MyData-TRUST

18b Av. Lavoisier, 1300 Wavre

BELGIUM

Response to Public Consultation on EDPB Guidelines 02/2026 on Anonymisation

 Date: October 29, 2026

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

MyData-TRUST ("MDT") welcomes the publication of the EDPB Guidelines on Anonymisation. Our response focuses on practical considerations relating to legal clarity, operational feasibility and the application of the Guidelines in the clinical research and health data context. This Executive Summary highlights our key recommendations, while the detailed comments provide further analysis, practical examples and proposed drafting improvements aimed at enhancing the clarity and practical usability of the Guidelines, particularly for clinical trials, genetic and genomic research, and other health research settings.

Each comment identifies the relevant paragraph number of the Guidelines and, where helpful, quotes the EDPB text under review. Each comment contains an MDT Opinion sub-section and an MDT Suggestion sub-section.

About us:
MyData-TRUST is registered under Belgian Laws, active since 2017 in the data protection area and dedicated exclusively to the health and life science. Our multi-disciplinary team includes Data Privacy Lawyers, IT Security Specialists and Health data/Clinical Experts providing GDPR related services (such as privacy risk assessments, external DPO as a service, etc.). Our clients include among others Pharmaceutical, Biotech and Medical Devices companies, Contract Research Organisations (CROs), Healthcare providers and Health associations.

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

Table of Contents

Detailed Comments *5*

Section 1. Introduction *5*

A. Paragraph 1- Revision of the introductory description of the GDPR to align with its legal objectives and terminology: **5**

B. Paragraph 2; Footnote 3 - Moving the Periodic Reassessment Principle from the Footnote into the Main Text **6**

C. Paragraph 4- Clarification that the qualification of an entity as controller or processor depends on both the personal nature of the data and the entity's role in the processing **6**

Section 2. Legal Analysis *7*

D. Paragraph 6 – Clarification that the assessment of anonymity must be contextual and entity-specific: **7**

E. Paragraph 8 – Support for the likelihood-based and entity-specific approach to identifiability: **7**

F. Paragraph 15- Clarification of the applicable perspective where the processor has additional means of identification **8**

G. Example 4- Clarification that the recipient does not receive the re-identification key: **9**

H. After Paragraph 21 – Addition of a clinical trial example illustrating recipient-specific identifiability in the context of pseudonymised data: **9**

I. Paragraph 34 – Recognizing Effective Contractual and Governance Measures in the Likelihood Assessment **10**

J. After Paragraph 35 – Addition of a clinical trial example illustrating that anonymity may need to be reassessed over time: **11**

K. Paragraph 36 – Separate treatment of records where anonymisation is not effective for all individuals: **11**

Section 3. The Technical Analysis of Anonymisation *11*

L. Paragraph 49 – Clarification of the limits of the simplified approach **11**

M. After Paragraph 65 – Addition of a clinical trial example illustrating the No Linkage criterion in the context of coded participant data: **12**

N. After Example 14 – Addition of a clinical trial example illustrating the No Inference criterion in the context of aggregated research data: **13**

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

Key Recommendations

- **Clarify the relationship between data qualification and role qualification,** in particular in controller-processor scenarios where the parties may have different identification capabilities or access to additional information.

  See Detailed Comments on Paragraphs 4 and 15.

- **Frame the entity-specific assessment of identifiability with clear safeguards,** making clear that the entity relying on anonymity shall demonstrate through a documented assessment, and that the absence of access to a re-identification key is not, in itself, sufficient to conclude that data is anonymous.

  See Detailed Comments on Paragraphs 6 and 8.

- **Require that any conclusion of anonymity be documented and that the DPO be consulted,** where one has been designated, in line with the accountability principle (Article 5(2) GDPR) and the tasks of the DPO (Article 39 GDPR).

  See Detailed Comment on Paragraph 6.

- **Provide clearer guidance on pseudonymised data,** including the relevance of access to the re-identification key and other practical means of identification, particularly in multi-party clinical research settings involving sponsors, sites and CROs.

  See Detailed Comments on Example 4 and Paragraph 21.

- **Recognise that clinical trial sponsors will generally not be in a position to consider coded participant data as anonymous,** given the regulatory obligations requiring that trial data can be traced back to participants.

