D7.1 Guideline on how to use data in a secure processing environment

TEHDAS2 – Second Joint Action Towards the European Health Data Space

27 May 2025

Co-funded by
the European Union

0 Document info

Disclaimer
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HaDEA. Neither the European Union nor the granting authority can be held responsible for them.

0.1 Authors

Lead Author(s)	**Lead organisation**
Irene Schlünder	TMF e.V., Germany
Antal Bodi	National Directorate General for Hospitals, Hungary
Victorien Hanché	Health Data Hub, France
Raitis Peculis	Latvian Biomedical Research and Study Centre, Latvia
Léa Rizzuto	Health Data Hub, France
Vita Rovite	Latvian Biomedical Research and Study Centre, Latvia
Inga Selecka	The Centre of Disease Prevention and Control of Latvia (SPKC), Latvia
Lise Skovgaard Svingel	Central Denmark Region, Denmark
Anna Szilagyi	National Directorate General for Hospitals, Hungary
Emmi Turunen	HUS Group, the joint authority for Helsinki and Uusimaa, Finland
Reviewers	**Lead organisation**
Marianne Benderra	Health Data Hub, France
Pia Brinkmann	BfArM - Federal Institute for Drugs and Medical Devices, Germany
Heikki Lehväslaiho	CSC – IT Center for Science Ltd., Finland

Lead Author(s)	Lead organisation
Helena Lodenius	CSC – IT Center for Science Ltd., Finland
Amélie Schäfer	Health Data Hub, France
Katharina Schneider	BfArM - Federal Institute for Drugs and Medical Devices, Germany

0.2 Keywords

Keywords	TEHDAS2, Joint Action, Health Data, Health Data Space

0.3 Document history

Date	Version	Editor	Change	Status
01/07/2024	0.1	Irene Schlünder	First draft	Draft
19/12/2024	0.2	Irene Schlünder	Draft to be reviewed by the Consortium	Draft
20/01/2025	1	Irene Schlünder	Document to be submitted for public consultation	Final
27/05/2025	2	Irene Schlünder	Document after public consultation (final deliverable)	Final

Accepted in Project Steering Group by written procedure on 27 May 2025.

Copyright Notice

Copyright © 2024 TEHDAS2 Consortium Partners. All rights reserved. For more information on the project, please see www.tehdas.eu.

Contents

1 Abbreviations

Term	Abbreviation
D	Deliverable
Data Governance Act	DGA
Data Protection Officer	DPO
Directorate-General	DG
European Health Data Space	EHDS
European Union	EU
General Data Protection Regulation	GDPR
Health Data Access Body	HDAB
Joint Action	JA
Multifactor authentication	MFA
Secure Processing Environment	SPE
The Finnish Innovation Fund	Sitra
Towards the European Health Data Space	TEHDAS
Work Package	WP

2 Executive summary

The aim of this guideline is to provide support to those who plan to access personal electronic health data for secondary use purposes through the infrastructure set up by the European Health Data Space (EHDS) regulation, the “HealthData@EU” infrastructure. The guideline is designed to support data users, specifically reflecting their activities from the moment they gain access to the approved datasets within a Secure Processing Environment (SPE) until the completion of their analysis and the export of results. An SPE is a secure digital workspace where authorised users can process electronic health data in a highly controlled manner.

The guideline takes the perspective of the data user and is intended to be consulted already from the project planning phase, i.e., before starting the data application process, after the access application form has been submitted, or granted. This is advisable since certain fees apply already when the data user, as data applicant, submits a data access application to a Health Data Access Bodies (HDAB). The data applicant will benefit from assessing the feasibility of conducting their analyses in an SPE at an early stage. In addition, the data applicant may state in the data access application which SPE appears

to be suitable for analysing the requested data. The proposal of a certain SPE must be justified in the application and will be part of the data permit.

It should be noted that drawing up a definitive guideline for data users remains challenging at this stage, as the implementation of the EHDS regulation (Regulation (EU) 2025/327, in force since 26 March 2025) by the HDABs is still evolving. The HDABs will be responsible for interpreting and applying the regulation in practice, and key implementation tools—such as guidelines and technical specifications—are still being developed. This document will therefore need to be updated as further implementing guidance becomes available.

3 Introduction

3.1 Advancing health data use in the European Health Union

As part of the European Health Union, the European Union (EU) is advancing the use of health data for secondary purposes, including research, innovation and policymaking. Smooth and secure access to data will drive the development of new treatments and medicines and optimise resource utilisation—all with the overarching goal of improving the health of citizens across Europe.

TEHDAS2, the second joint action Towards the European Health Data Space, represents a significant step forward in this vision. The project will develop guidelines and technical specifications to facilitate smooth cross-border use of health data, and support data holders, data users and the new health data access bodies in fulfilling their responsibilities and obligations outlined in the European Health Data Space (EHDS) regulation.

TEHDAS2 focuses on several critical aspects of health data use:

- Data discovery: Findability and availability of health data, ensuring it is accessible for secondary purposes;
- Data access: Developing harmonised access procedures and establishing standardised approaches for granting data access across Member States;
- Secure processing environment: Defining technical specifications for environments where sensitive health data can be processed safely;
- Citizen-centric obligations: Providing guidance on fulfilling obligations to citizens, such as communicating significant research findings that impact their health, informing them about research outcomes and ensuring transparency in how their data is used;
- Collaboration models: Developing guidance on collaboration and guidelines on fees and penalties as well as third country and international access to data.

TEHDAS2 will contribute to a harmonised implementation of the EHDS regulation through the concrete guidelines and technical specifications. Some of these documents and resources will also provide input to implementing acts of the regulation. Hence, the joint action will increase the preparedness for the EHDS implementation and lead to better coordination of Member States' joint efforts towards the secondary use of health data, while also reducing fragmentation in policies and practices related to secondary use.

The work performed in Work package 7 (WP7) addresses "Safe and secure processing" of electronic health data within the EHDS infrastructure. The goal is to enable secure processing of EU citizen's electronic health data while fostering a secure, interoperable, and efficient health data ecosystem. The output of this work package consists of guidelines and technical specifications that shall inform further decisions and technical frameworks to set up the EHDS.

The results of WP7 are distributed across five tasks. Task 7.1 provides guidance to users about their duties and responsibilities when analysing data in a secure processing environment. Next, guidelines for data minimisation and de-identification give guidance on how to address the challenges of health data minimisation, pseudonymisation, anonymisation and the generation of synthetic data (task 7.2 includes sub-tasks: 7.2.1, 7.2.2, 7.2.3 & 7.2.4). Specifications for the implementation of a common IT infrastructure (task 7.3) shall help member states to connect to the EHDS ecosystem. To ensure interoperability, common security requirements applicable to all secure processing environments are defined in addition to functional and technical services that should be part of all secure processing environments (task 7.4). Lastly, information about data linkage techniques and possibilities of quality control of linked data are collected (task 7.5).

