



# **BVDW response to the EDPB public consultation on Guidelines 02/2026 on Anonymisation**

Towards a legally certain and practicable standard for anonymisation

## EXECUTIVE SUMMARY

The BVDW welcomes the fact that the guidelines in principle assess anonymity from the perspective of the entity under consideration. However, this relative approach is not consistently applied: the guidelines extend the concept of personal data so broadly – through broadly construed criteria, theoretical re-identification scenarios and insufficient consideration of effective protective measures – that anonymity would be virtually unachievable in practice. What is required is a legally certain, operationalisable standard that assesses actual possibilities of identification and promotes effective anonymisation.

From the BVDW's perspective, five adjustments are key:

- Assess identifiability independently. Distinguishability, singling out, recognition, profiling and influenceability are merely indicators or possible precursors to identification; they are not equivalent to identification, either individually or cumulatively.
- Consistently apply the relative approach. The decisive factors are the legal, technical and actual capabilities of the entity in question at the relevant point in time.
- Only take into account means of identification that are reasonably likely to be used. Theoretical possibilities, accidental identifications and scenarios that presuppose a breach of the law must not become the standard. The decisive factors are actual access to additional information, legal permissibility, cost and time required, technical feasibility, accuracy and probability of success. The guidelines should bring these factors together in a structured, documentable assessment template, provide for appropriate requirements for SMEs, and require supervisory authorities to specify a concrete re-identification pathway.
- Assess technical, organisational and contractual safeguards collectively. Effective access restrictions and legally binding, verifiable and enforceable prohibitions on re-identification can significantly reduce the practical likelihood of identification and must be taken into account as risk-mitigating measures.
- Encourage anonymisation through the legal framework. Anonymisation is a processing operation within a processing activity and requires neither a separate purpose nor its own legal basis. Effectively anonymised information does not fall within the scope of the GDPR and must be usable for further purposes such as statistics, product improvement or research. Legal certainty and regulatory flexibility create the necessary incentive to invest in robust anonymisation procedures.

With these adjustments, the guidelines can transform the relative approach to personal data into a legally certain and practicable assessment standard that combines the protection of data subjects with responsible data use and innovation.

## Table of Contents

|                                                                                                                 |           |
|-----------------------------------------------------------------------------------------------------------------|-----------|
| <b>EXECUTIVE SUMMARY .....</b>                                                                                  | <b>1</b>  |
| <b>1. INTRODUCTION .....</b>                                                                                    | <b>2</b>  |
| <b>2. LEGAL ASSESSMENT (SECTION 2 OF THE GUIDELINES) .....</b>                                                  | <b>2</b>  |
| 2.1 THE TWO-STAGE ASSESSMENT FRAMEWORK: IDENTIFIABILITY AS THE ACTUAL ASSESSMENT CRITERION .....                | 2         |
| 2.2 THE APPLICABLE PERSPECTIVE AND EXCEPTIONS TO IT .....                                                       | 2         |
| 2.3 ANONYMISATION PRIOR TO TRANSFER: SCOPE OF THE OBLIGATION TO PROVIDE INFORMATION .....                       | 3         |
| 2.4 DATA PROCESSING ON BEHALF OF THE CONTROLLER .....                                                           | 3         |
| 2.5 THE 'RELATES TO' CRITERION: CONTENT, PURPOSE AND EFFECT .....                                               | 3         |
| 2.6 'IDENTIFIED OR IDENTIFIABLE' .....                                                                          | 4         |
| 2.7 ANONYMISATION WITHIN AN ORGANISATION .....                                                                  | 5         |
| <b>3. THE 'MEANS REASONABLY LIKELY TO BE USED' STANDARD .....</b>                                               | <b>5</b>  |
| 3.1 LACK OF OPERATIONALISATION .....                                                                            | 5         |
| 3.2 FUTURE-ORIENTED APPROACH AND PROPORTIONALITY .....                                                          | 6         |
| 3.3 SCOPE OF RELEVANT ENTITIES .....                                                                            | 6         |
| 3.4 MOTIVATION .....                                                                                            | 7         |
| <b>4. RECOGNITION OF CONTRACTUAL GOVERNANCE ('REGULATION BY CONTRACT') .....</b>                                | <b>7</b>  |
| <b>5. ON THE TECHNICAL ANALYSIS (SECTION 3 OF THE GUIDELINES) .....</b>                                         | <b>7</b>  |
| 5.1 DATASET AND DATA SEGMENTS; FOLLOW-UP QUESTIONS .....                                                        | 7         |
| 5.2 NO LINKAGE .....                                                                                            | 8         |
| 5.3 NO INFERENCE .....                                                                                          | 8         |
| <b>6. ANONYMISATION AS A PROCESSING OPERATION WITHOUT ITS OWN PURPOSE AND WITHOUT ITS OWN LEGAL BASIS .....</b> | <b>9</b>  |
| <b>7. CONCLUDING REMARKS .....</b>                                                                              | <b>10</b> |

