Bitkom views on EDPB Guidelines 02/2026 on Anonymisation

Position paper

bitkom

Bitkom views on EDPB Guidelines 02/2026 on Anonymisation

Background

Anonymisation is the most effective way to reconcile data protection with the use of data. Where individuals are no longer identifiable, risks for them are removed and data can be used for research, industrial applications and the development of AI in Europe. Whether this potential can be realised depends on how the threshold for anonymity is set in practice. Bitkom welcomes that the Guidelines confirm the contextual approach, accept that zero risk is not required, and build on the CJEU's recipient-based perspective in EDPS v SRB (C-413/23 P).

In their current form, however, the Guidelines risk turning anonymisation into a theoretical option on which no organisation will dare to rely. If companies must exclude every conceivable actor, means and future development, and justify and document this repeatedly, they will rather keep data in identifiable form. This serves neither data subjects nor the European data economy.

Bitkom assessment

The Guidelines should be guided by the question of how anonymisation can be enabled in Europe. This requires a standard applied as the CJEU describes it (what is reasonably likely, not what is conceivable), recognition of technical, organisational and contractual safeguards, no additional legal hurdles for a risk-reducing measure, and a procedure that companies and authorities can work with in practice.

Key priorities

- **Reasonable means, not conceivable means.** The assessment should rest on a weighing of the means the specific recipient is reasonably likely to use. Scenarios that are unlawful, sanctioned or practically unrealistic need not be considered. The Guidelines should remain principle-based and avoid catalogues that may be read as exhaustive.
- **Safeguards count.** Technical, organisational and contractual safeguards, including binding commitments within corporate groups, must be taken into account when assessing the means available to a recipient.

  No additional legal basis for risk-reducing anonymisation. Anonymisation is the functional equivalent of deletion and should not be subject to stricter requirements than retaining identifiable data.
- **A workable process.** Authorities that doubt anonymity should substantiate which concrete, realistic means they consider relevant. Documentation must be proportionate and integrated into existing records. Organisations must not be drawn into a spiral of justification.
- **Coherence.** Data should not be non-personal under the Data Act, the AI Act, the Data Governance Act or the European Health Data Space Regulation, but personal under the GDPR as read by the Guidelines.

  Practical Support. Illustrative positive examples and a recognised role for scientifically validated PETs would make the framework usable, without turning it into a checklist.

Content

1 General remarks 4

Consistent application of the contextual approach **4**

«Insignificant in reality» should remain the governing standard 4

Relevant entities and realistic threat modelling 5

Unlawful means 5

Give appropriate weight to controlled environments and safeguards **6**

Provide practical orientation without creating checklists **6**

Include positive and cross-sector use cases **7**

No Record Isolation, No Linkage and No Inference **7**

Privacy Enhancing Technologies and technical standards **7**

The temporal dimension and reassessment **8**

A workable process: substantiation, accountability and complaints **8**

Controller, processor and controller-to-controller scenarios **9**

No additional legal basis for risk-reducing anonymisation **9**

Relationship with pseudonymisation **10**

AI models **11**

Proportionate documentation **11**

2 Conclusion 12

1 General remarks

Bitkom welcomes the EDPB's initiative to update the European framework for anonymisation. The clarification of the contextual nature of anonymity and the probability-based assessment of identifiability represents an important development compared with earlier approaches.

In particular, Bitkom welcomes the recognition that the same information may be personal data from one entity's perspective while being anonymous from another entity's perspective, depending on the means reasonably likely to be used in the respective context. We also welcome the clarification that the probability of successful identification does not have to be zero.

These principles are essential for an effective framework. They reflect the reality that the risks associated with publicly released datasets are different from those associated with internal datasets or data made available within controlled environments.

At the same time, the Guidelines remain **difficult to operationalise** in several areas. Organisations need to be able to translate the legal standard into reproducible technical and organisational assessments. This is particularly relevant for SMEs and other organisations that cannot maintain highly specialised re-identification teams.

The final Guidelines should therefore **place greater emphasis on practical implementation**, **positive examples** and **proportionate ways of demonstrating that the standard has been met**.

