Position Paper

Bundesverband Digitale Wirtschaft e.V. · Schumannstraße 2 · 10117 Berlin

10. March 2025

Philipp Hagen, Director Legal Affairs & Data Privacy, hagen@bvdw.org

Position Paper on the Guidelines 01/2025 on Pseudonymization

About the BVDW

We welcome the opportunity to comment on the Guidelines 01/2025 on Pseudonymization of the European Data Protection Board (EDPB) as part of the public consultation.

The Bundesverband Digitale Wirtschaft (BVDW) e.V. represents the interests of companies based in Germany that operate digital business models or whose value creation is based on the use of digital technologies. The basis for this is the intelligent combination of data and creativity with a decisive focus on ethical principles. With over 600 member companies – from large and small digital companies to agencies and publishers – the association represents the interests of the digital economy in politics and society. Its network of experts provides orientation on a key field of the future with figures, data and facts.

As an association that represents the digital economy, we consider the practical interpretation of pseudonymization to be essential in order to reconcile data protection, innovation and economic development. Pseudonymization is a key instrument for reducing risk when processing personal data. The GDPR explicitly recognizes this and provides for pseudonymization as a measure that supports data protection through technology design (Art. 25 GDPR) and data security (Art. 32 GDPR). It can also strengthen the lawfulness of processing in the context of legitimate interest (Art. 6(1)(f) GDPR), facilitate purpose compatibility (Art. 6(4) GDPR) and serve as an additional protective measure for data transfers to third countries (Art. 44 et seq. GDPR).

We therefore expressly welcome the fact that the guidelines recognize pseudonymization as a privacy-enhancing technology (PET) and highlight its potential to reconcile data protection and data use. The EDPB should extend this recognition by providing specific guidelines for the application of PETs and the role that AI can play in achieving robust data protection.

However, BVDW must express its significant concerns that the Guidelines, through their overly stringent and often impractical requirements, threaten to undermine the intended benefits of pseudonymization and may inadvertently hinder its wider adoption.

We note that the standards and definitions chosen in the Guidelines go well beyond the requirements of the GDPR in several respects, making the practical implementation and acceptance of pseudonymization considerably more difficult.

Furthermore, the requirements formulated in the Guidelines are not in line with the previous case law of the European Court of Justice (ECJ), in particular the decision in the Breyer case (C-582/14) and the ongoing appeal proceedings in the SRB/EDPS case (T-557/20). These

decisions – and the recent opinion of the Advocate General in EDPS v SRB – confirm that pseudonymization must be considered in relative terms – i.e. from the perspective of the respective controller and not based on a global view that also includes (theoretical or illegitimate) re-identification possibilities by third parties.

In view of the considerable scope of the pending judgment of the ECJ, we urge the EDPB to suspend the finalization of these guidelines until the court has delivered its judgment. This would ensure that the guidelines are in line with established case law and prevent potential legal uncertainties for companies.

An overly restrictive approach to pseudonymization will increase the burden on businesses, especially small and medium-sized companies (SMEs). Data subjects will not benefit from such an approach. This will also have a negative impact on the digital economy within the European Union, especially in areas such as artificial intelligence, data-driven business models and research.

In view of these points, we suggest revising the guidelines and taking greater account of the practical applicability and innovation-friendliness of pseudonymization. European case law must be taken into account. The regulatory approach should maintain a balance between data protection and economic and technical feasibility in order to create incentives for companies to continue using pseudonymization as a key data protection tool.

1. Pseudonymization ≠ Anonymization

The EDPB guidelines are based on a de facto absolute criterion for effective pseudonymization, thereby blurring the crucial distinction between pseudonymization and anonymization. This blurring is not only incompatible with the GDPR and the relevant case law of the ECJ and the General Court, but also undermines the practical benefits of pseudonymization as a risk mitigation tool.

The GDPR defines pseudonymization in Art. 4 No. 5 as a processing technique whereby personal data is altered in such a way that it can no longer be attributed to a specific data subject without additional information. This additional information must be kept separately and protected by appropriate technical and organizational measures (TOMs).

The GDPR makes a clear distinction between pseudonymized data, which is still personal data, and anonymized data, which is no longer subject to the scope of the GDPR.

- Pseudonymization: The identification of a data subject by a controller is only possible if the information required for the assignment is available. This information must be protected by technical and organizational measures (TOMs) and stored separately.
- Anonymization: Identification is no longer possible for a controller, even taking into account all available means. Anonymized data is therefore no longer personal data within the meaning of the GDPR and is not subject to its requirements.