Here is an overview of the documents that are part of WP7:

- Guidelines for data users on how to use data in a secure processing environment (task 7.1);
- Guidelines for Health Data Access Bodies on data minimisation, pseudonymisation, anonymisation and synthetic data (task 7.2);
- Technical specifications for Health Data Access Bodies on the implementation of the common IT infrastructure (task 7.3);
- Technical specifications for Health Data Access Bodies on the implementation of secure processing environments (task 7.4);
- Guidelines for Health Data Access Bodies on linkage of health datasets (task 7.5).

4. Introduction to the guideline on how to use data in a secure processing environment

This guideline belongs to a set of guidelines and technical specifications supporting the implementation of the European Health Data Space (EHDS) as provided in the regulation.

Other TEHDAS2 guidelines and technical specifications that are relevant for data users:

- Deliverable 4.1 Guideline for Health Data Access Bodies on fees and penalties for non-compliance related to the EHDS regulation
- Deliverable 4.3 Guideline for Health Data Access Bodies on international and third country access and transfer of electronic health data
- Deliverable 5.4 Guideline for Health Data Access Bodies on enrichment of health datasets
- Deliverable 6.2 Guideline for Health Data Users on good application practice for data access and data requests
- Deliverable 7.2 Guidelines for Health Data Access Bodies on data minimisation, pseudonymisation, anonymisation and synthetic data
- Deliverable 7.4 Technical specification for Health Data Access Bodies on the implementation of secure processing environments
- Deliverable 8.1 Guideline for Health Data Access Bodies on how to implement opt-out from secondary use of electronic health data
- Deliverable 8.2 Guideline for Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data
- Deliverable 8.4 Guideline for data users on handling research Outcomes

4.1 Target audience

This guideline is written for data users before they submit an application for data access through the EHDS infrastructure or after they have received a data access permit from a competent HDAB (For the application process see D6.2 Guideline for Health Data Users on good application practice for data access and data requests).

4.2 Scope

The aim of this guideline is to provide support to those who plan to access electronic health data for secondary use purposes through the infrastructure set up by the European Health Data Space (EHDS) regulation. It is designed to support data users engaging with the EHDS framework for secondary use, specifically focusing on their activities from the moment they gain access to the selected datasets within an SPE until the completion of their analysis and the export of results. Thus, the guideline covers the following steps:

1. What to take into consideration regarding the use of an SPE when planning to access data through the EHDS infrastructure, even before submitting a data application, including:

- What is an SPE?
- Why and when is an SPE needed?
- Can the data user choose an SPE?
- What will be the expected cost of using an SPE?

2. How to access the approved data in the SPE, once the data user has received the data permit following their application regarding a certain set of personal data, including:

- How to communicate with the SPE manager/provider?
- How to get access to the data in the SPE?

3. What needs to be considered when analysing data in an SPE, including:

- What rules to follow?
- Who is accountable as data controller?
- What happens in case of rule violation?

4. What happens after completion of the data analysis and export of results, including:

- Export of authorised anonymised results in a statistical format
- Cold storage options within the SPE for reproducibility purposes, during the validity period of the data permit
- Deletion of the data in the SPE

- Transparency obligations

4.3 Legal framework

The main legal act for accessing data through the EHDS infrastructure is the EHDS regulation (2025/327, https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng). But processing personal data for secondary use under the EHDS also falls into the scope of the general data protection regulation (GDPR, regulation (EU) 2016/679). Its rules are applicable. Therefore, data users should involve their data protection officer (DPO) when processing personal health data even when the users are acting within an SPE.

The EHDS regulation, which forms the decisive legal framework for this guideline, has recently been adopted. It is therefore still quite open as to what different implementations there will be in detail. Thus, it is not yet possible to make a detailed recommendation on all points. Any gaps will have to be closed over time.

This guideline is based on the English language version. In fact, however, all EU language versions of the regulation are equally binding.

Data users are required to carefully review the data permit issued by the HDAB to understand the specific terms and conditions for using the data in an SPE. This is a binding administrative decision. This guideline offers a high-level overview but should always be read alongside the data access permit and relevant agreements to ensure compliance with the EHDS regulation and GDPR.

It should be noted that the EHDS exists alongside other mechanisms for getting access to data for research and innovation purposes. It does not replace traditional data sharing mechanisms or existing data sharing agreements. Users can continue using them. If they do so, their rules apply. They may differ from those in the EHDS (see also D6.2 Guideline for Health Data Users on good application practice for data access and data requests).

It is not permitted to combine or jointly analyse electronic health data obtained through the EHDS framework with data accessed via other mechanisms (e.g. national procedures, institutional agreements). Combining or jointly analysing electronic health data obtained through the EHDS framework with data from other sources (e.g. data already held by the user, or accessed via national procedures) may be permitted, but must be explicitly authorised in the data permit. In accordance with Article 68(1)(b) of the EHDS regulation, any planned data linkage or combination must be declared in the application and assessed by the HDAB. Only if included in the permit can such linkage be carried out within the SPE.

5 What is an SPE and why and when do data users need an SPE?

An SPE is a secure digital workspace where authorised users can process electronic health data in a highly controlled manner. In the context of the EHDS, SPEs are a core component of the infrastructure enabling secondary use of personal electronic health data.

The legal basis for SPEs is established in Article 2(1)(c) and Article 73 of the EHDS regulation (Regulation (EU) 2025/327). These provisions specify that SPEs must guarantee a high level of security and confidentiality when processing sensitive health data for permitted purposes under the regulation. The concept draws from the definition in Article 2(20) of the Data Governance Act (DGA) but is further specified in the EHDS regulation to reflect the particular requirements of the health sector.

An SPE must meet at least the following core criteria:

- Data security: Prevent unauthorised access, maintain confidentiality, and ensure data integrity;
- Restricted access: Allow users to process only those data covered by a valid data permit, and only within the permitted scope;
- Controlled outputs: Ensure that only non-personal data—that is, aggregated and anonymised results—can be exported, and only after authorisation by the competent HDAB.

Under the EHDS regulation, SPEs may be used in two complementary contexts:

1. By data users, under a data permit (Articles 68–74), to process personal electronic health data in a secure and compliant way.

2. By HDABs themselves, when preparing data such as in data linkage scenarios or to prepare anonymous statistical outputs in response to a data request (Article 69), for example. In such cases, the HDAB acts as the data controller and may rely on the same secure infrastructure to conduct the analysis internally before delivering the anonymised result to the requester[1].

Thus, while data permits allow approved users to access data within the SPE, data requests do not involve user access to personal data—but still rely on the technical capabilities of an SPE to ensure lawful and se-cure processing by the HDAB.

In both cases, the key safeguard is that personal data cannot be downloaded or exported from the SPE. Only anonymised, aggregate outputs may leave the environment, and only after validation. Once the analysis is completed, data must be deleted or archived in accordance with the terms of the data permit.

Further technical specifications will be adopted to detail SPE requirements, including the types of data that may be processed and exported, and the conditions for approval by HDABs.

