# AI Chamber's Position on the EDPB Guidelines 02/2026 on Anonymisation - Submission to the Public Consultation

AI Chamber welcomes the development of guidelines that provide businesses with clear and predictable rules on data anonymisation. Effective anonymisation should enable the safe use of data for training, fine-tuning and testing artificial intelligence models. This is particularly important for European small and medium-sized enterprises (SMEs), whose growth opportunities depend on access to useful data and the costs of preparing it.

The Guidelines should provide practical support for business operations. They should enable businesses to determine which conditions they must meet, how to demonstrate the effectiveness of anonymisation and when they may use data as anonymous data. The requirements should ensure the protection of privacy without imposing excessive legal, technical or organisational burdens.

**1. Clear confirmation that anonymous data may be used to train AI models**

Paragraph 1 of the Guidelines confirms that anonymous data falls outside the scope of the GDPR. We call for this principle to be expressly applied to the training, fine-tuning and testing of AI models. Businesses should receive unequivocal confirmation that effectively anonymised data may be used for these purposes without the processing of that data being subject to GDPR requirements. This does not affect obligations relating to the preceding processing of personal data or requirements arising under other legislation.

We also support the principle set out in paragraph 22 that the likelihood of identification need not be zero, but should be insignificant in reality. This principle should be consistently reflected in the requirements for anonymisation. Businesses should not be required to demonstrate that identification is impossible in every hypothetical scenario; the assessment should be confined to scenarios in which identification is realistically likely.

Preserving useful features and relationships within data is important for AI development. The Guidelines should clearly establish when these may be retained while meeting the standard for anonymity. In light of the risks described in paragraphs 77 and 82, a clear distinction should also be drawn between assessing the anonymity of a training dataset and assessing the information that can be obtained from the resulting model. This distinction should help determine the extent of the verification required at each stage.

**2. Making anonymisation accessible to SMEs**

The cost of implementing anonymisation and demonstrating its effectiveness should not constitute an unjustified barrier to developing AI models. Complex or ambiguous requirements may, in practice, favour organisations with substantial budgets, advanced tools and teams of experts. Smaller businesses may consequently refrain from using data or unnecessarily reduce its usefulness for training.

Paragraphs 29-30 provide for consideration of the context in which data is used and the capabilities of entities that may identify individuals. Footnote 25 clarifies that not all of the listed perspectives need to be assessed in every case. We call for this principle to be given greater prominence in the main text of the Guidelines and for the scope of the required analysis to be clearly defined. The analysis should address realistic possibilities of identification under the specific conditions in which the data is used.

Similarly, the role of safeguards and access restrictions, discussed in paragraphs 89-91, should be explained in a way that enables businesses to take them into account without having to commission extensive analyses and expert assessments in each case. These safeguards do not, by themselves, render data anonymous, but their actual effect on the possibilities of identification should be recognised in the assessment.

With regard to the documentation required under paragraph 41, we call for explicit confirmation that its scope should be proportionate to the complexity of the process and the possibilities of identification. Businesses should be able to rely on established methods and previous assessments where these remain appropriate to the data and the conditions of its use. This would reduce duplication of analysis without lowering the standard of privacy protection.

**3. Clear conditions for determining that anonymisation is effective**

The Guidelines should be understandable to the businesses and technical teams expected to apply them. The key conditions for effective anonymisation should be set out directly in the document, without requiring readers to reconstruct them from numerous references to other guidelines and judgments.

The relationship between the simplified and contextual approaches requires particular clarity. As paragraph 45 indicates, the simplified approach may result in data being treated as non-anonymous even where it would be anonymous for the relevant entities in a particular context. Paragraph 52 and paragraphs 98-103 further explain that failure to meet the No Record Isolation or No Linkage criterion does not necessarily establish that an individual is identifiable.

Businesses should be able to determine easily and unambiguously when the outcome of an assessment is sufficient and when further verification is required. Uncertainty surrounding these rules may discourage businesses from making lawful use of data solely out of concern that their assessment could be challenged.

AI Chamber therefore calls for Guidelines that unequivocally confirm that effectively anonymised data may be used to train AI models and clearly establish the conditions for doing so. While maintaining effective privacy protection, anonymisation should be an accessible tool for everyday business operations. Its implementation and documentation should not require resources available only to the largest organisations.