Summary page:
TEHDAS2 public consultation on draft technical specification for Health Data Access Bodies on the implementation of secure processing environments

This consultation has 3 pages and 19 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. Page 3 consists of questions specific to this document.

Demography

1. Country *

Netherlands

2. Type of responder *

Other
non profit foundation

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

If yes: On behalf of how many organisations?

No

4. Sector *

Other
health data research infrastructure

5. Organisation size *

Small to medium enterprise (10–249 employees)

6. Professional role / function

No answers

Quality

7. Is the document easy to understand? *

2

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

2

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.

The implementability of the guidelines constitutes a significant concern. It is essential that, at the outset, the workflow of the “data journey” can at least be executed end-to-end in a minimal form. This should then gradually evolve from a basic process into an increasingly comprehensive one. Accordingly, it is not advisable to attempt to regulate and operationalise all details from the very beginning through implementing acts. Instead, a learning-by-doing approach should be adopted.At the same time, a critical challenge lies in preventing the creation of excessive discretionary space for Member States to establish divergent national legislative arrangements (as illustrated by the shortcomings experienced under the GDPR). Therefore, particularly in the initial phase, a learning and growth perspective should be applied, combined with clearly defined, directly implementable requirements per phase regarding the HOW, which do not allow for differing interpretations or implementations across Member States.

Each guideline should be designed to incorporate an iterative learning and development trajectory. In this context, implementation should commence with a limited scope, including a reduced set of mandatory fields and/or requirements, while, at the same time, establishing predefined timelines at which additional obligations will be introduced, without predetermining in advance the specific nature of those future obligations. Each implementation phase should serve as a basis for evaluation, on the grounds of which decisions shall be taken as to the introduction of further mandatory elements in subsequent phases.

The guidelines set out in Chapter 4 are largely drafted from a cohort- and research-oriented perspective. Since the data in question predominantly originate from the healthcare sector, the guidelines should also be formulated from a clinical care perspective. Accordingly, in addition to research expertise, the appropriate (clinical) expertise should be duly involved in the development of the substantive guidelines, including expertise relating to Chapters 2 and 3 of the EHDS.
Each guideline should include cross-references to other relevant guidelines and should also contain explicit references to Chapters 2 and 3 of the EHDS. At present, the overall coherence between the guidelines is insufficiently ensured, and the timelines and processes for input and consultation meetings are, in some cases, (too) short. Moreover, there are significant differences in the level of detail, with some guidelines being highly high-level, while others are detailed and technical. In certain instances, the substantive content is also not fully aligned across the documents. The inclusion of an overall reader’s guide for the full set of documents would improve accessibility and usability; in addition, attention should be given to ensuring consistent terminology and a uniform roles and responsibilities model.

In the development of the TEHDAS2 documentation, which describes the full process of data application, data discovery and related procedures, it has been observed that the documentation is largely drafted from the perspective of a centralised analysis

environment. Insufficient clarity is provided regarding the concept of federated analytics, its implications (for example, the requirement that permits must also be capable of being ‘controlled’ by data stations), as well as the respective advantages and disadvantages of centralised versus federated approaches.

Restructure the document to increase readability, give context to requirements.

Add a more detailed description of both the processes that SPE should support and the interaction with other business capabilities (especially DAAMS).

Describe roles and responsibilities in relation to the “trusting” and “distrusting” use cases, i.e. for SPEs operated by HDAB, a data preparation environment and SPEs operated by third parties.

Make a clear distinction between requirements that follow from EHDS and other best practice frameworks and policy decisions that still need to be taken. For example, what is the position of EC on sovereign cloud?

Add a clear recommendation around what HDABs should offer in terms of federation SPEs rather than setting strict technical requirements. For example: should an implementation act require at least one per member state?

Hospitals must comply with a wide range of national and sectoral standards (e.g., ISO 27001 for information security, MDR/IVDR for medical devices, GDPR). The risk of conflicting, duplicative, or mutually incompatible compliance requirements is real.

We recommend that the specification explicitly maps EHDS/SPE requirements to existing frameworks, clarifies “compensatory controls” where possible, and offers illustrative compliance matrices. This will prevent redundant work and conflicting obligations.

The following questions are specific for TEHDAS2 draft technical specification for Health Data Access Bodies on the implementation of secure processing environments

11. What is your primary role in relation to SPEs? *

Other

12. If you are an SPE user, what best describes your experience with them?

Not applicable

13. What are your thoughts on the terminology used in the document? Is it clear and appropriate for the context? Please explain your answer.

Max. 5000 characters.

Even for experts, the document was hard to follow. Therefore, the terminology should be aimed at a wider audience.

14. How would you rate the functional requirements in Section 4.3? Are the functional requirements outlined in Section 4.3 appropriate and correctly

categorised (e.g., MAY, MUST, SHOULD)? Are there any requirements you feel are missing?

3

Please provide an explanation for your response.

The distinction between SDR-n and SPER-n requirements is not evident and some requirements apply to the landscape or users rather than the SPE. These requirements might still be needed, but restructuring the requirements categories would make it more clear.