The concept of an SPE under the EHDS regulation (Article 2(1)(c) and Article 73) builds upon the general definition in Article 2(20) of the DGA. In the EHDS context, an SPE is a technical and organisational framework ensuring that processing of electronic health data for secondary use purposes meets the highest standards of data security, confidentiality, and compliance with Union law—especially the GDPR and the EHDS regulation.

According to Article 73(2) EHDS, only *anonymised results* may be exported from the SPE by the user, subject to verification by the HDAB. But the data *within* the SPE can be pseudonymised (i.e., personal data), and not all data requests lead to SPE use—anonymised data may also be provided *outside* SPEs under Article 69 responding to a

[1] SPEs may also be used directly by HDABs themselves, for instance when producing anonymised statistical outputs in response to a data request under Article 69(4) of the EHDS regulation. In such cases, the HDAB remains the data controller and processes the data internally, using the SPE to ensure full security and compliance with the regulation.

health data request. The HDAB may need the SPE as a workspace to do the analyses needed to reply to such a data request.

5.1 Excursus - What is personal data?

The EHDS regulation uses the definition in Art. 4 (1) GDPR defining personal data as any information relating to an identified or – directly or indirectly - identifiable natural person. Identification can occur through information such as name, social security number, location data, email address, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. In many cases, the identity of a person can be determined by combining several pieces of information. Therefore, the process of anonymisation often consists of deleting or modifying identifying information in a data set so that the person is no longer identifiable through any means reasonably likely to be used. What those means are must be assessed considering all objective factors, such as the cost and time required for identification, the available technology and the likelihood of someone attempting re-identification.

It is important to understand that absolute and permanent anonymity is neither possible nor required by the GDPR. Anonymity is not a static concept, but depends on context, including the availability of other data sources and the knowledge of the person accessing the data. For example, „Harry Smith“ may not be enough to identify an individual in a global telephone directory (no „singling out“), but it probably is in a classroom. The crucial factor is the re-identification risk in a given context. Therefore, organisational measures such as access controls and purpose limitations also play a role in ensuring anonymity. For the distinction between personal and non-personal data please also refer to D7.2.

In accordance with this context-dependent approach, there are various technical concepts, methods and standards for anonymisation. Their application depends on the environment in which the data is used. The more openly accessible data is, the more robust the anonymisation must be, because more contextual information may be available, it is always possible to imagine a third party who—now or in the future—has additional data that could be used for re-identification. To prevent this, robust anonymisation often requires techniques such as aggregation, generalisation, suppression, and noise injection. These may reduce data utility for some purposes. It is always possible to imagine a third party who—now or in the future—has additional data that could be used for re-identification. To prevent this, robust anonymisation often requires techniques such as aggregation, generalisation, suppression, and noise injection. These may reduce data utility for some purposes. This is the case within the EHDS: when processing data in an SPE based on data access application and subsequent data permit, only anonymous data (Art. 73 Nr. 2 EHDS reg), i.e. in a highly aggregated manner will be allowed to retrieve from an SPE at the end of the processing.

If the users are sure that anonymised data in this sense is sufficient for their research question, they can submit a request using the data request mechanism (Art. 69 EHDS reg). In this case, the HDAB processes the data and provides anonymised statistical outputs for download. An SPE is not required in this workflow (see guideline D6.2 on Good Application and Access Practice). Nevertheless, anonymity remains a moving target. The final decision on whether the data requested is sufficiently anonymised to be made available for download—or whether it must instead be analysed within an SPE—is taken by the HDAB. If users require individual-level data, even with identifying elements removed or minimised, there is a strong likelihood that the dataset will **not** qualify as anonymous under the EHDS regulation and will therefore have to be processed within an SPE and cannot be downloaded as such.

5.2 In which format is personal data made available in an SPE?

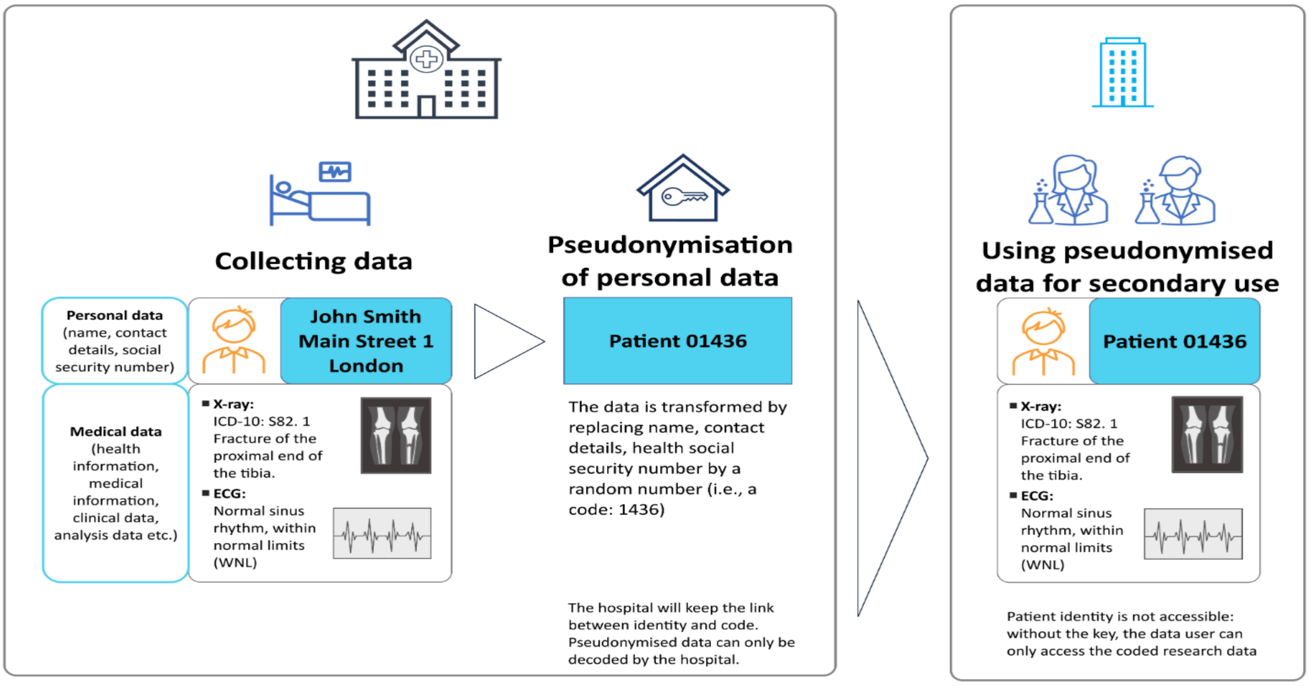
No directly identifiable personal data (e.g., names, addresses, social security numbers) will be made available to data users within an SPE. Instead, the data made available to users within an SPE will be in either pseudonymised or anonymised format, as defined in the data permit. In pseudonymised datasets, directly identifying information (e.g., names, addresses, social security numbers) is removed, but the data still refers to individual persons. This allows for analysis at the individual level, while preventing direct identification by the data user. In accordance with Articles 67(2)(e) and 68(1)(c) of the EHDS regulation, if the data are provided in pseudonymised format, this must be explicitly justified in the access application and approved in the data permit — in particular, where the intended analysis cannot be performed using anonymised data alone.

