D4.1 Guideline for health data access bodies on fees and penalties for non-compliance related to the EHDS Regulation

TEHDAS2 – Second Joint Action Towards the European Health Data Space

27 February 2026

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

Author(s)	Organisation
Julie Baussand	Health Data Hub, France (Lead)
Lucrezia Valieri	Ministry of Health, Italy (Lead)
Maya Bucciarelli	Ministry of Health, Italy (Lead)
Alexander Leander Knudsen	Danish Health Data Authority, Denmark
Anne Sofie Skødt	Danish Health Data Authority, Denmark
Aurēlija Usačova	Centre for Disease Prevention and Control, Republic of Latvia
Dora Talvard	Digital Health delegation, French ministry of health, France
Emer Doyle	Department of health, Ireland
Emilia Krawczyk	Ministry of health, Poland
Emilie Passemard	Digital Health delegation, Ministry of Health, France
Eva Zvirgzdiņa	Centre for Disease Prevention and Control, Republic of
Ida Møller Solheim	Norwegian Institute of Public Health, Norway
Inge Franki	Health Data Agency, Belgium
Juliette Chambon	Digital Health delegation, Ministry of Health, France
Katrine Højen Vad	Danish Health Data Authority, Denmark
Louisa Stüwe	Digital Health delegation, Ministry of Health, France
Mervi Siltanen	Finnish Social and Health Data Permit Authority (Findata), Finland
Minerva Alvarez	Ministry of Health, Spain
Richard Hrabcak	National Health Information Centre, Slovak Republic
Zdenek Gütter	Ministry of Health, Czech Republic

0.2 Keywords

Keywords	TEHDAS2, Joint Action, Health Data, European Health Data Space, Health Data Access Bodies, Health Data Holders, Fees,

0.3 Document history

Date	Version	Editor	Change	Status
06/03/2025	0.1	Julie Baussand Lucrezia Valieri	Initial document creation	Draft
30/06/2025	0.5	Julie Baussand Lucrezia Valieri	Finalised version	Modified
30/06/2025	0.5	Louisa Stuwe	Submitted to TEHDAS2 consortium and EC	
05/09/2025	0.8	Julie Baussand Lucrezia Valieri	Addressing comments from TEHDAS2 Community et EC	Modified
30/01/2026	0.9	Julie Baussand Lucrezia Valieri	Addressing comments from the public consultation	Modified
30/01/2026	0.9	Anne Sofie Skødt Jørgensen	Submitted to TEHDAS2 consortium and EC	
20/02/2026	1.0	Julie Baussand Lucrezia Valieri	Addressing comments from TEHDAS2 Community et EC	Modified
20/02/2026	1.0	Anne Sofie Skødt Jørgensen	Submitted from PSG decision	Modified
27/02/2026	1.1	Julie Baussand Lucrezia Valieri Anne Sofie Skødt Jørgensen	Addressing comments from PSG decision meeting	Final
31/03/2026	1.2	Louisa Stuwe Juliette Chambon Anne Sofie Skødt Jørgensen Alexander Knudsen Julie Baussand Lucrezia Valieri	Addressing comments from HaDEA's rejection letter	Modified

Accepted in Project Steering Group on 24 February 2026.

Contents

1 Executive summary

This document provides comprehensive, non-binding guidance to health data access bodies (HDABs) on both the fee structure for accessing electronic health data for secondary use under Article 62 of the European Health Data Space (EHDS) Regulation and the exercise of their supervisory and enforcement powers under Articles 63 and 64.

The EHDS establishes a common European framework for the lawful, transparent and trustworthy secondary use of electronic health data through the HealthData@EU infrastructure, and HDABs play a central role in ensuring its effective implementation. From a principles-based and operational perspective, the guidance clarifies which costs may be included in fees – focusing on operational and infrastructure costs directly linked to EHDS procedures such as data access applications and data requests – and which costs must be excluded, including data collection and processing carried out for medical purposes, the data discovery phase, costs related to informing natural persons of significant health findings, and costs already publicly funded. It addresses to whom and when fees should be paid, recommending in particular a centralised single-invoice model with conditional staged payments managed by the HDAB, while allowing sufficient flexibility for Member States to integrate the model into existing national systems and contractual arrangements. To promote transparency, fairness, non-discrimination, proportionality and competition neutrality across Member States, the document recommends EU-level safeguards to mitigate economic disparities, encourages a minimum baseline for any fee reductions applied to specific user categories, and calls for the proactive publication – via HDABs – of clear information such as price lists, illustrative examples, FAQs and cost simulators.

In parallel, the guidance supports HDABs throughout the full supervisory lifecycle, from the early detection of potential non-compliance by data users or holders, through corrective measures such as permit revocation or exclusion from access, to the imposition and proportionate quantification of administrative fines that are effective, dissuasive and consistent with EU and national law. It also recommends that each HDAB make publicly available its national governance framework and dispute settlement procedures. This document should be regarded as a living instrument, subject to future updates in light of implementing and delegated acts adopted by the European Commission in cooperation with the EHDS Board.

Abbreviations

Term	Abbreviation
European Health Data Space	EHDS
European Union	EU
General data protection regulation	GDPR
Joint action	JA
Health data access body	HDAB
Trusted health data holder	TDH
Health data holder	DH
Health data user	DU
Information technology	IT
Secure processing environment	SPE
Small and medium-sized enterprise	SME
Central processing unit	CPU
Graphics processing unit	GPU
Finnish Innovation Fund	Sitra
Towards the European Health Data Space	TEHDAS
Work package	WP

2 Introduction

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 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.

TEHDAS2 Work Package (WP) 4 "Collaboration models", coordinated between the Danish Health Data Authority and the Digital Health Delegation of the French Ministry of Health, aims at defining guidelines for the organisational implementation of the EHDS for health data access bodies in the EU. More specifically Task 4.1 is divided into two sub-tasks: 4.1.1. on fees led by the French Health Data Hub, and 4.1.2 on penalties, led by the Italian Ministry of Health. In this document, the recommendations for each subtask are organised into two separate sections, in light of the distinct nature of the topics addressed and the different methodologies employed.

This document should be understood as an expert opinion and guidance document developed within the TEHDAS2 framework, reflecting technical and expert input from the project partners. It is not legally binding and does not constitute a formal guideline or technical specification under the European Health Data Space.

This document does not represent the position of the European Commission.

Legally binding and enforceable requirements under the European Health Data Space are laid down in Regulation (EU) 2025/327 and, where applicable, in implementing acts adopted by the European Commission, within the limits of the empowerments provided by the Regulation.

Section 1: Guideline on fees related to the EHDS Regulation

3 Context for the guideline on fees

3.1 Purpose of the guideline

The purpose of the guideline is to provide guidance to health data access bodies (HDABs), trusted health data holders (TDHs) and health data holders (DHs) on the policy in respect of fees which can be levied on data users in order to access health data. The guidelines concern financial practices related to data access application, data request and simplified procedures with TDHs. Please note that any reference to DH shall be understood to include TDH, which are DHs assigned with specific missions only in the context of simplified procedures. Data access application (Article 67) refers to an application seeking to access individual-level electronic health data for secondary use in an anonymised or a pseudonymised format for the purposes referred to in Article 53 of the EHDS Regulation.

Data request (Article 69) refers to the procedure where the applicant may submit a health data request for the purposes referred to in Article 53 of the EHDS Regulation with the aim of obtaining a response only in anonymised statistical format.

The simplified procedure with TDH (Article 72) applies to both data access application and data request that concern only electronic health data held by the TDH. In such cases, the TDH may assume certain responsibilities normally carried out by the HDAB.

3.2 Problem being addressed

Health data is generated in various contexts in connection with the provision of health care. Re-using or re-purposing existing health data is a major priority for European health policies. One of the objectives of the EHDS is to create a common secure framework at European level to facilitate and supervise the reuse of health data for research, innovation and public policy purposes. In practice, this effort is associated with costs incurred by the various entities that cooperate to make data available. These guidelines address the need to support coherent and transparent practices across the EU regarding fee practises for health data access. The objective is to promote consistent financial practices across Member States in line with the principles of transparency, non-discrimination and competition neutrality set out in the EHDS Regulation.