  See Detailed Comment after Paragraph 21.

- **Recognise the practical value of effective contractual and governance measures** in reducing the likelihood of re-identification where they are supported by appropriate technical, organisational and enforcement mechanisms.

  See Detailed Comment on Paragraph 34.

- **Emphasise that anonymity is dynamic rather than necessarily permanent**, and may need to be reassessed where technological developments, new datasets or new linkage possibilities materially increase the likelihood of re-identification.

  See Detailed Comments on Paragraphs 2 and 35.

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

- **Clarify the limits of the simplified approach**, in particular by avoiding overly definitive conclusions of anonymity where the assessment does not fully reflect the capabilities and circumstances of the relevant entities.

  See Detailed Comment on Paragraph 49.

- **Include more practical life sciences and clinical research examples**, especially on linkage, inference, rare characteristics and coded datasets, to make the technical criteria easier to apply in real-world research environments.

  See Detailed Comments on Paragraph 36, Paragraph 65 and Example 14.

Detailed Comments

MDT provides below its observations and suggestions, organized by section of the Guidelines. Each comment identifies the relevant paragraph number of the Guidelines and, where applicable, sets out the wording under review, the proposed wording or addition, and an explanation of MDT's position.

Section 1. Introduction

A. Paragraph 1- Revision of the introductory description of the GDPR to align with its legal objectives and terminology:

Deleted wording:

"ensures that data processing is done in a way that benefits humankind while being safe for data subjects"

Proposed wording:

"…the General Data Protection Regulation *provides a framework to ensure that personal data is processed in a manner that protects the fundamental rights and freedoms of data subjects.* In other cases, it may be better to use anonymous information, *i.e*…"

Explanation:

We suggest replacing the current wording to better reflect the GDPR, which focuses on protecting individuals' rights and freedoms rather than requiring processing to "benefit humankind".

In the life sciences context, anonymisation may also reduce data utility. MDT therefore suggests acknowledging the need to balance privacy protection with scientific usefulness.

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

B. Paragraph 2; Footnote 3 - Moving the Periodic Reassessment Principle from the Footnote into the Main Text

Suggested improvement:

Footnote 3 provides that a controller which assessed a dataset as anonymous in accordance with Opinion 05/2014 before publication of the Guidelines is not expected to conduct a new assessment, while periodic reassessment of the likelihood of re-identification is considered good practice.

Given the importance of this point in practice, particularly in the life sciences sector, we suggest moving this statement into the body of the Guidelines and providing more concrete guidance on the frequency of reassessment. For example, reassessment could be required at appropriate intervals, and in any event no later than every three years, as well as whenever relevant circumstances change, including technological developments or the increased availability of additional information that may affect the risk of re-identification.

C. Paragraph 4- Clarification that the qualification of an entity as controller or processor depends on both the personal nature of the data and the entity's role in the processing

Deleted wording:
"on whether the data being tested is personal or not"

Proposed wording:
"…It is not possible, for example, to know if the person holding the data should be described as a controller or not, since that answer will depend *on whether the data being tested constitutes personal data and, where it does, on the entity's role and responsibilities in relation to the processing.* Therefore, rather than, for example, constantly referring to "the person who may or may not be a controller…"

Explanation:
We suggest clarifying that an entity's qualification as controller or processor does not depend solely on whether the data constitutes personal data. Where the GDPR applies, the entity's role must be assessed separately by reference to its actual responsibilities and decision-making powers in relation to the processing.

This is also consistent with Paragraph 15, which confirms the importance of identifying the relevant role of the entity involved in the processing. This distinction is particularly important where different entities may have different perspectives on identifiability, while their respective roles in the processing must still be assessed separately.

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

Section 2. Legal Analysis

D. Paragraph 6 – Clarification that the assessment of anonymity must be contextual and entity-specific:

Added wording:
"…If, *following an appropriate contextual assessment*, the answer to either of these questions is "no", then the data should be considered anonymous..."

Explanation:
We suggest adding a reference to an "appropriate contextual assessment" to clarify that anonymity cannot be determined in the abstract.

