Commentary on EPDB Guidelines (02/2026) on Anonymisation

Jochem W. Rieger, Department of Psychology Carl von Ossietzky University, Oldenburg, Germany

Mireille M Sant, Department of Media, Communications & Technology Law, Faculty of Laws, University of Malta, Msida, Malta

Alexandros Karakasidis, Department of Applied Informatics, University of Macedonia / Athena RC, Greece

Cyril Pernet, Neurobiology Research Unit, Rigshospitalet & Dpt of Health Technology, Danmarks Tekniske Universitet, Denmark

Claude J. Bajada, Department of Physiology and Biochemistry, Faculty of Medicine and Surgery, University of Malta, Msida, Malta

Link to Guidelines 02/2026 on Anonymisation Version 1.0: here

General assessments 1
Suggestions for text improvements 3
A critique of the risk assessment criteria 4
Summary 9
Acknowledgments 12
Signatories for endorsement 12

General assessments

The document aims to provide guidelines for the assessment of the question whether and under what circumstances a data entry or a dataset may be considered anonymous.

The recommendations make laudable attempts to refine the definition of some terms like personal data, singling out and linkage to make them more suitable to the outlined risk assessment procedure. For example, in paragraph 18 of the draft Guidelines it is rightfully recognised that:

“It is not enough for information to simply relate to a natural person. For this information to be personal data, that natural person must also be identified or identifiable using means reasonably likely to be used. This is especially important where information is anonymised for research or analytical purposes, where the goal is often to have an anonymous dataset which lets you learn

something about the people in question (i.e. information which is still related to those individuals) but does so in a way that keeps their identities private (i.e. they are not identified or identifiable).”

These clarifications help to better operationalise some steps of the suggested risk assessment procedures.

We welcome the fact that, while the EDPB (and its institutional predecessor the Article 29 Working Party) previously employed strongly absolute or entity-independent language (Article 29 Working Party Opinion 05/2014; EDPB Guidelines 01/2025 on Pseudonymisation), following the Court of Justice’s judgment of 4 September 2025, the EDPB expressly reassessed its position, accepting the relative approach and incorporating it into these draft anonymisation guidelines.

The recognition of relative anonymity is particularly useful for scientific research (paragraphs 6-8). A research institution that generated the data may retain identifiable source records or other information enabling identification, while a receiving entity may lack means reasonably likely to identify the participants. The assessment should therefore specify for whom the data is intended to be anonymous; requiring anonymity for the originating controller in every case would unnecessarily limit the practical value of this approach. Further, the requirement for controllers to consider “anybody directly or indirectly receiving the data, including unauthorised and malicious actors” (which includes rogue employees) is an unreasonable standard and has the potential to practically void the possibility of relative anonymity. This arguably goes against the standard of the CJEU in the Breyer ruling.

The operationalization of the three-criterion framework is a welcome step towards a clearer and more usable assessment of anonymisation (paragraphs 3 and 52). Its value would be strengthened by presenting the decision rule prominently at the outset: passing all three criteria supports a finding of anonymity, whereas a failed criterion requires the further analysis described in section 3.5.3. In particular, record uniqueness should not be presented as an automatic finding that the data is personal. We will discuss the value of the three criteria for establishing anonymity in a separate section of our comments on the guidelines.

Paragraph 15 and Examples 3 and 4 have important implications for scientific collaboration. Where a recipient genuinely determines its own purposes and means, anonymity can be assessed from its applicable perspective; a processor acting on behalf of the originating controller is assessed by reference to that controller's perspective. This can make sharing between independent research controllers particularly relevant, but the roles must reflect the actual processing arrangements rather than a contractual label chosen to obtain an anonymity finding.

