bitkom

Position Paper

2025 March

Bitkom views on EDPB Guidelines 01/2025 on Pseudonymisation

Summary

The European Data Protection Board (EDPB) has published new guidelines on pseudonymisation, specifying the application and legal framework under the General Data Protection Regulation (GDPR). Bitkom welcomes the EDPB's clarifications but sees a need for further adjustments regarding the practical implementation, legal certainty and technological openness.

Before the regulatory guidelines were introduced, industry-led initiatives had already developed practical frameworks for implementing GDPR-compliant pseudonymisation. At the 2019 German Digital Summit, the GDPR Code of Conduct for Pseudonymisation - developed by Bitkom, GDD, and SRIW e.V.—was presented as a risk-based, operational standard to help organisations meet GDPR requirements. Although the EDPB Guidelines and the Code of Conduct share basic principles, they differ in interpretation and application. While the Guidelines adopt several key concepts from the Code of Conduct, they tend to be more theoretical, unlike the Code's focus on practical implementation.

This consultation response aims to harmonise pseudonymisation practices across both regulatory and industry frameworks by critically comparing the EDPB Guidelines with the Code of Conduct and highlighting opportunities for more practical improvements.

Overall, the Guidelines should adopt a more positive and enabling tone regarding pseudonymisation. While acknowledging risks, they should strongly emphasize the benefits of pseudonymisation for businesses across sectors. Highlighting these benefits will encourage wider adoption and investment in pseudonymisation techniques, ultimately enhancing both data protection and innovation in the EU.

This paper highlights critical issues where further clarifications and revisions to the guidelines are needed. In particular, the following concerns should be addressed:

- The guidelines preempt the resolution of the EDPS v SRB case by the CJEU, whose outcome is pivotal to whether pseudonymised data should be considered personal data at all times.
- The guidelines conflate the two concepts of pseudonymisation and anonymisation, leading to an overly restrictive interpretation of pseudonymisation.
- The guidelines extend the scope of pseudonymisation too far and require unauthorised third parties to be taken into account.
- The guidelines contradict established legal interpretations regarding identifiability.
- The guidelines impose notification requirements that go beyond GDPR and should be reconsidered.
- The overly restrictive and absolute approach discourage investment in pseudonymisation and Privacy-Enhancing-Technologies (PETs).

1. Evaluation of the Guidelines

   a) Bitkom notes with concern that the Guidelines were adopted before the resolution of appeal in the EDPS v SRB case, in which the Court will rule on the circumstances in which pseudonymised data remains personal data. During the course of the current consultation, the Court's Advocate General published their Opinion, which directly contradicts the Guidelines' position that pseudonymised data remains personal data in all cases for third-party recipients, regardless of their ability to re-identify individuals.

   Indeed, the Advocate General clarifies that pseudonymised data may not be considered personal data for a third-party recipient if that recipient cannot reasonably re-identify the data subjects. This determination requires a case-by-case assessment of the recipient's means and the security measures in place.

   If the Court of Justice of the European Union (CJEU) follows the AG Opinion, the EDPB will need to significantly revise the Guidelines.

   Bitkom therefore strongly urges the EDPB to delay any finalisation of the Guidelines until after the CJEU judgment and publicly clarify that it will do so. This is crucial for providing legal certainty and a clear roadmap for organizations dealing with pseudonymised data.

   b) Effects on legal Bases and Compatibility Assessment (Art. 6 (1) lit. f & Art. 6 (4) GDPR)

   The Guidelines recognise the risk-reducing effect of pseudonymisation and clarify that it can be taken into account in the balancing of interests under Art. 6(1)(f) GDPR (p. 42). It can also contribute to the assessment of the compatibility of further processing under Art. 6(4) GDPR (p. 43).

   Bitkom requests that the Guidelines provide clear criteria for the application of the compatibility check under Art. 6(4) GDPR. Companies need practical examples to ensure the legally compliant use of pseudonymisation in the legitimate

interest assessment. For example, whether pseudonymisation using state-of-the-art technology is sufficient if the pseudonymisation secret is kept securely by a trustworthy third party. Without specific guidance, it remains unclear when and to what extent pseudonymisation can be effectively used a to legitimise processing.

c) Notification Obligations

The Guidelines state that data controllers should indicate how data subjects can obtain their pseudonyms and use them to exercise their rights (p. 19). However, they do not establish a general notification obligation.

Furthermore, the Guidelines' position on personal data breaches involving pseudonymised data (p. 16) creates a contradiction. They suggest that breach notifications (Art. 33 and 34 GDPR) depend on the effectiveness of pseudonymisation, which is inconsistent with the EDPB Guidelines 09/2022 on breach notification. Those guidelines state that breaches of encrypted data, where the decryption key is secure, likely do not require notification. The same logic should apply to data pseudonymised with state-of-the-art techniques, provided the additional re-identification information remains secure.

Bitkom requests that the Guidelines clarify that companies are not obliged to provide additional evidence of identifiability if they have technically excluded traceability. Moreover, any additional notification requirements beyond Art. 11, 33 and 34 GDPR should be reconsidered, as they represent an unnecessary burden without any added value for data protection.

d) Risk Analysis in the Context of Pseudonymisation

The Guidelines require data controllers to define the risks that pseudonymisation is intended to mitigate (p. 4). While this is consistent with existing data protection impact assessments (DPIAs) under Art. 35 GDPR, it creates uncertainty as to whether an additional, specific risk assessment is required for pseudonymisation.