The guidelines ignore this fundamental distinction. Paragraph 47 requires a level of irreversibility for pseudonymization that is indistinguishable from anonymization in practice. This directly contradicts Article 32 of the GDPR, which prescribes a risk-based approach to security that takes into account the "state of the art" and implementation

costs at the time of pseudonymization. The “state of the art” is dynamic by nature; absolute criteria are not. Imposing such rigid standards creates a significant risk: organizations that diligently adhere to current best practices could be retroactively judged non-compliant as technology evolves. This violates fundamental principles of legal certainty and proportionality

The guidelines suggest that pseudonymized data can only be considered “effectively pseudonymized” if no actor can re-identify it with reasonable effort. This seems to require consideration of a wide and sometimes theoretical range of re-identification possibilities, including those stemming from sophisticated cyber-attacks or the combination of pseudonymized data with publicly available information. Essentially, the EDPB is suggesting that pseudonymized data should only be considered pseudonymized when it is practically anonymized for all actors.

This contradicts the case law of the ECJ, which clarifies that pseudonymization must be considered from the perspective of the respective controller – taking into account separately the reasonable likelihood of re-identification for the respective controller in its specific operational context – and not from a hypothetical perspective that takes into account every conceivable possibility of re-identification.

- In the Breyer case (C-582/14), the ECJ found that an IP address is not automatically personal data for every actor. The decisive factor is whether the identifying information is actually available to the specific actor and whether its use is legally permissible.
- The General Court case SRB/EDPS (T-557/20) confirms this view: The possibility of identification must be assessed from the perspective of the controller in question – not with the involvement of hypothetical third parties.
- In his opinion in the SRB/EDPS case, Advocate General Spielmann clarified that an organization that is not in a position – does not have the appropriate means – to identify individuals cannot be obliged to implement data subjects' rights simply because hypothetical third parties could make an identification.

The guidelines ignore this case law and take an absolute view of the possibility of re-identification. As a result, data is de facto classified as personal even if the controller has no reasonable means of identifying a person.

The Guideline must focus on answering the question of when the threshold of disproportionate effort in identifying a natural person is reached for a controller. Controllers who have not carried out a pseudonymization themselves will have a higher re-identification effort, regardless of whether they are included in the “pseudonymization domain” invented by the EDPB.

The concept of a “pseudonymization domain”, although potentially useful, should not be interpreted as requiring absolute separation or the impossibility of re-identification within the same controller. Appropriate organizational and technical safeguards, including access controls and policies that prohibit unauthorized data aggregation, should be sufficient to demonstrate effective pseudonymization, even if there is a theoretical possibility of re-identification.

If the controller receiving pseudonymized data does not have adequate means to re-identify the data, the data should be treated as anonymous from the perspective of the controller receiving the data.

When assessing whether a controller has exceeded the threshold of proportionate effort for re-identification, the focus should be on lawful means. The theoretical possibility of re-

identification by malicious actors using unlawful means (which are constantly evolving, unpredictable techniques) should be excluded. The requirement in paragraph 42 to assess such threats is speculative, impractical and inconsistent with the focus on demonstrable, risk-based security measures enshrined in Article 32 GDPR. The effectiveness of state-of-the-art pseudonymization should be assessed based on appropriate safeguards, not on the potential for unlawful attacks.

2. Pseudonymization as a measure to protect personal data

The GDPR recognizes pseudonymization as a measure to protect personal data and actively promotes its use:

- Art. 25 (Privacy by Design & Default): Pseudonymization is mentioned as a recommended technique to improve data protection through technical measures.
- Art. 32 (Data security): Pseudonymization is a recognized measure to minimize data protection risks.
- Art. 6(4) (purpose compatibility check): The use of pseudonymization may facilitate further processing for another purpose if an adequate protection scheme is in place.
- Art. 44 et seq. (International data transfers): Pseudonymization is recognized as an additional protection measure to make data transfers to third countries more secure.

The Guidelines undermine this approach by de facto raising the requirements for pseudonymization to the level of anonymization. This could discourage companies from investing in pseudonymization, as the regulatory benefits would no longer be apparent.

Such a regulatory environment acts as a deterrent to companies wishing to develop innovative data-driven business models. Uncertainty about whether their pseudonymization measures meet the stringent requirements of the guidelines could lead them to refrain from certain data processing or to invest considerable resources in the development of complex compliance structures. This can be a significant burden, especially for SMEs, and can affect their competitiveness.

It is important that the directives take a balanced approach that ensures the protection of personal data without stifling business innovation. The requirements for pseudonymization should be clearly defined and practicable so that companies are encouraged to implement privacy-friendly technologies that promote both the protection of data subjects and the development of new business models.

