BDI

INNONATION

OPINION | DIGITILISATION | DATA PROTECTION

EDPB-Guidelines 02/2026 on Anonymisation

30 October 2026

General Remarks

The Federation of German Industries (BDI) welcomes the European Data Protection Board's (EDPB) revision of its guidance on anonymisation previously provided in Article 29 Working Party Opinion 05/2014 (para 2). Clarifying when data is considered anonymous and therefore falls outside the scope of the General Data Protection Regulation (GDPR), is of fundamental importance for data-driven innovation and creating a genuine Single Market for data, as envisaged by the European Commission's Data Strategy. Anonymisation is a key tool for enabling the privacy-compliant use of data for research and development purposes and for unlocking the societal and economic benefits of data-driven technologies while maintaining a high level of data protection.

BDI 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, the process of an effective anonymisation should be recognised as a privacy-enhancing and risk-reducing tool rather than being treated as a separate processing purpose that automatically requires an additional legal basis. The requirement of a distinct legal basis for anonymisation leads to unintended disincentives for organisations to reduce identifiability and data protection risks. The Guidelines should therefore ensure that organisations are encouraged, not discouraged, to deploy robust anonymisation measures and to facilitate the responsible use of anonymised data for research, innovation and AI development in Europe. At the very least, the Guidelines should recognise that the anonymisation of data lawfully held by a controller is a measure implementing the data protection principles, in particular data minimisation, for that processing (Article 25(1) GDPR) and should therefore be presumed to form part of the same processing activity and to serve the same purposes within the meaning of para 38, including, for special categories of personal data such as health data, as regards the applicable exemption under Article 9(2) GDPR. Equally, the deletion of the original data should not be treated as a precondition for recognising the risk-reducing effect of anonymisation (para 39), in particular where statutory retention obligations require the original data to be kept.

BDI supports the guidance's explicit recognition that the assessment of identifiability may depend on the specific actor and the means realistically available to that actor and embraces the relative, context-dependent notion of anonymity (paras 6–7, based on CJEU C-413/23 P EDPS/SRB). This confirms that the same dataset may constitute personal data for one actor while being considered anonymous

Dr Michael Dose | Innovation, Security and Technology | T: +49 30 2028-1560 | m.dose@bdi.eu | www.bdi.eu

for another. Such a context-specific approach reflects the realities of modern data ecosystems, in which different actors possess different supplementary information and, consequently, different capabilities to identify individuals.

At the same time, it remains questionable whether the draft guidance achieves its objective of providing practical, legally certain and innovation-friendly criteria for anonymisation. While the guidance confirms that a context-based assessment should form the legal benchmark, it also introduces a "simplified approach" that largely disregards differences in the actual identification capabilities of individual actors.

Closely linked to the question of the relevant assessment perspective is the issue of how far potential re-identification risks should be taken into account. From BDI's perspective, the guidance creates significant practical uncertainty in this regard. Beyond the capabilities of the specific recipient, organisations may be expected to consider additional information held by other actors, external datasets, future technological developments, AI-enabled analytics, potential data breaches and the possibility of combining information across multiple parties. There is a risk that the assessment of anonymisation shifts away from a realistic evaluation of actual identification possibilities towards increasingly theoretical and difficult-to-predict scenarios. The broad scope of the proposed re-identification risk assessment would inevitably result in substantial documentation and reassessment obligations. Companies risk being required not only to justify their anonymisation decisions in a transparent manner, but effectively to demonstrate why even future re-identification risks can be ruled out. Such an approach would significantly limit the practical usefulness of anonymisation as a mechanism for enabling the responsible and innovation-friendly use of data and would create additional compliance burdens without necessarily enhancing legal certainty.