## 1. Introduction

The Bundesverband Digitale Wirtschaft (BVDW) welcomes the opportunity to comment on the guidelines of the European Data Protection Board (EDPB). For businesses in the digital economy, the distinction between personal data and anonymous data is of considerable practical importance.

The guidelines are being published at a time when the Court of Justice has clarified the underlying principles. In its judgment in *EDPS v SRB* (CJEU, judgment of 4 September 2025 – C-413/23 P), it continued the line of the *Breyer* case law. Whether information is personal is determined from the perspective of the relevant entity and the means that this entity is reasonably likely to use. The BVDW welcomes the fact that the EDPB has endorsed this relative approach.

However, in their design, the guidelines fall short of this starting point in several respects. Broad interpretations of the term 'relates to', the equating of individualisability with identifiability, a very broad range of relevant entities, and the extensive exclusion of contractual measures ultimately mean that anonymisation is virtually impossible to implement in practice. At the same time, there is a lack of operationalisable criteria on the basis of which controllers can substantiate their assessments and supervisory authorities can review them.

## 2. Legal assessment (Section 2 of the guidelines)

### 2.1 The two-stage assessment framework: Identifiability as the actual assessment criterion

In the guidelines, the EDPB correctly divides the core test into two stages: the first question is whether the information relates to a natural person (a), and the second is whether that person is identified or identifiable (b). At the second stage, a genuine risk assessment must be carried out. However, in explaining the test, the EDPB essentially confines itself to the likelihood of occurrence, without developing the risk dimension methodologically.

The assessment set out in the guidelines – namely, whether the entity in question has access to or control over the data, or can obtain it – is appropriate, but should be applied more consistently, particularly where the guidelines subsequently consider very broad groups of recipients.

The guidelines should be supplemented by an explicit risk assessment that relates the likelihood of occurrence to the severity of the impact on the data subject.

### 2.2 The applicable perspective and exceptions to it

According to the guidelines, the starting point for assessing whether data is anonymous is the relevant entity and its perspective. However, the guidelines provide for exceptions to this principle without systematically cataloguing them.

Making the recipient's perspective the benchmark is only logical if the assessment is based solely on the recipient; the relevant point of reference is the recipient's capabilities. The 'feedback effect' on the transferring entity assumed in the guidelines – whereby the data also becomes indirectly personal for the transferring entity – would in effect weaken the relative approach. It is difficult to reconcile this with the case law.

Furthermore, the Board asserts that certain obligations under the GDPR may override this perspective. However, it remains unclear exactly which obligations these are.

## 2.3 Anonymisation prior to transfer: scope of the obligation to provide information

If personal data is collected and anonymised prior to its transfer, the guidelines state that the recipients must nevertheless be named because the data was personal at the time of collection. This gives rise to a key practical question: does this also apply if the original purpose of collection did not include the subsequent transfer, meaning that this was neither planned nor foreseeable at the time of collection? And does this also apply where the controller anonymises the data precisely in order to comply with an obligation to erase it, and the usefulness of the anonymised dataset for analysis only becomes apparent subsequently?

There is also an inherent contradiction: if the data is anonymised prior to transfer, the transfer process itself no longer involves personal data. It therefore falls outside the scope of the Regulation. An obligation to name recipients of anonymous information can therefore, at best, be justified from the perspective of the controller at the time of collection. It can – if at all – only extend to transfers that were already planned or foreseeable at that time.