Consistent application of the contextual approach

«Insignificant in reality» should remain the governing standard

This standard follows directly from the GDPR and the case law of the CJEU. Recital 26 refers to all the means reasonably likely to be used, taking into account objective factors such as the costs of and the time required for identification and the available technology. In Breyer (C-582/14), the CJEU held that this is not the case where identification is prohibited by law or practically impossible because it requires a disproportionate effort in terms of time, cost and manpower, so that the risk of identification appears in reality to be insignificant. In EDPS v SRB (C-413/23 P), the CJEU confirmed that the assessment must be made from the perspective of the individual recipient. Bitkom asks the EDPB to implement this case law consistently and not to go beyond it.

Which means are reasonably likely to be used calls for a reasonable weighing in the specific context, not for the exclusion of every conceivable possibility. The Guidelines should therefore remain principle-based and avoid going into too much detail on what is covered.

Bitkom supports the EDPB's conclusion that anonymity does not require the complete elimination of every conceivable possibility of identification.

Certain passages of the draft, however, risk being interpreted more strictly. In particular, the wording in paragraph 21 that identification capabilities of a recipient «cannot be ruled out» could be understood as requiring organisations to exclude hypothetical possibilities rather than assess their realistic likelihood.

The final Guidelines should use consistent terminology throughout. Where identification depends on an additional party, dataset or technique, the relevant question should remain whether the necessary chain of events and means is reasonably likely to materialise in the particular context.

Relevant entities and realistic threat modelling

Paragraph 30 contains a broad illustrative list of potential entities, including unauthorised and malicious actors. Bitkom agrees that such actors cannot categorically be ignored. However, neither should every conceivable attacker automatically form part of every anonymity assessment.

The final Guidelines should clarify that an entity is relevant where there is a realistic pathway through which that entity could obtain or contribute the means necessary for identification.

The range of relevant entities and reasonable means will necessarily differ depending on the context, for example between internal processing, controlled sharing between identified recipients, restricted environments and public dissemination. Such examples should be illustrative and non-exhaustive.

The assessment is a weighing of all objective factors named in Retrical 26 in the specific context. The Guidelines should not set out a catalogue of indicators that could be read as exhaustive or applied as a checklist. Means that do not realistically occur, because they are unlawful and effectively sanctioned, disproportionately costly or without any plausible incentive, need not be included.

Unlawful means

Bitkom welcomes the recognition that legal prohibitions can materially affect whether a means is reasonably likely to be used.

The final Guidelines should make clearer that the possibility of unlawful conduct does not automatically make an unlawful identification technique relevant. Unlawful means should be taken into account only where concrete indications exist that legal, organizational and technical barriers are ineffective and that circumvention is realistically likely.

This would allow organisations to distinguish actual re-identification risks from purely hypothetical unlawful conduct while preserving the ability to take malicious actors into account where the circumstances provide a concrete reason to do so.

Give appropriate weight to controlled environments and safeguards

The accessibility of both the data to be anonymised and any additional information required for identification is a core part of the contextual assessment.

Bitkom does not suggest that a contract alone transforms personal data into anonymous data. However, contractual and organisational commitments are a legitimate and necessary factor in determining which means a specific recipient is reasonably likely to use. This follows from the recipient-based perspective confirmed by the CJEU, and it would be inconsistent with the GDPR's own architecture, which relies on contractual safeguards elsewhere (e.g. Articles 28 and 46 GDPR). This applies in particular within corporate groups, where binding group-internal rules and effective control mechanisms provide a high degree of assurance that commitments will be observed. Safeguards should be assessed for their actual reliability, not disregarded as a matter of principle.

The final Guidelines should therefore expressly recognise a layered safeguarding model, where technical measures serve as the primary baseline to reduce identifiability, reinforced by operational and legal controls. Technical anonymisation measures may be supported by, for example, role-based access controls, segregation of identifying information, logging and monitoring, and enforceable contractual prohibitions and sanctions.

No single one of these measures should automatically establish anonymity. Their combined and demonstrable effect should, however, be reflected in the contextual assessment.

This principle should apply horizontally to controlled data-sharing environments across sectors rather than being limited to any particular regulatory regime; the secure processing environments for the secondary use of health data under Article 73 of the European Health Data Space Regulation (Regulation (EU) 2025/327) show that the Union legislator itself relies on controlled access as a safeguard, and comparable environments in other sectors should be treated alike.