3.3 Methodology

A survey aimed to collect insights on health data fee practices and to benchmark existing fee structures and policies across EU Member States was distributed to the competent authorities of TEHDAS2, covering 29 countries. A total of 24 responses were received, mainly from Member States, along with contributions from European institutions and industry federations. A comparative analysis of the responses was carried out, supported by targeted interviews with selected countries to explore specific aspects in more depth. Based on this preliminary work, several scenarios were developed and discussed in workshops with the work package members. These discussions formed the basis for the recommendations presented in this guideline (see Annex1 for details).

The draft document was then opened for public consultation for two months, receiving 83 comments. Respondents represented various roles, including data holders, public and private data users, and health data access bodies. Contributions came from 17 EU and EEA countries, although Eastern Europe and international organisations were underrepresented. Most participants were from public, academic, research, and private organisations. Changes were made to the text to reflect the main feedback from stakeholders (see Annex2 for details).

3.4 Target audience

This guideline is written for HDABs, TDHs and DHs to help to align practices at the EU level regarding fees that can be claimed from data users (DUs) by contributors in the health data access procedure (HDAB, DH, TDH).

4 Proposal for fee guidelines under the EHDS

In the context of the subtask 4.1.1 on fees, a comparative analysis of existing structures and pricing policies has been conducted and workshops organised to provide an overview of current approaches and experiences across Europe. The guidelines provided here state recommendations on which activities and costs may be considered eligible for fee calculation, and how financial flows between stakeholders may be structured under the EHDS frameworks. The work reported in this document aims to characterise the fees and invoicing that go with this framework while recognising that existing national mechanisms or contractual agreements may remain in place, provided they are consistent with the principles set out in the EHDS Regulation.

4.1 Scope of the work

This guideline is part of a series developed under TEHDAS2 to operationalise the EHDS regulation, specifically addressing Chapter IV on secondary use of health data.

Article 62 addresses the fee aspect of data access. HDABs, including the Union health data access service, as well as TDHs, may charge fees for making electronic health data available

for secondary use (62(1)). Fees may include compensation for the costs incurred by the DH for compiling and preparing the electronic health data to be made available for secondary use (Article 62(2)).

Recital 70 outlines the legislator intent regarding the fee structures and operational implementation. HDAB should be able to cover the costs of their operations with fees set up in a proportionate, justified and transparent manner. DHs should be allowed to also ask for fees for making data available which reflect their costs. The DU ought to be charged such fees by the HDAB in a single invoice.

The EHDS regulation identifies several steps in the DU journey that can be categorised as presented in Annex 3:

- **Data discovery**: the DU needs to investigate whether the data needed is available, and whether it is available in the necessary format for the secondary use purpose.
- **Data access**: the DU fills in and submits a data access application form or a data request to a HDAB.
- **Data preparation**: the DH delivers the necessary data to the HDAB, which starts to prepare the data for secondary use in accordance with the conditions set in the data permit or data request approval. In the case of a simplified procedure, the data are prepared and delivered by the TDH.
- **Use of data**: the DU performs analysis based on the received data for the purpose defined in the application phase.
- **Finalisation**: the DU performs the analysis and publishes the results.

The scope of this guideline begins with the data discovery phase, once the applicant has identified the datasets of interest in the dataset catalogue and finishes at the end of the use of data. Recommendations proposed here focus on compensation of costs related to the data access, data preparation and use of data phases. This document provides guideline for the following questions:

Which costs can be considered in the fees and what costs cannot: several activities are identified as necessary to answer requests for secondary use of health data. Those activities generate costs based on human and IT resources. The question addressed here concerns which costs can be recoverable through a fees mechanism, whether marginal (costs initiated by the request) or fixed (generated prior to the request and in order to optimise data access).

To whom the fees are to be paid: health data access procedures may involve multiple stakeholders depending on the type of application/request, and these parties need to be compensated for their activities and services. The question addressed here concerns how these contributors coordinate to invoice DUs and collect the fees.

When the fees are to be paid: health data access procedures involve several successive phases which may be subject to financial compensation. The question addressed here is when the payment of fees is due from the DU.

4.2 Current situation – feedback from survey and interviews

4.2.1 Findings: common patterns and divergences across Member States

The results of the survey, conducted following the methodology described in Annex 2, indicate that nearly half of the respondents (46%) reported the absence of formalised pricing practices for data provision, while 63% stated that there is no regulatory framework governing the application of fees for the sharing of health data. The varied responses to the survey questions reflect the differing levels of maturity on this matter among countries and underscore the heterogeneity of practices both between and within countries. For instance, while some respondents report full cost recovery (e.g., Sweden), others offer free access to data (e.g., Slovakia). In certain cases, price lists are available for data applicants (e.g., Statistics Denmark, Dutch Statistics Office, Statistics Lithuania), although these lists are limited to specific entities and do not represent the practices across the entire country. Where no national pricing framework exists, fees are typically set by DHs with varying degrees of transparency and standardisation.

Similarities were observed in the application of fees. Fees are generally stated to be based on the effort required for data preparation and mainly based on hourly rates. In addition to personnel salaries, these rates may include material, operation and infrastructure costs. Computational resources and disk space/cloud services costs, as well as administration overheads, are also frequently reported to be included in fees. Some entities offer fixed-price packages, drawing from their experience with use cases.

The profile of DUs is a common factor observed to modulate fees, and reduced fees are frequently reported with a different rate for academics, students, patient organisations and small enterprises (SMEs). The type of project is another factor for reduced fees depending on how the project is funded or whether it includes collaboration with the DH. Which may impact on the level of fees charged are the type of data, the required support for data analysis or the volume of data, which impact the time spent and resources consumed.

4.2.2 Challenges

The most frequently reported challenge anticipated by the respondents of the survey is the capacity to align fees and fee practices within countries (regions, entities) and among Member States. Some Member States already have implemented practices, future HDABs may have a different legal status with specific constraints and different resources. The EHDS framework will need to account for these specificities in promoting coherent implementation of fee practices, without undermining legitimate national arrangements. Moreover, economic situations differ amongst Member States, including in respect of salary levels and technological provisions costs, which will impact on the level of fees to be charged. This may potentially create an imbalance in the distribution of the HDAB burden across Europe when data is substitutable among countries. It may also impact cross-border access to health data for certain populations and undermine the representativeness of some countries in European studies. Such a phenomenon (limiting cross-border access to health data for users from certain Member States and reducing the participation of researchers from certain countries in European research) would undermine the intended effects of implementing the EHDS and may exacerbate differences between Member States.

In a more general manner, the capacity to maintain preferential pricing schemes for academics and small companies is perceived as an important matter to ensure a level playing field for research and innovation in the EU. Finally, several Member States highlighted the importance of cultural and organisational change, as well as the need for further guidance, capacity-building, and coordination mechanisms.

4.3 Principles guiding the fees

Article 62 sets out the principles that must guide the fees charged on DUs. These include transparency, non-discrimination, proportionality, and competition neutrality.

Transparency refers to the need to show the correlation between the fees charged and eligible costs incurred in reply to the DU's request for health data access. Before issuing a data permit or providing a response to a health data request, the HDAB shall inform the health data applicant of the estimated fees (Article 62(5)). When fees are claimed, the DU is provided with an invoice describing the amount of the fee (with the currency used) and what it covers.

Non-discriminatory practice involves equal treatment between actors. Non-discrimination requires that DUs of the same category are treated equally, regardless of nationality, and are charged equivalent fees in proportion to the actual costs incurred. Certain categories of DUs located in the EU may benefit from reduced fees, such as public sector bodies or Union institutions, bodies, offices and agencies with a legal mandate in the field of public health, university researchers or microenterprises (Article 62(1)). The category of DUs eligible to such reduction is defined at the discretion of each Member state.

The fees must be proportionate to the cost of making the data available and they shall not restrict competition. It implies that the conditions for application must not be used to distort or restrict competition in the market. This includes ensuring that fee structures do not create undue barriers to any categories of eligible DUs regardless of their size. The market whose competitiveness is to be supported by the fees is understood as the EU internal market, which follows from the policies that led to the creation of EU data spaces including the EHDS, and as specifically expressed in recitals 1 and 110 of the EHDS regulation.