According to Article 4(5) of the GDPR, pseudonymisation means:

“the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures...”

One key distinction between pseudonymisation and anonymisation lies in this “additional information” — often referred to as the pseudonymisation key or linkage secret. In a pseudonymised dataset, the individual is still theoretically re-identifiable by an authorised entity (e.g., the HDAB or data holder), but not by the data user operating within the SPE. Another aspect is the reduction of potentially identifying information.

Figure 1. Depiction of a pseudonymisation procedure of routine healthcare data.


Collecting data
Personal data (name, contact details, social security number)
John Smith
Main Street 1
London
Medical data (health information, medical information, clinical data, analysis data etc.)
X-ray:
ICD-10: S82. 1
Fracture of the proximal end of the tibia.
ECG:
Normal sinus rhythm, within normal limits (WNL)
Pseudonymisation of personal data
Patient 01436
The data is transformed by replacing name, contact details, health social security number by a random number (i.e., a code: 1436)
The hospital will keep the link between identity and code. Pseudonymised data can only be decoded by the hospital.
Using pseudonymised data for secondary use
Patient 01436
X-ray:
ICD-10: S82. 1
Fracture of the proximal end of the tibia.
ECG:
Normal sinus rhythm, within normal limits (WNL)
Patient identity is not accessible: without the key, the data user can only access the coded research data

Although the pseudonym replaces the direct identifier, the record still refers to one individual.

Within an SPE, data users work with pseudonymised data, which still represents individual persons, but without directly revealing their identity. Because these data are processed in a highly secure and controlled environment, they do not need to be heavily transformed (e.g., aggregated, generalised, distorted) to prevent re-identification.

In contrast, when data are made available for download, they must be fully anonymised, meaning that all identifying information and any possibility of indirect identification must be removed. This often requires significant modification of the dataset, which can reduce its detail, structure, and analytical value.

SPEs therefore allow data users to work with higher-quality, more detailed data—while still ensuring privacy—because the data remain protected within the secure environment and cannot be exported.

Under Article 73 of the EHDS regulation, HDABs must authorise the use of a given SPE and ensure that:

- The SPE is used exclusively for the purposes defined in the data permit;
- Only anonymised results are exported after analysis;
- The SPE complies with data protection and information security requirements;
- Audits are conducted regularly, including by third parties where appropriate;
- Corrective measures are taken in case of identified vulnerabilities or non-compliance.

The regulation does not define the precise technical architecture of an SPE but empowers the Commission to adopt an implementing act describing those technical specifications. These will cover requirements for:

- Technical and organisational safeguards;
- Data protection and confidentiality;
- Interoperability;
- Tools and functionalities available to users in the SPE.

For additional details, see technical specification for HDABs on the implementation of SPEs (D7.4).

6 How to suggest the appropriate SPE?

Under the EHDS regulation, HDABs are responsible for granting access to electronic health data for secondary use. This includes attributing the SPE where data will be made available for analysis.

There may be multiple SPEs available within a given country or across borders. In their data access application, applicants can suggest an SPE they consider suitable for their specific needs, but the final decision lies with the HDAB. The selected SPE will be specified in the data permit, issued under Article 68 of the EHDS regulation. Each Member State must ensure the availability of at least one functional SPE through which access to data can be provided. This means that even if several SPEs exist, the HDAB must always be able to fall back on a compliant "last-resort" SPE to guarantee access.

What to include in an application

A data applicant, if there is no publicly available information about which SPEs may be used, is advised to contact the HDAB early in the process to explore which SPEs may be available and suitable for their study. In the application, users must specify their expected technical requirements, in line with Article 67(2) of the EHDS regulation. These may include:

- Required computational power (e.g., RAM, CPU cores, GPU access);
- Data volume and storage needs;
- Required software tools or statistical packages;
- Specific types of data to be analysed (e.g. genomics, imaging).

Users may also suggest a specific SPE and provide reasons (e.g. cost considerations, prior experience) to support your proposal. This information will help the HDAB identify the most appropriate SPE for the use case.

What varies between SPEs

Different SPEs may offer different capabilities. A prospective user, should consider the following aspects:

- Software: Some SPEs may already include commonly used tools. Others allow users to request the installation of specific software, but for security reasons, installations are handled by the SPE operator— users will not have administrative rights inside the SPE. Licensing models vary: some SPEs may support bring-your-own-license (BYOL), while others require licenses to be purchased by the user or the operator.

- Data types and scalability: Users' needs in terms of amount and type of data may vary significantly. Not all SPEs are optimised to handle all data types (e.g. high-resolution medical images, longitudinal EHR data, or genomic sequences). If the users' project requires high scalability, they should confirm in advance whether the SPE infrastructure can support the dataset and processing needs.

- Computing power: While many SPEs provide standard computing environments, some projects may require advanced capabilities (e.g. parallel computing, GPU, or even HPC/quantum computing). These capacities are not guaranteed in all SPEs.

- Cost considerations: Pricing models may vary. Some HDABs or SPE operators may cover infrastructure costs; others may charge users for processing time, storage, or software licensing. Always verify the cost implications early, especially if budget constraints apply. See also chapter 7.

- Access modalities: Access to the SPE may be offered via web interface, virtual desktop, or (less commonly) physical access points (e.g., terminals in academic institutions). Some access models may be restricted by institutional firewalls or national regulations.

- Changing the SPE: If users need to change the SPE after a data permit has been granted—whether due to infrastructure limitations, access issues, or project redesign—they must request an amendment to the data permit. This includes any change to the SPE itself, modifications to user access, data availability, or the study team (Article 68(13), EHDS regulation). They should contact their HDAB to initiate this process.

7 What are the fees to use the SPE?

Under Article 62 of the EHDS regulation, HDABs may charge fees **for services** related to the secondary use of electronic health data. These fees are intended to cover (part of) the costs of services – such as SPE provision – provided by the HDAB, any potential external SPE provider, and data holders. Fees must be transparent, proportionate and non-discriminatory, while potential reductions may be available for specific user groups, as laid out in Article 62.1 and outlined in D4.1 Guideline for HDABs on fees and penalties for non-compliance related to the EHDS regulation.

These may include fees for use of the SPE, data preparation, or permit evaluation. The purpose of these fees is to cover part of the operational costs incurred by HDABs, external SPE providers, and data holders.

HDABs may charge fees for the following services (outlined in Article 62.1 and detailed in D4.1 Guideline for Health Data Access Bodies on fees and penalties for non-compliance related to the EHDS regulation):

- Evaluating the data access application: Including reviewing and assessing the data permit application or data request;
- Preparing the dataset: Covering costs for processes such as pseudonymisation, anonymisation, data linkage and consolidating datasets from multiple data holders;
- Using the SPE: Including SPE provision, user training, statistical software licenses (if required), processing capacities, data storage/archiving, and ongoing support for data use, including for preapproving scripts for upload to the SPE and checking the anonymity of any output before download from the SPE.

