Anonymisation: How to assess the anonymity of data



EDPB European Data Protection Board

GUIDELINES AT A GLANCE

October 2026

When your organisation uses or shares data, anonymising any personal data can be a valuable way to unlock its potential while simultaneously protecting individuals' rights.

The **EDPB Guidelines on anonymisation** bring clarity to the notion of anonymous data and provide a practical framework for organisations to determine if anonymisation is successful.



When is data anonymous?

Data is anonymous for a particular entity if **it does not relate to an identified or identifiable natural person**. This can depend on that entity's particular circumstances and capabilities, and so information may be anonymous for some entities but not others.

Information can **relate** to an individual because of its **content, purpose,** or **effect.** This connection may not be immediately obvious and might require further analysis.

An individual is considered 'identified or identifiable' if they can be distinguished from others in a specific context in a way that makes it possible to treat them different and **using means reasonably likely to be used.**

Practical examples

Here are specific scenarios extracted from the Guidelines:

Example

Means reasonably likely to be used
(section 2.4.2, paragraph 28, pages 11, example 7)

Context: An organisation wants to share certain information with its business partner. They try to anonymise the data but, when testing the strength of the anonymisation, quickly realise that the individuals could be re-identified through a certain re-identification technique.

Assessment: The organisation knows that their business partner would not itself be able to perform this re-identification technique. However, they could easily hire a third party to do it. That technique therefore qualifies as a means reasonably likely to be used by the business partner.

Example

Identifying the relevant perspective
(section 2.2, paragraph 15, pages 7 and 8, examples 3 and 4)

Context: One entity processes information on behalf of another, which is a data controller.

Assessment: The controller's perspective will be relevant for both parties. In practice, this means that if the information is personal data for the controller, it is also personal for the entity which is actually doing the work, and that processing entity should be subject to the GDPR obligations applicable to processors.

The technical analysis of anonymity: two approaches

When testing if anonymisation has been successful, you can apply one of two approaches:

1. The contextual approach

- This approach reflects the full nuances in the legal standard for anonymisation. It assesses the means of each relevant entity and the likelihood of their use. This gives a comprehensive analysis but requires that you can properly account for the relevant contextual elements involved.

2. The simplified approach

- This approach ignores the differences between entities' capabilities, asking if means for identification are reasonably likely to be used in the abstract. This can be more convenient than the contextual approach. However, this approach could lead you to treat information as personal data, even though it is actually anonymous for all of the relevant entities. Therefore, while it can offer greater confidence in a finding that information is anonymous, it cannot be used to definitively prove that it is not.

In practice, a combination of both approaches may also be helpful.

Criteria to test if data is anonymous

In some cases, it may be immediately apparent that information is not anonymous. In others, you should use three criteria to assess the effectiveness of possible (re-) identification techniques:

1. No record isolation

- This criterion is met if the data does not contain a unique combination of attribute values that relate to a single individual.

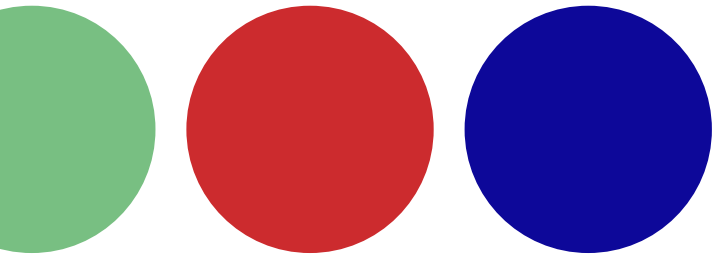
  On the contrary, when record isolation is possible, there is a risk that the individual can be singled out (i.e. can be identified by matching that unique combination of attributes to the particular person).



2. No linkage

This criterion is met if the data does not contain an individual's record which could be linked to another record that (a) also relates (with certainty or high likelihood) to that same individual, and (b) comes from a different dataset.

On the contrary, when linkage is possible, it may reveal more information about the individual, which could then lead to identifiability.



