MedTech Europe's Contribution to the EDPB's Public Consultation on Guidelines 01/2025 on Pseudonymisation

Introduction

MedTech Europe welcomes the adoption of the European Data Protection Board's (EDPB) draft Guidelines 01/2025 on Pseudonymisation (hereinafter the '**Guidelines**'). These Guidelines will assist data controllers and processors in selecting appropriate methods to transform original data with a view to reducing privacy risks to an acceptable level, considering the sensitivity of the data, the context, and the purposes of the processing.

As the European trade association representing the medical technology industry, MedTech Europe recognises the crucial role that pseudonymisation plays in enabling the responsible and secure use of health data. In the healthcare and medical technology sectors, pseudonymisation is a key tool for protecting individuals' privacy while facilitating vital research, innovation, and regulatory compliance.

We appreciate the EDPB's efforts to provide guidance on this critical topic and welcome the opportunity to contribute to the public consultation by sharing our industry's perspectives and practical considerations. Below, we outline key concerns identified in the Guidelines, followed by our recommendations to ensure a balanced approach that supports both data protection and technological progress.

Key Considerations and Challenges

Overly strict interpretation of pseudonymised data as personal data

The Guidelines assume that pseudonymised data remains personal data even when the dataset and the additional identifying information are held by separate entities. This interpretation conflicts with the GDPR's risk-based approach and established case law, such as the CJEU's[1] rulings in **Breyer (C-582/14)**[2] and **SRB v EDPS (T-557/20)** (currently under appeal to the CJEU).[3] The assumption of perpetual identifiability disregards scenarios where no reasonable means exist for a given party to re-identify data subjects. Such an approach risks undermining the utility of pseudonymisation as a privacy-enhancing technique.

Legal uncertainty regarding the distinction between pseudonymisation and anonymisation

The Guidelines establish a particularly high threshold for anonymisation, largely due to the strict conditions placed on pseudonymisation. For instance, Paragraph 21 suggests that additional information, such as social media posts, must always be considered when assessing the effectiveness of pseudonymisation. However,

[1] Court of Justice of the European Union.

[2] The CJEU ruled that dynamic IP addresses qualify as personal data "in relation to" an online media services provider (emphasis added) only if the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person. The CJEU held that the question whether certain data must be answered from the perspective of the respective actor ("in relation to that provider", "which enable it") and not in the absolute. Also, the logical inverse of this ruling is that, in the absence of such legal means, the dataset should be considered anonymised. The current guidelines, however, fail to acknowledge this important nuance and instead assume that any potential for re-identification, even if legally or practically improbable, is sufficient to classify data as personal.

[3] This case further reinforces the principle that the same dataset may be considered pseudonymous in one context and anonymous in another. The SRB classified data as anonymous because Deloitte, the recipient of the data, did not have access to the information necessary for re-identification. The General Court ruled that the EDPS failed to consider whether Deloitte had legal means to access additional identifying information, instead assessing re-identification solely from the SRB's perspective. This ruling reinforces a context-dependent approach to anonymisation, which the guidelines fail to acknowledge. The fact that a dataset may be pseudonymous in the hands of one entity does not necessarily mean it is pseudonymous in the hands of all entities.

the Guidelines do not provide clear criteria for determining when data can be considered anonymised. This creates significant legal uncertainty for organisations handling such data and adds unnecessary operational complexity. Companies may have to reassess data sets continuously, making compliance impractical and inconsistent.

Furthermore, the Guidelines classify certain anonymisation methods (i.e. generalisation in Paragraph 131) as aspects of pseudonymisation, making it more difficult to achieve full anonymisation under the GDPR. This is particularly concerning for business models that rely on anonymised data, such as the development of AI applications. An overly restrictive interpretation of anonymisation could undermine EU-wide and national efforts to facilitate responsible health data use, inadvertently limiting the usability of data within the EU without providing meaningful additional privacy protections.

Increased compliance burdens and documentation obligations

The Guidelines introduce new requirements, such as the need for controllers to define specific objectives for pseudonymisation. This suggests the necessity of conducting a comprehensive *'pseudonymisation risk assessment'* with extensive documentation obligations. The inclusion of quasi-identifiers further complicates compliance efforts, making it more difficult for organisations to apply pseudonymisation effectively while meeting regulatory expectations.

Additionally, the introduction of the concept of a *'pseudonymisation domain'* imposes additional technical requirements, expertise, and costs that go far beyond legal compliance. This may place an undue burden on organisations, particularly smaller entities, that lack the specialised resources to implement the complex technical measures outlined in the Guidelines. A more proportionate approach should be considered to ensure that pseudonymisation remains a feasible and effective privacy-enhancing tool for all stakeholders.