## 2.4 Data processing on behalf of the controller

It is crucial to note that classifying processing on behalf of the controller as falling within the controller's sphere merely addresses the question of whether the data is personal from the controller's perspective, not from that of the processor. It does not follow from this whether the data is personal to the processor itself; this must be determined separately. Roles within the meaning of the GDPR are functional and relate to the individual processing operation. The EDPB's statement on processing on behalf of a controller must therefore be clarified and must not go beyond what is inherent in the regulatory purpose and scope of the GDPR. If the processor has no means that are reasonably likely to be used to identify the data subjects, the classification of the data as personal is not based on the application of Article 4(1) of the GDPR and Recital 26, but on a legal fiction linked solely to the processing relationship.

This legal fiction cannot be based on the case law of the Court of Justice. In the *EDPS v SRB* judgment, the Court of Justice held that information does not have to be personal in every case or for every entity, and that technical and organisational measures may result in information not being personal to a recipient who is unable to identify the data subject. The Court of Justice left open the question of whether the information was personal from the recipient's perspective.

Furthermore, there is a risk of circular reasoning. Under Article 4(8) of the GDPR, a processor is defined as a person who processes personal data on behalf of the controller. To infer from this role that the data is also personal for the processor presupposes a conclusion that would first need to be examined.

The processing relationship may be a significant factual circumstance in the context of the identifiability test, but it is not a substitute for it. This is in line with the statement in the guidelines that the relationship between the parties involved and the processing on behalf of another entity are circumstances that are relevant to the applicable perspective. However, this does not render the examination of the actual legal, technical and organisational circumstances superfluous.

Furthermore, the conclusion drawn – namely, the application of the processor's obligations, inter alia under Articles 28, 29, 30(2) and 32 of the GDPR – must be described in the further statements in the guidelines for what it actually is: effective contractual control over the data. Consequently, the same assessment must also apply when evaluating contractual measures. The EDPB itself acknowledges in the guidelines that contractual agreements and obligations under the GDPR work together to ensure that the processor handles personal data appropriately (more on this later).

## 2.5 The 'relates to' criterion: content, purpose and effect

The underlying triad of content, purpose and effect has become too broad in its scope and conceptual formulation. At least the content element remains unproblematic.

The situation is different with regard to the 'purpose' element. According to this, it is sufficient that the information relates to the individual or something connected with them and is intended to be used to assess, treat or influence the individual in a particular way. The information neither generates an identifier in its own right, nor is it necessarily attributable to the individual. If the sole determining factor were the intention pursued through the processing, the classification would depend on subjective circumstances that cannot be determined in advance; it would be virtually impossible to predict reliably.

The 'effect' element covers information about objects whose processing merely has an effect on the individual. However, the 'concrete possibility' of unequal treatment required by the guidelines remains undefined. Without such a limitation, there is a risk that the criterion could bring almost any data processing within the scope of the GDPR.

The EDPB also states in the guidelines that a link is deemed to exist even if the connection must first be established through further processing steps; this explicitly applies to aggregated information as well. Taken together with the 'effect' element, this would mean that aggregated information would regularly have to be treated as potentially personal data. This contradicts the statement also made in the guidelines, according to which aggregated data regularly fulfils the No Record Isolation criterion.

The 'effect' element must be interpreted restrictively and in line with the case law of the Court of Justice; the decisive factor must be a concrete, not merely theoretical, effect on a specific individual. The 'purpose' element should be clarified to mean that what matters is an objectively ascertainable association with a specific individual established at the time of processing – not a hypothetical intended use. Otherwise, even purely object-related information – such as that relating to objects, processes or technical systems – would, in a large number of cases, be classified as personal data. The distinction between personal and non-personal data, upon which the GDPR is based, would thus lose its clarity.

## 2.6 'identified or identifiable'

The guidelines essentially define identification (direct and indirect) on the basis of two elements: a natural person must be distinguishable from others in a specific context, and this distinguishability must make it possible to treat them differently. This approach goes too far. Distinguishability and the possibility of influence may be indicators of identifiability; however, they are not equivalent to it, either individually or cumulatively. Article 4(1) of the GDPR requires, as a separate element in addition to the relation of the information to a natural person, that this person be identified or identifiable. This constituent element must not be replaced by indicators.