The expected fees must be communicated by the HDAB to the data user before the permit is issued, allowing the data user to decide whether to withdraw or proceed with the application (please also refer to D6.2 Guideline for Health Data Users on good application practice for data access and data requests, section 8.5). All applicable fees, corresponding to the services provided, must be paid at the time the specific service is delivered, as detailed in the data permit. If a data user requests changes after the permit has been issued (e.g., extending the permit duration or modifying the dataset), additional fees may apply to cover the costs of these adjustments.

For detailed information on fee structures and conditions, refer to D4.1 (Guideline for Health Data Access Bodies on fees and penalties for non-compliance related to the EHDS regulation).

8 Communication with SPE provider

Once access to the data has been granted by the HDAB, the HDAB activates the user’s access to the SPE specified in the data permit.

If the SPE is managed directly by the HDAB, all communication—whether technical, operational, or related to support—goes through the HDAB.

If the SPE is operated by a third-party provider, a distinction applies: Communication related to data governance and supervision continues to go through the HDAB. Communication regarding technical specifications, access modalities, and services may be handled directly between the user and the SPE provider, however any communication outside of the scope of the data permit has to be done via the HDAB. An example would be extending the SPE usage.

However, under Article 62(6) of the EHDS regulation, the single invoice principle applies: The HDAB is responsible for issuing a single invoice covering all applicable fees, including those charged by third-party providers (such as external SPE operators or data holders). This means that even when communication with a third-party SPE provider takes place, all payments must be made through the HDAB. Users should not receive or process separate invoices from different entities. This principle ensures transparency, simplifies the administrative process for users, and guarantees that all service-related costs are coordinated through the HDAB.

9 How to get access to the SPE

Access to the SPE is a strictly regulated process that ensures and guarantees the protection of health data as a special category of data. Access is managed and controlled at several levels as follows: Access is granted only to individuals who are explicitly named in the data permit and have completed the enrolment and identification process.

The access process generally involves the following steps:

Enrolment and Identification: First, the individuals who should have access to the data and are therefore named in the data permit must enrol before getting access. The enrolment phase consists of thorough identification measures. Cybersecurity measures will integrate robust security strategies like Zero Trust Policy: Trust no one, identify everything.

Login Credentials and Password Policy: Users receive individual login credentials (login ID and password). Passwords must meet strong security requirements—typically based on recognised standards such as the NIST guidelines (e.g., length, complexity, regular renewal).

Multifactor Authentication (MFA): Strict multifactor authentication (MFA) is required. This may involve:

- Something you know (e.g., password);
- Something you have (e.g., token, smart card);
- Something you are (e.g., fingerprint, facial recognition).

Most systems will rely on device-based authentication (e.g., hardware tokens or certificates), which can be replaced in case of compromise—unlike biometric credentials.

Continuous Monitoring and Reporting: All access to the SPE is logged and monitored. Usage is subject to continuous auditing to detect anomalies or unauthorised behaviour. Any change to the list of authorised users (e.g., adding a team member or re-placing one) must be formally requested and approved by the HDAB as an amendment to the data permit (Article 68(13) EHDS regulation).

Access will be denied to any person:

- Not named in the permit,
- Whose identity cannot be verified,
- Or whose credentials have expired or been revoked.

10 How to analyse data within the SPE

SPEs are designed to allow the analysis of personal electronic health data in compliance with the EHDS regulation and the GDPR. All EHDS-compliant SPEs implement strict security and accountability standards to protect sensitive data and to ensure lawful processing by authorised users. Users must not attempt to circumvent or disable any SPE security features. All activities in the SPE are logged, monitored, and subject to audit by the HDAB. User training is provided to help researchers use the SPE correctly, avoid mistakes, and understand the available features and compliance requirements.

1. Tools and environment for data analysis

SPEs offer a set of pre-approved analytical tools. The availability and type of tools (e.g. R, Python, STATA) may vary between SPEs. If other software is required, users may request its inclusion. Installation is subject to the SPE provider's approval and HDAB oversight, and users do not have administrative access. Due to security concerns, commonly used collaboration platforms (e.g. Slack, Microsoft Teams) may not be allowed within the SPE.

2. Conducting analysis

Users may only conduct the analyses authorised in their data permit. Intermediate results must be stored within the SPE; these outputs are not visible externally but may be logged for oversight purposes. Federated analysis (i.e., analysing data stored in multiple SPEs without centralising it) is possible, subject to HDAB oversight. Technical implementation details are covered in Task 7.4.

3. Preparing and exporting results

- Only anonymised, aggregate results may be exported from the SPE;
- All outputs must be reviewed to ensure they do not permit re-identification;
- The HDAB must validate the results before authorising export (Article 74 EHDS regulation);
- Export occurs via the SPE's secure export mechanism.

4. Accountability and user roles

Under Article 74(1) of the EHDS regulation, the data user is the data controller for the analysis conducted in the SPE (see chapter 11). As such, users are responsible for:

- Complying with all legal, ethical, and security requirements;
- Observing the restrictions specified in the data permit (e.g. authorised users, approved purposes);
- Ensuring that access to data is strictly limited to what is necessary.

User behaviour in the SPE must reflect this responsibility. In particular: Use of mobile phones, screen recording, or video calls is prohibited in or around the SPE. Users must not take notes that could identify individuals. All user activity is logged chronologically to support auditing and investigate security events.

5. Team collaboration in the SPE

When multiple researchers work together in the same SPE:

- A clear organisational structure must be in place;
- Roles and responsibilities should be defined and documented;
- Access levels may differ between team members depending on their tasks;
- Real-time collaboration features may be limited, and communication about the data must not take place outside the SPE environment.

6. Breaches and consequences (see also chapter 12)

Any violation of the data permit or SPE rules—such as unauthorised access, re-identification attempts, or processing for unauthorised purposes—may result in:

- Revocation of access;
- Administrative sanctions under the EHDS Regulation;
- Penalties under the GDPR.

The security and logging features of the SPE are designed to prevent, detect, and document such breaches. Please also refer to chapter 10 for possible training activities.

11 Who is accountable as data controller?

Under the EHDS regulation, the term "data controller" follows the definition set out in Article 4(7) of the GDPR. A controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

In the context of the EHDS, however, the role of the data controller is more narrowly defined than in general GDPR practice. The regulation itself determines many of the purposes and essential means of processing. As a result, the discretion of the data user acting as controller is significantly limited.

According to Article 74(1) of the EHDS regulation, the data user becomes the data controller for the processing activities carried out within the SPE, and only within the scope of the data permit issued by the HDAB. This means that the user-controller is responsible for how the permitted analysis is performed but cannot decide on the broader legal basis for data access or the technical environment. Those aspects are governed by the regulation, the data permit, and the technical setup of the SPE.

The controller is responsible for ensuring that all processing complies with the GDPR and the EHDS regulation. This includes observing purpose limitation, data minimisation, and safeguarding data subject rights. The controller must also respect the restrictions and conditions set out in the data permit.

