 (breach risk and data classification). Official source

a practical requirement: assess what the safeguard changes for the relevant actor. Securing a system against outsiders does not resolve the identifiability of information available to its authorised operator.

We recommend that paragraph 34 requires the assessment to connect a material safeguard to the identification route it addresses. Where contractual compliance is decisive, the explanation should identify the conduct restricted, the practical basis for expecting the restriction to operate, and the consequence of its failure. An existing contract, system configuration, or assurance report may supply that evidence. Calling the remaining likelihood "residual" does not answer whether the combined protection makes it insignificant.

This also gives practical effect to a common standard across voluntary and compulsory sharing. Neither a statutory access entitlement nor a trusted commercial relationship determines identifiability. Both may shape the relevant context, which must be assessed. Where access is conditional on anonymity, the value of detailed data can justify seeking a better technical solution; it cannot supply the missing evidence that an identification route has been addressed.

Add at the end of paragraph 34

> Where safeguards operate in combination, the assessment should explain which reasonably likely identification route each material safeguard removes or constrains, and why the combined result makes identification likelihood insignificant. Where a contractual restriction is material, its practical effect on the relevant entity's access or conduct must be supported by evidence. A promise not to identify cannot negate identification already apparent from accessible information. Neither the compulsory or voluntary character of a transfer nor the usefulness of the information determines the outcome. The same evidential standard applies where the material circumstances to identifiability are equivalent.

Each safeguard must make a demonstrable contribution to the combined protection; technical measures need not independently eliminate every theoretical identification possibility.

4 Recognise anonymous outputs without extending the conclusion to their inputs

Priority amendments to paragraphs 36 and 91 with examples applying paragraphs 67 to 71

The Guidelines should distinguish access to individual records from access to the results of computation over those records. This distinction gives organisations a practical choice where releasing a richer dataset would leave identification routes open. It also provides a useful way to explain secure multiparty computation, trusted execution environments, and other privacy enhancing technologies without granting a safe harbour to a technology name.

Consider an independent analytics customer allowed to obtain only predefined aggregate outputs. Individual records remain inaccessible to that customer. The system limits small-group disclosure and the information obtainable by differencing or repeated overlapping requests. The assessment accounts for auxiliary information reasonably available to the customer and verifies the relevant access and output controls. If those measures establish insignificant identification likelihood, the conclusion applies to the outputs in that setting. It does not exempt the processing of personal inputs, including processing performed on a controller's behalf. Giving the customer a row-level export would be a materially different operation, even under the same contract.

This example preserves useful computation while limiting identifying information. For cryptographic or hardware-based implementations, the assessment would address keys, privileged access, relevant cooperation between participants, and output disclosure. Paragraph 148 of the

Italian IQVIA decision illustrates distributed computation as one conditional route within a wider compliance design.[15]

The same distinction makes paragraph 36 more usable. A mixed dataset requires GDPR-compliant handling of its personal component and operations that encompass it. That does not make every item personal merely through co-location. Effective separation must be assessed against each relevant entity's actual means: selecting a subset through an interface does not remove identification means otherwise available to that entity. The analogy with Bundeskartellamt in footnote 31 should remain limited to the treatment of inseparable processing; it does not replace the prior Article 4(1) inquiry.[16]

Replace the final sentence of paragraph 36

> Where personal and anonymous information are processed together, the operation encompassing personal data falls within the GDPR. This does not, by itself, make every other item personal data. A separately processed subset or output may be anonymous where effective separation and the relevant entity's other reasonably available means support that conclusion. Separation must be effective in practice and cannot rest solely on selecting a subset while retaining reasonably usable identification means. The assessment should also distinguish the people to whom information within a record relates.

Add after paragraph 91

> An arrangement may preserve useful computation while preventing a relevant entity from obtaining intelligible individual records or identifying outputs through reasonably likely means. Its effect should be assessed separately for the inputs, information accessible to each participant, and outputs, including cumulative disclosure. An anonymity conclusion about an output does not exempt the processing of personal inputs or extend to access capabilities outside the assessed arrangement. The effectiveness of a privacy enhancing technology depends on its implemented protections, including material assumptions about keys, privileged access and cooperation between parties.

For example, anonymity of a record's author does not establish anonymity of a third person named in that record, or vice versa. Equally, useful population-level predictions do not, without more, establish failure of anonymisation. The distinction in paragraphs 67 to 71 should govern the examples: applying general knowledge to an identified person may produce personal data in the output without making the statistical source personal. Evidence that an output reveals attributable information from an original record calls for a different analysis.[17]

5 Allow reliance until a material assumption changes

Priority amendment to paragraph 35

An adequately supported assessment should remain a usable basis for action while its material conditions continue to hold.

We recommend specifying the events that require a focused review: a materially different release, new access to relevant auxiliary information, a change in recipient capability, an onward disclosure, a compromised safeguard or a change in model behaviour relevant to extraction or attribution. The party positioned to observe such a change should assess its implications for the conclusion on which

---

15 Garante, IQVIA Solutions Italy, decision No 710 of 23 September 2026, paragraph 148; the distributed-computation option is part of a conditional compliance route. Official source

16 Court of Justice, Meta Platforms and Others v Bundeskartellamt, C-252/21, 4 July 2023, ECLI:EU:C:2023:537, paragraph 89, cited in footnote 31 of the draft Guidelines. Official source

17 EDPB, Guidelines 02/2026 on Anonymisation, paragraphs 67–71. Official source

it relies. This can be supported by existing security, change management, and contractual arrangements.

Review should follow the affected assumptions and information. A change affecting a particular recipient need not invalidate the conclusion for all recipients. A newly identified personal component requires examination of the operations that include or can link to it, rather than a presumption that every previously anonymous output has changed status. If the original evidence remains adequate for unaffected uses, it should remain reusable. This approach gives paragraph 36 a practical consequence as well as a classification rule.

For models, evaluation should address extraction or attribution where these are plausible, with further testing directed at material changes in the model, its interfaces or accessible auxiliary information. Periodic review may be appropriate where the expected evolution of relevant means warrants it. A fixed interval for all arrangements would add little.

Add at the end of paragraph 35

> An organisation may rely on an adequately supported assessment while its material conditions remain applicable. Reassessment should address reasonably available evidence of a change capable of materially affecting identifiability, focusing on the affected assumptions, information, and operations. Where a reassessment concern prohibited identification means, the rule in paragraph 33 should apply. Existing evidence remains reusable for unaffected circumstances. Periodic review, where appropriate, should reflect the expected evolution of relevant means and safeguards. If the anonymity conclusion can no longer be supported, the affected processing must be brought into compliance or suspended as necessary. A later change does not by itself establish that the earlier assessment was defective.

The final anonymisation and pseudonymisation guidance should express these conditions consistently, including the distinction between the source controller's obligations and an independent recipient's position. In regulated sharing, the same technical and assurance evidence should be usable by the competent authorities within their respective powers. Recipient-specific facts may be verified through independent assurance without unnecessary disclosure of proprietary auxiliary datasets to the source controller.

The resulting decision sequence is practical: establish the relevant means; address the information that enables identification; accept adequate evidence of success; and revisit the conclusion when its material basis changes.