Distinguishability initially merely indicates that a data record, profile, device, browser or connection can be distinguished from others. Even the 'singling out' referred to in Recital 26 merely describes a possible means towards identification, not its result.

Nor does the possibility of differential treatment close this gap. It merely shows that a distinguishable technical object or profile can be targeted. For example, serving adverts based on a cookie ID, advertising ID or fingerprint treats a browser, an end device or a pseudonymous profile differently from others. It does not follow from this that the acting entity knows the natural person behind it, nor that it can identify that person by means reasonably likely to be used.

The guidelines thus confuse distinguishability with a possible consequence of identification. If a natural person is identified or identifiable, this may enable the entity in question to target them specifically. However, the reverse does not follow: that every possibility of targeting or distinguishability presupposes or proves direct or indirect identifiability. The relationship is asymmetrical. Identifiability may enable influenceability; influenceability, however, does not in itself establish identifiability.

This is illustrated by a simplified example based on the display of advertising. A system can select content on the basis of an identifier and thereby actually influence a natural person's user experience, without the entity acting being able to determine which person is involved. The effect then occurs via a device, a browser or a pseudonymous profile. It is effectively directed at a user, but does

not yet establish a reliable link between the processed information and a specific or identifiable natural person.

Nor does the cumulative combination of distinguishability and influenceability eliminate this logical flaw. Both characteristics can co-exist without identifiability. A profile can be distinguished from other profiles, recognised and treated individually, even though the natural person behind it cannot be identified by means that are reasonably likely to be used. Taken together, these two indicators do not constitute a substitute for the identifiability required by law.

This is consistent with the structure of the GDPR. Pseudonymised datasets remain distinguishable by means of an identifier, but cannot be attributed to a natural person without additional information stored separately. Similarly, Article 11 of the GDPR provides that a controller may process personal data without identifying the data subject. If any form of distinction or individual treatment were in itself to constitute identification, these distinctions would largely be rendered meaningless.

The same applies to IP addresses, cookie IDs, advertising IDs, MAC addresses, fingerprints, social security numbers and similar identifiers. These initially refer to a connection, a device, a browser, a user account or a data record. Whether a natural person can also be identified as a result depends on additional means of attribution. A robust link between the identifier and a natural person is required.

The decisive factor therefore remains the filter of the means reasonably likely to be used for identification. From the perspective of the relevant entity, particular consideration must be given to actual access to additional information, the legal permissibility of obtaining and linking such information, cost and time required, technical feasibility, as well as accuracy and the probability of success.

The guidelines should therefore make it clear that distinguishability and influenceability are neither alternative nor cumulative substitute characteristics of identification. In particular, it must not be inferred from a possible effect that the person is identifiable: the effect may be a consequence of identification, but it also occurs in relation to merely distinguishable devices, browsers or pseudonymous profiles.

## 2.7 Anonymisation within an organisation

The guidelines recognise in principle that anonymisation is possible even without the deletion of the original data. However, all examples illustrating this principle are tailored to external disclosure, whilst any description of anonymisation within an organisation is linked to the deletion of the original data. This gives rise – even if this is probably not the intention – to the impression that a controller can only anonymise data for its own internal purposes if it deletes the original data.

This goes beyond the standard set out in the guidelines themselves and is counterproductive: controllers who invest in internal anonymisation receive no regulatory recognition for doing so. The contextual, perspective-based methodology of the guidelines is perfectly capable of treating a ring-fenced internal environment as the relevant point of reference; this is directly in line with the principle of data minimisation under Article 5(1)(c) of the GDPR.

The BVDW therefore recommends clarifying that anonymity can also be assessed within an organisation and that the retention of the original data elsewhere within the organisation does not, in itself, preclude anonymity, provided that re-identification from the relevant internal perspective is not reasonably likely. The definition of the ‘relevant entity’ and the comments on the ‘applicable perspective’ should be expanded accordingly and supplemented with at least one example of internal anonymisation within an organisation without the deletion of the original data.