One major problem is that the text is structured and worded in a way that invites ambiguity and misunderstandings about the criteria relevant for the decision whether a dataset is anonymous or not. This problem starts already in the executive summary which states ‘a natural person is “identified or identifiable” if they can be distinguished from others’. Similar statements that suggest record isolation (singling out) as the criterion for the failure of anonymisation, i.e. unique

record -> identifiable personal data. The document should avoid such misinterpretations that can create the impression that the EDPB recommendations wants to go beyond court rulings. This is impression only resolved in the very last examples in section 3.5.2. where some positive examples are provided that are based on a GDPR compatible definition of failure of anonymisation.

Suggestions for text improvements

Generally, the document would greatly gain from improving clarity and logical consistency. In this section we provide some suggestions for improvement.

Provide a clear context first: One aim of the recommendations is to “clarify the notion of anonymous data and provide a practical framework for determining whether data has been successfully anonymised.” The challenge here is to ensure compatibility of the legal definition of ‘anonymous’ and ‘anonymisation’ with the technical processes carried out on data in practice. These Guidelines should seek to address a readership that goes beyond the legal community and indeed specifically connects with the scientific community who are expected to have recourse to them in the course of their data processing activities. The deductive approach the recommendations take is defendable in a scholarly context. However, in a more general context the introduction of new technical knowledge is best done with worked examples demonstrating the suggested processes. These are provided, but only after a long read at the end of the recommendations. In order to significantly improve clarity we strongly suggest to begin the recommendations with examples that demonstrate successful/unsuccessful anonymisation and then motivate the notion and the framework. This approach provides a clear anchor point on which later statements can be interpreted and disambiguated. Moreover, to provide examples informative and relevant for different fields the EDPB could work with people/bodies with domain knowledge like professional societies or EU COST Actions.

Distinguish technical from legal statements: Moreover, the text should distinguish more clearly between technical and legal statements. For example, in section “Whether the natural person is “identified or identifiable”” paragraph 19 reads: “To identify a natural person means to distinguish them from others within a given context, consequently making it possible to treat them differently from those other people.” This only makes sense as a technical statement that draws on the fact that if someone is identified then it is possible to distinguish them from others and to treat them differently. Similarly, in the same section para 22 states: “for information to be anonymous, the likelihood of the individual being successfully distinguished from others within the given context does not need to be zero”. This exemplifies the risk based approach but mixes in the technical fact that an identified person is distinguishable from others implies that this distinguishability is a sufficient condition for data to become personal under GDPR, i.e. distinguishable -> identifiable. This is at odds with the legal definition restated in paragraph 18 and would significantly extend the set of data falling under GDPR beyond the scope definition in the law.

Avoid the assumption that the ground truth about the data record is known before the anonymity assessment. Technically, the assertion that a singled out record that can be related to an identified natural person must be considered personal data is not granted. From

an attacker’s perspective there is still uncertainty about ground truth. For example, if the record contains noise or if the linking process went wrong. From a legal perspective it is still necessary to consider such a record as personal data. However, the recommendations do not make prescriptions of how data has to be classified, e.g. according to Article 4(1). Rather they serve as technical guidelines on how to relate a risk assessment procedures to the law. For clarity they should be clear about assumptions and clearly distinguish technical from legal statements.

Technical feasibility and realistic access. The discussion of means reasonably likely to be used could include a biomedical example distinguishing technical feasibility from realistic access (paragraphs 26 and 32-33). Matching research images against identifiable hospital records may be technically possible, while legal prohibitions and effective access restrictions may make the use of those records insignificant in practice for a particular recipient. This conclusion should be supported by the actual safeguards and reconsidered where there is concrete evidence of unlawful access, weak enforcement or previous breaches; neither technical feasibility alone nor a general reference to hospital regulation settles the assessment.

Probabilistic risk assessment. The guidelines provide a risk assessment framework for anonymisation breaches. Although “risk” can be conceptualized in different ways most concepts consider risk a a composite construct that includes the severity of adverse effects in addition to the probability of their occurrence. This a position taken in several recitals of GDPR (e.g 75, 76, 84, and 90). However, the guidelines appear to focus almost exclusively on the probability of an event. Although in practice a significant portion of data in question will require decisions based on statistical probabilities, the severity of adverse effects can vary largely. The guidelines would gain tremendously from providing examples of probabilistic risk assessment in the sense outlined in the Recitals.

