To the European Data Protection Board (EDPB)

Danish Regions

Danish Regions' response on behalf of the regions of Denmark to the EDPB's draft Guidelines 02/2026 on anonymisation

30-10-2026

1. Introductory and general remarks

Danish Regions appreciates the opportunity to comment on the EDPB's draft Guidelines 02/2026 on anonymisation. As the association representing Denmark's five regions, Danish Regions has prepared a joint response on their behalf.

Overall, the regions welcome the EDPB's preparation of comprehensive guidelines intended to provide greater clarity on when information may be considered anonymised and thus falls outside the scope of the General Data Protection Regulation (GDPR). Recent case-law from the Court of Justice of the European Union, including the judgment in Case C-413/23 P, EDPS v SRB, together with significant technological developments in this area, has highlighted the need for an updated and more operational framework for assessing anonymity.

In particular, the regions welcome the fact that the Guidelines allow for a contextual approach, under which the assessment of whether information may be considered anonymous depends on the relevant party's access to information, technological capabilities and other resources. This approach is particularly relevant in areas such as research, the use of health data and the development of AI solutions, where data types, purposes of use and risks may vary considerably. However, in the regions' view, the Guidelines should clarify which external actors and identification scenarios should reasonably be

included in the assessment. This issue is elaborated in greater detail in section 4.1.

At the same time, the regions consider that the Guidelines could be clarified and supplemented on a number of points in order to reduce legal uncertainty and enhance their practical applicability. This applies particularly in the health sector and in the field of research, where data exchange between independent controllers provides an important basis for innovation, quality improvement and research. In particular, there is a need for clearer delineation of the perspectives and possible chains of identification that must be included in the assessment of anonymity, the extent of the required documentation, and the extent to which anonymity must be reassessed over time. It is therefore essential that the Guidelines establish clear and operational parameters that both ensure a high level of data protection and support the lawful and responsible use and exchange of data.

The regions also recommend that the Guidelines include more coherent and practical examples, particularly from the health sector. The need for such examples, as well as more active use of the flowchart in Annex 1, is elaborated in greater detail in section 7.

Finally, the regions request that the Guidelines provide further guidance on how developments in AI should be taken into account in the assessment of anonymity. This applies particularly to the secondary use of health data and other datasets containing extensive free text, where new technological capabilities may affect the risk of re-identification. This issue is discussed in section 5.

2. Assessment of anonymity from the perspective of the relevant party

The regions welcome the clarification in the Guidelines that, where a party processes information on behalf of and on the instructions of a controller, the assessment must be made from the controller's perspective. If the information constitutes personal data for the controller, it must also be treated as personal data by the receiving party acting as a processor, irrespective of whether the processor itself is able to identify the data subjects. In the regions' view, the Guidelines thus help remove uncertainty about the scope of the judgment of the Court of Justice in Case C-413/23 P, *EDPS v SRB*, in situations where a controller transfers pseudonymised personal data to a processor. They also clarify that the parties cannot refrain from entering into a data

processing agreement under Article 28 of the GDPR on the grounds that the information appears anonymous to the processor.

In the regions' view, the Guidelines will therefore be of primary practical relevance in situations involving disclosure between two independent controllers. In such cases, the information may continue to constitute personal data for the disclosing controller but, following a case-by-case assessment, be considered anonymous for the receiving controller.

For the sake of completeness, the regions recommend that the Guidelines also clarify how the assessment should be conducted in cases of joint controllership.

3. The point in time at which anonymity must be assessed

The regions note that the Guidelines do not appear to address unequivocally when information is to be considered anonymised.

In a Danish context, this is particularly relevant to determining whether prior authorisation for disclosure for disclosure is required under section 10(3) of the Danish Data Protection Act.

In the regions' view, the Guidelines should clarify when information is to be considered anonymised where the assessment of anonymity differs between the disclosing and receiving parties. In particular, the Guidelines should specify whether anonymity is to be assessed at the time of transfer, during transmission, or only once the information has come into the recipient's possession and can be assessed from the recipient's perspective. This distinction is crucial where the information continues to constitute personal data for the disclosing party but is considered anonymous for the recipient, as it directly determines whether the disclosure and transmission require a legal basis under data protection law.

4. Documentation and ongoing reassessment

4.1. Assessment and documentation of anonymity in relation to subsequent recipients (chain of identification)

The regions note that the Guidelines appear to impose a relatively extensive obligation to document the assessment of whether information may be considered anonymous. In particular, the Guidelines state that if it can reasonably be expected that a party may transfer information to a third party, and it

cannot be ruled out that this third party has the means to identify the data subject, the information must be considered personal data both in connection with the transfer and during the recipient's subsequent processing.

The anonymising party may therefore have to assess not only whether the specific recipient is able to identify individuals, but also the identification capabilities of potential subsequent recipients and other external actors, including cybercriminals. In the regions' view, the Guidelines should clarify how broadly the assessment must cover such actors and when less likely identification scenarios may be disregarded. They should also clarify the extent to which the assessment must take account of unintended identification resulting from accidents, negligence or changes in external circumstances

The regions acknowledge that the assessment and documentation of anonymity must address realistic means of identification and cannot be limited to the specific recipient's own technical resources. However, it is important that the applicable requirements must remain proportionate and practically manageable. Without further delineation, the requirement of controllers to identify every conceivable combination of external data sources, actors and possible future developments could make the framework difficult to apply in practice.