## 3. The ‘means reasonably likely to be used’ standard

### 3.1 Lack of operationalisation

It is worth noting positively that the EDPB sets out objective factors in the guidelines: the properties of the data and its vulnerability to various attack vectors, the context of the processing including

effective and permanent access restrictions, access to additional information, costs and time involved, and the available technology. These factors should be further developed into a transparent, structured and documentable assessment template, on the basis of which controllers can substantiate their assessment and supervisory authorities can review it.

From a procedural perspective, it must also be clarified that the burden of presentation and proof that the data is personal lies, in principle, with the supervisory authority. It is true that the accountability principle (Article 5(2) of the GDPR) extends to the anonymisation process as such. However, the guidelines must not amount to an assumption of a secondary burden of substantiation or a de facto reversal of the burden of proof, which would require controllers to demonstrate that no conceivable re-identification pathway exists. Particularly problematic in this regard is the description of a finding of anonymity as a 'false positive' in the guidelines. This classifies the conclusion of anonymity as an error to be avoided and, as a result, establishes a presumption of personal data status. A supervisory authority asserting personal data status should, rather, be required to identify a specific re-identification pathway and should not be able to limit itself to a theoretical possibility.

SMEs and start-ups often lack the legal and technical expertise to identify all relevant actors, additional datasets, possible re-identification chains and technical developments. The simplified approach appears more manageable to them; however, when applied systematically, it leads to data that is in fact anonymous being treated as personal data. The contextual approach, on the other hand, requires resources and a level of documentation that can be overwhelming for smaller companies. The proposed structured assessment template should therefore draw on established international standards, namely ISO/IEC 27559:2022 (Framework for de-identification) and ISO/IEC 20889:2018 (Terminology and classification of de-identification techniques).

A structured, documentable assessment template ('anonymisation assessment') should be included in an annex, including an appropriate depth of documentation for SMEs. Such a template would also make the documentation of the anonymisation process, as required by the guidelines, manageable.

### 3.2 Future-oriented approach and proportionality

The EDPB's clarification in the guidelines that the test relates solely to possible future identification is to be welcomed. Equally welcome is the clarification that means whose use would require a disproportionate expenditure of time, cost and labour are to be disregarded. However, this standard is subsequently watered down. For instance, the guidelines maintain that time and costs are generally not prohibitive. In doing so, the guidelines contradict themselves, as time, cost and labour are explicitly identified as relevant factors earlier on. Furthermore, the reference to AI-supported re-identification, when linked to the resources of the respective organisation, leads to the absurd conclusion that it is precisely highly capable organisations that would never be able to achieve anonymity. It should be made clear that superior resources alone do not preclude anonymity.

The guidelines should specify the thresholds at which an expenditure of time, cost and labour is to be regarded as disproportionate, and should set out quantitative benchmarks or recognised metrics against which controllers can validate their procedures. Furthermore, the guidelines should deal substantively with privacy-enhancing technologies (PETs). Practical examples should be used to explain how differential privacy, secure multi-party computation, homomorphic encryption and synthetic data can contribute to anonymisation under suitable circumstances. This does not affect the fact that their effectiveness must always be assessed in the respective context. Such guidance would better reflect the state of the art and encourage investment in methods that make effective anonymisation achievable, particularly for SMEs. The proposed **structured assessment template** in the annex should be supplemented with SME-specific examples demonstrating how a robust contextual assessment can be carried out with limited resources. Practical examples relating to PETs should be included.

### 3.3 Scope of relevant entities

In the guidelines, the EDPB includes both direct and indirect recipients to a very broad extent. These entities may, where appropriate, play a role in the assessment of information security. However,

when it comes to distinguishing between anonymous and personal data, such a broad approach means that anonymity is practically unachievable, as the behaviour of third parties acting unlawfully can never be ruled out. The list set out in the guidelines must not serve as the basis for a mandatory assessment programme. Only those entities for which there are actual grounds to believe they have access to the data in the specific processing context should be included.