Specific questions regarding research data

The guidelines would benefit from worked examples distinguishing open research-data release from controlled access (paragraphs 11-13 and 47-49). Open release requires consideration of a broad range of relevant entities and may make the simplified approach a practical starting point. Controlled access can support a more differentiated assessment of recipients and their available means.

Paragraph 34 is especially important for research data-use agreements. It is unclear whether a contractual prohibition on re-identification is not equivalent to a prohibition by law, and the guidelines state that contractual terms should complement technical measures. Research practice would benefit from examples showing how reliability, verifiability and enforce-ability can be demonstrated through access controls, monitoring, audit arrangements and credible consequences for breaches.

A critique of the risk assessment criteria

The definition of anonymous data builds on Recital 26 which states: “The principles of data protection should therefore not apply to anonymous information, **namely information which**

does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.” Anonymity follows from the logical negation of the definition of personal data in GDPR Article 4(1). Importantly, this allows the direct comparison of the set of data included in the GDPR with the set of data that is considered anonymous according to the EDPB recommendations by checking the complement. We appreciate that the recommendations aim to define a procedural strategy that allows for a safety margin. However, this margin must stay in limits. Inappropriate criteria and procedures that do not consider the context of a data controller can easily result in over inclusivity, inequality (e.g. due to resource limitations) and neglect of legitimate competing societal and research interest over individual rights. In the following we asses the three criteria from a technical perspective, namely their ability to provide information for anonymisation risk assessment.

The “**Record isolation**” or “**Singling out**” criterion outlined in 3.4.1 is considered as critical and in connection with the qualifier “**NO**” defined (section 3.4.1) as sufficient to fail anonymisation in the simplified approach. In the contextual approach it is taken as a criterion to start more detailed risk assessment. This approach has several problems.

- First, logically the “no record isolation” criterion together with the simplified approach establishes a classification criterion that is incompatible with the definition of the scope of the GDPR in Article 4(1). This combination establishes the criterion:
  record isolation -> potentially personal data
  whereas Article 4(1) and Recital 26 together establish the criterion:
  (Isolation AND link to an (identifiable OR identified) natural person) -> personal data
  This assessment path can be much more inclusive than the legal definition. But how inclusive would it be and does it provide meaningful information?
- Second, in all non-trivial data records that include continuous variables it is almost always possible to isolate any record. Therefore, the criterion “no record isolation” in combination with the simplified approach would classify all datasets including continuous variables as personal data although it remains unclear if this fact is informative .
- Third, the “no record isolation” criterion is only informative for the assessment process in an artificial setting in which the success of de-anonymisation can be evaluated based on a known ground truth. In practice, an attacker does not know the ground truth and successful isolation may in most cases not be informative for predicting the success of de-anonymisation, for example if record isolation is simply due to measurement noise.
- Fourth, for an attacker it is not necessary that a record is unique as long as valuable information can be linked to an identified natural person (see also example 12). This further illustrates the hidden assumption about ground truth knowledge in the evaluation of the scenarios.

Neuroimaging provides a useful worked example of the distinction between record uniqueness and identifiability. Many high-dimensional imaging records may fail No Record Isolation, but this alone does not establish that the corresponding person can be identified. Paragraph 99 and Example 24 explicitly allow a unique record to remain anonymous where singling out the

individual cannot be achieved and the other two criteria are met. This qualification should appear alongside paragraph 19 and the initial definition of No Record Isolation. It should also inform the critique above: the guidelines do not make record isolation an automatic failure of anonymisation, including under the simplified approach (paragraphs 52 and 97-100).