Specifically, the requirement to consider means "reasonably likely to be used by cyber-crime actors" in risk assessments is impractical and overly burdensome. Cyber-crime techniques are constantly evolving and unpredictable.

Bitkom advocates for recognising DPIAs as sufficient and avoiding redundant bureaucratic obligations. The guidelines should be formulated in a technology-neutral way to give companies flexibility in assessing risks, while ensuring compliance with the principles of the GDPR.

e) Multiple Pseudonymisation – A Risk-Based Approach

The guidelines recommend replacing pseudonyms when sharing data to mitigate risks (p. 28). However, this should not be interpreted as a blanket requirement, but rather as a measure to be applied on the basis of a risk analysis.

Bitkom calls for clear guidance on when multiple pseudonymisation is actually necessary and what specific risks it mitigates. The importance of alternative

measures, such as data minimisation or organisational safeguards, should be more explicitly recognised. Companies need practical and effective solutions, not unnecessarily complex procedures.

Technical Guidance on Pseudonymisation

The Guidelines do not provide detailed technical guidance on how to implement secure and efficient pseudonymisation (pp. 21-29), which poses challenges, especially for SMEs.

Specifically, the lack of concrete guidance on "reasonable means" for re-identification creates uncertainty. The EDPB should provide examples of relevant techniques, resources, costs, and legal processes to consider, and clarify that this assessment happens before pseudonymisation.

The Guidelines also set absolute criteria for the effectiveness test of pseudonymisation, which conflicts with the general "reasonable likelihood" approach in the rest of the guidance. This risks retroactive judgment of organisations against evolved technological standards. The EDPB should adopt a risk-based approach, emphasizing state-of-the-art security at the time of pseudonymisation, aligning with Article 32 GDPR.

Guidance should explicitly reference Privacy Enhancing Technologies (PETs), as these offer advanced methods for robust pseudonymisation and should be encouraged. Finally, the scope of the case studies in the Annex, primarily focusing on health/medical data, should be expanded to improve their usefulness for organisations in all sectors.

Bitkom urges the EDPB to refer to existing standards and best practices for pseudonymisation techniques, as many companies rely on practical guidelines for efficient implementation. Without specific recommendations, standardised and legally secure implementation will remain difficult.

f) Distinction Between Pseudonymisation and Anonymisation

Bitkom expresses its regrets that the pseudonymisation Guidelines have been published separately from the EDPB's planned guidelines on anonymisation, as both concepts address the identifiability of individuals, and their assessment criteria significantly overlap. This approach risks inconsistencies and practical difficulties for organisations and departs from international best practices from other data protection authorities who have addressed both concepts in parallel (UK ICO; Irish DPC).

Following the Case T-557/20, the Advocate General stated in his Opinion in Case C-413/23 P, that it cannot be ruled out that pseudonymous data may, under certain conditions, fall outside the scope of the concept of ‘personal data’. One of the key factors is whether the pseudonymization is robustly secured (see N. 51 - 59) of the Opinion). Depending on the CJEU's ruling in this case, it would be helpful to address these aspects in the guideline.

Furthermore, the Guidelines sometimes blur the distinction between pseudonymisation and anonymisation. In particular, the meaning of "identify" in

the pseudonymisation context is unclear. While anonymisation analysis uses ”singling out”, ”linkability” and ”inference”, these don’t directly translate, as pseudonymous data may contain unique identifiers allowing for ”singling out”. The EDPB must clarify these points and differentiate the standards and expectations for anonymisation and pseudonymisation, acknowledging that they have distinct purposes and levels of risk mitigation.

Bitkom calls for a clearer boundary between these two concepts. An overly restrictive definition of anonymisation could hinder the use of health data and AI applications. Companies need a realistic and legally secure framework to promote data-driven innovation in the EU.

2. Conclusion

Bitkom welcomes the EDPB’s initiative to provide further clarification on pseudonymisation as a data protection measure. The Guidelines contain valuable insights that can support companies in their implementation. However, significant practical uncertainties remain and the upcoming judgment in EDPS v SRB risks invalidating several core assumptions underpinning the Guidelines..

In order to promote a legally sound and innovation-friendly approach, and in addition to any changes required to align with the CJEU judgement once adopted, Bitkom recommends the following improvements to the Guidelines:

- A stronger and more positive emphasis throughout the Guidelines on the innovation and societal benefits enabled by pseudonymisation.
- Clearer criteria for the application of Art. 6(1)(f) and Art. 6(4) GDPR regarding pseudonymisation.
- Removal of excessive notification obligations beyond Art. 11, 33 and 34 GDPR.
- Avoidance of a mandatory, stand-alone ”pseudonymisation risk assessment”, ensuring alignment with existing DPIA requirements and Art. 32 GDPR.
- A more flexible approach to multiple pseudonymisation, based on an actual risk assessment rather than a default expectation.
- Inclusion of references to existing technical standards and best practices to facilitate practical implementation.
- Inclusion of references to existing technical standards and best practices to facilitate practical implementation, including specific guidance on Privacy Enhancing Technologies (PETs).
- A clearer distinction between pseudonymisation and anonymisation to ensure legal certainty and support data-driven innovation.

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 500 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 Stroot | Policy Officer Data Privacy

P +49 30 27576-228 | i.stroot@bitkom.org

Responsible Bitkom committee

AK Datenschutz