Whether information relates to an identified or identifiable person depends on the circumstances in which it is held and processed, including the means reasonably likely to be used for identification and the information and resources available to the relevant entity. The assessment is therefore contextual and may lead to different conclusions for different entities. However, a conclusion of anonymity should remain the exception rather than the default for pseudonymised data, and the entity relying on it should bear the burden of demonstrating it.

This is consistent with Case C-413/23 P, EDPS v SRB, which confirms that pseudonymised data is not necessarily personal data in all cases and for every entity, and with the remainder of Paragraph 6, which recognises that the same information may be anonymous for some entities but not for others. This judgment does not, however, mean that pseudonymised data should be presumed anonymous for entities that do not hold the re-identification key.

The proposed wording therefore helps avoid the impression that anonymity can be assessed solely by examining the dataset in isolation and better reflects the approach developed in the Guidelines.

In line with the accountability principle (Article 5(2) GDPR), MDT also suggests that the Guidelines recommend that any anonymity assessment be documented, including the methodology followed, the means of identification considered and the conclusion reached, and that the DPO be consulted where one has been designated (Article 39(1)(a) GDPR).

E. Paragraph 8 – Support for the likelihood-based and entity-specific approach to identifiability:

We support the approach taken in Paragraph 8, which correctly frames the assessment of identifiability as a question of likelihood rather than as an absolute or purely theoretical possibility.

This formulation is particularly useful because it reflects the contextual nature of the identifiability assessment and avoids suggesting that any conceivable possibility of identification would be sufficient to treat information as personal data. The relevant question is instead whether the individual could be identified by means reasonably likely to be used in the circumstances and from the perspective of the relevant entity. This assessment should nonetheless take into account all

MyData-TRUST

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

means reasonably likely to be used, including any legal or contractual right to obtain additional information, and should be documented.

This point is also consistent with the approach developed later in the Guidelines, including Paragraph 22, which further confirms the importance of assessing identifiability by reference to the means and circumstances realistically available to the relevant entity.

We therefore consider this clarification particularly important and helpful, as it provides a clear conceptual basis for the practical assessment of anonymity developed throughout the Guidelines.

F. Paragraph 15- Clarification of the applicable perspective where the processor has additional means of identification

Proposed wording:

"…That entity should, therefore, be considered a processor under the GDPR and be subject to the obligations applicable to processors. *Conversely, where the processing entity has access, in the context of the processing carried out on behalf of the controller, to additional information or other means reasonably likely to be used to identify the individual, those means should also be taken into account when assessing the data from the controller's perspective. Where the processing entity uses such means independently and for its own purposes, its role in relation to that processing should be assessed separately.* This follows from a teleological application of the GDPR…"

Explanation:

We suggest clarifying how the applicable perspective should be determined in different controller-processor scenarios. The assessment should first consider the circumstances in which the data is held and processed and the means of identification available in that context.

Paragraph 15 already makes clear that where the data is personal from the controller's perspective, a processor acting on its behalf must also treat the data as personal, even if the processor would not itself be able to identify the individuals.

Conversely, where the controller does not itself hold the information necessary for identification but the processor has access to such information or other means reasonably likely to be used in the context of the processing carried out on the controller's behalf, those means should also be taken into account from the controller's perspective. The controller should therefore not conclude that the data is anonymous solely on the basis of the information it directly holds.

Where the processor uses such information or means independently and for its own purposes, its role and the personal nature of the data in relation to that separate processing should be assessed separately.

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

G. Example 4- Clarification that the recipient does not receive the re-identification key:

Added wording:

"…to an independent institute for research purposes. *The institute does not receive the key linking the pseudonymised data to the patients.* The data will never be returned to the hospital, and the institute is free to determine means… its own perspective. *In particular, the assessment should consider whether the institute nevertheless has means reasonably likely to be used to identify the individuals, including through access to or combination with additional information.*"

Explanation:
In Example 4, we suggest clarifying that the independent research institute does not receive the key linking the pseudonymised data to the individuals concerned.

This is relevant to the entity-specific assessment of identifiability. Where the recipient does not hold the key, the assessment should focus on whether it nevertheless has means reasonably likely to be used to identify the individuals, including through access to or combination with additional information.