Provide practical orientation without creating checklists

Terms such as «insignificant in reality», «sufficiently close» and «sufficiently high confidence» are central to the assessment but remain difficult to translate into operational decisions.

Bitkom does not suggest that numerical thresholds or fixed catalogues can appropriately cover all datasets and contexts. Nevertheless, the EDPB could substantially increase legal certainty by providing:

- qualitative risk levels and assessment factors, expressly non-exhaustive;
- accepted testing methodologies;
- illustrative representative reference scenarios; and
- references to appropriate standards, certification schemes and codes of conduct.

The Guidelines should also clarify what constitutes proportionate evidence for an anonymising controller to demonstrate that the relevant standard has been met. This evidence should be proportionate to the risk and the context and should not require a stand-alone documentation exercise.

Include positive and cross-sector use cases

The current draft contains useful illustrations of risks but fewer examples showing when organisations can conclude that anonymisation has successfully been achieved.

Positive examples are particularly important because they turn the Guidelines from a catalogue of potential failures into a practical compliance tool.

The final Guidelines should therefore include representative and illustrative use cases involving, for example, aggregated commercial analytics, product and device telemetry, industrial and IoT data, online data, mobility data, research datasets, medical imaging, digital pathology and genomic data, other high-dimensional datasets and AI-related processing. They should state clearly that the examples are not exhaustive conditions. This would also help demonstrate how the same legal principles apply to data with different levels of sensitivity, dimensionality and accessibility.

No Record Isolation, No Linkage and No Inference

Bitkom welcomes the EDPB's clarification that failure of one of the three criteria does not automatically establish that information is personal data.

This clarification is particularly important for high-dimensional datasets. A record may be unique within a dataset without there being any realistic way for a relevant entity to connect that record with a particular natural person. The final Guidelines should make this distinction more prominent in the section on No Record Isolation.
Uniqueness should not be treated as synonymous with identifiability.

Similarly, for No Linkage and No Inference, the effectiveness of the relevant linkage or inference technique should remain subject to the general standard applicable to re-identification techniques. A theoretical linkage or inference that cannot provide sufficiently reliable information about an identifiable individual should not in itself determine the result.

Privacy Enhancing Technologies and technical standards

The Guidelines provide an opportunity to encourage investment in technologies that reduce identification, linkage and inference risks.

Bitkom therefore encourages the EDPB to provide more explicit guidance on the role of Privacy Enhancing Technologies and other state-of-the-art approaches. Depending on the use case, relevant measures may include differential privacy, synthetic data techniques, secure computation and cryptographic measures.

The Guidelines should remain technology neutral. No individual technology should automatically establish anonymity. Conversely, scientifically validated technical measures that demonstrably reduce the relevant identification risks should be capable of constituting significant evidence in support of an anonymity assessment.

The EDPB should clarify that proportionate evidence, for example a reference to recognised methods, is sufficient to demonstrate such effectiveness.

The temporal dimension and reassessment

Bitkom recognises that identifiability can change over time. New additional information, a security incident or a material technological development may alter an earlier assessment. At the same time, the obligation to reassess should remain proportionate and practicable.

The final Guidelines should clarify:

- which entity is responsible for reassessment after data has been transferred;
- which events should trigger a new assessment;
- how the appropriate frequency and depth of reassessment should be determined; and
- how recipients that legitimately relied on a reasonable and properly documented anonymity assessment should deal with a later material change.

A material-change approach would provide greater predictability than a general expectation to reassess in response to every theoretical technological development. The fact that circumstances later change should not, by itself, retrospectively invalidate an assessment that was reasonable, state-of-the-art and reasonably conducted when it was carried out.

A workable process: substantiation, accountability and complaints

The Guidelines should address how anonymity assessments are handled in practice, including in supervisory proceedings and complaints. Without this, organisations risk a spiral of justification in which any assessment can be called into question again, irrespective of concrete indications. The final Guidelines should clarify that:

- a controller that has carried out a reasonable assessment, proportionate to the context, may rely on it until a material change occurs;
- an authority that doubts anonymity should substantiate which concrete, realistic means or actors it considers reasonably likely to lead to identification, as an abstract possibility is not sufficient;
- a complaint concerning allegedly identifiable data should prompt an examination of concrete indications of identifiability rather than a general reversal of the burden; and
- documentation requirements are proportionate and can be met through existing records.