Contextual Approach vs. Simplified Approach

BDI welcomes the EDPB's explicit recognition that the assessment of anonymisation should be based on the specific actor and the actual circumstances of the processing activity. This "context-based approach" appropriately reflects the reality of modern data ecosystems, where different organisations have access to different information and therefore possess different capabilities to identify individuals. It also aligns with the principle that anonymisation should be assessed on the basis of realistic rather than purely theoretical re-identification risks.

At the same time, we are concerned about the practical role assigned to the "simplified approach" in the Guidelines. While the Guidelines confirm that the contextual approach constitutes the relevant legal benchmark, the simplified approach places greater emphasis on the characteristics of the dataset itself and potential theoretical identification risks. This creates a risk that, in practice, assessments may increasingly be driven by abstract possibilities of re-identification rather than the actual capabilities of the specific recipient.

From our perspective it is therefore essential to clarify that the contextual approach remains the primary benchmark not only as a matter of legal interpretation but also in practical implementation and supervisory practice. Furthermore, the role of the simplified approach should be clearly defined as a voluntary and complementary assessment tool that does not create additional legal requirements or evolve into a de facto minimum standard for anonymisation decisions.

(Re-)Identification criteria

BDI welcomes the EDPB's efforts to establish a structured framework for assessing anonymisation and re-identification risks. In particular, the concepts of "means reasonably likely to be used" and the criteria of "No Record Isolation", "No Linkage" and "No Inference" can provide useful guidance when evaluating the effectiveness of anonymisation measures.

However, the Guidelines risk setting an excessively broad benchmark for re-identification assessments. By extending the analysis beyond the actual capabilities of the relevant recipient to include third-party knowledge, external datasets, future technological developments, AI-enabled analytical tools and potential misuse scenarios, the assessment may increasingly be based on hypothetical rather than realistic identification risks. In particular, the list of potentially relevant entities in para 30, which extends to foreign intelligence agencies, should not be read as a presumption of their relevance. The Guidelines themselves note that not all of these perspectives need to be considered systematically in each case (footnote 25); this statement should be moved into the body of para 30.

This challenge becomes particularly apparent when applying the criteria of "No Record Isolation", "No Linkage" and "No Inference". The mere technical uniqueness of a dataset, the theoretical possibility of linking data with information held by other parties, or speculative assumptions about future analytical capabilities should not automatically prevent data from being considered anonymous. Instead, the assessment should focus on whether identification can realistically be achieved in the specific processing context, taking into account the actual means and information available to the relevant actor. This is particularly relevant for records with many attributes, such as medical images or digital pathology data, which are frequently unique (cf. para 56). The Guidelines themselves recognise that violating a criterion does not necessarily mean that the data must be considered personal (para 52) and that a unique record may still be anonymous if singling out cannot be achieved or the record is not intelligible, provided the other two criteria are met (paras 98–99, Example 24). The final Guidelines should state clearly that a violation of No Record Isolation alone does not establish identifiability and that the singling-out test under paras 98–99 is the decisive next step.

BDI is furthermore concerned that the Guidelines provide limited clarity regarding the role of technical and organisational safeguards. In practice, many datasets are processed within controlled environments protected by access restrictions, governance mechanisms, contractual safeguards, encryption and other security measures. The contribution of such safeguards to reducing re-identification risks should be given appropriate weight in the overall assessment. Access-restricted environments of the kind provided for in sector-specific Union law, with binding, verifiable and enforceable access regimes, are a case in point. The Guidelines themselves acknowledge that, where data are subject to appropriate security controls, access constitutes a means reasonably likely to be used only for the authorised users (para 89), and they name the right yardstick for contractual measures, namely that they should be reliable, verifiable and enforceable (para 34). Such access regimes, combined with technical measures, should therefore be given decisive weight in determining which entities' perspectives are relevant under the contextual approach, while the capabilities of the authorised users continue to be assessed (para 90).

Without further clarification, there is a risk that anonymisation assessments become dependent on factors that organisations cannot reasonably control or predict, including future technologies, external datasets or information held by unrelated third parties. This would undermine legal certainty and could significantly reduce the practical usefulness of anonymisation as a tool for enabling the responsible use of data for research, innovation and economic growth.

