MedTech Europe
from diagnosis to cure

MedTech Europe's contribution to EDPB's public consultation on Guidelines 02/2026 on Anonymisation

Executive summary and key recommendations

MedTech Europe welcomes the contextual approach in the draft Guidelines and supports the EDPB's objective of protecting individuals while enabling responsible and secure use of health data. To support proportionate and consistent implementation, the final Guidelines should provide greater practical clarity in the following areas:

- **Clarify the three criteria:** Clearly distinguish No Record Isolation, No Linkage and No Inference, including the relationship between record isolation, record uniqueness and singling out.
- **Define a workable standard for auxiliary information:** Confirm a reasonable-discovery approach that starts with information known to or held by relevant entities and extends only to information reasonably discoverable or foreseeable in the circumstances.
- **Recognise the effect of safeguards:** Explain when effective technical, organisational, contractual and legal safeguards can make particular means of identification no longer reasonably likely to be used.
- **Provide practical assessment tools:** Recognise established technical and statistical re-identification-risk assessment methods, including ISO/IEC 27559, and provide a step-by-step approach, templates and worked examples.
- **Clarify context, roles and data-sharing scenarios:** Provide workable criteria for assessing relevant entities and their capabilities, responsibilities across controllers, processors and recipients, mixed datasets, and information that may be anonymous in one context but not another.

The detailed comments and recommendations below explain each of these points and identify the relevant paragraphs and examples in the draft Guidelines.

Introduction

MedTech Europe welcomes the publication of the European Data Protection Board's (EDPB) draft Guidelines 02/2026 on Anonymisation (hereinafter the 'Guidelines') and appreciates the opportunity to contribute to the public consultation.

As the European trade association representing the medical technology sector, MedTech Europe recognises the crucial role of anonymisation in enabling the responsible and secure use of health data. Clear and practical guidance on when information may be considered anonymous, or rendered anonymous through anonymisation, is essential to protect privacy while enabling responsible data use and innovation.

MedTech Europe welcomes the contextual approach reflected throughout the Guidelines, which recognises that identifiability depends not only on the data itself, but also on the relevant entities, the means available to them and the surrounding context.

At the same time, further practical guidance would be valuable on how the three criteria of **No Record Isolation, No Linkage** and **No Inference** should be operationalised in practice, particularly regarding population uniqueness, the scope of external information to be considered, the role and effect of safeguards, technical and statistical re-identification-risk methods and the relationship between the three criteria.

The comments below highlight elements MedTech Europe welcomes and areas where further clarification could support proportionate and consistent application while maintaining a high level of protection for individuals.

Elements particularly welcomed

Several aspects of the Guidelines provide useful clarity. **Paragraphs 8 and 11** clearly reflect the contextual approach to identifiability and the perspective of the relevant entity. **Paragraph 29** also provides useful clarification on "means reasonably likely to be used" and the factors relevant to this assessment.

Paragraph 35 importantly recognises that anonymity is not permanent and may require reassessment as circumstances change. **Paragraphs 43 and 44** further clarify that the outcome of anonymisation should be assessed and demonstrated, aligning with the risk-assessment approach in the MedTech Europe Anonymisation Framework.

Paragraph 66 clearly explains inference. **Paragraphs 84 and 85** recognise the expertise required to assess anonymisation and the need to develop that expertise. **Paragraph 89** also clearly distinguishes publicly available information from information subject to technical, organisational and contractual controls.

Scope of the Guidelines

The Guidelines would benefit from clarifying that anonymous information may include both information that has been successfully anonymised and information that was non-personal from the outset. The assessment framework should also acknowledge that, depending on the relevant entities and circumstances, information may already be anonymous without requiring a further anonymisation process.

The Guidelines should also clarify how the assessment applies when information is transferred between entities with different knowledge, access and capabilities. A transfer should not automatically be assumed to make previously anonymous information personal data for the recipient. Rather, identifiability should be assessed in the relevant context, taking into account both the recipient's reasonably likely means of identification and the implications for the transferring entity where disclosure to an entity capable of re-identification is reasonably likely. Clearer criteria for determining when such circumstances affect the status of the information would support legal certainty for lawful data sharing, including in the context of the European Health Data Space (EHDS), without weakening the protection of personal data.