Controller, processor and controller-to-controller scenarios

The contextual approach raises important practical questions concerning different processing roles.

The Guidelines provide useful examples distinguishing processing on behalf of a controller from independent processing. However, more complex situations are common in practice. An organisation may initially process information as a processor and subsequently act independently in relation to effectively anonymised output data for example when producing system-level metrics, aggregated diagnostic signals, or cross-fleet operational reporting under technical controls that prevent access to customer-held keys. The final Guidelines should clarify in paragraph 15 that anonymity in such secondary scenarios must be evaluated against the recipient's own practical means, avoiding an automatic, blanket attribution of the controller's status.

Similarly, controller-to-controller transfers raise questions concerning which party is expected to perform or verify the anonymity assessment, what information must accompany the transfer, and how onward transfers should be addressed. Bitkom asks the EDPB to **include additional examples** dealing with these scenarios and to clarify how changes in processing roles affect the applicable perspective.

No additional legal basis for risk-reducing anonymisation

Bitkom agrees that the GDPR applies for as long as personal data are being processed and that the processing preceding successful anonymisation must comply with the GDPR. However, we ask the EDPB to reconsider and not to maintain its conclusion that the act of anonymising lawfully processed personal data necessarily requires an additional legal basis in its own right.

Anonymisation is, in its effect, the functional equivalent of deletion. It irreversibly severs the link to the individual. The GDPR obliges controllers to delete data or render them non-identifiable once they are no longer needed (Articles 5(1)(e) and 17) and encourages risk-reducing measures (Articles 25 and 32). Nobody anonymises for its own sake. The purpose is to reduce risk, to meet storage limitation requirements, or to enable the subsequent use of non-personal data, including for research, industrial applications and the development of AI in Europe. Requiring a separate legal basis places anonymisation in a worse position than the continued storage of identifiable data.

Successful anonymisation fundamentally differs from processing operations that expand, intensify or prolong the use of personal data. Its very purpose and effect are to irreversibly remove identifiability, reduce risks for individuals and bring the resulting information outside the scope of the GDPR.

Against this background, requiring controllers to identify a separate legal basis for the transformation of lawfully held personal data into anonymous information may create a counterproductive result. Organisations could face fewer legal questions when retaining and continuing to process identifiable information than when taking an additional step specifically designed to remove the personal nature of that information.

In Bitkom's view, the final Guidelines should therefore recognise effective anonymisation, where it serves to reduce risk and does not entail an independent use of the personal data for another substantive purpose, as a privacy-enhancing safeguard applied to lawfully processed data rather than automatically treating it as a separate processing purpose requiring an additional legal basis. The subsequent use of the anonymous output, for example for research, analytics or AI development, falls outside the scope of the GDPR. This does not mean that the anonymisation process falls outside the GDPR before anonymity has actually been achieved. Controllers must continue to comply with the applicable principles and safeguards during the transformation process, including security, data minimisation and accountability requirements. The distinction concerns the legal justification for carrying out the risk-reducing transformation itself.

At the very least, if the EDPB maintains the position that a legal basis is required, the final Guidelines should clarify that:

- the legal basis applicable to the preceding lawful processing, and the compatibility assessment under Article 6 (4) GDPR, will normally also cover anonymisation as a data-protection or risk-reduction measure, without requiring identity of purpose;
- the legal assessment distinguishes the anonymisation operation from the later statistical, analytical, research or innovation use of the anonymous output; and
- equivalent clarity is needed for special categories of personal data under Article 9 GDPR, in particular for health and genetic data, so that the Article 9(2) exemption relied on for the preceding processing also covers the anonymisation step.

The same considerations apply where the controller is required to retain the original personal data for another lawful purpose or pursuant to a legal retention obligation. Deletion of the source data should therefore not be treated as a necessary condition for recognising the privacy-enhancing effect of creating a separate anonymous dataset.

More generally, the regulatory framework should create incentives for organisations to reduce identifiability wherever this is technically and organisationally feasible. The final Guidelines should avoid an interpretation under which the legal requirements associated with anonymisation itself discourage the deployment of one of the most effective measures for reducing data-protection risks.

Relationship with pseudonymisation

The final Guidelines should more clearly explain the relationship between the anonymity assessment and the EDPB's yet to be finalised Guidelines 01/2025 on Pseudonymisation.