A data processor is an entity that processes personal data on behalf of the controller. Under Article 28(3) GDPR, the relationship between controller and processor must be governed by a binding contract or other legal act under Union or Member State law. This agreement must set out the subject matter, duration, nature and purpose of the processing, and limit the processor to acting only on documented instructions from the controller.

In the EHDS context, technical operators of the SPE or providers of support services may act as processors. However, they too are bound by the regulation and the structure of the data permit, which means the controller cannot instruct them freely beyond those legal constraints.

In cases where two or more parties jointly determine the purposes and means of processing, they may qualify as joint controllers. This requires a joint controllership agreement in line with Article 26 GDPR, clearly allocating their respective responsibilities.

Articles 74 and 75 of the EHDS regulation establish specific responsibilities. Under Article 74(1), the data user is the controller when analysing data in an SPE. Under Article 74, the HDAB is the processor on behalf when it processes data in response to a data request.

These provisions clarify accountability depending on whether the data is processed by a user in an SPE or by the HDAB in response to a request.

Table 1: Summary of controllership for a simple exemplary scenario (*data holder/HDAB/data user without intervention of a trusted data holder and data intermediation entity*)

Processing activity	**Data controller**
Data preparation (data targeting, quality control, additional pseudonymisation, etc.)	Data holder & HDAB[2]
Data matching / linkage	HDAB
Transfer of data to the SPE	Data holder
Ingestion and additional pseudonymisation	HDAB
Validation of data on the SPE (assessing if the data requested are correct, complete and fit for purposes in relation to content of the data access permit)	Data user
Pseudonymisation between workspaces, if foreseen by national regulation	HDAB
Import of data in the project's dedicated analysis workspace on the SPE	HDAB
Data analysis	Data user
Export of anonymised data from the technological platform from the SPE to the data user, after verification of the degree of aggregation and anonymisation by HDAB	Data user
Cold storage within the time of the permit	Data user
Security measures on the SPE with regards to data processing including back-up, maintenance and traceability	HDAB
Deletion	HDAB

[2] Under Articles 68 and 75 of the EHDS regulation, the HDAB can indeed ensure or coordinate certain data preparation tasks (including pseudonymisation), either as part of the data permit process or when acting as data controller in the context of a data request. Therefore, while preparation at source is important and should be the preferred option, this role is not necessarily limited to the data holder.

Where two or more national contact points or authorised participants put electronic health data in the secure processing environment managed by the Commission, they shall be joint controllers, and the Commission shall be processor for the purpose of processing data in that environment (Art. 75 (9) and (10) of the EHDS regulation).

Where the EHDS regulation does not provide for specific rules regarding controllership, the general rules from the GDPR apply.

If the applicant/data user consists of more than one individual or entities (e.g., a research consortium), all members of the group could be joint controllers.

12 What happens in case of rule violation?

While using SPEs, the data user's activities are monitored and logged. Data users must strictly adhere to the obligations set out in the EHDS regulation, the GDPR, and the specific conditions laid down in their data permit. These safeguards ensure that the secondary use of health data does not harm individuals, public trust, or societal interests.

Prohibited actions include (Articles 54 and 61 of the EHDS regulation):

- Using data to take decisions that have detrimental effects on individuals (e.g. related to insurance, employment or banking);
- Engaging in advertising or marketing activities;
- Developing harmful products or services;
- Conducting activities in conflict with ethical provisions laid down in national law;
- Attempting to re-identify individuals or or to draw identifiable group-level information from pseudonymised data;
- Providing access to data or the SPE to third parties not listed in the data permit.

Data users must immediately report any breaches or security incidents directly to the HDAB. Failure to do so may result in additional penalties.

- Non-compliance may result in enforcement measures under the EHDS regulation, including fines based on the severity and nature of the violation;
- Suspensions: Revocation of the data permit or exclusion from the EHDS for secondary use;
- Damage compensation: Liability for damages caused to natural persons or SPE providers;
- Legal actions: Depending on the severity of the breach, further legal or criminal actions may be pursued in accordance with national law.

If a finding of non-compliance indicates a possible breach of the GDPR, the HDAB is required to immediately inform the supervisory authorities and provide them with all relevant information regarding this finding.

Detailed information about enforcement measures is outlined in D4.1 Guideline for Health Data Access Bodies on fees and penalties for non-compliance related to the EHDS regulation.

The HDAB will give the health data user an opportunity to state their views on suspected breaches within a reasonable period that does not exceed four weeks (Article 63 of the EHDS regulation and D4.1 Guideline for Health Data Access Bodies on fees and penalties for non-compliance related to the EHDS regulation).

13 What happens after finishing data analysis?

Once data analysis is completed, only anonymised and non-personal results may be exported from the SPE. These must be in statistical format and comply with the conditions set out in the data permit. Before authorising the export, the HDAB will verify that the outputs do not present a risk of re-identification, as required under Article 74(2) of the EHDS regulation.

In some cases, the data user may no longer require full computing capacity but may still need access to the SPE for limited purposes, such as verifying reproducibility or responding to peer review requests. In such situations, the SPE may offer a reduced-capacity archiving function, which allows continued access to the analysis environment while lowering infrastructure usage and potentially reducing associated costs. This archiving function is intended for temporary use within the period of the data permit. It does not extend the duration of the permit or the retention period for the dataset.

According to Article 68(12) of the EHDS regulation, data permits are granted for the duration necessary to achieve the declared purpose, for a maximum of 10 years. This duration may be extended once, for an additional period of up to 10 years, if the user submits a justified request at least one month before the permit expires.

Once the data permit expires, the electronic health data stored in the SPE must be deleted within six months. However, at the user's request, the formulas or processing scripts used to generate the dataset may be retained by the HDAB for transparency or reproducibility purposes.

In line with Article 72 and accompanying guidelines, HDABs must ensure transparency by publishing information on data access applications, data requests, and permits granted. This is further detailed in D8.3 (Guideline for Health Data Access Bodies on informing natural persons about the use of health data – "Citizen Information Point").

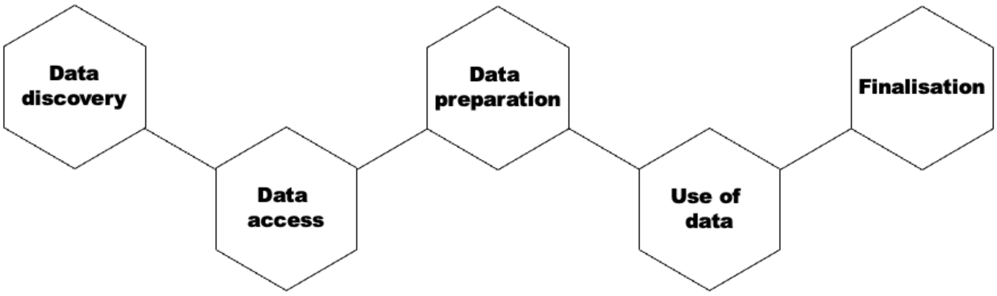
Data users must also publish the results of their work using electronic health data, and inform the HDAB of any findings of significant relevance to public or individual health, as outlined in D8.4 (Guideline for data users on handling research outcomes).