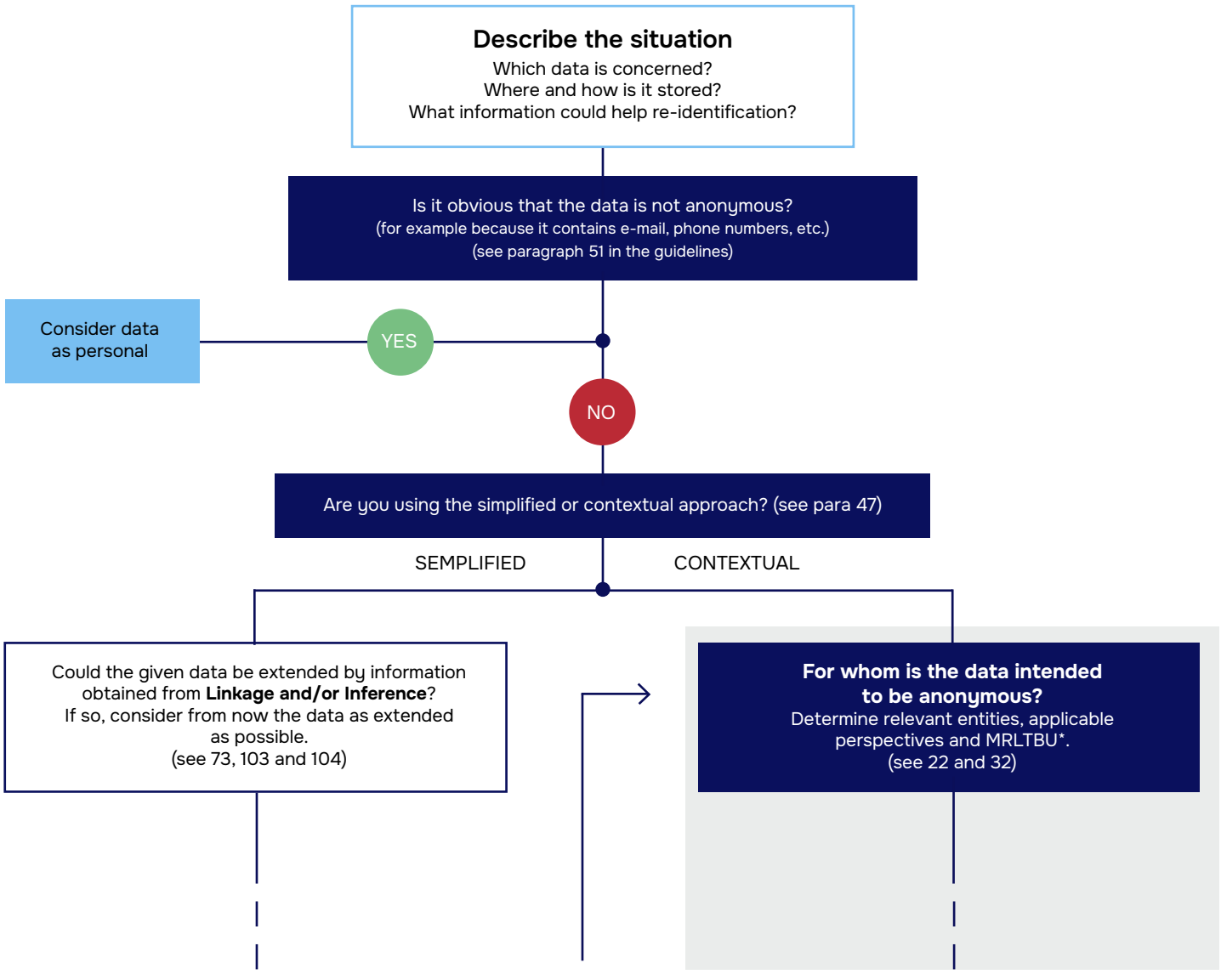
3. No inference

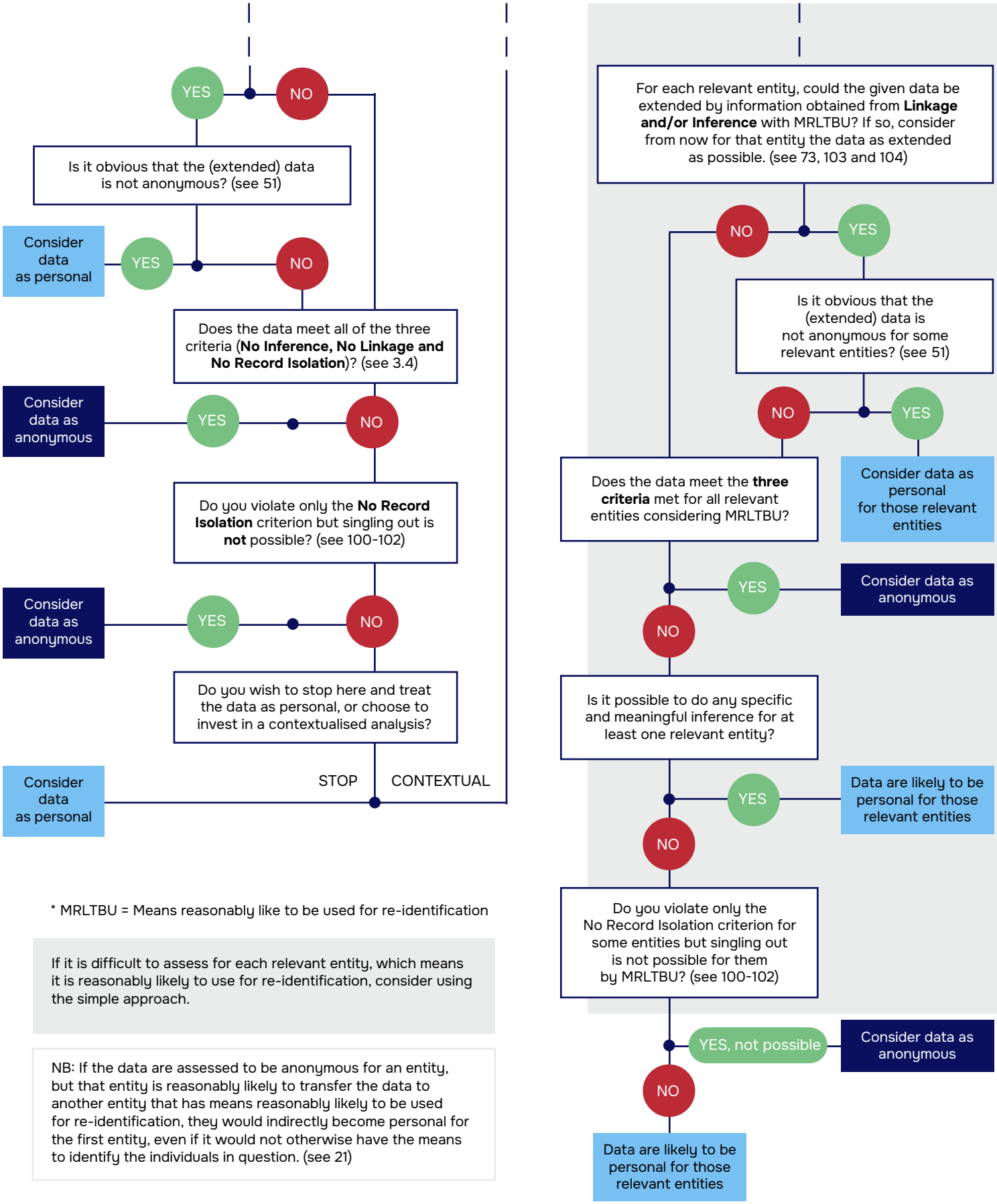
This criterion is met if no specific and meaningful conclusions can be drawn from the given data. Inferences may be based on the given data and/or on additional information, including information about the anonymisation process. In particular:

- An inference is specific if the inferred information relates to a single identified or identifiable individual; and
- An inference is both specific and meaningful if the processing of the inferred information is also liable to have an effect on the individual's rights and interests, relies on the given data and could not be obtained from general knowledge or from data about the population at large.

If all 3 criteria are met, the data can be safely considered anonymous. If any of these criteria are not satisfied, you **should conduct further analysis** to determine if the data may still be considered anonymous.

Check how the assessment could be done in line with the guidelines:





* MRLTBU = Means reasonably like to be used for re-identification

If it is difficult to assess for each relevant entity, which means it is reasonably likely to use for re-identification, consider using the simple approach.

NB: If the data are assessed to be anonymous for an entity, but that entity is reasonably likely to transfer the data to another entity that has means reasonably likely to be used for re-identification, they would indirectly become personal for the first entity, even if it would not otherwise have the means to identify the individuals in question. (see 21)

This document provides a simplified overview of the guidelines. For more comprehensive legal explanations and examples, please consult the full text of the guidelines.

Read the complete guidelines

EDPB European Data Protection Board

edpb.europa.eu