4.4 Which costs may be claimed as fees

Fees should reflect the eligible and necessary costs actually incurred in responding to a DU's request. Cost eligibility must remain strictly linked to the actual costs incurred in making data available for secondary use, in full compliance with the legal scope defined by the EHDS Regulation. This section outlines the relevant costs associated with data access applications, data requests, and the simplified procedure involving TDHs, and distinguishes between costs that can be recovered through fees and those that must be excluded.

Excluded costs

Three main categories of costs are excluded from the fees.

- **Data collection and processing realised for medical purposes**: All costs associated with data collection and processing carried out for medical purposes (primary use) are excluded from the fees. These costs cannot be recovered from DUs. However, specific efforts deployed to support the future secondary use of these data ("by design"), used in the primary care context, could be eligible if they are necessary to enable access for a specific secondary use request and are not related to already funded primary use costs (i.e. no double compensation). Collection costs may also be eligible for registries dedicated to secondary use by design.
- **Data discovery phase**: All costs related to the creation, updating, and maintenance of the metadata records and catalogue (Article 77) including quality labelling (Article 78), as well as the use of the metadata catalogue by the DU to identify datasets are out of scope (see Annex 5 for list of costs). These costs are not directly related to a data access or request and cannot be recovered from DUs since the dataset descriptions and the catalogue are regulatory obligations, not user-specific services, and therefore not fee-eligible. However, although the EHDS Regulation generally excludes costs related to the data discovery phase from recoverable fees, there may be specific cases where project-specific discovery activities required substantial effort and led to key preparation work. As an example, some projects, relating for example to emergencies, operating rooms, cancer, etc., sometimes involve searching for dozens or hundreds of variables scattered across multiple databases and tools that are not configured in the same way and use different languages. Since the data is collected in real life using tools not designed for research and innovation, this phase also involves analysing its usability (structured/unstructured, pseudonymisable personal data or not, etc.), completeness, and quality. This step is a prerequisite for integrating new data and is clearly a very significant cost centre that cannot be avoided for making data available for secondary use. While not foreseen in the Regulation, these situations deserve further reflection for related costs to be eligible for fees.
- **Information on significant findings**: All costs related to informing a natural person about significant health findings identified by DUs (Recital 67, Article 58(3)) are out of scope for fees. While complying with this obligation under the EHDS regulation may require significant time and resource investment from DHs, these costs cannot be recovered from DUs.

In addition to the excluded categories of costs, any costs that are already covered by funding cannot be used to justify fees (i.e. no double compensation). The purpose of the fee is to compensate HDABs and/or DHs for the actual costs incurred in making health data available for secondary use. Therefore, any expenses already financed through other sources, whether public or private, must be excluded from the fee calculation.

Eligible costs

Costs which may be considered for fees (also referred as "Eligible costs") have been grouped based on activities related to:

- Receipt of a data access application/ data request
- Data permit/Data request approval

- Data preparation for the request
- Provision of the data
- Use of the data

Costs may vary depending on the practices and infrastructure in place at the national level or within individual DHs' organisations. A detailed cost breakdown is provided in Annex 3. This table serves as a reference framework for fee calculation, illustrating the types of costs that are eligible and identifying the parties responsible for them. However, it is intended to be adaptable by each Member State, HDAB or DH, in line with their specific infrastructure and operational practices. For example, costs labelled as "fixed" in the table may be considered "marginal" depending on the chosen method for carrying out the task (see section 4.4.3 for example). Additionally, costs associated with HDABs (in Annex 5 or in the text below) may be borne by different stakeholders depending on how responsibilities are distributed among them. Similarly, in cases where the HDAB is a data controller and acts as a DH, the HDAB may claim related costs incurred in the same way as any other DH. Lastly, it should be noted that as data technology evolves, the list of eligible costs presented in this document may also change and it cannot be regarded as exhaustive.

In all cases, fees can only be related to costs incurred to reply to the access request, they must be transparent and clearly stated to the DU. Fee eligibility must remain strictly linked to the costs of making data available for secondary use. If a DU legitimately cancels its application, the process shall be terminated, and the DU shall be charged only for the costs incurred up to the time of cancellation.

4.4.1 Receipt of a data access application/data request

Once submitted by the data applicant, the completeness and the plausibility of the application are verified to ensure the HDAB has all the necessary information to proceed with the request. Further details on the application check process are provided in [2].

Once checked, the HDAB shall make public the application through electronic means (Article 57(1 j(ii)). The HDAB must contact the relevant DH (holder of dataset identified by the DU) to determine whether the data can be extracted in the manner indicated by the applicant. The DHs will provide to the HDAB a fee estimate associated with the data extraction. The HDAB consolidates the estimated fees from all relevant contributors and communicates a single transparent fee estimate to the applicant. At this stage, the applicant shall be given the possibility not to accept the fees estimation and either review the application to reduce the estimated costs or withdraw the application (Article 62(5)). The DU should be provided with a breakdown of the data preparation fees for each dataset to allow for the application to be reviewed and costs reduced. If the application is withdrawn, the applicant shall only be charged for costs incurred so far. For this step, HDAB may charge fees to the data applicant for all actual project-specific eligible costs incurred:

- the management of the application (application check process),
- the running and updating of the public information system (transparency portal),
- the regulatory feasibility,
- the assessment of the datasets to be requested to DHs
- the preparation of the fee estimates to respond to the request.

- related administrative overheads directly linked to the request (see Annex 5 for the list of proposed overheads)

DHs may charge fees to the data applicant for all actual project-specific costs related to:

- the examination of the protocol and feasibility study to assess the capacity to provide the requested data based on the protocol
- the preparation of the quote to respond to the request.
- related administrative overheads directly linked to the request

Further guidance is provided regarding the examination of the protocol and feasibility study in [1]. The list of identified costs that may be incurred for the various tasks across this step of the EHDS procedures is provided (Annex 5).

4.4.2 Data permit/data request approval

Once the application is deemed complete and the DU accepts the costs estimate as provided, the assessment process to grant the permit or approve the data request continues. Details on the assessment process are provided in [2].

If the data requested include materials subject to intellectual property rights or containing trade secrets, the HDAB must assess whether and/or under which conditions the reuse can be authorised in accordance with Article 52. Further guidance on assessing the intellectual property rights as part of the HDAB's application assessment is provided in [3]. In the specific case of a Data Access Application and if required by the laws of the Member State, the project must be submitted to an ethics committee prior to processing.

Based on the completed assessment, the HDAB shall issue a decision to either grant or deny access to the requested data. All decisions, whether approved or refused, must be published, including the reasoning in case of refusal, in accordance with Article 58(1) point (f).

For this step, HDAB may obtain compensation for eligible, project-specific costs incurred for the following activities during the assessment phase:

- the assessment of the application against the criteria in EHDS (Article 68(1)), including the ethical evaluation where required (Article 68(1) point (f)
- the risk mitigation analysis for IP and trade secrets (Article 52)
- the permit/data request decision with justification
- the risk analysis for national defence, security, public security and public order (Article 63 and Article 68)
- the updating of the public information system
- project contracting and monitoring
- related administrative overheads directly linked to the request

The list of identified costs that may be incurred for the various tasks across this step of the EHDS procedures is provided (Annex 5).

4.4.3 Data preparation for the request

Upon issuing a data permit in the case of a data access application or data request approval in the case of a data request application, the HDAB shall request data extraction from the respective DHs (Article 68(7)). DHs shall put the requested electronic health data at the disposal of HDAB. Further guidance is provided for DHs in [1].

Database constitution and data collection upon request

DHs may adopt different data preparation strategies to make data available for secondary use, depending on their technical architecture, internal capacity, and the anticipated reuse potential of their datasets.

For instance, the strategy based on the collection of data upon request is likely best suited for DHs with a limited number of data sources and/or relatively simple data, where the costs and time required to extract and prepare the data are deemed manageable. This strategy involves marginal costs and therefore incurred for each DU request.

The strategy based on the constitution of a database is more adapted to DHs for which the scope of effort for compiling data is high and/or expect a high number of permits concerning their data. This is particularly relevant for hospitals for instance which generate a high volume of diverse data across multiple information systems and with a significant potential for re-use. By identifying, extracting, combining and pre-processing data in advance for secondary use, these DHs can anticipate future requests, accelerate data access and share costs among DUs. This strategy involves fixed costs or structuring costs, which may be compensated for proportionally across multiple data access requests, using a transparent and non-discriminatory cost-sharing methodology.

