VATM e. V. • Frankenwerft 35 • 50667 Köln

European Data Protection Board
Rue Wiertz 60,
1047 Brussels, Belgium

Contact person	Email	Telephone	Date
Lilyana Borisova	lb@vatm.de	+32 2 446 00 77	30.10.2026

VATM Position Paper on EDPB Draft Guidelines 02/2026 on anonymisation

Dear Sir/Madam,

VATM (Verband der Anbieter im Digital- und Telekommunikationsmarkt e.V.) welcomes the Guidelines 02/2026 of the European Data Protection Board adapting the framework for data anonymisation to the legal and technical developments of recent years. Since the Article 29 Working Party issued its opinion in 2014, there have been significant developments, particularly in the case law of the Court of Justice of the European Union (CJEU) as well as in the wider context of artificial intelligence, European data spaces and new methods of re-identification.

For telecommunications companies, the question of when data can be deemed anonymous is of considerable practical importance. This concerns, for example, the use of anonymised traffic, location, and network usage data for statistical analyses or mobility analytics applications. It is therefore particularly positive that the EDPB adheres to a relative and context-dependent understanding of personal data. At the same time, important questions regarding the scope of the Draft Guidelines remain unresolved. From the VATM's perspective, the Draft Guidelines need to expand clarifications in areas where broad possibilities for identification and re-identification could, in practice, undermine the relative approach.

I. Consistently uphold the relative approach to identifiability

The Draft Guidelines rightly recognise that the same data may need to be assessed differently depending on the entity processing it. The key question is whether the entity in question can identify an individual using the means available to it or the means that it could reasonably be

expected to use. VATM expressly welcomes this relative approach. VATM expressly welcomes this relative approach.

In practice, it is essential that data should not be treated as personal data as a precaution simply because identification is theoretically conceivable. This is particularly important for traffic and location data, where the relevant consideration is what additional information an entity holds or could obtain without disproportionate effort. Future technological developments should only be taken into account to the extent that they are reasonably foreseeable.

Further clarification is needed regarding the distinction between identifiability and mere distinguishability. The fact that a data set can be distinguished from others based on a unique combination of characteristics does not necessarily mean that the natural person behind that data set can also be identified.

The mere ability to isolate a data set, or the uniqueness of a combination of characteristics, should therefore not in itself be sufficient to establish that the natural person behind it can be identified. The decisive question must remain whether a specific person can be identified using means whose use is reasonably likely to be used under the given circumstances.

II. Assess technical criteria in the context of the actual processing environment

The criteria of ‘No Record Isolation’, ‘No Linkage’ and ‘No Inference’ can provide useful guidance when assessing whether data are anonymous. However, it is essential that they are applied in the context of a specific processing activity. Failure to meet any one criterion should not automatically result in data being classified as personal data.

The decisive factor must instead be whether re-identification is realistically possible for the entity concerned in the specific circumstances. This assessment should consider existing additional information, actual access possibilities, as well as the effort involved, costs, and foreseeable technical developments. Purely theoretical possibilities for linking or re-identification should not be sufficient for this purpose.

III. Give due weight to legal and contractual restrictions

The EDPB recognises statutory prohibitions as a relevant factor when assessing the risk of re-identification. As a general principle, compliance with applicable law may be assumed. However, it should be possible to rebut this assumption if there are concrete indications that unlawful means may nevertheless be used.

#Wettbewerberbindet

Association of Providers in the Digital and Telecommunications Market (VATM) e.V.
Frankenwerft 35 • 50667 Cologne • Tel.: 0221 3767725 • E-Mail: vatm@vatm.de

Executive Committee: Valentina Daiber (President), Wolfram Rinner (Vice-President), Timm Degenhardt, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Reinhard Sauer, Rickmann v. Platen, Peter Zils • Managing Director: Dr. Frederic Ufer

In VATM's view, the Draft Guidelines should clarify more precisely the circumstances when such a presumption may be rebutted. The mere theoretical possibility of a legal breach should not be sufficient. As a general rule, companies must be able to rely on statutory prohibitions being observed unless there are no concrete circumstances indicating otherwise.

Effective and enforceable contractual restrictions should also be given appropriate weight in the assessment. The decisive factor here should not be their formal classification alone, but their actual effect on the risk of re-identification. Where contractual provisions effectively restrict access to additional information or prevent re-identification, this should be taken into account in the overall assessment.

IV. Assess source data and complex processing chains on a case-by-case basis

The EDPB clarifies that successful anonymisation does not require the deletion of the original personal data. VATM considers this an important point. The mere fact that an entity holds possession of source or raw data should not mean that a dataset derived from those data must be considered as personal data by that entity and by all other entities involved, provided that the data cannot be combined for technical and/or organisational reasons.

The assessment must instead remain entity specific. A dataset may constitute personal data for the original data holder, while being anonymous to an independent recipient if that recipient cannot identify the individuals concerned using means reasonably likely to be used in the specific circumstances.