In conclusion, whether the record isolation or singling out criterion is failed will in most application cases likely neither provide logically necessary, nor sufficient information to assess the risk of re-identification of anonymised data. It may not even be relevant for the attacker. Therefore, it should be considered as a low efficiency screening criterion and as such treated with caution as it may trigger burdensome further analysis with high likelihood for datasets where record isolation is trivially common, even though the data may ultimately be anonymous. It appears to be mainly helpful in educational toy examples with simple record structures and under unrealistic assumptions about knowledge of an attacker. Given these limitations the qualification in paragraph 99/Example 24 should be more prominently placed alongside the initial definition of No Record Isolation to avoid misinterpretation. Moreover, its limitations and cases where its application is meaningful and valid should be clearly outlined. Otherwise, might create more burden than support for the re-identification risk assessment procedure.

We agree that linkage is generally accepted as an attack that may increase re-identification risk if the linked records contain complemental information. However, linking two records does neither determine whether they were recorded from the same natural person, nor does it necessarily determine the identity of the person. Similar points as for record isolation need to be considered:

- First, linkage works at the record level. Therefore, one must be cautious, what conclusions are possible. In general, the observation that two records can be linked does not necessarily mean that they can be related to an identified natural person. Thus, the criterion no linkage alone would establish a criterion incompatible with of the GDPR inclusion criterion in Article 4(1).
- Second, the crucial question is not if two records can be linked, this can always be done at some level of confidence (paragraph 64), even without the critical additional assumption that the linkage is correct. For realistic data including continuous variables with noise one may be able to define a probability for correct linkage if the ground truth is known (e.g. a test experiment or paragraph 62) but this probability may be hard or impossible to determine in practice and therefore guesses may become rather arbitrary.
- Third from an attacker perspective the ground truth is unknown and therefore even best linkage does not guarantee correct re-identification. Again, assumptions about knowledge of ground truth should be avoided when assessing re-identification risk.
- Fourth, the test for the criteria “specific and meaningful" test conflates epistemic (e.g. relates to a single identified or identifiable individual) and normative questions (“is the inference liable to affect the data subject's rights and interests). While questions about epistemic status can have an objective answer, answers normative questions are subject to many factors ranging from subjective to societal expectations. Moreover, it is not clear how the four criteria stated should be logically connected. Do they all have to be met or only some to trigger the No linkage criterion?

- Fifth, we appreciate that the guidelines add here a weighting of the anticipated effects on the data subjects’ rights and interests. However, what is meant by that appears underspecified. Examples would help here. Is it sufficient if knowledge about a data subjects’ preference for coffee over tea can be obtained? Or, does this fail the “meaningful” requirement for linkage?
- Sixth the No Linkage criterion requires knowledge of other datasets, which may be impossible to gather exhaustively in practice. This can trigger an open ended search without a clearly defined criterion to stop the search. Without further clarification this requirement of knowledge poses the risk that the risk assessment fails under both, the simplified and the contextual approach.

From these considerations we conclude that the cruical feature for linkage is that it is “meaningful”. However, this feature includes is better developed in the next criterion. “No linkage” alone cannot logically serve as a criterion to assess the risk of re-identification of anonymised data. It at least requires that the link to an identifiable natural person can be established (paragraph 101). Whether this link was established must be evaluated from the attacker perspective who likely has no knowledge about ground truth.

In sum, No Linkage is not sufficient on its own to assess re-identification risk; it must be combined with the additional step of determining whether linked data leads to identifiability of a natural person. On order to improve clarity of the guidelines, the qualification stated in paragraph 101 should be more prominently placed alongside the initial definition of No Linkage to avoid misinterpretation. When used as a decision criterion in the simple approach it bears the risk of extending the set of data considered personal significantly beyond the legal definition and rulings, potentially without any true benefit. When used as a screening criterion it bears a high risk of triggering additional burdensome analyses. This risk can turn almost into certainty in frequent cases where a criterion guaranteeing the objective correctness of linkage cannot be established. Therefore, its limitations and cases where its application is meaningful and valid should be clearly outlined. Importantly, it should be clearly stated that performing linkage (paragraph 64) and establishing its correctness (paragraph 60) as well as meaningfulness (paragraph 101) are separate questions. Otherwise, and similar to the No record Isolation criterion, No Linkage might create more burden for the controller than support for the re-identification risk assessment procedure.