The regions therefore recommend that the Guidelines establish operational criteria for determining which categories of subsequent recipients and other external actors that should reasonably be included in the assessment, together with the documentation required for each stage of a potential identification chain. In particular, the Guidelines should distinguish realistic identification chains from hypothetical or less likely scenarios and clarify how far into the future, and how broadly, a controller is expected to conduct and document its assessment.

4.2. Ongoing reassessment

The Guidelines emphasise that anonymity is not necessarily a permanent characteristic of a dataset and that it is good practice to reassess the likelihood of re-identification on an ongoing basis. The regions recognise that technological advances, the emergence of new data sources and changes in access may mean that information previously considered anonymous must subsequently be regarded as personal data.

Although the Guidelines do not appear to impose an unconditional, continuous obligation, the regions understand the Guidelines to mean that ongoing reassessment of anonymity is relevant where the party concerned continues to process the anonymised information.

The regions recommend that the Guidelines clarify whether the original controller is expected to continue reassessing anonymity after disclosure to an independent controller, including where the disclosing controller no longer has access to or control over the disclosed dataset. The Guidelines should also describe the factors that should trigger a new assessment, such as significant technological advances, the publication of new data sources, personal data breaches, or changes in the use and accessibility of the dataset.

5. AI and technological developments

The regions welcome the Guidelines' recognition that the assessment of which means are reasonably likely to be used for identification requires consideration of both of current available technology and reasonably foreseeable technological developments.

At the same time, the regions request a more detailed explanation of how the Guidelines' approach to anonymisation applies to the secondary use of health data, research and the development of AI solutions. These areas offer considerable potential for socially beneficial uses of data, while the protection of individuals' information must be maintained.

In this connection, the regions refer to the findings presented in the article '*Large-scale online deanonymization with LLMs*'[1]. The article indicates that modern language models can combine information from multiple sources and thereby increase the risk of re-identification, even where direct identifiers have been removed. In the regions' view, these findings support the need for a cautious and forward-looking approach to anonymisation.

Among other things, the article illustrates that:

- assessments of the risk of re-identification increasingly need to take account of advanced AI tools,
- removing direct identifiers is not necessarily sufficient to achieve anonymisation,

[1] '*Large-scale online deanonymization with LLMs*', Swanson J, Lerman S, Aerni M, Paleka D, Carlini N & Tramèr F, 18 Februar 2026

- the No Linkage and No Inference criteria become increasingly important as technological capabilities for combining data develop, and
- free text, including health records and research data, may entail a greater risk of re-identification than previously assumed.

Against this background, the regions recommend that the Guidelines elaborate on how developments in AI should be taken into account in the assessment of anonymity, particularly in relation to health data and other datasets containing extensive free text. In particular, the Guidelines should provide a fuller description of how the risk of re-identification may change over time as a result of technological developments and how such changes affect the assessment of whether data may continue to be regarded as anonymous.

6. Aggregated data and datasets with mixed content

The regions welcomes the Guidelines' emphasis that aggregation does not necessarily mean that information has been anonymised. They also welcome the clarification that where a dataset contains a mix of personal data and information that may be regarded as anonymous, a differentiated approach cannot be taken; the entire dataset must be treated as containing personal data.

7. Need for more coherent and practical examples

The regions consider it important to clarify that the individual sections and assessment criteria in the Guidelines must be read together. Reading individual sections or examples in isolation may result in an incomplete assessment of anonymity, particularly because relevant parameters and nuances are introduced later in the Guidelines. The Guidelines should therefore emphasise more clearly that application of the No Record Isolation, No Linkage and No Inference criteria forms part of an overall assessment .

Although the Guidelines contain several illustrative examples, the regions consider that more in-depth and coherent examples from the health sector are needed to demonstrate how the No Record Isolation, No Linkage and No Inference criteria are applied in practice. The flowchart in Annex 1 could be used more actively by concluding the Guidelines with summary examples that take a specific dataset through every relevant stage of the anonymity assessment. This would reduce the risk of examples being read in isolation and enhance the practical applicability of the Guidelines.

8. Comments on selected sections of the Guidelines

8.1. Section 2.2 – Identifying the applicable perspective(s)

The regions note that the following wording in Example 4 may give rise to uncertainty: "A hospital transmits excerpts from patient records, which in and by themselves do not allow identification of the individuals [...]".

The wording may be understood to mean that it can be established solely on the basis of the information that it does not enable identification. In the regions' view, this does not appear to accord with the general approach of the Guidelines, under which a specific and contextual assessment must be conducted to determine whether the information constitutes personal data for the relevant party.

The regions therefore recommend that the example be reformulated and that similar isolated statements in the Guidelines, which may lead to erroneous conclusions, be avoided.

8.2. Section 2.4.2 – Means reasonably likely to be used

The regions consider it important for the Guidelines to clarify that an assumption that there is no motivation or interest in identifying the data subjects is not in itself sufficient for information to be considered anonymous.

In practice, there may be a tendency to attach importance to the fact that the information is not immediately considered to be of such interest or value to others. The regions agree that the assessment of anonymity cannot be based solely on a party's subjective intention.

8.3. Section 3.4.3 – No Inference

The regions consider the No Record Isolation, No Linkage and No Inference criteria useful as an overall framework for assessing anonymity. However, the criteria may be difficult to apply in practice without considerable technical expertise.

As regards the No Inference criterion, the regions see a need for a clearer distinction between legitimate statistical and research conclusions and inferences that in fact result in identification or the processing of personal data. For example, the Guidelines state that inferences relating to individuals may mean that data is no longer anonymous, even where the inferences are derived from aggregated datasets. The regions are concerned that this could unintentionally restrict opportunities for innovation, research and quality improvement in the health sector.