Annex 1: EHDS user journey description

User journey

When a data user[3] applies for electronic health data for secondary use purposes, such as research and innovation activities, education, and policy-making, within the European Health Data Space (EHDS), the user journey consists of several stages (see Figure 1). Access for certain purposes (public or occupational health, policy-making and regulatory activities, and statistics) is reserved for public sector bodies and Union institutions (see Chapter IV, Art. 53(1) and 53(2)).

Figure 1: EHDS user journey consists of five main phases: data discovery, data access, data preparation, use of data and finalisation.



Data discovery

Before being able to use the data, the user needs to investigate whether the data needed is available, and whether it is available in the necessary format for the secondary use purpose. This phase is called data discovery. Datasets available in the EU can be found in a metadata catalogue at https://qa.data.health.europa.eu/. Once the data discovery is completed, the user can begin the process of applying for the data.

Data access

In the data access phase, the user fills in and submits a dedicated and standardised data access application form or a data request to a health data access body (HDAB)[4]. The user must complete the information required in the form, upload necessary documents, and provide justifications as needed.

Data access application form is used when the user seeks to use personal level data. Data request is for cases when the user wants to apply for anonymised statistical data.

Data preparation

During this phase, the data holder(s)[5] deliver(s) the necessary data to the HDAB, which starts to prepare the data for secondary use. Techniques for pseudonymisation, anonymisation, generalisation, suppression, and randomisation of personal data are

[3] Data user = a person using electronic health data for a secondary use purpose

[4] Health data access body (HDAB) = the authority responsible for assessing the information provided by the data user who applies for electronic health data for a secondary use purpose

[5] Data holder = Any natural or legal person, public authority or other body in the healthcare or the care sectors that has the right or obligation to provide electronic health data for secondary use purposes or the ability to make such data available (see more EHDS Regulation Art. 2 (1t))

employed. The data minimisation principle (as per the GDPR) must be respected to ensure privacy.

Use of data

In this phase, the user performs analyses based on the received data for the purpose defined in the application phase. Analysing personal level data must be performed in a secure processing environment[6]. The duration of this phase is specified in the regulation (Art 68(12)).

Finalisation

This last phase of the user journey concerns data user's duties regarding analysis outcomes derived from secondary use of data. Data user must publish the results of secondary use of health data within 18 months of the completion of the data processing in a secure processing environment or of receiving the requested health data. The results should be provided in an anonymous format. The data user must inform the health data access body of the results. In addition, the data user must mention in the output that the results have been obtained by using data in the framework of the EHDS.

[6] Secure processing environment = an environment with strong technical and security safeguards in which the data user can process personal level electronic health data

Annex 2: Glossary

Table 2: Preliminary glossary according to wave 1 in TEHDAS2. It will be aligned across all TEHDAS2 deliverables in a next step. Please note, that the current version of the glossary is not exhaustive. Please refer to the master glossary for TEHDAS2 for more information.

Term	Description
Anonymisation	The process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party. Anonymised data falls outside the scope of data protection laws such as GDPR. (GDPR Recital 26)
Data access	Processing by a data user of data that has been provided by a data holder, in accordance with specific technical, legal, or organisational requirements, without necessarily implying the transmission or downloading of such data. (DGA, Article 2(8),(9)&(13))
Data controller	A data controller is a person or organisation that determines the purposes and essential means of the processing of personal data. The role of the data controller can be shared by several people or organisations. In that case, they are defined as joint controllers. The controller is accountable and responsible for establishing a lawful data processing workflow and observing the rights of data subjects. (GDPR, Article 4(1)(7))
Data minimisation	A principle mandating organisations to only collect, store and process the minimum necessary amount of personal data for a specific purpose. This principle is fundamental under GDPR and relevant to the tasks outlined in EHDS. (GDPR Article 5(1)(c))
Data permit	An administrative decision issued to a health data user by a health data access body to process certain electronic health data specified in the data permit for specific secondary use purposes, based on conditions laid down in Chapter IV of this Regulation; (EHDS, Article 2(2)(v))
Data processor	The data processor should handle data exclusively in the manner prescribed by the controller. A data processor acts under the detailed instructions of the data controller only, by processing personal data on his behalf. (GDPR, Article 4(1)(8))
Dataset	Means a structured collection of electronic health data. (EHDS, Article 2(2)(w))

Term	Description
Health data access body (HDAB)	Member state-designated authority that facilitates the secondary use of electronic health data. HDABs assess the information provided by the health data applicant and decide on health data requests and access applications, authorise and issue data permits, obtain data from data holders and make data available in Secure Processing Environments. HDABs systematically track the data request and data access applications received and the data permits issued. As per Article 58 of the EHDS, HDABs are required to publicly list information on the data permits issued. Reference to the EHDS regulation: Recital 52: […] providing access to health data through the involvement of health data access bodies, […] In addition, the health data access body should assess the information provided by the health data applicant, based on which it should be able to issue a data permit for the processing of personal electronic health data pursuant to this Regulation that should fulfil the requirements and conditions set out in Chapter IV of this Regulation. […]
Health data holder	Any person, organisation or public body involved in healthcare, care services, health-related products, wellness apps or health(care) research, that has the right to process data for health care provision or for public health purposes, reimbursement, research, policy making, official statistics or patient safety. This includes, for example, hospitals, insurers, research institutes and EU institutions Reference to the EHDS regulation: Article 2(2)(t)): 'health data holder' means any natural or legal person, public authority, agency or other body in the healthcare or the care sectors, including reimbursement services where necessary, as well as any natural or legal person developing products or services intended for the health, healthcare or care sectors, developing or manufacturing wellness applications, performing research in relation to the healthcare or care sectors or acting as a mortality registry, as well as any Union institution, body, office or agency, that has either: i. the right or obligation, in accordance with applicable Union or national law and in its capacity as a controller or joint controller, to process personal electronic health data for the provision of healthcare or care or for the purposes of public health, reimbursement, research, innovation, policy making, official statistics or patient safety or for regulatory purposes; or

Term	Description
	ii. the ability to make available non-personal electronic health data through the control of the technical design of a product and related services, including by registering, providing, restricting access to or exchanging such data;
Health data user	A natural or legal person, including Union institutions, bodies, offices or agencies, which has been granted lawful access to electronic health data for secondary use pursuant to a data permit, a health data request approval or an access approval by an authorised participant in HealthData@EU; (EHDS, Article 2(2)(u))
Pseudonymisation	The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person. (GDPR Article 4(5))
Secure Processing Environment (SPE)	'Secure Processing Environment' means the physical or virtual environment and organisational means to ensure compliance with Union law, such as Regulation (EU) 2016/679, in particular with regard to data subjects' rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, as well as with applicable national law, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms. (DGA, Article 2(20); EHDS, Article 2 (1)(c))

Annex 3: How this Guideline has been developed

This guideline is the outcome of task 71. of the joint action TEHDAS2. A team of multinational and multidisciplinary experts has developed the first draft of the guideline from May 2024 until January 2025 in constant dialogue with the EU Commission and other stakeholders like ministry representatives. Every expert worked on one of the chapters they had specific expertise about. The chapters were then discussed in weekly meetings with the whole team.