This distinction is particularly important for anonymised traffic, location and network usage data.

Further clarification is required in the case of multi-stage processing chains and data processing carried out on behalf of third parties, i.e. by processors on behalf of controllers. The EDPB should explain more clearly from whose perspective identifiability is to be assessed in each case, and which knowledge and access capabilities should be attributed to the parties involved. This is particularly important where roles or access rights change over the course of the processing chain.

V. Clarify the rules on anonymisation for subsequent use for new purposes

The EDPB clarifies that anonymisation itself constitutes the processing of personal data and therefore requires a legal basis. Where anonymisation takes place as part of the same processing activity and for the same purposes, the existing legal basis may generally continue to apply.

However, it remains unclear which criteria should apply when data are anonymised precisely in order to be used for a different purpose, such as statistical analyses or data-driven applications.

VATM therefore insists that the Draft Guidelines explicitly address those concerns and provide greater clarity on the legal basis for the anonymisation process in such cases. A clear distinction should be drawn between the anonymisation itself and the subsequent use of data that are genuinely anonymous from the perspective of the entity processing them and thus no longer falls within the scope of the GDPR.

VI. Provide greater clarity on terminology used in international contractual relations

In international contractual relations, terms such as ‘anonymised’, ‘pseudonymised’ and ‘aggregated’ may be understood differently by the parties involved. This can create significant uncertainty, particularly in contractual relationships between European and non-European parties.

The EDPB cannot, and should not be expected to, harmonise the different legal systems involved. However, it can help ensure that the terminology used in European data protection law is defined as clearly and practically as possible. The glossary approach included in the Draft Guidelines provides a good basis for this.

VATM therefore calls for further clarifying, in particular, the distinction between anonymous, pseudonymised and aggregated data. Clear and operational criteria would facilitate cross-border contractual arrangements and help prevent misunderstandings regarding the data protection status of a data set.

VII. Conclusion

In VATM’s view, the Draft Guidelines address a number of important issues in the right way. The relative approach to identifiability and the possibility of assessing data in their specific

Association of Providers in the Digital and Telecommunications Market (VATM) e.V.
Frankenwerft 35 • 50667 Cologne • Tel.: 0221 3767725 • E-Mail: vatm@vatm.de

Executive Committee: Valentina Daiber (President), Wolfram Rinner (Vice-President), Timm Degenhardt, Michael Jungwirth, Michael Martin, Carina Panek, Karsten Rudloff, Reinhard Sauer, Rickmann v. Platen, Peter Zils • Managing Director: Dr. Frederic Ufer

context are particularly welcome. The key challenge now is to ensure that these principles are not undermined in practice by overly broad assumptions regarding the potential for re-identification.

For telecommunications companies, it must remain practically possible to achieve legally reliable anonymisiation, including in the context of complex data sets and processing chains. The assessment should therefore focus on actual access possibilities and re-identification risks that are reasonably likely to arise. The mere technical ability to isolate a data set, purely theoretical possibilities to linking data, or technological developments that are only abstractly conceivable must not automatically result in data being classified as personal data.

At the same time, clearer criteria are needed for taking statutory and contractual restrictions into account, for assessing multi-stage processing chains and processor arrangements, and for anonymisation undertaken with a view to subsequent use for different purposes. Key terminology should also be defined as clear as possible, particularly to facilitate cross-border contractual relationships. The context-dependent approach must remain a fully-fledged method of assessment. The simplified approach must not become the de facto minimum standard.

VATM therefore calls for a framework that consistently maintains the relative and context-dependent approach. Such a framework should provide companies with reliable criteria for assessing whether data are anonymous, while ensuring effective protection for individuals concerned.

Yours faithfully,

Lilyana Borisova
Head of VATM-Brussels Office

#Wettbewerberbindet

VATM represents Germany's leading telecommunications companies, uniting over 200 network operators, service providers and suppliers – many of them active at the regional and European level. The association also speaks for key investors driving the rollout of fibre networks across Germany. VATM members serve almost 70 percent of all fixed-line customers and nearly all mobile customers outside Deutsche Telekom. Since the liberalization of the market in 1998, competitors in both fixed and mobile segments have invested around 136 billion Euro. Today, they are the principal investors in the fibre-to-the-home (FttH) deployment in Germany, providing 70 percent of all gigabit-capable connections currently in use.

Association of Providers in the Digital and Telecommunications Market (VATM) e.V.
Frankenwerft 35 • 50667 Cologne • Tel.: 0221 3767725 • E-Mail: vatm@vatm.de

Executive Committee: Valentina Daiber (President), Wolfram Rinner (Vice-President), Timm Degenhardt, Michael Jungwirth,
Michael Martin, Carina Panek, Karsten Rudloff, Reinhard Sauer, Rickmann v. Platen, Peter Zils • Managing Director: Dr. Frederic Ufer