Secondary use strategy-dependent costs

In this step, DHs may be compensated for the actual, eligible costs incurred in preparing the requested data from the data applicant for:

- project monitoring
- patient information for the use of their data in the concerned project for which the data are requested
- data selection, extraction including data minimisation and pseudonymisation/anonymisation (either from operational information systems or from a data warehouse)
- data consolidation
- data export to HDAB

Depending on the DH's strategy, certain additional cost structures may apply. If using a data warehouse model, DHs may be compensated for fixed or structuring costs associated with:

- data extraction from the initial information system

- data quality improvement related to data compiling and preparation activities (see Annex 3 for details)
- data linkage between data from different data systems and related quality assessment
- data storage and infrastructure costs for running, maintaining and updating
- regulatory obligation to inform natural persons on the treatment of their data in the data warehouse
- If operating on a per-request basis, DHs may be compensated for marginal costs specific to each request, including:
- data quality improvement related to data compiling and preparation activities
- data linkage between data from different data system

When requested data are partly available in a warehouse but require additional data extraction, a combination of fixed and marginal cost recovery is appropriate, using a transparent methodology proportionate to the actual effort incurred. The list of identified costs that may be incurred for the various tasks across this step of the EHDS procedures is provided (Annex 5).

4.4.4 Provision of the data

Once the HDAB receives the data from the DHs, the data is prepared to be made available to the DU.

In this step, HDAB may charge fees to the data applicant for all project-specific costs related to

- project monitoring
- data quality, linkage (with linkage quality assessment) and consolidation
- pseudonymisation or anonymisation
- data treatment to preserve protection of intellectual property and trade secrets
- dataset validation
- related administrative overheads directly linked to the request
- technical resources used (e.g. CPU time, disk space allocation, cloud services, licenses)

In the specific case of a data request, the HDAB shall provide the DU with access to anonymised, aggregated statistical results. The HDAB may also obtain compensation for the actual, eligible costs related to:

- preparation of the analysis plan for data aggregation and implementation
- generation of the aggregated data

In the specific case of a data permit access, the HDAB shall provide the data applicant with access to anonymised or pseudonymised electronic health data within a secure processing environment (SPE). The HDAB may also obtain compensation for the actual, eligible costs related to:

- preparation of the project space in the SPE

- data export to the project space
- adaptation and development of tools
- licences for tool provision
- validation of the project space
- access to the SPE, additional services from SPE providers and environment updates (software and maintenance)
- project and analysis space provision (user training and support)

The list of identified costs that may be incurred for the various tasks across this step of the EHDS procedures is provided (Annex 5).

Please note that if HDAB or TDH has more than one SPE available, these SPEs may offer different prices. Where possible, DUs should be able to choose the SPE that provides the most favourable pricing.

4.4.5 Use of the data

The DU can perform analyses based on the received data in the SPE for the purpose defined in the permit and for the duration of the data permit (Article 68). An extension of the permit can be asked by the DU (Article 68(12)).

In this step, HDAB may obtain compensation for eligible costs related to the data applicant for all project-specific costs related to:

- project closure, activities, including final reporting, data archiving, and controlled data destruction
- long-term storage of metadata or audit logs, where required under national law
- In the specific case of data access application where project-specific and scalable SPE costs incurred, HDAB may also obtain compensation for costs for:
- continued allocation of computing resources and storage
- permit extension and related SPE updates linked to the permit extension

More details on the secure processing environment are provided in [4]. The list of identified costs that may be incurred for the various tasks across this step of the EHDS procedures is provided (Annex 5).

4.4.6 Simplified procedure with a trusted health data holder

Where an HDAB receives a health data access application or a health data request that only covers electronic health data held by a TDH, a simplified procedure for access shall be applied (Article 72).

Health data access applications and health data requests are forwarded to the relevant TDH who assesses the health data access application or health data request against the same criteria as the HDAB. The HDAB shall not be bound by the proposed assessment submitted by the TDH and makes the decision to issue the data permit or to approve the health data

request. Once the permit is granted or the data request approved, the TDH prepares the health data and provides access to the data applicant via an SPE.

In addition to standard DH costs, a TDH may obtain compensation for actual, eligible costs incurred in performing its specific responsibilities under Article 72, including data preparation and SPE configuration (see Article 72 for details on TDH responsibilities). These costs correspond to those borne by the HDAB in the other procedures (see Annex 5 for more details on costs).

4.4.7 How are the fees calculated

The EHDS Regulation does not mandate charging fees; compensation may range from partial to full, depending on the chosen national approach and the funding context of the actors involved. However, any such approach must be non-discriminatory, documented and consistently applied.

Both marginal and fixed eligible costs may be recovered through these fees. In all cases, fees must be transparent, non-discriminatory and not restrict competition (see section 4.3).

> **Marginal costs**: Fees are calculated based on the specific resources used to process the application. For human resources, the cost is determined by the time required to handle and deliver the application, applying an hourly rate derived from staff salaries. For technological resources, the cost is based on the consumption of infrastructure required by the project (e.g., disk space, CPU, GPU).
>
> **Fixed or structuring costs**: These are expenses incurred to build or maintain infrastructure for secondary use independently of any specific application (e.g., database development, data modelling, data quality, standardisation, licences). They may be annually compensated for through proportional allocation among users, using a transparent methodology.

Although the regulation does not mandate a harmonised method for calculating fees, the general principles of proportionality, fairness, and transparency must still be respected. To uphold these principles, the HDAB and DH should publish the methodology they use for fee calculation and ensure that no general infrastructure investments are recovered beyond the costs directly attributable to secondary use. The method may be determined at the national level, according to applicable standards. Over time, efforts should be made to foster convergence across Member States.

As an example, a simplified method is proposed to illustrate a way to calculate extraction and processing fees for data pre-processed in a secondary-use database, aiming to ensure a fair, proportionate and rational fixed costs distribution for DUs. The method relies on an annual estimation of the costs allocated to health data categories, along with the projected number of projects (i.e. it requires annual recalibration to remain proportional to the evolving volume of applications and projects). Note that the simplified method below is provided as an example to illustrate a possible way to compute fees related to fixed costs for secondary-use database only and is representative of a later phase since three-year costs retrospective is required.

First, data blocks are identified, and the associated eligible costs are isolated. Data block refers to a coherent set of health-related variables, for instance that are extracted and processed together due to their clinical, analytical, or operational relevance. These variables form a meaningful unit of information, as they are typically collected, interpreted, or used in combination to support a specific medical, research, or administrative purpose. For example, in hospitals, data block could include laboratory data, medication administration data, medical questionnaires, intensive care monitoring data, radiology reports, etc.

The annual estimated costs directly attributable to secondary use for extracting and pre-processing each data block from the information system to the databases ($Cost_{DBk}$) can be calculated as the average of the eligible costs incurred for the extraction and processing of that block over the preceding three years. The amount of data for each block can be formalised by the number of patients it concerns (Nb $patients_{DBk}$). For each data block, a weighted average cost (WAC_{DBk}) is calculated as follows:

$$WAC_{DBk} = Cost_{DBk} / \text{Nb patients}_{DBk}$$

For each DU's application, the fees represent the cost allocated per project among the DUs for each requested data block and depending on the number of patients requested by each DU (Nb $patients_{REQ}$). The anticipated number of projects using a specific block of data can be estimated by the average number of projects that used that block of data over the last three years (Nb $project_{DBk}$).

The fees related to the extraction and pre-processing of data in a secondary-use database (i.e. fixed costs) for a given project (F_{REQ}) is calculated by the sum of the costs per data block and weighted by the number of patients requested by the DU:

$$F_{REQ} = \Sigma_{DBk} [(\text{Nb patients}_{REQ} \times WAC_{DBk}) / \text{Nb project}_{DBk}]$$

It is not intended that this example be taken as mandatory or binding and can be adapted by stakeholders or replaced by a more relevant approach respecting the general principles of proportionality, fairness, and transparency. As long as these general principles are respected, predefined rates, usage-based pricing, or package-based approaches, together with regular review and updating of cost models are also encouraged to be considered.

