Opinion on EDPB Guidelines 02/2026 on Anonymisation

1. Introduction

Mölnlycke Health Care AB ("**Mölnlycke**") welcomes the EDPB's draft Guidelines 02/2026 on Anonymisation (the "**Guidelines**") and supports the objective of providing greater legal certainty regarding the distinction between personal and anonymous data under the GDPR.

Mölnlycke particularly welcomes:

- the recognition that anonymity is assessed from the perspective of relevant entities and is therefore contextual rather than absolute;
- the introduction of a practical framework intended to support organisations in assessing anonymisation outcomes.

As a MedTech company engaged in scientific research and the development of innovative health technologies, Mölnlycke considers effective anonymisation to be a critical mechanism for balancing patient privacy with scientific advancement and innovation.

The comments below are intended to support the objective of the Guidelines by addressing certain areas where additional clarification would enhance legal certainty and practical applicability.

2. Key requests and concerns

2.1 Interpretation of "means reasonably likely to be used"

Mölnlycke welcomes the EDPB's recognition in paragraphs 7-12 that whether information is anonymous is a contextual question that must be assessed from the perspective of the relevant entity. This reflects the relative nature of identifiability and aligns with CJEU case law on the concept of personal data.

However, Mölnlycke is concerned that the subsequent discussion of "means reasonably likely to be used", particularly in paragraphs 29-35, appears to broaden the assessment beyond the standard established by Article 4(1) GDPR and Recital 26 GDPR.

Paragraphs 29-35 indicate that organisations may need to take into account a wide range of factors, including the potential actions of third parties, unlawful actors, cybercriminals, foreign intelligence services, future disclosures of additional data and future technological developments. While some of these factors may be relevant in specific circumstances, the cumulative effect of the examples provided risks shifting the assessment from what is reasonably foreseeable and likely to occur towards what is theoretically possible.

In Mölnlycke's view, this approach introduces uncertainty regarding the practical meaning of anonymisation under the GDPR.

Recital 26 requires consideration of "all the means reasonably likely to be used" to identify an individual. This necessarily entails an assessment of probability and foreseeability. If anonymisation assessments must account for highly speculative future developments, unknown future datasets, unlawful conduct by unrelated third parties, or technological capabilities that cannot reasonably be

anticipated at the time of the assessment, it becomes difficult to identify *any* circumstances in which anonymisation can reliably be achieved.

Request for clarification:

- Clarify that the assessment of "means reasonably likely to be used" should remain grounded in objective, realistic and foreseeable circumstances, consistent with Recital 26 GDPR and relevant CJEU case law.
- Clarify that theoretical possibilities, highly speculative attack scenarios, or remote future developments should not by themselves prevent data from being regarded as anonymous.
- Clarify that organisations may rely on anonymisation assessments based on the state of the art and reasonably foreseeable developments at the time the assessment is performed.
- Provide practical examples illustrating the distinction between reasonably foreseeable and merely theoretical identification scenarios.

2.2 Unlawful conduct is not always "reasonable"

Mölnlycke recognises that realistic and foreseeable security risks should not be ignored when assessing whether data is anonymous. The assessment required by Recital 26 necessarily involves consideration of the practical realities of modern data processing environments, including reasonably foreseeable attempts by actors to gain access to information and the effectiveness of safeguards implemented to prevent such access.

However, the Guidelines appear to go beyond an assessment of realistic and foreseeable risks and instead suggest that controllers should take into account identification scenarios that depend on hypothetical unlawful conduct by third parties, while at the same time significantly reducing the relevance of an actor's motivation or intention to undertake such efforts (paragraph 31).

In Mölnlycke's view, the mere fact that unlawful conduct cannot be ruled out does not necessarily mean that it should be considered reasonably likely. If the possibility of future unlawful access is sufficient in itself, then almost any anonymised dataset could theoretically remain personal data indefinitely, since it can never be demonstrated with certainty that no future actor will unlawfully obtain additional information capable of supporting re-identification.

Request for clarification:

- Confirm that the existence of a theoretical possibility of unlawful access does not by itself prevent data from being regarded as anonymous.
- Recognise that legal, contractual, organisational and technical restrictions remain relevant factors when assessing whether access to supplementary information is reasonably likely in practice.
- Clarify that the assessment should remain focused on realistic identification pathways rather than scenarios that depend on speculative breaches of law, contractual obligations or security measures.