This clarification would make clear that, for cases where the relevant perspective to be analysed is that one of the recipients of the data, both elements listed in paragraph 13 are important: specific nature and context of the processing. For instance, in our proposed example 4, the absence of the key is not sufficient to conclude that the data is anonymous for the institute. The institute should demonstrate, through a documented assessment, that it has no other means reasonably likely to be used to identify the individuals.

Finally, the EDPB could clarify the allocation of roles in Example 4: the identifiability assessment from the institute's perspective should be carried out and documented by the institute, as the sole to be able to assess the means reasonably likely to be used. The hospital, which remains a controller of personal data, should provide the required information for that assessment and exercise appropriate due diligence before disclosure. On a DPO perspective, it might be difficult, especially if on actor is outside EEA, to determine if standard contractual clauses are required. If the assessment define means reasonably likely to be used as low, are transfer measure still applicable.

H. After Paragraph 21 – Addition of a clinical trial example illustrating recipient-specific identifiability in the context of pseudonymised data:

Proposed addition:

"Example X: A sponsor receives clinical trial data from a CRO in pseudonymised form. The trial site retains the key linking the participant codes to the participants' identities. Where the sponsor can reasonably request the site to provide the additional information or can obtain access to identifiable information through monitoring activities, the data may constitute personal data for the sponsor. Conversely, where the recipient does not hold the key and there are no means

MyData-TRUST

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

reasonably likely to be used to obtain or combine the additional information necessary for identification, the assessment may differ from the recipient's perspective. Where the recipient processes the data on the instructions of an entity for which the data is personal, paragraph 15 applies and the assessment is not made from the recipient's own perspective."

Explanation:
We suggest adding a clinical trial example after Paragraph 21 to illustrate recipient-specific identifiability in the context of pseudonymised data.

In clinical trials, coded or pseudonymised data are often shared between sites, CROs and sponsors while the re-identification key is retained by another party. The example would clarify that the absence of the key is not determinative: the assessment should also consider whether the recipient has means reasonably likely to be used to obtain or access the additional information necessary for identification, including through monitoring arrangements.

Conversely, where the recipient is genuinely independent and has no such means, the assessment may differ from its perspective. This would provide useful practical guidance for the clinical research sector and reinforce the contextual and entity-specific approach to identifiability.

More generally, MDT invites the Board to make a reference to the fact that clinical trial sponsors will generally not be in a position to consider coded participant data as anonymous. The applicable regulatory framework requires that trial data can be traced back to the participant, including for source data verification, the follow-up of serious adverse events, pharmacovigilance, inspections by competent authorities and the archiving of the trial master file for 25 years under Regulation (EU) No 536/2014. These obligations constitute means reasonably likely to be used to identify participants and should be taken into account in the assessment from the sponsor's perspective.

I. Paragraph 34 – Recognizing Effective Contractual and Governance Measures in the Likelihood Assessment

We agree that a prohibition set out in a contract should not be treated as a prohibition by law, and that contractual measures should complement rather than substitute for technical measures. However, in practice, there is a meaningful difference between a simple contractual undertaking not to attempt re-identification and a data use agreement supported by access controls, audit rights, defined penalties and an institutional data access committee. MDT therefore invites the Board to provide further guidance on the features that may make contractual and governance measures effective in reducing the likelihood that means of re-identification will be used. Such contractual measures should, however, never be sufficient on their own to conclude that data is anonymous. Their effectiveness should be assessed on a case-by-case basis and documented as part of the anonymisation assessment, together with the technical measures in place.

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

J. After Paragraph 35 – Addition of a clinical trial example illustrating that anonymity may need to be reassessed over time:

Proposed addition:

"*Example X: Data from a clinical trial may initially be considered anonymous following aggregation and removal of direct identifiers. However, the subsequent availability of additional datasets, including public registries or other research datasets, may create new possibilities for linking or combining information and increase the likelihood of re-identification over time. The anonymity assessment should therefore be revisited where relevant.*"

Explanation:
We suggest adding a clinical trial example after Paragraph 35 to illustrate that anonymity may need to be reassessed over time as the factual or technological context evolves.

This is particularly relevant in clinical research, where datasets may be retained for long periods and later become linkable with newly available sources, such as public registries, genomic databases or other research datasets. Such developments may increase the likelihood of singling out or re-identifying individuals.