Missing requirements:

Although it is discussed in the document, I miss the explicit mention of eIDAS compliance of identity and access management in the requirements.

Requirements around the use of (custom) software and requirements around how to satisfy user needs around access to reference data

Requirements allowing for output and/or archival of combined and enriched data, archival of analysis pipelines and other measures to ensure reproducibility.

Sections 4.3–4.5, pp. 13–41 The document uses mixed requirement modalities (MUST vs. mandatory, SHOULD, etc).

Recommendation: A harmonized requirements language with a summary table mapping each requirement to a preferred verification mode (audit, test, documentation) is recommended.

Sections 4.3.3 and 4.5 (pp. 17–22) and Annex E commentary (pp. 81, 85) While the document acknowledges the balance between security and usability, the guidelines would benefit from explicit recommendations for user-friendly, compliant workflows, robust exception management, and effective, adaptive user training approaches.

Sections 4.3–4.3.3 (pp. 13–18) and Annex B (p. 66+) These sections broadly rely on “MUST” and “SHOULD” statements without sufficient actionable guidance. More scenario-driven examples, compliance templates, and step-by-step operational guidance (for topics like lifecycle, network segmentation, incident response, and decommissioning) would make implementation more practical and auditable.

Sections 4.3–4.5, 4.5.3/4.5.4, and Annex B The specification generally prescribes comprehensive technical and operational safeguards (e.g. for auditing, monitoring, and documentation) that are appropriate for large-scale or national authorities. However, for smaller healthcare institutions, research organizations, or SPE operators with more limited resources, these requirements may result in disproportionate operational or financial burdens—potentially hindering equitable participation in EHDS-based data use.

Recommendation:

Include guidance for proportional application of requirements based on organization size, risk profile, and/or maturity level;

Clarify where flexible or risk-based implementation is permissible (e.g., tiered audit/monitoring depth for smaller institutions);

Consider referencing existing maturity models or best practices for differentiated compliance, to promote inclusiveness and practical feasibility across Member States.

Section 4.4, p. 21; Section 4.3.3, p. 17; Annex E, p. 89; and Table 4.9 "While the specification mandates that only anonymised (non-personal) data may be exported from an SPE, the requirements for tooling and support for (semi-)automated anonymisation reviews are limited. This could lead to significant interpretative variation or administrative overhead.

Recommendation: Please define minimum requirements for anonymisation expertise and standardized tooling or processes as mandatory for SPE providers, to ensure efficient, reproducible, and auditable export procedures. Also consider outlining recommended technical controls (e.g., integrated anonymisation-check tools or workflows)."

15. How would you rate the operational requirements in Section 4.5? Are the operational requirements outlined in Section 4.5 appropriate and correctly

categorised (e.g., MAY, MUST, SHOULD)? Are there any requirements you feel are missing?

4

Please provide an explanation for your response.

OPR-32: staff trained in information security is a must for SPE operators.
Sections 4.5.1, 4.5.2, and diagrams on pp. 23–27 (see Table 4.13, p. 28) There's a lack of practical clarity for handovers and accountability (especially where outsourcing or federation is involved).

Recommendation: Decision flowcharts, swimlanes, or RACI matrices would help clarify responsibility and liability in daily operations.

Sections 4.5.3 (pp. 30–33), 4.5.4 (pp. 34–36), Table 4.14 (p. 32), Table 4.15 (p. 35), and Annex B (p. 66+) The specification would be improved by concrete minimum log profiles, schematic audit datasets, and clearer guidance for role-based access to operational logs. This will streamline compliance, especially during external audits.

Section 4.5.6 (pp. 39-41) The specifications lack a process for ongoing service improvement based on changing user/dataholder requirements. Including references to continual improvement management (e.g. FitSM's approach) would enhance adaptability and future readiness.

Section 4.5.1 (pp. 23-26) The proposed approach for the "anonymous reviewer" role may not align with current research practices. Requirements for anonymous review need more precise definition, or alternatively, consider commissioning a dedicated, time-limited SPE instance for this function.

Section 4.5, audit/logging; data export; Annexes: End-to-end traceability from data source (patient or clinical system) to research publication or secondary use is a key requirement for academic hospitals committed to both research integrity and patient trust. The current specification could be strengthened by requirements or examples for data lineage capture, long-term auditability, and process transparency—across care, research, and cross-institutional boundaries. Please clarify how such auditability can be practically achieved within SPE boundaries.

Section 4.5.6, Annex E, and all mentions of user training/onboarding: For user adoption, “human factors” are critical; overly complex SPE workflows risk driving users away. The specification should include recommendations for effective user onboarding, continuous training, workflow usability testing, and rapid feedback mechanisms. This will ensure that practical barriers are reduced and compliance is strengthened through positive user engagement.

Sections 4.5.2, p. 27; Table 4.13, p. 28; Article 68(12), p. 29: The specification requires that all electronic health data in the SPE must be deleted or rendered irrecoverable within 6 months after permit expiration. While this is clear from an information security

perspective, for scientific reproducibility this requirement is problematic—especially on long timelines between analysis and publication.