What is decisive is not whether identification is theoretically possible, but whether it is reasonably foreseeable under the specific circumstances. Foreseeability is inherent in the standard of 'means reasonably likely to be used' as set out in Recital 26, sentence 3 of the GDPR. A merely theoretical possibility is not sufficient, and consideration must be given only to persons and means that have access to the necessary additional information or can reasonably obtain it.

### 3.4 Motivation

In the guidelines, the EDPB warns against treating a lack of motivation for re-identification as a factor, particularly with regard to entities where there are concrete indications of unlawful access. It should be made clear that re-identification scenarios which presuppose a breach of the law are, in principle, disregarded and should only be taken into account where there are concrete, verifiable indications. Consequently, actors acting without authorisation and unlawfully should be excluded from the group of relevant entities. The same applies to accidental identification. **Accident** and negligence must be taken into account in the context of the security assessment, but not when determining whether personal data is involved within the meaning of Article 4(1) of the GDPR.

## 4. Recognition of contractual governance ('regulation by contract')

The GDPR itself relies to a considerable extent on contractual governance. Article 28 of the GDPR establishes the data processing agreement as an instrument of control over the data; Article 46(2)(c) of the GDPR designates standard contractual clauses as appropriate safeguards for transfers to third countries; Article 40 of the GDPR recognises codes of conduct with binding effect. Elsewhere, therefore, contractual obligations are regarded as sufficiently effective to ensure the protection of fundamental rights; when assessing anonymity, however, they are to be regarded as essentially irrelevant. This contradiction in assessment should be resolved.

Even though a contractual obligation can neither alter the fundamental nature of data nor replace effective technical de-identification, enforceable contractual terms constitute an essential, supplementary safeguard. The guidelines should recognise that, in controlled environments, legally binding and monitored contractual obligations (backed by remedies such as audit rights, damages, contractual penalties and interim relief) measurably reduce the practical likelihood of re-identification.

Finally, the Board recognises effective and permanent access restrictions and security controls as factors that limit the group of relevant actors to authorised users. In practice, contractual and technical measures are particularly effective when used in combination.

The exclusion of contractual measures should therefore be replaced by a standard of proof. If a prohibition on re-identification is legally binding, verifiable through audits or technical evidence, accompanied by enforceable consequences, and supported by effective technical measures, it must be taken into account as a risk-mitigating factor when assessing the means reasonably likely to be used. Even a measure that does not meet these requirements may carry less weight; however, the weight must be assessed and should not be dismissed outright.

## 5. On the technical analysis (Section 3 of the guidelines)

### 5.1 Dataset and data segments; follow-up questions

The distinction made in the guidelines between the anonymity of the dataset as such and that of

individual parts is appropriate. The legal consequence attached to this – namely, that a dataset is only anonymous if it is so for all persons covered by it; otherwise, the entire dataset is deemed to be personal data – is, however, very far-reaching. It should be supplemented by practical options for separation. A distinction must then be made as to whether the data can be separated or not. The parallel drawn in the guidelines with the *Meta Platforms v Bundeskartellamt* judgment does not hold. The reasoning set out in that case concerns special categories of data and other personal data that cannot be separated at the time of collection, but does not address the legal status of anonymous information. Recital 26, sentence 5 of the GDPR expressly excludes anonymous information from the scope of the Regulation. In this context, it must be assessed whether the components can be separated and whether identifiable data records compromise the anonymity of the remainder. The re-identification of an individual may trigger this assessment, but does not automatically determine the status of data records that are not affected. The decisive factor is whether the circumstances that enabled the identification of one data record significantly increase the identifiability of the remainder. Furthermore, the guidelines amend the wording used by the Court of Justice. Whereas the Court's ruling focused on whether it was possible to separate the data, the guidelines focus on whether the data are treated separately – that is, on a decision regarding their handling. Correctly, the assessment should address two questions: whether the risk of re-identification across the dataset is negligible, and whether identifiable data records can be separated.