The contextual approach means that the same technical transformation may have different legal implications for entities with different access to additional information. Clear cross-references and consistent terminology between the two Guidelines would help organisations determine whether particular data should be treated as personal, pseudonymised or anonymous from the relevant perspective.

This is particularly relevant for data-sharing structures in which identifying information and the data intended for further use are deliberately separated between different parties. It therefore seems appropriate that the finalisation of the pseudonymisation guidelines should be paused. This would have the added benefit of

making time for the EDPB to consider wider contexts around anonymisation and pseudonymisation, including recent court judgments and the ongoing Omnibus.

AI models

Anonymised data are a key input for the development of AI in Europe. Legal certainty on anonymisation therefore directly affects the ability of European companies to develop and train AI systems without using identifiable data. The Guidelines refer to AI both as a potential tool for re-identification and in connection with inference and model-related risks. Given the practical importance of AI, a **more coherent explanation** would be useful.

The assessment should distinguish between an AI model that enables specific and meaningful information about an identifiable individual to be extracted and a model that generalises patterns without exposing information attributable to a particular person.

Potential membership-inference, model-inversion or extraction attacks should be assessed according to the same principles as other re-identification techniques: effectiveness, accuracy, confidence, accessibility and whether their use constitutes a means reasonably likely to be used in the actual deployment environment.

Where access to a model is technically restricted, for example through controlled interfaces, monitoring, rate limits or other system-level safeguards, those restrictions should form part of the contextual assessment rather than analysing the model in isolation. The final Guidelines should also ensure coherence with EDPB Opinion 28/2024 on AI models.

Proportionate documentation

Anonymisation assessments should not give rise to new, stand-alone documentation burdens. Bitkom asks the EDPB to clarify that documentation must be proportionate to the risk and the context, that assessments can be integrated into existing documentation (such as records of processing activities, data protection impact assessments and information security documentation) where the relevant information is already available, and that the Guidelines do not create documentation obligations beyond what Articles 5(2) and 24 GDPR require. This is consistent with the EU's declared aim of reducing administrative burdens, in particular for SMEs.

2 Conclusion

Bitkom welcomes the move towards a contextual, perspective-based and probability-based assessment of anonymity. This approach has the potential to provide a modern framework that protects individuals while enabling organisations to reduce privacy risks through effective anonymisation.

To fulfil that potential, the Guidelines should be guided by the question of how anonymisation can be enabled in Europe. Bitkom asks the EDPB in particular to:

- apply the ”insignificant in reality” standard consistently, based on a reasonable weighing of the means the individual recipient is reasonably likely to use, in line with the CJEU’s case law;
- recognise technical, organisational and contractual safeguards, including binding commitments within corporate groups;
- refrain from requiring a separate legal basis for risk-reducing anonymisation;
- ensure a workable process in which authorities substantiate concrete, realistic means, organisations are not drawn into a spiral of justification, and documentation remains proportionate;
- ensure coherence with other EU data legislation; and
- as practical support, include illustrative positive examples and give scientifically validated PETs an explicit role in the assessment.

A clearer and more operational framework would make it easier for organisations of all sizes to invest in robust anonymisation techniques and to demonstrate that those techniques effectively protect individuals. Legal certainty on anonymisation is also a prerequisite for the use of data and AI and industrial applications in Europe.

Finally, the EDPB should avoid creating regulatory disincentives to anonymisation. Bitkom asks the EDPB to refrain from requiring an additional legal basis for the act of effectively anonymising lawfully processed data and, at a minimum, to provide a broad and workable pathway for treating anonymisation as a privacy-enhancing and risk-reducing measure.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 700 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Isabelle Görg | Head of Data Protection Law and Policy
P +49 30 27576-228 | i.goerg@bitkom.org

Responsible Bitkom Committee
WG Data Privacy

Copyright
Bitkom 2026

This publication is intended to provide general, non-binding information. The contents reflect the view within Bitkom at the time of publication. Although the information has been prepared with the utmost care, no claims can be made as to its factual accuracy, completeness and/or currency; in particular, this publication cannot take the specific circumstances of individual cases into account. Utilising this information is therefore sole responsibility of the reader. Any liability is excluded. All rights, including the reproduction of extracts, are held by Bitkom.