We agree that **inference** is the critical step in the process of re-identification. It requires detailed considerations regarding what counts as re-identification of anonymised data. Here the recommendations seems to have to problems and inconsistencies.

- First, according to example 22 a record that can be isolated can be considered anonymous as long as it cannot be linked to an identified natural person. This example appears to provide the full reasoning: *(Isolation AND link to an (identifiable OR identified) natural person) -> personal data*. This type of inference is supported by court rulings and GDPR Article 4(1). Unclear, examples (e.g. 5 & 6) and statements using a different definition (e.g. paragraph 25) should be avoided.

- Second, it is important to distinguish between record and natural person. Example 5 in section 2.4.1 is only about records. The statement “ “the person in a black suit who is also walking a dog” only refers to the dataset of records represented by the image. If the photograph is showing the person from back or only partly, it may not be linkable to a natural person. Similarly, example 6 suggests that “fingerprinting” data records that are sufficiently unique should be considered personal data. Both examples come with the problems discussed in the section on record isolation and only support the probabilistic inference *record isolation-> potentially personal data*.
- Third, such ambiguities in the text are non trivial and create significant uncertainty and tension with data processing needs in non-commercial areas that are in the public interest and/or the freedom of scientific research. The latter often have less resources or DPOs with the necessary domain knowledge for complex risk assessment approaches based no vague criteria. They are therefore disadvantaged with recommendations of overly inclusive criteria for inference targeted at commercial actors with significantly more resources to cope with such recommendations.
- Fourth, all inference on non-trivial datasets is probabilistic. In the suggested reasoning (e.g. footnote 41, sections 2.3 and 2.4) the observed record must be considered probabilistic. The update of the reasoning must consider the likelihood of the new data given the current belief, not only the probability new data. The latter would be a classical reasoning error that can result in a vast overestimation of risk, in particular when a critical observation has a low base rate.
- Fifth, given the probabilistic nature of the data, further clarification is necessary how “meaningful” inference (particularly unclear are here paras 69-72 and examples 13 and 14), “significance”, and “reasonably likely” can be operationalised in practice beyond simplified examples and overly generalized language.
- Sixth, the No Inference criterion directly puts personal data protection in conflict with other important values. Inferences about individuals are at the heart of biomedical and basic scientific research, and can provide information for society oriented services provided by public/governmental institutions for the good of society. Paragraph 18 acknowledges that the processing of anonymised data “[...] is especially important [..] for research or analytical purposes, where the goal is often to have an anonymous dataset which lets you learn something about the people in question“. Thus the “no inference” criterion is contrast to research and societal interest. However, the guidelines seem to distinguish between goals of inference. We appreciate this but legitimate goals must be made clearer and should be judged outside of GDPR realm. This is particularly important because the use or human data for research is still not well regulated in most EU countries and the recently published EDP recommendations on the use of personal data in scientific research mainly cover the exemptions for data falling under GDPR.
- For neuroimaging, appropriate sampling and careful treatment of demographic information may help avoid disclosing participant-specific attributes, but they do not by themselves establish No Inference. The assessment should consider whether knowledge of recruitment, cohort membership or selection criteria, together with the released data and available external information, supports a specific and meaningful inference about an identified or identifiable person. Paragraph 67 concerns personal

information generally, not only sensitive attributes, and distinguishes such inferences from general knowledge about a population. A worked research example should make that distinction explicit and explain how sampling affects the result.

- Taken together, paragraph 99 and Example 24 provide a promising basis for assessing some neuroimaging data, particularly derived outputs, as anonymous for specified recipients despite unique records. This remains a case-specific conclusion: adequate handling of demographics and sampling must be accompanied by evidence that the individual cannot be singled out through means reasonably likely to be used and that No Linkage and No Inference are satisfied. An example applying these steps to imaging derivatives would make the guidelines substantially more useful for research without suggesting that either all brain data are identifiable or all derived brain data are anonymous.