The example would therefore reinforce that anonymity is not necessarily a one-off assessment and may need to be revisited where new data sources or linkage possibilities materially affect the likelihood of identification.

K. Paragraph 36 – Separate treatment of records where anonymisation is not effective for all individuals:

We suggest clarifying that, where anonymisation is not effective for all individuals in a dataset, specific records or categories of records may be treated separately rather than requiring a uniform approach across the entire dataset. This is particularly relevant in clinical research, where datasets may contain outliers, such as participants at the extremes of an age distribution, individuals with rare co-occurring conditions, participants from very small populations or individuals with rare genotypes. Techniques such as generalisation, top- and bottom-coding, suppression or separate treatment of particular records may be appropriate depending on the circumstances. We invite the Board to clarify this possibility and illustrate it with a practical example. Such separate treatment should be based on a documented, record-level assessment, and the remaining records should still be assessed against all anonymisation criteria.

Section 3. The Technical Analysis of Anonymisation

L. Paragraph 49 – Clarification of the limits of the simplified approach

Deleted wording:
"can safely be considered anonymous"

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

Proposed wording:
"…For example, an anonymising controller might wish to begin with the simplified approach, asking if re-identification is even possible in theory. If this is not possible, the data *may be considered anonymous based on that assessment.* If, however, the simplified approach identifies the existence of certain re-identification methods…"

Explanation:
We suggest avoiding the wording "can safely be considered anonymous", as it may give excessive confidence in the simplified approach.

The simplified approach can be useful as a conservative screening tool, particularly where it identifies possible means of re-identification and therefore leads the controller to treat the data as non-anonymous. However, because it deliberately disregards differences between the capabilities and circumstances of relevant entities, a conclusion of anonymity should not be presented as risk-free or absolute.

The proposed wording would therefore better reflect the respective risks of both simplified and contextual assessments and avoid suggesting that the simplified approach necessarily provides a definitive conclusion of anonymity.

M. After Paragraph 65 – Addition of a clinical trial example illustrating the No Linkage criterion in the context of coded participant data:

Proposed addition:
"*Example X: A sponsor holds a dataset containing coded clinical trial records with participants' age, sex, treatment group, visit dates and adverse events. The identification key is retained by the trial site. Although no individual record is unique within the sponsor's dataset, the records could be linked to the site's records using the participant code, or by combining several attributes such as age, visit dates and treatment information. If such linkage is reasonably likely from the relevant perspective, the No Linkage criterion would not be met.*"

Explanation:
We suggest adding a clinical trial example after Paragraph 65 to illustrate how the No Linkage criterion applies to coded participant data.

In clinical trials, sponsors may receive datasets without direct identifiers while the identification key is retained by the site. The absence of direct identifiers, or of unique records within the sponsor's dataset, does not in itself exclude linkage with other information.

The example would clarify that linkage may occur through a common identifier, such as a participant code, or through a combination of attributes such as age, visit dates or treatment information. The assessment should therefore consider whether the data can reasonably be linked with additional information available to the relevant entity or obtainable through means reasonably likely to be used.

MyData-TRUST

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

This would also help distinguish the No Linkage criterion from the No Record Isolation criterion and provide practical guidance for clinical research settings.

N. After Example 14 – Addition of a clinical trial example illustrating the No Inference criterion in the context of aggregated research data:

Proposed addition:
"*Example X: A clinical trial dataset intended to be anonymised contains aggregated information on treatment groups, rare adverse events and genetic characteristics. By combining these data with publicly available information about a participant's age, treatment and rare condition, it may be possible to infer that a particular participant was included in the study and experienced a specific adverse event. Where this inference is specific and meaningful and relies on information contained in the original dataset, the No Inference criterion would not be met.*"

Explanation:
We suggest adding a clinical trial example after Example 14 to illustrate how the No Inference criterion may apply where aggregated research data contains sensitive or distinctive clinical or genetic information.

Even where individuals cannot be directly identified or singled out, combining the dataset with external information may allow specific and meaningful conclusions to be drawn about a particular person, such as their participation in a study, treatment received, adverse event or genetic characteristic.

The example would therefore help distinguish inference from singling out and linkage and provide practical guidance for clinical research settings where sensitive health information may make such inferences particularly significant.

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.