2.2 Limited role afforded to contractual and governance safeguards

Paragraph 34 states that contractual measures should not be treated as prohibitions by law and should only complement technical measures. While Mölnlycke recognises that contractual commitments alone cannot create anonymisation, the Guidelines appear to give insufficient weight to the role of governance frameworks, access controls, contractual restrictions, ethical oversight and accountability mechanisms, as factors that may influence the likelihood of identification.

In practice, life science research environments frequently rely on layered protection models that combine technical controls, organisational measures, contractual limitations, access governance; and regulatory oversight. These mechanisms are widely recognised across European health-data initiatives and data-sharing ecosystems, such as those established under EHDS.

Request for clarification

- Recognise more explicitly the role of governance and accountability frameworks as part of the overall contextual assessment.
- Clarify how contractual, technical and organisational measures should collectively be weighed when assessing realistic re-identification risks.
- Provide examples involving trusted research environments, EHDS-related infrastructures and regulated healthcare collaborations.

2.3 Documentation of anonymisation assessments and burden of proof

Mölnlycke welcomes the Guidelines' recommendation that organisations document their anonymisation assessments. Thorough documentation can play an important role in demonstrating accountability and supporting internal governance.

However, Mölnlycke is concerned that the discussion in paragraphs 40-41 may inadvertently suggest a shift in the burden of demonstrating whether information constitutes personal data. In particular, paragraph 41 states that an anonymisation assessment should be documented in order to demonstrate compliance with the GDPR. While this statement may be appropriate where organisations are processing personal data and are required to demonstrate compliance with applicable GDPR obligations, it is less clear in the context of information that is considered anonymous.

Under Recital 26 GDPR, anonymous information falls outside the scope of the GDPR. The question addressed by an anonymisation assessment is therefore not how an organisation complies with the GDPR when processing the information, but rather whether the information remains subject to the GDPR at all.

Request for clarification

Mölnlycke recommends that the EDPB:

- clarify that documentation supports accountability but does not alter the legal test for determining whether data is anonymous.

2.4 Practical limitations of the simplified approach

Mölnlycke appreciates the EDPB's attempt to provide controllers with a more accessible methodology for assessing anonymisation. However, Mölnlycke questions the practical value of the simplified approach as currently described in the Guidelines.

Under the simplified approach, controllers may find themselves in the position that:

- if no record can be isolated, no linking is possible and no inferences can be drawn, the information may be anonymous;
- however, if a record can be isolated, linked or used to support an inference, the information may still be anonymous following a contextual assessment.

This means that the criteria do not operate as clear legal tests with predictable outcomes. Instead, they function primarily as indicators of potential risk that ultimately require the controller to return to the contextual analysis. The result is that the simplified approach may provide neither a conclusive finding of anonymity nor a conclusive finding of identifiability in a significant number of cases.

Request for clarification

Mölnlycke recommends that the EDPB:

- Clarify the intended legal and practical value of the simplified approach
- Explain how the simplified approach improves legal certainty where failure to satisfy one of the three criteria does not determine whether the data is personal data or anonymous data.
- Confirm that the contextual approach remains the primary mechanism for assessing anonymisation under the GDPR.

2.5 'No Record Isolation' should not be equated with identification

Mölnlycke welcomes the EDPB's attempt to provide operational criteria through the concepts of No Record Isolation, No Linkage and No Inference. However, Mölnlycke has concerns regarding the treatment of the No Record Isolation criterion.

The fact that a record exhibits unique characteristics or can be distinguished from other records does not necessarily mean that a natural person has been identified or is identifiable within the meaning of the GDPR. For example, a healthcare dataset may contain a record that is statistically unique within the dataset. However, unless that uniqueness can realistically be connected to a specific patient or utilised to take decisions or actions relating to that patient, the existence of uniqueness alone should not automatically lead to the conclusion that anonymisation has failed.

Equating record isolation with identification risks setting an overly restrictive threshold that is particularly difficult to satisfy for health, clinical and scientific datasets, where rare conditions, uncommon treatment pathways and unique combinations of characteristics frequently occur.

Request for clarification

Mölnlycke recommends that the EDPB:

- Clarify that record isolation is an indicator of potential risk rather than a standalone demonstration of identifiability.

3. Conclusion

Mölnlycke appreciates the EDPB's efforts to provide updated guidance on anonymisation and welcomes the recognition already established in case law that anonymity must be assessed in a contextual manner. We submit the above comments with the aim of further strengthening the clarity and usability of the Guidelines.

Mölnlycke remains at the EDPB’s disposal for any further engagement or clarification.

Yours faithfully,

Sofia Sjöö

Chief Digital Legal and Public Affairs Officer

Mölnlycke Health Care AB