4.4.8 Fee applicability

In this work, actors such as SPE providers or data intermediaries are considered subcontractors, and their costs are therefore borne by the service contractor (HDAB, DH, or TDH) who can report those costs in the fees if they fall within the eligible costs. Health data intermediation entities are legal persons mandated to carry out the duties of certain categories of DH. The question whether these intermediaries are subject to the same fee policies as the DH is suggested in recital 59 indicating that "the data shall nevertheless be considered as being made available by several health data holders." It is recommended to clarify the fee policies applied to data intermediaries regarding their tasks in processing health data for secondary use.

It should be noted that disparities in national cost structures, salaries, purchasing power, pricing maturity, and legal frameworks will directly affect fees. It is therefore recommended that safeguards be put in place at EU level to prevent imbalances in the distribution of the HDAB burden across Europe when data are substitutable between countries, and to ensure competitive neutrality. Additionally, safeguards against national mechanisms that could lead to price dumping or competitive distortions are encouraged in order to prevent market imbalances.

In addition, it is recommended that non-EU (third countries) data users requesting access to European health data pay a significantly higher fee, in order to create a genuine preference for European actors and ensure a meaningful contribution to the European system from which the DU will benefit through the EHDS.

Finally, Member States may establish reduced fees for certain types of DUs located in the Union (Article 62(1)). The category of DUs eligible to such reduction is defined at the discretion of each Member state. A minimum EU-level baseline where such reductions are applied is recommended in order to prevent national divergence as well as ensure consistency for DUs and sustainability for DHs. This baseline could include criteria to define harmonised reduction rates per user category and should also encourage the provision of alternative compensation mechanisms for DHs at national level.

4.5 To whom the fees are paid

To address this question, three invoicing scenarios were considered. Each model presents distinct advantages and implementation challenges, particularly regarding administrative complexity and legal compatibility with national systems.

4.5.1 Scenario overview

Scenario 1 (Centralised model): This scenario, inspired by Recital 70 (non-binding), Article 62 and the enacting terms, involves a centralised invoicing system where all fee estimates are sent to the HDAB. The HDAB then consolidates these costs into a single invoice directed at the DU. Fees are paid to the HDAB who redistributes to stakeholders based on incurred costs. This scenario is found to limit the burden for the health data applicants who receive one invoice from all stakeholders but to increase the administrative burden for HDAB as it brings many additional invoicing steps and possibly considerable delays by DHs between data delivery and invoicing.

Scenario 2 (Decentralised model): Under this model, HDAB, TDHs and DHs issue their own invoice directly to the data applicant. Fees are paid to each stakeholder based on their invoice. While this reduces the workload for the HDAB, it poses a challenge for smaller DHs, both public and private, who may lack the resources to manage invoicing for activities outside their core activities. It also increases the burden on DUs, who must handle multiple invoices and make payments that are not coordinated with each other, nor aligned with the centralised data delivery managed by the HDAB.

Scenario 3 (Hybrid model): The hybrid approach allows for flexibility in invoicing. The HDAB offers to either centralise the invoicing or allow DHs to issue their own invoices if they have the maturity to do so. Fees are paid to the invoice sender. This model gives DHs autonomy in managing their fees when relevant, while offering the HDAB the option to streamline the process as necessary. In this scenario, TDHs operate independently in invoicing and fee collection when the request concerns only the electronic health data they hold.

4.5.2 Recommendations

The centralised model (scenario 1) is the recommended implementation baseline, as it reflects the approach described in Recital 70 of the regulation. While not legally binding, this recital provides a strong interpretive indication of the legislator's intent to streamline interactions between DUs and the overall system. In this model, the HDAB acts as the sole financial interface: it collects fee estimates from all the relevant actors, issues a single consolidated invoice to the DU, collects payments from DUs and redistributes the relevant shares to the contributors. This approach ensures simplicity and transparency for the DU, while consistent with the centralised procedural logic of the regulation. The single invoice should clearly identify the costs attributable to each stakeholder, providing users with transparency on which costs originate from which actor, thereby supporting trust and accountability. An invoice template jointly defined and validated by the HDABs of all Member States is encouraged to harmonise invoices at EU level and clarify what is expected from DH. However, flexibility must be preserved to account for divergent national legal frameworks, administrative traditions, and operational maturity. Member States may therefore adopt a model adapted to their specific national context, provided that the principles of transparency, consistency, and proportionality are respected, as required under Article 62(6).

In particular, while centralising invoicing at the HDAB level is encouraged, the HDAB should have the option to delegate its invoicing responsibilities to DHs when a single source of data is required by the DU and when this aligns with local practices and with the maturity of those actors. In such a case, HDAB and DH could either assume responsibility for their respective invoices or DH could centralise invoices. In particular, the role of TDHs could be further reinforced in the simplified procedure in this scenario, where they may operate autonomously in invoicing and fee collection. In this reinforced procedure, the HDAB retains responsibility for issuing the final permit, but the TDH manages the technical implementation and associated billing. Such flexibility is considered essential to ensure operational efficiency and alignment with local realities.

4.6 When the fees are paid

Two scenarios have been discussed regarding when fees should be invoiced to and paid by DUs during the data access procedure.

4.6.1 Key concepts

To support the scenarios, the following key concepts are introduced:

- **Invoice**: A legally binding commercial document, detailing the complete cost structure with breakdowns by services and DHs. It contains disaggregated cost elements (fixed costs and estimated components), typically at the task level to favour clarity and transparency.
- **Request for payment**: A formal request submitted to the DU for payment of the actual costs corresponding to work completed during a specific period. It follows the structure defined in the original invoice and refers to the relevant cost components outlined therein.
- **Payment instalment**: One of several scheduled payments made in response to requests for payment. Each instalment corresponds to a portion of the total cost, aligned with the progress of the procedure or delivery of services.
- **Payment**: The financial transaction by which the user transfers the requested amount to the HDAB, TDH or the DH in response to a request for payment.

4.6.2 Scenario overview

Scenario 1 (Single invoice with conditional staged payments model): a single invoice is issued to the DU at the beginning of the procedure, once the HDAB has received fee estimates from all relevant stakeholders in response to a data request or data access application (as indicated in section 3.4.1) prior to the data permit/data request approval phase. The invoice details all potential cost components that may arise throughout the procedure and clearly indicates which costs are payable upfront and which are conditional upon progression to later phases. While fixed prices should be used whenever possible, any estimated components must be clearly identified as such on the invoice and presented with appropriate ranges or formulas to account for variability (e.g., hourly rates, per gigabyte charges, etc.). Payment instalments are predefined in the invoice, specifying when each conditional payment becomes due. These instalments may be scheduled periodically or based on key milestones, or a combination of both, depending on the phase of the procedure. Requests for payment are submitted to the DU in accordance with the instalment schedule, triggering the corresponding payments of the actual costs as the procedure advances and services delivered.

Scenario 2 (Two-stage milestone-based invoicing model): Unlike Scenario 1, where a single invoice covers the entire procedure from the outset, this model splits invoicing into two distinct stages aligned with key milestones. The first invoice is issued at the beginning of the procedure, once the HDAB has received all relevant fee estimates in response to a data request or data access application prior to the data permit/data request approval phase. It covers cost components referred in sections Receipt of a Data (4.4.1), Data permit/Data request approval (4.4.2) and Data preparation for the request (4.4.3). The second invoice is sent when the data are ready to be delivered in the SPE. It covers costs components referred in sections Provision of the data (4.4.4), and Use of the data (4.4.5). As in Scenario 1, both invoices include predefined payment instalments, which may be scheduled periodically, by milestone, or both. Requests for payment are issued in line with the instalment plan, triggering the corresponding payments as the procedure progresses.

4.6.3 Recommendations

The single invoice with conditional staged payments model (scenario 1), inspired by Recital 70 of the regulation, is the recommended implementation as it best reflects the legislator's intent. A single invoice is issued at the beginning of the procedure and outlines the full potential cost structure of the procedure, along with a schedule of payment instalments and to whom the costs are associated with. This approach requires estimating the total cost of the entire procedure from the outset. It enables the HDAB to provide the DU with a clear view of their potential financial exposure throughout the process. If the user proceeds beyond the application stage, the combination of payment instalments and requests for payment ensures that the DU is only charged for costs that have actually been incurred as the procedure progresses. Payment instalments should be made by the DU as soon as payment request is received, and no further actions in relation to the application should be taken until payment is completed. However, accurately estimating all costs from the beginning can be challenging. As the use cases for projects involving health data continue to evolve and HDABs gain operational maturity, the risk increases that the initial estimates from both HDAB and DH may diverge significantly from the actual costs incurred. This is particularly relevant in data access applications involving data use in an SPE, where infrastructure assumptions and computational needs must be projected long before the project is executed. The challenges associated with early transparent price calculation and managing operational expenses during data exploitation is something many HDABs may not yet be equipped to do confidently or that cannot be done as long as data is not prepared.

