Oct 30, 2026

Anu Talus, J.D.
Chair, European Data Protection Board
Re: Public Consultation: Guidelines 02/2026 on Anonymisation
Via electronic filing
(<https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en>)

Dear Ms. Talus,

We welcome the EDPB's effort to clarify the requirements for anonymisation under the GDPR through the proposed guidelines.

We have spent much of our careers studying data privacy protection. This comment reflects our evaluation of the current state of research and practice in information privacy protection and draws specifically on our prior research on these topics [1-8].

As researchers in computer science, cryptography, statistics, and information science, we focus our comments on three structural areas of the framework that are central to our expertise and the guidelines' goals. We focus on recommendations to enable reliable, systematic, and effective privacy protection. We note generally that corresponding changes are also needed in other portions of the guidelines -- including the examples -- for consistency with the proposed changes.

Anonymisation is a consequence of how data is processed.

Information theory teaches that the information contained in any output or communication, and what can be learned from it, depends on the process that produces it. In particular, it depends on the informational relationship the process creates between its input and output. One consequence of this fundamental rule is that effective anonymization, and privacy more broadly, depends on controlling how data is processed. It cannot be determined merely by checking the output [1,2,5].

The Guidelines focus primarily on properties of the "given data", namely the output of an anonymisation process. However, anonymisation cannot be assessed based on the given data alone.

The Guidelines recognize this critical point in its description of the No Inference criterion: "Inferences may be based on the given data and/or on additional information, *including information about the anonymisation process*." This principle applies to all aspects of identifiability, including singling out and linkage.

We recommend adding the following language after paragraph 7.

> Whether the information relates to a natural person depends on the relationship between the given data, the source data, and the anonymisation process. Therefore, properties of the given data alone are typically insufficient to support a finding of anonymisation. Relevant factors of the procedure, including any data-dependent decisions, must be included in the assessment (e.g., criteria for grouping, generalizing, or suppressing attributes, and selecting attributes).

"No Record Isolation" does not prevent singling out

A less obvious consequence of the fundamental role of processing, is that the premise of the No Record Isolation criterion is false. No Record Isolation (as defined in the guidelines) does *not* prevent singling out. Even if the given data contains no unique records -- satisfying No Record Isolation -- it may be possible to use the given data and information about the anonymisation process to single out an individual uniquely within the source data or even within the population [3, 7, 6].

We recommend that the guidelines shift their focus from isolated records in the output to singled-out persons *in the source data*. The risk of singling out should be measured against an appropriate baseline, taking into account the anonymisation method and prior information about the relevant population or context [3, 7, 8].

Anonymisation must provide durable publication-ready protection

Absent another law restricting its use, anonymised data may be freely shared and used without further restriction. For the GDPR to effectively protect data subjects, anonymisation must provide durable protection in the face of long-term, repeated, and widespread sharing and reuse.

We recommend adding the following to the Guidelines.

> It is presumed that every third party that could possibly receive the anonymised data eventually will. A controller may rebut this presumption and rely on the contextual approach to exclude particular recipients only where legal or other protections (i) will persist regardless of the future context within which the given data is used, and (ii) provide minimal risk of the release ever reaching entities beyond those considered in the analysis. Absent such protections, the default assumption should be that the release may reach any recipient.

Moreover, multiple releases of data relating to the same person increase identification risk. We recommend adding the following to the Guidelines.

> Determinations of anonymisation should limit not only the incremental risk from the release, but the accumulated risk of the data subject being identified, and the potential for subsequent harm.

Effective data protection is founded on rigorous scientific and technical analysis.

The proposed Guidelines do not distinguish between a controller's inability to identify vulnerabilities and a scientifically and technically justified assessment that relevant vulnerabilities are absent, and protections are reliable.

A lack of known attacks should not, by itself, be treated as sufficient evidence that no vulnerability exists now or may soon appear. Because computing technology advances rapidly, data protections that rely on outdated methods, obscurity, or heuristics, many of which are in common use, have failed dramatically or are likely to fail soon. Reliable protection requires a rigorous scientific foundation and systematic technical analysis [1,2,7].

We recommend clarifying that the assessment should be proportionate to the risks and supported by appropriate technical expertise, transparent documentation, rigorous methods, and, where warranted, independent testing.

Sincerely,

Micah Altman, Research Scientist, Massachusetts Institute of Technology
Aloni Cohen, Assistant Professor of Computer Science and Data Science, University of Chicago
Kobbi Nissim, Professor of Computer Science, Georgetown University, Affiliate Professor of Law, Georgetown Law

References

[1] Altman, M., Cohen, A. and Nissim, K., 2024. ACM TechBrief: Data Privacy Protection. ACM. <https://dl.acm.org/doi/book/10.1145/3679004>

[2] Cohen, Aloni, Micah Altman, Francesca Falzon, Evangelina Anna Markatou, and Kobbi Nissim. "Properties of Effective Information Anonymity Regulations." arXiv preprint arXiv:2408.14740 (2024). <https://arxiv.org/abs/2408.14740>

[3] Cohen A, Nissim K. Towards formalizing the GDPR's notion of singling out. Proceedings of the National Academy of Sciences. 2020 Apr 14;117(15):8344-52. <https://www.pnas.org/doi/10.1073/pnas.1914598117>

[4] Fluitt A, Cohen A, Altman M, Nissim K, Viljoen S, Wood A. Data protection's composition problem. European Data Protection Law Review (EDPL). 2019 Sep 9;5(3). <https://edpl.lexxion.eu/article/EDPL/2019/3/4>

[5] Wood, Alexandra, Micah Altman, Kobbi Nissim, and Salil Vadhan. 2022. “Designing Access with Differential Privacy.” In: Cole, Dhaliwal, Sautmann, and Vilhuber (eds), Handbook on Using Administrative Data for Research and Evidence-based Policy, J-PAL. < https://admindatahandbook.mit.edu/book/v1.1/diffpriv.html >

[6] Cohen, Aloni: "Attacks on Deidentification's Defenses." USENIX Security Symposium 2022: 1469-1486 <https://www.usenix.org/conference/usenixsecurity22/presentation/cohen >

[7] Altman, Micah, Cohen, Aloni, Nissim, Kobbi and Wood, Alexandra. “What a hybrid legal-technical analysis teaches us about privacy regulation: The case of singling out.” BUJ Sci. & Tech. L. 27, 1. <https://www.bu.edu/jostl/archives/vol-27-1-winter-2021/>

[8] Cohen, Edith, Kaplan, Haim, Mansour, Yishay, Moran, Shay, Nissim, Kobbi, Stemmer, Uri, and Tsfadia, Eliad. Data Reconstruction: When You See It and When You Don't. ITCS 2025: 39:1-39:23 <https://doi.org/10.4230/LIPIcs.ITCS.2025.39>