3. Misinterpretation of the information obligations pursuant to Art. 11 GDPR

The EDPB Guidelines fail to recognize the correct application of Art. 11 GDPR, which provides for an exemption from the information obligations for controllers in certain cases. The Guidelines falsely suggest that Article 11 increases the obligations for controllers who lack the means to identify data subjects – and thus achieve the exact opposite of its intended purpose. The purpose of Article 11 is to reduce burdens where identifiability is not reasonably possible, not to create new ones. In particular, the Guidelines misunderstand:

1. When a controller must inform data subjects about the application of Art. 11(1) GDPR

2. Which information must be passed on to data subjects in accordance with Art. 11(2) GDPR

These misinterpretations lead to a disproportionate burden for companies.

The Guidelines imply in paragraph 79 that a controller is always obliged to inform data subjects about the application of Art. 11 GDPR as soon as it stores pseudonymized data. However, this contradicts the wording of Art. 11(1) GDPR, which reads as follows

"If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation."

This results in two central points:

- Art. 11(1) GDPR only applies in the event that the controller has already processed personal data but identification of the data subject is no longer required.
- If the controller had no means of identification from the outset and therefore no personal data, Art. 11(1) GDPR is not applicable.

However, the Guidelines seem to assume that Art. 11(1) already applies if the controller of the data possesses the data that was previously pseudonymized by another party – regardless of whether the controller of this data had an identification option or not.

The Guidelines also require data controllers to inform data subjects about how they can obtain their pseudonyms and how they can use them for identification purposes. Specifically, the Guidelines state:

"Therefore, in order to give full effect to the rights of the data subjects, the controller should indicate in the information provided to data subjects according to Art. 11(2) GDPR how they can obtain the pseudonyms relating to them, and how they can be used to demonstrate their identity. In this case, the controller may need to provide the identity and the contact details of the source of the pseudonymised data or of the pseudonymising controller." (vgl. Guidelines, Rn. 79)

The wording of Art. 11(2) GDPR is much narrower:

" Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible."

As a result:

- The only obligation under Art. 11(2) GDPR is to inform data subjects that identification is not possible – nothing more.
- There is no obligation to provide data subjects with information about the source of the pseudonymized data.

However, the guidelines require data controllers to provide additional information that goes beyond the legal requirements. This could lead to companies having to disclose confidential information.

This misinterpretation of Article 11 creates significant practical difficulties for both data subjects and controllers. The guidelines appear to require controllers to enable re-identification even if they cannot independently identify individuals from pseudonymized data, provided a data subject provides the relevant pseudonyms. This places an undue

burden on data controllers and overlooks the potential obstacles that data subjects may face in obtaining these pseudonyms, particularly if the entity that originally pseudonymized the data is not subject to the GDPR or is unwilling to cooperate.

The guidelines should clarify that Art. 11(2) GDPR only requires that controllers – where possible – inform data subjects that identification is not possible. There is no obligation to provide further information.

4. Lack of consideration of established standards and industry-specific use cases

The guidelines do not take into account any established international standards, although there are already comprehensive normative frameworks for the practical implementation of pseudonymization.

Relevant industry standards:

- ISO/IEC 20889:2018 – provides a standardized taxonomy and technical methods for pseudonymization
- ISO/IEC 27559:2022 – provides clear guidelines for implementing pseudonymization in various scenarios
- NIST Frameworks (e.g. NIST 800-122) – define best practices for protecting sensitive information through pseudonymization

These standards are already widely implemented by companies and offer tried and tested solutions for data protection requirements.

Why the lack of consideration is a problem:

- Companies that already adhere to these internationally recognized standards have no clear guidance on whether their implementations meet the requirements of the Guidelines.
- The development of new, deviating requirements by the EDPB could lead to companies having to incur considerable costs for the adaptation of existing data protection measures – even though established standards already exist.

The guidelines should be based on existing international standards in order to enable a practical and realistic implementation of pseudonymization. This could be done by making direct reference to ISO/IEC 20889:2018, ISO/IEC 27559:2022 or NIST frameworks.

In addition, the guidelines should contain a broader selection of application examples from different economic sectors. However, the Annex's valuable focus on the healthcare sector and special data categories limits its practical relevance for many organizations, especially SMEs. Expanding the examples to include a variety of processing scenarios and industries would provide more concrete guidance and enable context-specific implementation that goes beyond a purely theoretical approach to pseudonymization.

Finally, the EDPB should publish its guidelines on pseudonymization in conjunction with its planned guidelines on anonymization. Given the significant overlaps and interactions between these two concepts, a unified approach would promote greater consistency, avoid potential contradictions and provide much-needed clarity to data controllers grappling with the complexities of data identifiability. This would be in line with best practice from other data protection authorities such as the UK ICO and the Irish DPC.