Therefore, flexibility should be granted to HDAB to apply a two-stage (or more) invoicing model when all costs cannot be reliably estimated at the outset. This alternative allows for more accurate fee estimation in the next invoice and helps avoid disputes or confusion with DUs in case of major discrepancies. Even when later stages are difficult to predict, the first invoice should still provide as much initial cost information as possible over the whole procedure to ensure transparency and user confidence. Consistent with this recommendation, this guideline does not prescribe a specific or detailed model for fee collection and distribution, as sufficient flexibility must be preserved to ensure operational efficiency and to accommodate national and local contexts.

To support prospective applicants, it is recommended that DHs optionally provide illustrative examples of past projects, potentially included in dataset descriptions or published on HDAB websites. FAQs and cost estimation tools (such as price lists, price ranges, maximum costs or simulators) available on the HDAB website are also encouraged to help users anticipate potential costs prior to applying. Although the EHDS regulation does not require any formal preliminary exchange between the DH and the DU, stakeholders may conduct a feasibility analysis and cost estimate beforehand through direct discussions under their chosen contractual terms. Pursuant to Article 57(1) point (l), HDABs are also encouraged to offer DUs a free consultation service, beyond their core regulatory duties, to provide basic guidance on key procedural steps and available datasets before submitting an application.

5 Modalities to resolve disputes

Article 62(4) sets out the procedure for resolving fee disagreements. If the DH and DU cannot agree on the fee within one month of data permit issuance or request approval, the HDAB may set a proportionate fee based on the costs of providing electronic health data for secondary use. The TDH cannot determine fee levels in the event of a disagreement between the DH and DU, as this falls under HDAB competence. Any disputes over the HDAB-set fee may be referred to dispute settlement bodies under Article 10 of Regulation (EU) 2023/2854.

Besides disagreements on fees at the outset, other disputes may arise during the process such as discrepancies between estimated and actual costs, payment instalment is not paid, insolvency, issues with data quality or reimbursement for data that does not meet the agreed specifications. To ensure all stakeholders have access to legal recourse, each HDAB should publish the national governance framework and procedures of dispute settlement bodies on its website and proactively communicate them to EHDS actors. Dispute settlement bodies should be independent from any EHDS actors in order to avoid conflicts of interest.

6 Areas for further exploration

Survey feedback, interviews and workshops realised in the context of the WP4.1.1 led to questions that appear to be important to raise while defining rules for fees.

Sanitary crisis: While many countries successfully adapted their practices to facilitate data sharing at the national level during the COVID-19 crisis, it is important to establish clear, EU-wide guidelines for managing similar situations in the future. In particular, guidance is needed on how fees should be handled in times of crisis – whether they should be waived, reduced, or remain in place, and for which types of users or purposes. A coordinated approach would ensure fairness, consistency, and rapid response across Member States during future public health emergencies. Although Article 62(1) allows fees to be charged “where appropriate”, a EHDS board-level guidance should clarify this point for crisis settings.

Data user solvency: The Regulation does not clearly specify how the solvency of the DU should be assessed prior to the launch of a project by the DH, nor how the HDAB should respond in insolvency situations. Solvency should be verified at an early stage of application handling, as part of the application completeness check. Where an applicant is found to be insolvent, the application should not proceed and should be terminated as early as possible, in order to minimise application handling costs and avoid such costs being borne by DH.

Cost discrepancies: Since the invoice is issued at the start of the procedure, actual costs may differ from the initial fee estimates, potentially leading to disputes between stakeholders. The procedure should therefore clearly define how such cost discrepancies are to be managed. Relying solely on estimated fees may result in overestimations that could discourage or exclude many potential DUs. Special attention should be paid to categories of applicants who, before submitting an application for health data request or access to HDAB, apply for external funding for their (usually research) projects and whose initial fee estimate becomes a fixed part of the project proposal. Conversely, basing charges only on actual costs when discrepancies are significant may jeopardise the successful execution of the DU’s project due to unforeseen financial burdens. Although scenario “Two-stage milestone-based

invoicing model" proposed in section 4.6.2 aims to mitigate this point, further guidance should be investigated.

Enriched datasets: A DU can enrich data in datasets provided to him in the SPE. The enriched dataset may have value for future DUs, so the question is how to do this and who bears the costs. The EHDS Regulation leaves the precise mechanisms for the processes associated with data enrichment at national level. Article 51(3) of the Regulation says: Member States may establish rules for the processing and use of electronic health data containing improvements related to the processing of those data, such as correction, annotation or enrichment, based on a data permit pursuant to Article 68. There are (at least) two deliverables in TEHDAS2 that define framework for data enrichment [5] and its handling in SPE [6]. The costs associated with data enrichment processes can be tracked for the following entities:

- SPE (possible longer period for dataset retain before it is moved to the destination DH, transfer of the enriched dataset to HDAB)
- HDAB (processing of announcements from DU who managed to enrich data in particular datasets, negotiation of these enrichments with the DH of the original dataset, temporary storing the enriched dataset (in local HDAB SPE), secure transfer of the enriched dataset to the DH, support of personal data protection tasks
- DHs (negotiation and tasks related to acceptance of the new dataset, creation or update of metadata to the new dataset, possible maintenance of two datasets instead of one original dataset)
- TDHs may have a partial combination of the costs indicated for HDAB and DHs

Effectively, there are costs also at DU level, as they should describe what they enriched in the dataset, and they shall report the enrichment. A framework for allocating and recovering these costs should be thoroughly examined and clearly defined.

Research costs for data access: optimally, researchers should be aware of the costs related to a data access application or data request in advance. They probably need this information when applying for a research grant. However, many problems arise with this:

- The researcher already requires some funding for the initial evaluation of the request and cannot include that part of the costs in the anticipated budget in the research grant proposal
- Research grants proposals are usually written at a very early stage and sometimes, 1 or 2 years pass until the research grant is actually granted so the estimation of the costs might not be accurate anymore

Public-facing cost estimation tools or standardised case examples could be provided by HDABs to address this point, the guidance that DH could provide to DU before they apply for the data should be further investigated and described.

Section 2: Guideline on penalties for non-compliance related to the EHDS Regulation

7 Context for the guideline on penalties

7.1 The role of health data access bodies under the EHDS Regulation

As part of the European Health Union, the EU is advancing the structured and lawful use of electronic health data for secondary purposes such as research, innovation, statistics, and public health policymaking. A key aspect of this effort is ensuring that access to data is not only effective across borders, but also subject to consistent oversight and enforcement mechanisms. These mechanisms are crucial for building trust, protecting individual rights, and guaranteeing the responsible use of sensitive health data throughout the EHDS.

TEHDAS2, the second joint action Towards the European Health Data Space, supports this ambition by providing practical tools and interpretive guidance for all actors involved in the implementation of the EHDS Regulation. In addition to developing technical specifications and user-facing documents, TEHDAS2 plays a vital role in supporting HDABs – the national authorities responsible for granting, monitoring, and enforcing access to health data under the Regulation.

Among the key areas of work undertaken in TEHDAS2 is the development of clear and operational guidelines to support HDABs in exercising their supervisory and sanctioning powers. These powers are articulated primarily in Articles 63 and 64 of the EHDS Regulation, which set out the conditions and procedures for taking enforcement actions, including revocation of data permits, imposition of exclusions from future access, and the application of administrative fines. HDABs are thus positioned not only as facilitators of secondary data use, but also as regulators tasked with ensuring compliance through proportionate and transparent means.

The overarching goal of this guideline is to foster a coherent interpretation and implementation of these enforcement provisions. It aims to support HDABs in determining when and how to intervene in cases of non-compliance, and how to ensure that penalties, including administrative fines, are applied in a manner that is legally sound, proportionate to the breach, and consistent with national procedures and fundamental rights.