Recommendation: Consider permitting (optional) archiving of data and/or export results via a controlled, tiered-access repository, to enable future verification and research transparency while upholding data protection standards.

16. How would you rate the SPE federation requirements in Section 5? Are the SPE federation requirements outlined in Section 5 appropriate and correctly

categorised (e.g., MAY, MUST, SHOULD)? Are there any requirements you feel are missing?

3

Please provide an explanation for your response.

Federation requirements in themselves are appropriate and it is great to see federation discussed extensively. However, the requirements need more context and rationale. What are the federation scenarios that SPEs should support? Is there a growth path from simple scenarios to more complex scenarios? And which requirements does an SPE need to fulfil to support which scenarios?

Chapter 5 and Sections 5.1/5.3 (pp. 42–49), along with Annex B FSPE requirements (p. 70): The specification lacks sufficient detail on governance, trust, and technical standards necessary for seamless, cross-border SPE federation. Please include explicit references to standards (as is done with OMOP CDM), clearly phase implementation guidance for federated SPEs, and rationalize choices (e.g., why GA4GH standards are mentioned over alternatives).

Sections 5.3, pp. 48–49; 6.1, p. 50; and Annex B, pp. 70+: The document rightly recognises the importance of federated interoperability. However, the stated requirements remain rather generic; in real-world operations, harmonisation of user role models and access control (see e.g., ISO 27001/NIS2, GDPR) is substantially more complex in federative scenarios. The specification currently lacks concrete guidance on federated identity and access management.

Recommendation: Please elaborate how engines for federated user authentication and authorisation (such as eIDAS and GA4GH Passports) will be used, referenced, or mandated as a standard mechanism for secure cross-organisational SPE access and auditability."

Sections 5.3 (pp. 48–49) and Annex E (p. 89): The specification suggests both manual processes and automation.

Recommendation: expand technical requirements for API-driven lifecycle management, automated permit processing, and audit/test procedures to enhance scaling across organizations.

Section 5.2 (pp. 46-47): The statement "SATRE 2.2.9. Your TRE must control and manage all of its network infrastructure" and the subsequent discourse on public cloud suitability are not clear. Is use of public cloud (e.g. Microsoft Azure) allowed, and if so, under which (minimum) requirements? Is 'must' here a requirement? Please clarify.

17. How would you rate the federated computing requirements in Section 6? Are the federated computing requirements outlined in Section 6 appropriate and correctly categorised (e.g., MAY, MUST, SHOULD)? Are there any requirements you feel are missing?

2

Please provide an explanation for your response.

Federated computing requirements are appropriate for federated compute and correctly categorized. However, the level of detail is not very appropriate for the aims of the document. Outlining the policy decisions needed around federation of SPEs and what the authors would expect the landscape to look like would be a more appropriate for this document. TIR requirements go into technical details and should be regarded as suggestions on how to build an SPE federation that can handle complicated federated computing scenarios. Although this is useful to bring under discussion, I think that the document that informs an implementation act should stay on a functional level. It should also be made explicit that the whole of chapter 6 only applies if an SPE is part of a federation that might support federated compute. In my view, it would suffice in this document to outline some functional requirements for federation and provide a rationale for why HDABs should consider building a federation SPE or even an SPE federation. For example, the potential of (national) SPE federations to support data requests is not discussed.

Section 6.5.3 (pp. 57): Protocols like RDP, VNC, SSH are designed primarily for local networks. Over public internet they pose security and performance issues. Please elaborate or require mitigation measures (e.g. gateways, advanced encryption, session recording) for remote use of these protocols.

Section 6 (pp. 50-51): The specification does not mention Multi-Party Computation (MPC) or confidential computing concepts.

Please amend:

How would these paradigms fit into the SPE architecture?

Figure 6.1 does not capture typical MPC network topologies, such as all-to-all node connections.

18. Do you consider the proposed approach to data export from EHDS SPE (Annex E: Data export from SPE) to be a feasible solution?

Not sure

Please explain your answer.

In case of large volumes of data exports of complex formats the concerns voiced around feasibility of manual output checking are justified. However, I would advise against completely abandoning manual output checks from the outset, when volumes might still be low. A balanced approach where data holders (with specialized knowledge of the data) and automation might share the load might be complex, but would provide better protections. So, yes, it is more feasible than the alternative to treat output as logs, but this only allows HDAB to intervene after identifiable output might have already leaked.

19. Does the document provide sufficient detail to support the practical implementation of Secure Processing Environments (SPEs)?

If not, please elaborate on what you think is missing or could be improved to better support implementation.

It does not provide sufficient information on some topics and too detailed information on others. Some sections (5 and 6) provide very detailed information that would be enough to support implementation and might impede innovation if frozen in legislation. On the general process that the SPE should support and its interactions with other HDAB business capabilities, however, the document does not provide sufficient detail. This might be due to the scope of the document, describing technical, functional and security specifications rather than business flows.