It may well be true that the anonymity of data can change with technological progress, the state of the art and the capabilities of the entities involved. However, information that is in fact anonymous falls outside the scope of the GDPR. The review referred to as 'good practice' must therefore not be allowed to turn into a continuous monitoring obligation without any specific trigger under the GDPR for data that was originally and correctly classified as non-personal. Furthermore, the guidelines leave open the question of who is subject to the review: the anonymising controller, the entity currently using the dataset, or even processors and sub-processors. Instead of an indefinite, ongoing obligation to review, defined triggers should be specified: a significant security breach affecting a protective measure that has actually been relied upon, or an evidenced re-identification pathway. The original assessment must be judged against the information and technology available at the time it was carried out. New data, technologies or procedures do not retrospectively render an earlier assessment, based on the state of knowledge at the time, incorrect. If the risk of identification subsequently becomes significant, the relevant entity must treat the data as personal from the point in time at which it became aware of the change or should have become aware of it. A subsequent change in circumstances does not render earlier processing unlawful if the original assessment was defensible.

## 5.2 No Linkage

Although the EDPB clarifies in the guidelines that, in the contextual approach, the question is whether, from the relevant perspective, the linkage is possible with 'means reasonably likely to be used', the definition of linkage provided there and the accompanying examples follow the simplified approach. The guidelines should emphasise more clearly that linkage must be assessed against the standard of 'means reasonably likely to be used' – that is, taking into account actual access to the additional data as well as the legal and contractual permissibility of the linkage.

## 5.3 No Inference

The criterion is met if no specific and meaningful conclusion can be drawn from the data. However, drawing this distinction is hardly practicable in application. The comparative test proposed in the guidelines (evaluation with and without the dataset of the data subject) can, in practice, only be implemented for aggregated data and AI models at considerable expense. The rebuttable presumption provided for therein is to be welcomed as a fallback solution; however, it is only available if neither tracing nor the comparative test is possible, for example following the aggregation and deletion of the original data.

Overall, the following applies: an inference is irrelevant if the information obtained does not itself constitute personal data. This principle should be stated more clearly at the outset of the guidelines.

Practicable means of proof should be included for the inference test, in particular the recognition of established and documented procedures as the basis for a presumption of compliance with the criterion. At the same time, it should be made clear that the attack techniques described in the guidelines – in particular membership inference and model extraction – must be assessed against the ‘means reasonably likely to be used’ standard and do not automatically result in failure to meet the ‘No Inference’ criterion. The comparison of results with and without an individual’s dataset, as provided for in the guidelines, is one of the few practical specifications and is to be expressly welcomed.

## 6. Anonymisation as a processing operation without its own purpose and without its own legal basis

According to the guidelines, anonymisation is said to require its own legal basis under Article 6 of the GDPR and, in the case of special categories of personal data, its own exemption under Article 9(2) of the GDPR; the legal basis and exemption are to correspond to those of the preceding processing, provided that the anonymisation forms part of the same processing activity and the controller pursues the same purposes with it.

This approach is not convincing. In practice, anonymisation is not applied to data collected for a single purpose on a single legal basis, but to consolidated datasets derived from numerous collections and serving multiple purposes on different legal bases. Both conditions set out in the guidelines are therefore regularly rendered meaningless, and the guidelines leave open what the consequence of this should be.

The purpose and legal basis relate to the processing activity as a whole, not to the individual processing operation. Article 4(2) of the GDPR defines processing as any operation or set of operations; the assessment of necessity under Article 6(1) of the GDPR can only be carried out once the intended purpose has been determined. If anonymisation were to require its own legal basis, this would have to apply equally to storage, retrieval, transmission and erasure. Erasure and encryption demonstrate this: both constitute processing within the meaning of Article 4(2) of the GDPR, both are carried out on personal data, and neither requires a separate legal basis; encryption is expressly provided for as a security measure in Article 32(1)(a) of the GDPR. Article 6(4)(e) of the GDPR lists pseudonymisation amongst the safeguards and not amongst the operations requiring justification; the EDPB itself describes pseudonymisation as a security and data protection measure. Anonymisation is the strongest measure in this category and cannot be the only one requiring authorisation.

Otherwise, a contradiction in assessment arises. The processing operation that most effectively reduces the risks to data subjects would be the most difficult to justify, whilst the continued processing of identifiable data in its unaltered form requires no additional legal basis. This contradicts Article 25 of the GDPR. In this respect, the guidelines are also internally contradictory, as on the one hand they require a statement that the data is being processed to generate anonymous information – thereby treating the process as a purpose – whilst on the other hand they incorporate anonymisation into the legitimate interest balancing test for the preceding processing, which specifically presupposes that it is not a purpose in its own right.