While other TEHDAS2 work packages focus on operational and technical aspects of the EHDS infrastructure – such as secure processing environments (SPEs), data minimisation, and interoperability – this particular guideline complements them by addressing the legal and procedural responses to non-compliance. It provides HDABs with the necessary tools to act decisively and consistently in situations where obligations under the EHDS Regulation have not been met.

This document contributes to the broader TEHDAS2 effort to harmonise implementation across Member States, reduce legal and administrative fragmentation, and reinforce the credibility of the EHDS framework. It will also serve as a foundation for further implementing acts and European Commission guidance related to enforcement, as foreseen in Article 63(8). *Enforcement actions by health data access bodies under the EHDS Regulation complement, but do not replace, the supervisory and sanctioning responsibilities of national*

data protection authorities under the GDPR in cases where personal data protection issues are also at stake.

7.2 Methodology

A survey aimed at collecting insights on national practices related to penalties for the secondary use of health data was developed and distributed to the competent authorities participating in TEHDAS2. The objective was to benchmark existing approaches across Member States, with particular focus on criteria for the imposition and quantification of administrative fines, types of enforcement measures, and procedural safeguards.

A total of 11 responses were received (Netherlands, Czech Republic, Finland, Denmark, Norway, Lithuania, France, Portugal, Ireland, Latvia and Spain). The responses provided qualitative input on existing or emerging national frameworks, as well as expectations and challenges related to the implementation of the EHDS Regulation.

A comparative analysis of the responses was carried out, focusing on identifying common elements, divergences, and key areas requiring further clarification at EU level. Particular attention was given to recurring issues such as the assessment of proportionality, the role of aggravating and mitigating factors, and coordination with data protection authorities.

The findings of this analysis, together with the legal assessment of the EHDS Regulation, formed the basis for the development of this guideline. The drafting process was carried out iteratively within the TEHDAS2 work package, ensuring alignment with the Regulation while reflecting the practical input received from Member States.

7.3 Target audience

This guideline is written for HDABs responsible for supervising compliance with the rules on secondary use of electronic health data under the EHDS Regulation. It is particularly intended for officials and enforcement teams within HDABs who are tasked with conducting investigations, applying enforcement measures, and determining whether to impose administrative fines in cases of non-compliance.

7.4 Scope

The aim of this guideline is to provide support to HDABs in applying their supervisory and sanctioning powers under Articles 63 and 64 of the EHDS Regulation. It is designed to assist HDABs in fulfilling their responsibilities to monitor compliance, issue enforcement decisions, and impose administrative fines where necessary, in the context of the “HealthData@EU” infrastructure for secondary use of health data. The guideline offers practical and interpretative guidance to ensure that enforcement actions are consistent, proportionate, and legally grounded across Member States. It does not address the application of penalties

under national data access schemes or bilateral arrangements outside the EHDS infrastructure, which remain subject to national law.

Specifically, the guideline covers the following areas:
How HDABs may carry out their monitoring and investigative tasks, including:

- What types of information HDABs are entitled to request from data users and data holders;
- How to conduct assessments of compliance and document findings.

How HDABs should respond to identified breaches, including:

- **Notification and right to be heard:** Establishing a clear process for promptly informing affected parties of the breach and ensuring their right to present observations before enforcement action is taken;
- **Administration of enforcement:** Setting out structured internal procedures for recording, assessing, and managing breaches, with defined responsibilities, timelines, and coordination mechanisms across competent bodies;
- **Transparency and accountability:** Guaranteeing openness by publishing decisions, providing anonymised case summaries, and issuing regular reports on enforcement activity, thereby fostering trust and consistency;
- **Criteria for enforcement measures:** Defining proportionate and risk-based criteria for selecting appropriate measures, such as permit revocation, suspension of processing, or exclusion from future access

How HDABs may impose administrative fines under Article 64, including:

- How to assess the nature, gravity, and context of an infringement;
- How to quantify fines based on legal criteria and proportionality principles;
- The relationship between fines and other enforcement measures.

How HDABs should coordinate and communicate enforcement actions, including:

- Notification through the shared HealthData@EU IT tool;
- Transparency obligations and potential publication of enforcement decisions;
- The role of the Commission and future implementing acts.

This guideline is intended to be high-level, leaving it to the MS to determine their respective national implementation strategies. MS retain procedural autonomy, as long as it is in compliance with EU law.

This guideline is intended as a living document and will be updated to reflect evolving practices, additional guidance from the European Commission, and experience gained during the implementation of the EHDS Regulation across the Member States.

7.5 Legal framework

The principal legal foundation for the supervisory and sanctioning responsibilities of HDABs is the EHDS Regulation, in particular Articles 63 and 64[1]. These provisions empower HDABs to monitor compliance, enforce the obligations set out in the Regulation, and impose appropriate administrative penalties in cases of infringement. In doing so HDABs play a critical role in **ensuring the lawful and responsible access to and secondary use of personal electronic health data** through the "HealthData@EU" infrastructure.

These enforcement powers complement, but do not replace, the supervisory and sanctioning responsibilities of national Data Protection Authorities (DPA) under the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679); where non-compliance with the EHDS Regulation also involves potential breaches of data protection law, HDABs are required to inform and coordinate with the competent DPA.

While the EHDS Regulation establishes the specific framework for enforcement actions in the context of health data, these activities intersect with the GDPR. Where a potential breach of the EHDS Regulation also implies a breach of data protection law, HDABs are required to inform the competent supervisory authorities under the GDPR and coordinate with them accordingly. HDABs must coordinate with national supervisory authorities when enforcement concerns involve potential personal data breaches under the GDPR.This reinforces the need for HDABs to ensure that any sanctioning activity is carried out in compliance with broader EU data protection principles and procedural guarantees.

As of the drafting of this guideline, the EHDS Regulation has entered into force on the 26th of March of 2025; but it has **not yet started to apply**, and therefore its provisions are not yet legally operational. The exact forms of national implementation also remain to be seen. While the Regulation establishes the core enforcement tools available to HDABs (e.g. permit revocation, exclusions, administrative fines), the **procedural conditions for their application** – such as time limits for appeal, administrative steps, or the identity of competent national bodies – may vary depending on Member States' legal traditions. This reflects the principle of **procedural autonomy**, which allows Member States to shape the details of enforcement within the bounds of EU law. For this reason, this guideline offers a high-level interpretative framework designed to support early implementation. As national procedures evolve and additional EU-level guidance becomes available, HDABs will be able to complement and refine this framework within their respective legal systems.

HDABs are advised to consult both the Regulation and national complementing acts as well as general national laws related to the enforcement of administrative decisions to determine how enforcement powers, including administrative fines, are applied within their jurisdiction.

It is also important to note that the EHDS operates alongside other legal frameworks for accessing and using health data. Traditional mechanisms, such as national data access schemes or bilateral data-sharing agreements, continue to exist in parallel. Where these are used instead of the EHDS infrastructure, they remain subject to their respective national rules and enforcement regimes and it is out of scope of this document.

This guideline does not apply to traditional national data access mechanisms or bilateral agreements, which remain subject to their respective national legal frameworks

8 Supervisory powers of HDABs under Article 63

8.1 Investigative and monitoring mandate

Under Article 63(1), HDABs are empowered to request and receive all information necessary to verify compliance with the EHDS Regulation. This includes the right to obtain documentation, records, logs, reports or any other material deemed necessary for evaluating whether a data user or data holder is fulfilling their obligations under Chapter IV of the Regulation. The scope of this authority is broad and enables HDABs to carry out assessments, audits and inspections, including on-site checks or remote evaluations if appropriate.

The mandate also covers situations in which the HDAB deems it necessary to proactively verify compliance, **whether as part of routine supervisory functions or reactively in response to suspicions, complaints, or alerts**. These may originate from other competent authorities, **data users, data holders, affected individuals, or internal monitoring mechanisms**. This approach allows for both preventive and corrective oversight as well as regular monitoring, which is essential for safeguarding the functioning of the EHDS infrastructure.

The ability to carry out monitoring activities in a timely and effective manner is crucial for the credibility of the enforcement system. HDABs should be equipped with clear internal procedures for initiating investigations, evaluating the relevance and completeness of the information obtained, and deciding whether further measures under Article 63(2) are necessary. HDABs are encouraged to establish standard operating procedures for initiating audits or inspections, including risk-based triggers and escalation criteria. Close coordination with other competent authorities may be required in situations involving cross-border data access or complex legal implications, particularly where breaches could also fall under the scope of the GDPR.

