Summary page:
TEHDAS2 public consultation on Draft guideline for Health Data Access Bodies on data minimisation, pseudonymisation, anonymisation and synthetic data

This consultation has 4 pages and 25 questions. The first and the second pages are common to all TEHDAS2 public consultations and cover demography of the responder and overall quality of the document. Pages 3 and 4 consist of questions specific to this document.

Demography

1. Country *

Belgium

2. Type of responder *

Other
European Doctors

3. Are you responding on behalf of several organisations? *

If yes: On behalf of how many organisations?

No

4. Sector *

Health care provider

5. Organisation size *

Not applicable / Individual citizen

6. Professional role / function

Senior Policy Advisor

Quality

7. Is the document easy to understand? *

3

8. How well does the document address the key issues related to its subject matter? *

4

9. How feasible do you find the guidelines or technical specifications to implement, as outlined in the document? *

3

10. Generic feedback

Do you have any suggestions for improving the document? Are there any additional topics or areas that should be covered? Max. 5000 characters.

EHDS will impose heavy burdens on small healthcare entities, considered to be health data holders. The obligatons to make data available as being described in this document, the regular communication required with HDABs and, in some cases, the need to be involved in negotiations with the applicant on mediation between study objectives and data minimisation requirements, can represent a significant administrative burden for smaller enterprises, that operate with relatively limited resources and rely on revenue-generating, patient-oriented activities. Despite these obvious adminsitrative burden, exemptions are limited to microenterprises, possibly also general practitioners' offices and contracted specialists, but still to be decided by national law.

See also 1.6.1, for comments on health data intermediation entities.

As is already stated on page 5, this document was written before the judgement in the case EDPS vs SRB (4 September 2025). We assume that the consequences of this judgement by the Court of Justice of the EU, for the concepts of pseudonymization and anonymization, will be covered in the final version.

Furthermore, the guideline gives good examples of pseudonymization techniques and best practices that can be applied (par. 4.4). However, we wonder whether a technique like Multi Party Computation should not also be mentioned and explained?

A reference to the Digital Omnibus should be made and a brief analysis of the possible risks/impact it brings to the EHDS Regulation due to the amendments of the GDPR Regulation.

In relation to Q7 (document easy to understand), we would like to specify that for doctors rate is 1 (very low); for lawyers rate is 3 (high)

The following questions are specific for TEHDAS2 draft guideline for Health Data Access Bodies on data minimisation, pseudonymisation, anonymisation and synthetic data

Part 1: General questions

11. What are you representing, according to the definition of the EHDS Regulation? *

(Trusted) data holder

12. From your perspective, how well does the guideline provide practical and actionable guidance for HDABs, data holders and data users regarding safe and secure processing of electronic health data within the EHDS?

2

Please elaborate on any areas where the guidance could be made more practical or actionable.
Max. 5000 characters.

The guideline is very theoretical, and could focus more on concrete examples (practical tools) of measures to take. However, the examples of applicable tools for anonymisation and generating synthetic data (in par. 7.5.5) are very helpful.
Please provide more examples on how to pseudonymise, anonymise, etc.

13. Are there any critical aspects or challenges regarding data minimisation, pseudonymisation, anonymisation, or synthetic data generation within the EHDS that you believe are not sufficiently addressed in the guideline?

Max. 5000 characters.

See response to Q,10 regarding the case EDPS vs SRB C-413/23 P.

14. To what extent do the guidelines offer clear and harmonised approaches for implementing the EHDS regulation's requirements concerning data minimisation, pseudonymisation, anonymisation, and synthetic data across Member States?

3

What improvements would you suggest to enhance the overall clarity, comprehensiveness, and practical applicability of the guideline (i.e., specific sections, terms or concepts)?
Max. 5000 characters.

Enhance clarity where the guideline deals with technical aspects, so that the text is better understandable for non-technicians.

15. From your professional perspective, do you currently have the technical and organisational capacity to implement the recommendations (e.g., tools for data protection risk assessment, synthetic data generation)?

1

What capacity gaps or resource needs would require support?
Max. 5000 characters.

More examples of practical tools and techniques.

Part 2: Data minimisation

16. Does the guideline clarify when and by whom data minimisation should be performed throughout the data lifecycle (data collection, application assessment, data processing and result export)?

4

Do you have suggestions for improving clarity on roles and timings?
Max. 5000 characters.

Data minimisation must be applied during data collection and preparation, and the principle applies equally to data holders, as data holders are deemed controllers for the initial processing and provision of data to the HDABs. In order to avoid a disproportionate burden, natural persons and microenterprises should be exempted from the obligations on data holders. In case that does not apply at national level, for example general practitioners' offices and contracted specialists are often to be considered microenterprises, in order to reduce the administrative burden, Member States should be able to require in national law that health data intermediation entities carry out the duties of certain categories of data holders. Such entities should be able to process, make available, register, provide, restrict access to and exchange electronic health data for secondary use. For instance, a Member State might designate a public sector body managing a centralised electronic patient file as a health data intermediation entity. Member States can designate multiple health data intermediation entities. The data shall nevertheless be considered as being made available by several health data holders.
Such health data intermediation entities are not mentioned in the guideline. As the entities are meant to carry out the duties of certain categories of health data holders, it would be of use if their role and responsibility was explained in the guideline – as far as possible, or as examples, seeing this is a possibility for Member States to make regulations in their national law.