Unclear notification obligations and risk mitigation measures

Under Article 11(1) GDPR, controllers are not obliged to maintain or acquire additional data for re-identification purposes. However, the Guidelines appear to introduce new obligations under Article 11(2) GDPR, requiring controllers to inform data subjects about the additional information that could potentially re-identify them at the time they seek to exercise their data protection rights. This not only adds complexity but could also lead to unintended compliance burdens that extend beyond the GDPR's original intent.

Excessive complexity in pseudonymisation requirements

In paragraph 72, the Guidelines recommend multiple layers of pseudonymisation, such as modifying or replacing pseudonyms when sharing data with third parties. This requirement adds unnecessary complexity without a clear justification for why such an approach is superior to existing data minimisation techniques. The added technical burden may discourage organisations from applying pseudonymisation altogether, reducing its practical use as a safeguard.

The Guidelines also stress that, for *'external processing, i.e. processing under instruction by a processor or transmission to an independent controller, more extensive measures and risk assessment may be necessary to prevent attribution to data subjects.'* However, the Guidelines lack specific details on what these measures should entail. More clarity is needed to ensure legal certainty and help organisations determine appropriate safeguards, particularly regarding the transmission of pseudonymised data to an independent controller.

Data breach obligations

Paragraph 62 of the Guidelines recognises that pseudonymisation can serve as a measure contributing to security by limiting the impact of a personal data breach. It emphasises that pseudonymisation *'may be*

regarded as an appropriate technical and organisational measure that limits the impact of a personal data breach in the sense of Art. 34(3)(a) GDPR.' However, clarification is needed on whether, in cases where pseudonymisation is effective, breaches involving such data would not require notification to supervisory authorities under Article 33(1) GDPR. A case-by-case assessment should be considered.

Third country data transfers

According to Paragraph 64 of the Guidelines, pseudonymisation may also constitute a 'supplementary measure' to ensure compliance with Articles 44 and 46(1) GDPR. However, the Guidelines propose new conditions that appear to go beyond the Chapter V of GDPR. We would suggest that these additional conditions be reconsidered. Additionally, it is unclear who the *'members of a group of persons'*, referred to in the third condition, are. The recommended process of pseudonymisation, which requires an assessment of both the legal and unlawful means available to a public authority of a recipient country as outlined in Paragraph 65, may place an undue burden on the pseudonymising controller or processor.

Our Recommendations

1. Adopt a context-based approach to pseudonymisation and anonymisation

Pseudonymised data should not always be classified as personal data, particularly when the necessary additional information is not accessible to a given controller or third party. The Guidelines should align with case law and the position of other data protection authorities, such as the UK ICO,[4] which recognises that the identifiability of data depends on the specific party holding it.[5]

2. Clarify the criteria for anonymisation

The Guidelines should provide clearer criteria for when pseudonymised data can be considered anonymised, in line with Recital 26 of the GDPR. The assessment should take into account the cost, time, and technical means required for re-identification, rather than relying on a theoretical possibility of re-identification. This approach would provide greater legal certainty and align with established case law.

If certain anonymisation methods are outside the scope of these Guidelines, we would suggest that the EDPB consider removing the references to them and addressing them in the forthcoming Anonymisation Guidelines. For the sake of legal clarity, it would have been beneficial for organisations to receive both Guidelines at the same time, and we would appreciate it if the EDPB could publish the upcoming Anonymisation Guidelines at the earliest opportunity.

3. Reduce unnecessary compliance and documentation burdens

Instead of imposing additional documentation requirements, the Guidelines should focus on practical guidance that helps organisations implement pseudonymisation in a way that enhances privacy while maintaining operational feasibility. Overly rigid documentation obligations could discourage the adoption of pseudonymisation rather than promote its use.

4. Reassess the need for multiple layers of pseudonymisation

The Guidelines should take a more flexible approach to pseudonymisation techniques, recognising that different contexts require different levels of pseudonymisation. Requiring multiple layers of

[4] Information Commissioner's Office.

[5] ICO's anonymisation, pseudonymisation and privacy enhancing technologies guidance of February 2022, Chapter 3, page 5.

pseudonymisation in all cases is not always necessary or practical. Data minimisation principles should be considered alongside pseudonymisation to achieve an appropriate balance between privacy and usability.

5. Ensure alignment with other EU legislation

Pseudonymisation is increasingly relevant in the context of new EU digital legislation, such as the Data Act and the European Health Data Space (EHDS). The Guidelines should explicitly acknowledge the role of pseudonymisation in these frameworks to ensure consistency and facilitate compliance with broader data governance obligations.

Conclusion

MedTech Europe acknowledges the EDPB's efforts in offering guidance on pseudonymisation, a critical technique for protecting personal data while enabling responsible data use. The Guidelines introduce a particularly strict interpretation that risks creating legal uncertainty, unnecessary compliance burdens, and reduced practical usability of pseudonymisation.

We urge the EDPB to provide further clarification and refine the approach to pseudonymisation, ensuring it is both effective and proportionate. This would help foster a regulatory environment that supports both robust data protection and innovation, particularly within the healthcare and medical technology sectors.