Summary of the public consultation results and main feedback

A draft version of this document was in public consultation between the 20th of January and 28th of February 2025. This document was commented in total for 78 times. The number of responses may contain some duplicates as there was no individual identification and verification required to respond to the surveys. Some respondents have also responded both from data holder's and data user's perspective. The responses came from 18 different countries from the EU countries and the European Economic Area countries. Responses from Eastern European countries and international organisations were largely missing. The respondents were primarily from three main types of organisations, listed in order of prevalence: Data management/processing (15), information technology (13) and research and development (12).

Classification of comments from the public consultation

1. Style and Language

The style received mixed feedback—some considered it appropriate, others found it overly complex or insufficiently justified from a legal perspective. As it was challenging to meet all expectations, the following principles were adopted:

- Clarity for a broad audience was prioritised. The viewpoint of a student preparing a research project was used as a baseline. Laypersons unlikely to seek access to health data were not targeted, though professionals outside of research were still considered.
- The text was kept as concise as possible. While this requires careful reading, it avoids the inclusion of unnecessary information.
- Quotations from legal texts were minimised to improve readability for non-specialists. Nevertheless, alignment with the EHDS regulation was ensured. All statements are based on applicable legal provisions, which were thoroughly discussed with the European Commission and several ministries. The underlying legal reasoning was deliberately excluded, as it was considered of little practical use to end users. In our view, theoretical legal debates are not appropriate in a user guideline.

2. General comments on EHDS and requests for more information

As the guideline entered the process of public consultation very early on, namely before the EHDS regulation had been finally adopted and before other guidelines dealing with the basic technical components of secondary use had been finalised, many commentators rightly missed essential information. Quite a few of the comments are therefore based on requests for additional information and explanations. Below is a summary of points that were raised:

- Legal and regulatory clarity
    - It is unclear how GDPR obligations (e.g., patient rights relating to pseudonymised data) will be fulfilled;
    - Cross-border legal and ethical differences are insufficiently addressed;
    - The responsibilities of data holders in relation to compensation and legal recourse against HDAB decisions require further clarification.
- SPE definition and governance
    - The nature of SPEs—whether physical or virtual, centralised or decentralised—is not defined;
    - It is unclear who is authorised to provide SPEs (HDABs, third parties, or the users' own infrastructure);
    - The rationale for requiring multiple SPEs based on data sensitivity, processing complexity, or geographical factors is not explained.
- Technical and operational details
    - Information is lacking regarding user journeys, necessary tools, and data access mechanisms within SPEs;
    - Requirements for computational resources or scalability for intensive tasks such as genomics are not specified;
    - The challenges of managing large, frequently updated datasets within SPEs have not been addressed;
    - There is no discussion of the potential use of federated learning or confidential computing.
- Cross-border and interoperability concerns
    - It is unclear how data originating from different countries or SPEs will be handled;
    - There is no clear framework for collaboration between SPEs or for ensuring interoperability across HDABs and EU member states.
- Enhancements and recommendations
    - The inclusion of open-source analytics tools should be considered to enhance SPE functionality;
    - The potential for SPEs to be dedicated to specific entities or collaborative initiatives is not explored.

It was not possible to fulfil all these requests because deliverables, especially D7.4 were still not available. However, the writing team has endeavoured to maintain contact with other teams working in parallel on related deliverables to close as many gaps as possible. The present deliverable, however, remains a first high-level guidance document which must be updated over time as details become clearer.

In the end, a common terminology is being developed for all deliverables that will address major open questions.

As this guideline was one of the first in the public consultation, quite a few people took the opportunity to critically reflect on the EHDS and below is a summary of points that were raised:

- Data access and export restrictions

    - Data access should be free of charge overall;
    - The requirement to export authorised anonymised results only in a "statistical format" is overly restrictive and goes beyond EHDS/GDPR provisions. The phrase "statistical format" should be removed to allow more flexibility;
    - Export limitations risk undermining data quality improvements made during research and may lead to unethical data deletion.
- Burden on HDABs and funding
    - HDABs are assigned significant responsibilities, which must be matched by appropriate funding and resources;
    - The lack of local legislation in countries like Poland may hinder implementation and create disparities across the EU.
- Access process and usability Issues
    - The access process is seen as overly burdensome, involving script reviews, reapplications, and linear approvals, which increases costs and delays;
    - These hurdles could make the system less usable than alternatives, such as clinical trial frameworks.
- Overregulation and imbalance
    - The proposed system is seen as over-regulating data privacy, neglecting the broader balance of scientific value, societal benefit, and ethical data use;
    - TEHDAS2's approach restricts scientific methods by mandating only pre-approved tools and limited data export, which conflicts with how modern research, especially in AI, is conducted.
- Technical and resource concerns
    - Implementation will demand major technical and human resources (e.g., programmers, data engineers), making it expensive and difficult to realise in the short term;
    - Integration with other infrastructures is seen as unrealistic without substantial investment.
- Risks to innovation and competitiveness
    - EHDS regulations may impose operational constraints, especially on private sector data holders, potentially reducing their competitiveness;
    - Compliance costs and data-sharing obligations may disproportionately burden smaller organisations.
- Concerns from the AI research community
    - The current SPE definition does not support the needs of AI research, particularly in model training and deployment;
    - AI researchers may be forced to work outside EHDS, which undermines the initiative's relevance to one of the fastest-growing scientific fields.

On the other hand, hopes and expectations are high. People noted that implementing these recommendations could significantly benefit researchers by improving access to valuable health data often withheld due to GDPR concerns. A secure, standardised system would encourage healthcare institutions to share data more confidently, fostering better collaboration and more comprehensive studies. However, successful implementation would require a clearer technical description of the SPE and a step-by-step guide on its use.

Disclaimer: The information in this chapter expresses the opinions of the commentators.

3. Processable input:

Finally, several very helpful comments were received, which were implemented as far as possible. In many cases, however, the interpretation of provisions of the EHDS Regulation has not yet been clarified in detail. It will be the task of the Member States to fill in the remaining gaps when implementing the regulation. The Member States will work together with the EU Commission and the EHDS Board to do this. This guideline therefore cannot answer all questions or take account of all the comments made.

Method of processing the comments

Every first author reviewed comments per chapter and amended the guideline text accordingly. Three main chapters were identified, that needed major revision, amendment and rewriting:

- A Chapter on “Anonymisation/Pseudonymisation” was re-added in alignment with T7.2;
- “How to suggest an SPE” was expanded and clarified after intensive discussion with the Finnish Ministry of Health and EU Commission;
- Security measures regarding access to the SPE and analysis of the data in the SPE was expanded and more details provided in alignment with T7.4.

The team rediscussed audience and style in the group and with relevant legal experts.