In sum, No Inference on the level of the record alone is not sufficient on its own to assess re-identification risk; it must be combined with the additional step of determining whether the inference leads to identifiability of a natural person. Over inclusive suggestions like taking fingerprinting as a criterion for personal data suggest that record isolation is sufficient to consider data as personal. While the motivation for such an approach might be understandable in some commercial or intelligence application domains, it would create a severe hurdle in other domains of public interest and research. It would be of utmost importance to consider the weighting of interests mentioned in paragraph 1 in the text instead of focusing exclusively on the protection of personal data. Furthermore, conceptual ambiguities in the text blurring the borders between the record level and the level of the identifiable natural person should be avoided and this relevant distinction needs to be clearly made early in the text. In a similar line key terminology (meaningful, significant, reasonably likely etc) should be defined in a way that makes them better operationalisable and less subjective. Worked examples from different domains can contribute to this. Finally, the attack likelihood should be explicitly stated as part of the contextual approach in order to avoid overly cautious and burdensome evaluation procedures that may prevent processing for societal or research purposes where an identification attack is highly unlikely.

Summary

We thank the EPDB for the opportunity to comment on the 02/2026 Guidelines on Anonymisation. While we genuinely welcome the significant progress these guidelines represent. Particularly the recognition of relative anonymity following the CJEU's 2025 ruling, the refined definitions of key terms, and the operationalisation of the three-criterion framework. However, we have serious concerns that the current draft could inadvertently extend the scope of what counts as personal data well beyond the legal definition in GDPR Article 4(1) and Recital 26. Our core worry is that the guidelines blur the crucial distinction between the record level (what can be isolated, linked, or inferred in a dataset) and the level of the identifiable natural person (whether a real individual can actually be identified). This conflation, combined with an over-reliance on record-level criteria that assume knowledge of ground truth can introduce open end research, risks creating overly inclusive and burdensome assessment procedures that may disproportionately disadvantage research and public-interest data

processing — exactly the domains the guidelines themselves acknowledge as important beneficiaries of anonymisation.

Our core suggestions are:

General / Structural:

- Begin with worked examples: Start the guidelines with concrete examples of successful/unsuccessful anonymisation to anchor later statements and disambiguate interpretations. Ideally these would be developed with domain experts.
- Distinguish technical from legal statements — clearly separate technical observations (e.g., "identify means to distinguish") from legal requirements (e.g., Article 4(1) identifiability), avoiding statements that imply distinguishability alone is sufficient for personal data.
- Avoid ground-truth assumptions — be explicit that attackers do not know ground truth and their inferences are often probabilistic, e.g. Due to noise, and likely include erroneous inference.
- Incorporate severity into risk assessment in order to align with GDPR Recitals 75, 76, 84, 90 by treating risk as a composite of probability and severity, and provide examples of probabilistic risk assessment.

No Record Isolation:

- Place the paragraph 99/Example 24 qualification prominently alongside the initial definition of No Record Isolation to ensure that unique records are not misread as automatically personal.
- Acknowledge the criterion's limitations because for high-dimensional/continuous data, record isolation is trivially common. Outline cases where the criterion is meaningful and valid as well as where it is not.
- Treat it as a low-efficiency screening criterion rather than a decision criterion.

No Linkage:

- Place the paragraph 101 qualification prominently alongside the initial definition of No Linkage, clarifying that linkage must lead to identifiability of a natural person.
- Clearly separate the three tasks: performing linkage (paragraph 64), establishing its correctness (paragraph 60), and establishing its meaningfulness (paragraph 101). They are distinct and should be treated as such.
- Clarify the "specific and meaningful" test. It conflates epistemic and normative questions. Also clarify the logical connection between the four criteria and provide examples of what counts as "meaningful."

- Address the open-ended search problem originating from the requirement to know all potentially (present and future) linkable external datasets. Because this is practically impossible provide a clearly defined stopping criterion.