Operationalising the three criteria

The Guidelines establish three criteria for assessing whether information can be considered anonymous: **No Record Isolation, No Linkage and No Inference**. MedTech Europe supports this structure but sees a need for greater clarity on the terminology and boundaries of the criteria, the role of the applicable population, the scope of auxiliary information and the relationship between the criteria.

The Guidelines should further clarify how residual re-identification risk can be assessed and documented in practice, taking into account the relevant population, reasonably likely means of identification, applicable context and limitations of statistical methods. In particular, they should explain how measures such as equivalence class sizes and population uniqueness can inform the assessment without being treated as conclusive evidence of identifiability.

No Record Isolation: greater clarity on record uniqueness and singling out

Under **section 3.4.1**, No Record Isolation focuses on whether the given data contains a unique combination of attribute values relating to a single individual. However, uniqueness within the given data does not necessarily establish uniqueness within the applicable population or that the corresponding individual can be singled out.

This distinction is particularly relevant in the medical technology sector, where small datasets are common in clinical investigations and specialised studies. Such datasets may contain many unique records simply because of their limited size, even where the same attribute combinations are not unique within the applicable population.

This concern is further amplified where attributes are inherently dynamic, such as vital signs or other physiological measurements. A value or combination of values may appear unique at a particular observation point but occur frequently across the applicable population over time. Record uniqueness should therefore be assessed in its temporal and population context, rather than on the basis of a static snapshot alone.

Treating uniqueness within the given data as sufficient evidence of singling out may therefore lead to unnecessary transformations and loss of data utility without necessarily reducing actual re-identification risk.

Paragraphs 98–100 appear to recognise this distinction by requiring further consideration of whether an isolated record actually enables singling out. However, the relationship between **record isolation, record uniqueness and singling out** remains unclear. This distinction should already be explained in section 3.4.1, where No Record Isolation is introduced.

MedTech Europe's recommendations

MedTech Europe recommends that **record isolation, record uniqueness and singling out** be clearly defined and distinguished when No Record Isolation is first introduced in section 3.4.1. In particular, it would be helpful to clarify whether:

- **record isolation** refers to the ability to distinguish a record relating to one individual from other records in the given data;
- **record uniqueness** refers to a combination of attribute values occurring only once, either within the given data or, where relevant, within the applicable population; and
- **singling out** refers to the ability to distinguish an individual from others within the applicable population, rather than merely identifying a unique record within the given data.

The Guidelines should clarify that uniqueness within the given data does not necessarily imply uniqueness within the applicable population or that the corresponding individual can be singled out. Further clarification would also be valuable for **dynamic and longitudinal datasets**. For growing datasets, the Guidelines could clarify when record isolation should be reassessed. For longitudinal data, they could clarify what constitutes the relevant "**record**", particularly where a unique trajectory within the given data is not unique within the applicable population.

Paragraph 98 should clarify what is meant by "larger records" where the number of attributes is mentioned separately. **Paragraph 99** should clarify how "matching" differs from No Linkage, what is meant by "intelligible", and from whose perspective this is assessed.

No Linkage: greater clarity on the scope of auxiliary information

Under **section 3.4.2**, No Linkage considers whether information relating to the same individual can be linked across the given data and other available information. Removing direct identifiers alone does not prevent linkage, as indirect identifiers and combinations of attributes may still enable it. A key practical challenge is **how far an organisation is expected to search for auxiliary information**, an issue also raised by **paragraphs 51 and 68**.

In practice, there appear to be three possible approaches:

1. **Known information within the relevant entities:** considering auxiliary information already held by or known to the relevant entity, or, where multiple entities are involved, across the relevant processing chain (e.g. controller, processor and other relevant recipients). This provides a clearly bounded assessment but may be too narrow where relevant external information is readily discoverable.
2. **Exhaustive discovery**: actively identifying all information that could potentially enable linkage in a lawful manner. This may be **practically impossible** given the scale and continuous evolution of publicly accessible information.
3. **Reasonable discovery**: starting with information already known to or held by the relevant entities, and extending the assessment to information that is reasonably discoverable or foreseeable in the circumstances. This approach recognises that known information alone may be insufficient, while avoiding an exhaustive search for all potentially available information. The scope of reasonable discovery should be clearly bounded, taking into account the relevant entities, nature of the data, effort, cost, time and proportionality.