It should therefore be clarified that anonymisation is a processing operation which has neither a purpose of its own nor its own legal basis, but is covered by the processing activity of which it forms part. The condition that the controller must pursue ‘the same purposes’ should be deleted. It should also be made clear that anonymisation is not to be specified as a separate processing purpose under Articles 13 and 14 of the GDPR.

Furthermore, the guidelines should explicitly recognise that anonymisation enables controllers to use data for further purposes, such as statistical analysis, product improvement or research. As anonymous information, according to Recital 26, sentence 5 of the GDPR, does not fall within the scope of the Regulation, its further use is subject neither to the principle of purpose limitation under Article 5(1)(b) of the GDPR nor to the compatibility assessment under Article 6(4) of the GDPR. This, in particular, provides a significant incentive to invest in effective anonymisation procedures. The guidelines should explicitly address this context, rather than treating anonymisation primarily from

the perspective of obligations and risks.

## 7. Concluding remarks

By endorsing the relative approach to personal data, the guidelines have chosen the right starting point. The EDPB should now consistently translate this approach into operationalisable and verifiable criteria. This will enable controllers and supervisory authorities to reliably assess identifiability, whilst ensuring that effective data protection and responsible data use go hand in hand. At the same time, the EDPB should seize the opportunity to grant companies greater regulatory flexibility with regard to data protection-friendly anonymisation. Those who invest in effective anonymisation should be granted legal certainty and scope for the further use of the data. The BVDW is happy to engage in further dialogue.



## Bundesverband Digitale Wirtschaft (BVDW) e.V.

The Bundesverband Digitale Wirtschaft (BVDW) e. V. represents the interests of companies that operate digital business models or whose value creation is based on the use of digital technologies. With its members from across the digital economy, the BVDW is already shaping the future today – through creative solutions and state-of-the-art technologies. As a catalyst, guide and driver of digital business models, the association advocates fair and clear rules and champions innovation-friendly framework conditions. In doing so, the BVDW always keeps the economy, society and the environment in mind. In addition to DMEXCO, the leading trade fair for digital marketing and technologies, and the German Digital Award, the BVDW also organises the CDR Award – the first awards ceremony in the DACH region for digital sustainability and responsibility – as well as a wide range of specialist events.

**Author:** Philipp Hagen, Director Legal Affairs & Data Privacy, [hagen@bvdw.org](mailto:hagen@bvdw.org)

[www.bvdw.org](http://www.bvdw.org)

### Legal notice

**Place and date of publication** Berlin, 29. Oktober 2026

**Publisher**

Bundesverband Digitale Wirtschaft (BVDW) e.V.  
Obentrautstraße 55,  
10963 Berlin  
  
+49 30 2062186 – 0  
[info@bvdw.org](mailto:info@bvdw.org)  
[www.bvdw.org](http://www.bvdw.org)

**Management Board pursuant to Section 26 of the German Civil Code (BGB)** Carsten Rasner

**President**

Dirk Freytag

**Vice-Presidents**

Thomas Duhr, Anke Herbener, Corinna Hohenleitner, Dr Moritz Holzgraeffe, Björn Kaspring, Julian Simons

**Contact**

[politik@bvdw.org](mailto:politik@bvdw.org)

**Association registration number** Charlottenburg Local Court VR 42449 B  
**ber**

**Legal disclaimer**

All details and information contained in this publication have been carefully researched and verified by the Bundesverband Digitale Wirtschaft (BVDW) e.V. This information is provided as a service by the Association. Neither the Bundesverband Digitale Wirtschaft (BVDW) e.V. nor the companies involved in the preparation and publication of this work can accept liability for its accuracy, completeness or timeliness. The contents of this publication and/or references to third-party content are protected by copyright. Any reproduction of information or data, in particular the use of texts, parts of texts, images or other content, requires the prior consent of the Bundesverband Digitale Wirtschaft (BVDW) e.V. or the rights holders (third parties).