17. How practical are the recommendations for identifying and managing direct and indirect/quasi-identifiers in line with data minimisation principles, particularly regarding the trade-off between reducing privacy risks and maintaining data utility?

3

Please provide examples of challenges or alternative approaches for managing indirect/quasi-identifiers:
Max. 5000 characters.

No answers

18. Does the detailed examination of the five dimensions of data provision ("Who," "What," "When," "Where," "How") provide sufficient guidance for data users and HDABs in preparing and assessing data permit/request applications to ensure data minimisation?

3

Are there any dimensions that require more elaboration or specific examples?
Max. 5000 characters.

No suggestions

Part 3: Pseudonymisation

19. Are the described purposes and goals for processing pseudonymised data within the EHDS clearly articulated and comprehensive?

4

Are there any additional purposes or challenges of pseudonymisation that should be highlighted?
Max. 5000 characters.

Yes, by describing what the consequences of the judgement in the case EDPS vs SRB (4 September 2025) are in this context.

20. Does the guideline provide adequate detail and recommendations on the practical implementation of pseudonymisation transformations?

3

What are the main practical challenges you foresee in implementing these recommendations, and what further guidance would be helpful?
Max. 5000 characters.

A practical challenge might be deciding what pseudonymization technique to choose in a specific situation. The overview of techniques and best practices in par. 4.4 is helpful for that. However, we wonder whether a technique like Multi Party Computation should also be mentioned and explained?

21. s the guidance on pseudonymisation across the different phases of the EHDS user journey (data discovery, access application, data preparation, data processing, and finalisation) clear and actionable for relevant actors (data holders, HDABs, data users)?

3

Are there any stages where the responsibilities or procedures related to pseudonymisation need further clarification?
Max. 5000 characters.

No answers

22. Are there further ambiguities in the pseudonymisation section that should be addressed regarding the recent judgement of the Court of Justice of the EU in the case EDPS vs SRB (C-413/23 P)?

Max. 5000 characters.

Yes. Please pay attention to the conditions formulated by the Court of Justice to determine when pseudonymised data can be considered anonymous or not.
In the case, the court assessed whether pseudonymised data, transferred by an EU authority to an external service provider, are to be considered "personal data" within the meaning of Regulation (EU) 2018/1725 (which is equivalent to the GDPR for EU institutions).
Whenever the provisions of this Regulation follow the same principles as the provisions of Regulation (EU) 2016/679 (GDPR), those two sets of provisions should, under the case law of the CJEU, be interpreted homogeneously. Therefore, the clarification delivered in the judgment is also relevant to GDPR.
The definition of, inter alia, 'personal data' in GDPR applies for the purposes of EHDS, cf. Article 2.
The court states that pseudonymisation may have an impact on whether or not data are personal within the meaning of Article 3(1) of Regulation 2018/1725, provided that technical and organisational measures are actually put in place and are such as to prevent the data in question from being attributed to the data subject, in such a way that the data subject is not or is no longer identifiable. Pseudonymised data are not necessarily personal data if the pseudonymisation effectively prevents anyone other than the controller from identifying the data subject.
In order to determine whether a natural person is identifiable, account should be taken of 'all the means reasonably likely' to be used by the controller or by 'another person' to identify the natural person 'directly or indirectly'. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as personal data. The court states 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.
Natural persons shall have the right to opt out at any time, and without providing any reason, from the processing of personal electronic health data relating to them for secondary use under EHDS, cf. article 71.
'Personal electronic health data' means data concerning health and genetic data, processed in an electronic form, whereas 'non-personal electronic health data' means electronic health data other than personal electronic health data, including both data that have been anonymised so that they no longer relate to an identified or identifiable natural person (the 'data subject') and data that have never related to a data subject.

EDPS vs SRB C-413/23 P will affect the right of the data subject to opt out from the processing of their data for secondary use under EHDS, if the data in some cases no longer will be considered 'personal data'. It would then no longer fall within the wording of EHDS Article 71. The judgment's significance for the interpretation of the EHDS is expected to be clarified.

Secondary use shall of course be transparent, and natural persons must be made aware and understand whether their data are being made available for such use.

Part 4: Anonymisation and synthetic data generation

23. Does the guideline adequately describe how anonymisation and synthetic data generation can be applied within the EHDS?

2

Please elaborate:
Max. 5000 characters.

[The description of how anonymisation and synthetic data can be applied is quite technical. Therefore, probably better to understand for technicians than for doctors, or lawyers. However, this chapter is also of importance for data users, like doctors doing scientific research.]

24. How clear and applicable are the proposed use cases (Table 2) and the high-level architecture (Figure 6) for implementing anonymisation, synthetic data generation, and privacy risk assessment within the EHDS framework?

3

Do you have additional examples of use cases where anonymisation or synthetic data might be relevant?
Max. 5000 characters.

No answers

Are there specific use cases or architectural components that require more detailed explanation or examples?
Max. 5000 characters.

No answers

25. How effectively do the guidelines address the requirements for documentation of anonymisation/synthetic data generation, privacy risk assessment, and tooling recommendations for supporting these processes?

2

What specific suggestions do you have for improving these areas?

No answers