Social media illustrate this challenge. Information may be added or removed continuously, may be public or private, and may be spread across platforms, forums and other sources. Auxiliary information may therefore consist not

only of structured datasets, but also of fragmented and unstructured information that can collectively enable linkage or identification.

MedTech Europe's recommendations

MedTech Europe recommends that the Guidelines **confirm a reasonable-discovery approach as the appropriate standard** for assessing auxiliary information under No Linkage. Information already known to or held by the relevant entities should provide the starting point. Where this is insufficient, the assessment should extend to information that is reasonably discoverable or foreseeable in the circumstances, without requiring an exhaustive search.

Crucially, the Guidelines should establish **clear and practicable boundaries for reasonable discovery**, including which sources need to be considered and when further searching is no longer required. Without such boundaries, the approach risks becoming disproportionate, impractical and inconsistently applied.

The Guidelines should explicitly recognise foreseeability as an important factor in determining which auxiliary information and means of identification are reasonably likely to be used. The assessment should focus on information that relevant entities are reasonably likely to identify, obtain or use in practice, taking into account effort, cost, time and other relevant circumstances. Information that is merely theoretically available, but not reasonably foreseeable or accessible in practice, should not automatically fall within the scope of the assessment. This would help distinguish realistic and objectively supportable identification scenarios from speculative or hypothetical possibilities.

A practical assessment could start from the attributes and combinations of attributes in the given data and identify which external information sources could reasonably be linked to them.

The Guidelines should also clarify that auxiliary information is not limited to structured datasets and may include **unstructured information** from publicly available sources.

No Inference: greater clarity on different forms of inference

The Guidelines provide a clear explanation of inference in **paragraph 66**, but some of the subsequent applications of the No Inference criterion would benefit from further clarification. **Paragraph 70** distinguishes between information concerning the population at large and information that can be specifically inferred about an individual. The conclusion is understandable, but the first situation could benefit from a clearer example demonstrating when general knowledge becomes a specific and meaningful inference about an individual.

> For example, consider a record containing: **Age:** 48, **Country:** Netherlands, **Condition:** Pregnancy. Sex is not explicitly included in the record, but general knowledge about pregnancy allows the individual's sex to be inferred as female. This shows how general or population-level knowledge can result in a specific inference about an individual.

MedTech Europe's recommendations

MedTech Europe recommends that the Guidelines:

- provide a clearer example in **paragraph 70** distinguishing **general or population-level knowledge from a specific and meaningful inference about an individual**;
- introduce and clearly explain the concept of **membership inference in paragraph 79**, which differs from the forms of information deduction discussed immediately before it. A short introduction explaining that membership inference concerns determining whether an individual was included in the source data would improve clarity;
- clarify how the **source population affects the significance of membership inference**. Establishing that an individual was included in a dataset derived from the general population may reveal little, whereas establishing membership in a dataset consisting exclusively of patients with a particular rare disease may itself reveal meaningful information. An example contrasting these situations could help illustrate this distinction; and
- clarify the distinction between **linkage under the No Linkage criterion and "inferred linkage" under No Inference** in **paragraphs 80–82**. It is currently unclear when probabilistic matching or combining information should be assessed under No Linkage, No Inference, or both. A simple worked example showing when each criterion applies would provide greater clarity.

The following examples could also benefit from clarification:

Example 14: The lending and credit-risk scenario may involve population-level assumptions that reflect bias or discrimination. As the Guidelines do not otherwise address the potential role of bias in such inferences, a more neutral example may better isolate the anonymisation question.

Example 16: The example would be clearer if it explicitly stated that five of the six engineers work in Product Engineering and the sixth works elsewhere. It should also distinguish between inferring the sixth engineer's salary and identifying that engineer.

Example 20: The conclusion should be considered in light of Example 16. If additional information enables the sixth engineer to be identified, the inferred salary could be attributed to that individual. Re-identification may therefore be possible depending on the context.

Practical methodologies and recognised standards

MedTech Europe recommends that the Guidelines explicitly recognise established technical and statistical re-identification-risk assessment methods, including relevant international standards such as ISO/IEC 27559, and clarify how these can be applied to assess and demonstrate compliance with the three criteria.