No Inference:

- Avoid record/person conflation like in examples 5 and 6. They treat record uniqueness as sufficient for identifiability. Clearly state from the begin, that a unique record does not necessarily mean a natural person can be identified.
- Clearly state that inference on non-trivial data is probabilistic and Include Bayesian reasoning that considers posterior probabilities and base rates, not just the likelihood of the data.
- Operationalise key terms like "meaningful," "significant," and "reasonably likely" in ways that are less subjective and more applicable in practice. Provide worked examples from different domains.
- Acknowledge the tension between data protection and research/societal interests (as paragraph 1 and paragraph 18 do). Make legitimate goals clearer and considers including examples for this tensions and how this may impact the suggested approach.
- The CJEU has held that a means of identifying the data subject is not reasonably likely to be used where the risk of identification appears in reality to be insignificant, in that the identification of that data subject is prohibited by law or impossible in practice (see, to that effect, judgment of 7 March 2024, OC v Commission, C-479/22 P, EU:C:2024:215, paragraph 51 and the case-law cited). Therefore the contextual approach should not need to include explicit consideration of whether an attack is likely to occur at all provided appropriate security measures are in place, to avoid overly cautious procedures that may prevent legitimate research.

Research-Specific:

- Provide worked examples for open vs. controlled access and distinguish open research-data release from controlled access in the assessment.
- Clarify contractual prohibitions and provide examples how reliability, verifiability, and enforceability can be demonstrated.
- Add a worked example demonstrating how sampling data and demographic handling affect No Inference, and how paragraph 99/Example 24 can apply to data like derived neuroimaging outputs.

Simplified and Contextual Approach

- Reconsider the simplified approach. Inefficient criteria can make it over inclusive without good justification on realistic datasets.
- Redesign and clarify crucial steps of the contextual approach to make it manageable for institutions with limited resources available and to avoid introducing discrimination.
- Remove vague and subjective criteria as much as possible from the contextual approach. When this is not possible try to add clarifying examples.
- Add examples performing the approaches on realistic real world data rather than unrealistically simple datasets.

Sincerely,

The authors

Acknowledgments

MMS and CJB are supported by the University of Malta Data Integrity and Stewardship Cluster (DISC)

JWR was supported by DFG Device Center 184/261-1

All authors form part of Cost Action CA24161 - Improving Neuroimaging Data for Sharing (INDoS)

Signatories for endorsement

Daniel Margulies	University of Oxford
Mehmet Akif Özçoban	Gaziantep University
Xhilda Dhamo	University of Tirana
Ruiqing Ni	
Panagiotis Alexiou	University of Malta
Paola Galdi	Cancer Research UK Scotland Institute
Marco Aiello	IRCCS SYNLAB SDN, Naples, Italy
Carmel J. Caruana	University of Malta
Marek Bundzel	Technical University in Kosice, Slovakia
Mikkel C. Vinding	University of Copenhagen
Jorge F. Bosch-Bayard	Carl von Ossietzky Universität Oldenburg, Faculty of Psychology
Maximilien Chaumon	Paris Brain Institute
Anđela Šoškić	University of Belgrade
Jordan Lee Gauci	University of Malta
Sephora Galea	University of Malta
Alexandra Reichenbach	Heilbronn University
João Miguel Alves Ferreira	University of Coimbra
Javier Marta-Moreno	IIS-Aragon. Grupo de Neurociencias; Spain
Sergiu Nisioi	University of Bucharest
Gabriela Mariana Marcu	Lucian Blaga University of Sibiu

Timo Kvmme	omputational Neuroimaging Lab, Biobizkaia Health Research Institute, Barakaldo, Spain
Melanie Ganz-Benjaminsen	University of Copenhagen
Karam Sidaros	Danish Research Centre for Magnetic Resonance
Jan Petr	Helmholtz-Zentrum Dresden Rossendorf
Barbara Strasser-Kirchweger	University of Salzburg
Andrea Vranic	Department of Psychology, University of Zagreb
Rebecca Jackson	University of York, UK
Alex Wade	University of York
Daniele Marinazzo	Ghent University