BDI therefore calls for greater clarity that re-identification assessments should be based on realistic and objectively foreseeable risks, that hypothetical future scenarios should not become a de facto zero-risk standard, and that effective technical and organisational safeguards should be appropriately recognised when evaluating anonymisation measures. We encourage the EDPB to provide more explicit guidance on the role of Privacy Enhancing Technologies and other state-of-the-art approaches, while the Guidelines should remain technology neutral. Depending on the use case, relevant measures may include differential privacy, synthetic data techniques, secure computation and cryptographic measures.[1] For trained AI models, evidence based on documented testing against state-of-the-art membership inference and other inference attacks should be accepted as a way of demonstrating that a model generalises rather than relying on the records of individuals, and thus that the No Inference criterion is met (paras 71(b) and (c), 79 and 82, footnote 44). The Guidelines should also be coherent with EDPB Opinion 28/2024 on AI models (footnote 45).

Proportionate Documentation Requirements

BDI supports the EDPB's objective of ensuring transparency and accountability in anonymisation processes. Appropriate documentation can help demonstrate compliance and improve the traceability of anonymisation decisions.

However, the Guidelines risk creating disproportionate documentation obligations. By requiring organisations to consider not only the capabilities of the specific recipient, but also external datasets, third-party information, future technological developments, AI-enabled analytical methods and potential data breaches, the scope of the assessment becomes increasingly broad and uncertain. As a result, documentation requirements may evolve beyond explaining and justifying an anonymisation decision towards demonstrating the absence of any conceivable future re-identification risk.

Such an expectation would be neither realistic nor practicable. Organisations cannot reliably assess future data sources, technological developments or analytical capabilities that may emerge over time. Documentation should therefore focus on the rationale underlying the anonymisation decision and the effectiveness of the measures applied at the time of the assessment, rather than requiring predictions about hypothetical future developments including assumptions based on unlimited AI capabilities.

BDI also notes that the Guidelines leave considerable uncertainty regarding potential reassessments of anonymised data. While a reassessment may be appropriate where there are concrete and objectively verifiable changes in the risk environment, anonymisation decisions should not remain indefinitely subject to reassessment based on speculative future developments. Legal certainty requires that the effectiveness of anonymisation be assessed against the facts known and the state of the art available at the time the anonymisation is carried out. Legal certainty about the initial assessment is of particular importance for products that may remain in use for many years, such as medical devices and their AI components. The EDPB should therefore confirm that a reversion to personal data under para 35 operates only for the future, so that an assessment carried out carefully and documented according to the state of the art at the time does not retroactively call the lawfulness of the earlier processing into question. For the same reason, the statement in footnote 3 that a controller which has assessed a dataset as anonymous under Opinion 05/2014 is not expected to conduct a new assessment should be moved into the body of the Guidelines.

---

[1] BDI, Handbook on Anonymisation of personal data (2020), p. 20 ff.

We therefore call for further clarification that documentation obligations are intended to ensure transparency and accountability of anonymisation decisions, rather than to establish proof of absolute non-identifiability. In addition, reassessments should be limited to situations involving concrete and objectively demonstrable changes in the level of re-identification risk. Documentation under para 41 should be proportionate to the risk and may be integrated into existing compliance documentation, such as records of processing activities, data protection impact assessments and, in regulated sectors such as medical devices, the risk management and quality management documentation required by sector-specific law.

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, building operation and energy consumption data, online data, mobility data, research datasets, health data prepared for the development and validation of medical devices, 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.

Imprint

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

EU Transparency Register: 1771817758-48

German Lobbyregister: R000534

Editor

Dr Michael Dose
Senior Expert Data Protection and Data Economy
Directorate Innovation, Security and Technology
T: +49 30 2028-1560
m.dose@bdi.eu

Document number: D 2399