The Guidelines should also provide practical implementation support, such as a step-by-step assessment approach, templates and worked examples, including medical device and pharmaceutical use cases. This would help organisations translate the criteria into consistent, documented and demonstrable risk assessments.

Mixed datasets containing personal and anonymous information

The Guidelines would benefit from further clarification on the assessment of mixed datasets containing both personal and anonymous information. In practice, organisations may encounter datasets where a limited number of records remain identifiable while others satisfy the anonymisation criteria.

MedTech Europe's recommendations

MedTech Europe recommends that the Guidelines clarify whether and under what conditions individual records or distinguishable components may be assessed as anonymous independently of the dataset as a whole, particularly where personal and anonymous information are not processed separately. Further guidance on the practical implications would support proportionate assessments while ensuring that identifiable information remains subject to the GDPR.

Role of TOMs, contractual safeguards and unlawful access

The Guidelines recognise that **technical and organisational measures (TOMs) and contractual controls form part of the context** in which identifiability is assessed. MedTech Europe agrees that such safeguards alone do not establish anonymity, and re-identification risk must still be assessed.

Paragraphs 33 and 34 raise an important practical question regarding the extent to which effective safeguards may influence whether a particular means of identification is considered "reasonably likely to be used". Paragraph 34 recognises that a contractual prohibition may be relevant where it is reliable, verifiable and enforceable. This is particularly important in the medical technology sector and clinical research, where cross-border data sharing between multiple organisations frequently relies on contractual restrictions alongside technical and organisational safeguards.

MedTech Europe's recommendations

MedTech Europe recommends that the Guidelines expressly recognise that **effective technical, organisational and contractual safeguards** should be capable, depending on the circumstances, of making particular means of identification no longer reasonably likely to be used. The Guidelines should provide clear criteria for determining when such safeguards are sufficiently reliable and effective to support this conclusion.

In particular, the Guidelines should clarify how unlawful-access scenarios, such as security breaches, theft or misuse of credentials, should be assessed. Organisations should not be required to consider every conceivable unlawful scenario, but only those for which there is an objectively supportable basis to regard the means of identification as reasonably likely to be used in the circumstances. Clear criteria would also allow organisations to demonstrate when particular unlawful-access scenarios are no longer reasonably likely, avoiding unnecessary data transformations that reduce data utility without materially improving protection.

The Guidelines should further clarify that reliable, verifiable and enforceable contractual safeguards may themselves **materially restrict access to additional information** and should not automatically require supplementary technical measures to be considered effective. Their effectiveness should be assessed in context, taking account of applicable legal obligations, organisational controls and the circumstances in which the information may be accessed.

Similarly, where access to additional information is legally prohibited or restricted, those restrictions should be given appropriate weight in the assessment, without automatically assuming that unlawful access is reasonably likely.

Practical examples from health-data research could illustrate how medical confidentiality and comparable legal obligations may restrict the disclosure of additional information that could otherwise enable re-identification. This would help organisations assess when access to such information is not reasonably likely in practice.

These clarifications would also support consistent application of **paragraph 89**, which distinguishes publicly available information from information whose accessibility is restricted through technical, organisational and contractual controls.

Documentation should not itself increase re-identification risk

MedTech Europe supports the documentation and accountability principles reflected in **paragraph 41**. However, documentation should not itself increase re-identification risk. Detailed transformation parameters, mappings or other implementation information could, depending on the method used, facilitate reversal or otherwise compromise anonymisation.

MedTech Europe's recommendations

MedTech Europe recommends that the Guidelines clarify that documentation should be **sufficiently detailed to demonstrate and support the anonymisation assessment, while being appropriately protected and not itself materially increasing re-identification risk**.

This would preserve the accountability objective of paragraph 41 without requiring documentation that could itself undermine anonymisation.

Anonymisation as deletion

Paragraph 39 introduces anonymisation as a possible way to fulfil a deletion obligation, but the distinction between the anonymisation process and its outcome could be clearer. The process remains subject to the GDPR while the information is personal. Once effective anonymisation is achieved, the resulting information is no longer personal data and falls outside the GDPR.

