

# Memo

**To:** European Data Protection Board

**By:** Zorgverzekeraars Nederland  
**Location:** Zeist

**Date:** 14 March 2025

---

## Response to EDPB Guidelines 01/2025 on Pseudonymisation

The Dutch collective (umbrella organization) of health insurers 'Zorgverzekeraars Nederland', appreciates the opportunity to submit feedback on the draft European Data Protection Board's Guidelines 01/2025 on Pseudonymisation.

The Dutch health insurers, wish to address a critical aspect of the proposed guidelines, which adopt a restrictive approach to pseudonymization and raise significant concerns regarding the practical implications for data processing. In particular, the Dutch health insurers consider that a robust pseudonymization process may, under certain conditions, effectively render data anonymous for third parties.

The draft guidelines emphasize that pseudonymization is primarily a security measure and that data processed in this manner should continue to be treated as personal data, even when received by a third party. Such oversimplified interpretation tends to diverge from established case law and raises uncertainty regarding the actual risk of re-identification. The GDPR itself, in Recital 26, states that data protection rules should not apply to anonymous information. By not adequately addressing situations where pseudonymization results in effective anonymization for third parties, the guidelines risk creating legal uncertainty and discouraging the implementation of further privacy-enhancing techniques.

The CJEU<sup>1</sup> has repeatedly ruled that the identifiability of personal data must be assessed in a contextual and practical manner rather than based on the mere existence of theoretical re-identification possibilities. The Dutch health insurers align with the opinion of Advocate General Spielmann, who emphasizes that if a third party does not have access to the additional information necessary for re-identification, the data should be regarded as effectively anonymous.<sup>2</sup> A strict interpretation that always classifies pseudonymized data as personal, regardless of whether re-identification is reasonably feasible for the recipient, would go beyond what is necessary to protect data subjects and risk discouraging the use of robust pseudonymization in practice.

Further, imposing full GDPR obligations on entities that lack the ability to re-identify data subjects is disproportionate. If a recipient does not possess the reasonable legal, technical, or organizational means to re-link pseudonymized data to individuals, requiring compliance with the full scope of GDPR protections places an unjustified regulatory burden on those entities.

The Dutch health insurers also observe that the approach in the guidelines differs from regulatory practices outside the EU. In the UK, the Information Commissioner's Office recognizes that pseudonymized data may, under specific circumstances, be considered anonymous to a recipient who lacks the ability to re-identify the data subjects. Similarly, the UK courts have ruled that pseudonymized data can, in some cases, fall outside the definition of personal data.<sup>3</sup> This difference in regulatory interpretation

---

<sup>1</sup> *Breyer (C-582/14), Nowak (C-434/16).*

<sup>2</sup> Paragraphs 58-60 of the Opinion of Advocate General Spielmann, Case C-413/23/P, 6 February 2025.

<sup>3</sup> *Common Services Agency v. Scottish Information Commissioner (C-2010).*

could create challenges for organizations operating across jurisdictions, leading to compliance uncertainty and increased regulatory fragmentation.

For Dutch health insurers operating within a public-private healthcare system, pseudonymisation is essential for the secure processing of data in secondary use scenarios, for the improvement of the availability, affordability, and timeliness of quality healthcare. Third parties—including research institutions, policymakers, and public authorities—frequently request data from insurers for scientific research and policy analysis. Where these parties lack any additional identifying information, and the insurer does not share such data, a robust form of pseudonymisation effectively renders the information anonymous for those recipients. This approach enables insurers to support crucial public health initiatives—such as tracking disease prevalence or evaluating treatment cost-effectiveness—while upholding individuals' privacy. A restrictive interpretation of pseudonymization could hinder responsible data sharing and innovation in healthcare by making it unnecessarily complex to use pseudonymized data in a legally sound manner. The Dutch health insurers underscore the importance of a balanced and practical approach to pseudonymization that recognizes its value in enabling privacy-conscious data processing while ensuring compliance with data protection requirements.

The Dutch health insurers encourage the EDPB to consider a more nuanced approach in its final guidelines—one that ensures a contextual and proportionate assessment of re-identifiability, recognizes that robust pseudonymization may, under specific conditions, render data effectively anonymous, and ensures that obligations are only imposed where there is a realistic risk of re-identification. A workable and legally sound framework for pseudonymization will support both effective data protection and responsible data use.

The Dutch health insurers look forward to continued engagement on this issue and remain available to clarify their position.

\*\*\*