MedTech Europe's recommendations

MedTech Europe recommends that the Guidelines provide **further guidance** in paragraph 39 **on anonymisation as a means of fulfilling a deletion obligation**, clearly distinguishing the processing required to achieve anonymisation from the status of the resulting anonymous information.

The Guidelines should also clarify how retaining or erasing the original personal data affects the assessment of the anonymised information, particularly where the original data could enable re-identification. Practical examples illustrating different scenarios, including where the original data is retained or erased, would help organisations understand the implications for the anonymisation assessment and the fulfilment of deletion obligations.

Relevant entities and capabilities

The contextual approach requires consideration of the **knowledge and capabilities of relevant entities**. MedTech Europe supports this principle, but assessing those capabilities can be difficult, particularly where relevant entities extend beyond known recipients of the data.

Example 22 illustrates this challenge. The research institution **concludes** that acquaintances are extremely unlikely to receive the data following a leak, but does not explain how this conclusion was reached. Acquaintances may already know an individual's membership of the relevant population, year of birth, location or postal code, significantly increasing their ability to single out or re-identify that individual.

MedTech Europe's recommendations

MedTech Europe recommends that the Guidelines provide **clearer and workable criteria for determining which entities should be included in the assessment** and how their knowledge and capabilities should be reasonably bounded in practice. A structured approach could consider which entities are reasonably likely to access the data, the additional information they are reasonably likely to possess or obtain, their realistic capabilities, and the safeguards restricting their access or means of identification. This should include realistic threat actors, such as malicious third parties or employees acting outside their authorised access, where their means of identification are reasonably likely to be used in the circumstances.

The Guidelines should also clarify **when categories of entities may reasonably be excluded from the assessment**. Entities whose access or capabilities are merely remote, speculative or theoretical should be capable of being excluded on the basis of objective criteria, without requiring organisations to consider every conceivable actor or means. Clear guidance on these boundaries would support proportionate and consistent assessments.

For **Example 22**, the Guidelines could explain how the research institution determined that acquaintances were extremely unlikely to receive the data following a leak. Alternatively, if this is not intended to demonstrate such an assessment, the Guidelines should state that this is an assumption made for the example.

The Guidelines should further clarify **how responsibilities and assessments apply across a chain of controllers, processors and recipients, recognising that their knowledge, access and capabilities may differ.** In the medical technology sector, processors may have limited or no access to additional information held by controllers due to medical confidentiality obligations or purpose-based access restrictions. Such information should not automatically be treated as available to the processor.

The Guidelines should **distinguish between the controller's and processor's responsibilities when assessing identifiability**. The controller should assess the broader context, while the processor should assess its own knowledge, access and technical capabilities. However, this distinction in assessment responsibilities does not change the fact that **the controller's perspective remains relevant when determining whether information processed on its behalf is personal data**. The knowledge and capabilities of other relevant entities may also need to be considered. The Guidelines should also recognise that an organisation may have different roles in relation to different processing activities.

Conclusion

MedTech Europe welcomes the EDPB's efforts to provide updated guidance on anonymisation and particularly supports the **contextual approach to identifiability**, recognising that whether information can be considered anonymous depends on the relevant entities, the means available to them and the surrounding context.

The Guidelines provide an important foundation, but further practical guidance would strengthen their consistent application. In particular, clearer definitions and boundaries for **No Record Isolation, No Linkage and No Inference**, together with greater clarity on the scope of auxiliary information, the role of safeguards, and the assessment of relevant entities and their capabilities, would provide organisations with a more practicable basis for assessing and demonstrating anonymisation.

Further clarification on the scope of anonymous information, including the assessment of mixed datasets and the circumstances in which information may be anonymous to different entities, would also support legal certainty and responsible data sharing.

MedTech Europe therefore encourages the EDPB to address these areas in the final Guidelines through clear definitions, recognition of established re-identification risk-assessment methods and practical examples. This would support proportionate and consistent anonymisation while maintaining a high level of protection for individuals.

About MedTech Europe

MedTech Europe is the European trade association for the medical technology industry including diagnostics, medical devices and digital health. Our members are national, European and multinational companies as well as a network of national medical technology associations that research, develop, manufacture, distribute and supply health-related technologies, services and solutions.

www.medtecheurope.org

For more information, please contact: Mirella Kavadaki (m.kavadaki@medtecheurope.org)