Finally, the information gathered during monitoring exercises serves not only to detect non-compliance, but also to promote transparency, foster trust among data holders and users, and ensure a consistent interpretation of the Regulation across Member States. HDABs are encouraged to document their monitoring activities and share insights with other national counterparts as part of a coordinated supervisory network under the EHDS.

8.2 Notification obligations and the right to be heard

When a HDAB determines that a health data user or health data holder has not complied with one or more requirements of Chapter IV of the EHDS Regulation, it must act promptly to address the breach. In accordance with Article 63(2), the HDAB is required to notify the non-compliant party without delay. This notification must be explicit, written, and substantiated with evidence, describing the specific facts, obligations breached, and any relevant contextual information. The purpose of this communication is to ensure transparency and to formally initiate the enforcement process.

Alongside the notification, the HDAB must grant the concerned party a fair opportunity to respond. The Regulation sets a clear procedural requirement: the health data user or holder must be given a reasonable period to present their views, with a strict upper limit of four weeks. During this period, the party may submit written arguments, factual clarifications, supporting documents, or evidence of remedial actions already taken. The HDAB must fully consider these submissions before deciding on the enforcement measure to apply. This procedural safeguard is a core element of due process and ensures that enforcement decisions are not taken unilaterally or prematurely.

In cases where the identified non-compliance may also constitute a breach of the GDPR, the HDAB has an additional duty to inform the competent supervisory authority without delay. This requires the HDAB to assess whether the facts in question fall within the scope of GDPR – for example, if the breach involves the unlawful processing of personal data, failure to implement appropriate technical or organisational safeguards, or unauthorised re-identification of individuals. If so, the HDAB must forward all relevant documentation, including the findings and supporting evidence, to the competent supervisory authority. This mechanism ensures that GDPR violations are investigated and sanctioned under the appropriate legal framework and promotes regulatory coherence between the EHDS and existing EU data protection law.

To operationalise this provision effectively, HDABs are encouraged to develop internal protocols for issuing timely notifications, managing responses within the four-week window, and coordinating with national data protection authorities. Templates for notifications and structured response forms may help streamline this process and ensure that both HDABs and stakeholders comply with the procedural requirements of the Regulation. In addition, in cases of a suspected breach or infringement, each HDAB will remain free to decide whether to take precautionary action in order to prevent potential further damage.

8.3 Enforcement measures against data users: revocation, suspension and exclusion

Where a HDAB has determined that a health data user has failed to comply with its obligations under Chapter IV of the EHDS Regulation, it is empowered to adopt enforcement measures with immediate effect. One of the primary tools at the HDAB's disposal is the revocation of the data permit issued under Article 68. This step serves as a direct and formal suspension of the user's legal entitlement to access and process electronic health data through the EHDS infrastructure. The HDAB must also, without undue delay, order the cessation of any ongoing processing operations carried out under that permit. The cessation must be effective and immediate to prevent further unauthorised use, risk to individuals' rights, or compromise of data integrity within the system. To ensure operational effectiveness, this may require the adoption of technical enforcement measures – such as disabling the user's access credentials to the SPE or revoking remote access rights – to block continued data processing in practice. In parallel, the HDAB must communicate the enforcement decision without delay to all relevant operational actors, including the SPE operator and any trusted data holders concerned, to ensure coordinated and effective implementation of the measure.

In addition to these immediate corrective actions, the HDAB is required to assess and apply further measures that are proportionate and tailored to the nature of the infringement. These measures may include requiring the health data user to implement remedial technical or organisational safeguards, submit to enhanced oversight, or provide formal undertakings not to repeat the breach. The goal is to restore compliant processing practices and prevent future violations in a way that is effective yet balanced.

Importantly, in cases where the breach is particularly serious, repeated, or indicative of a systemic failure by the data user to respect the legal conditions for secondary use, the HDAB may also decide to exclude the entity from accessing electronic health data within the EHDS for a fixed period of time. This exclusion may last up to five years and is designed to protect the system from ongoing risk while signalling the gravity of the non-compliance. Whether applied directly or through formal proceedings, the exclusion must always be grounded in national law and be supported by a reasoned decision that clearly explains its necessity and proportionality. Such exclusions do not operate EU-wide unless mutual recognition mechanisms are established at national or Union level. In cross-border situations, HDABs should apply administrative fines and other measures in a manner that respects the limits of their competence and promotes consistency, transparency and cooperation with other competent authorities, in order to reduce the risk of forum shopping and conflicting decisions.

HDABs should ensure that decisions related to permit revocation, processing suspension, and exclusion are communicated to the affected parties in writing and in a timely manner, outlining the legal basis, evidence considered, and any steps required for future reinstatement. Internal guidelines and decision-making protocols should be established to support consistency, procedural fairness, and compliance with national administrative law. Where applicable, HDABs should also record and share these enforcement measures with other competent authorities and through the HealthData@EU IT platform to ensure cross-border visibility and alignment. In particular, revocations and exclusions should be systematically notified to other HDABs via the HealthData@EU IT tool to prevent forum shopping by non-compliant data users seeking access in other Member States.

8.4 Enforcement measures against health data holders

In situations where a health data holder fails to comply with its obligations under Chapter IV of the EHDS Regulation – particularly by withholding electronic health data or failing to meet mandatory deadlines for data transmission – HDABs are granted the authority to impose enforcement measures designed to restore cooperation and prevent obstruction. Specifically, Article 63(4) enables the HDAB to impose a periodic penalty payment on the data holder for each day of delay, provided that the withholding of data is carried out with the manifest intention of obstructing the lawful use of electronic health data, or when the data holder fails to meet the deadlines set out in Article 60(2).

The objective of this penalty mechanism is to exert proportionate financial pressure on the non-compliant party, thereby compelling them to meet their obligations in a timely manner. These penalty payments must be calculated in a transparent manner and be proportionate to the nature and duration of the breach. HDABs should determine the amount of the daily fine based on criteria established under national law, ensuring that the penalty is neither arbitrary nor excessive, but sufficiently dissuasive to encourage compliance. Documentation

of the rationale for the amount imposed is recommended to ensure legal defensibility and procedural transparency.

Where a pattern of non-cooperation emerges – such as repeated delays, systematic obstruction, or persistent failure to provide data – the HDAB may consider taking escalated enforcement action. Sanctions or measures against non-compliant data holders may be taken in accordance with national administrative enforcement frameworks. All such actions must be based on a well-reasoned decision and must respect the principles of necessity and proportionality.

It is essential to emphasise that exclusion from submitting new applications does not relieve the health data user of their continuing obligations under the Regulation. Even during the exclusion period, the data holder remains legally obliged to make electronic health data available for secondary use, wherever such obligations apply. HDABs must clearly communicate this continuing duty when issuing the exclusion decision.

To operationalise this provision effectively, HDABs should establish internal criteria for determining when an intent to obstruct is present, how to assess the seriousness of delays, and how to calculate daily penalties in a consistent manner. Procedures should also be in place to ensure that repeated breaches are identified, documented, and appropriately escalated, including the decision to initiate exclusion proceedings. Where necessary, HDABs should coordinate with other national authorities and use the shared HealthData@EU IT infrastructure to notify peer bodies of enforcement actions and promote coherent implementation across the EU.

8.5 Communication of enforcement measures and compliance deadlines

Once a HDAB has decided to take enforcement action under Articles 63(3) or 63(4) of the EHDS Regulation – whether against a health data user or a health data holder – it must ensure that the enforcement decision is communicated promptly and transparently to the affected party. The communication must clearly identify the specific measure adopted (e.g. revocation of a data permit, suspension of data processing, imposition of periodic penalty payments, or exclusion from future access) and must include a detailed statement of reasons. This explanation should refer to the factual findings, legal provisions breached, the rationale behind the choice of measure, and how the HDAB has assessed its proportionality in the context of the infringement.

Timeliness is a key requirement: once the enforcement decision has been taken, the HDAB must communicate it to the affected party **without undue delay**. This obligation concerns the **notification** of the measure – not the duration of the preceding investigation or deliberation process. What constitutes ‘undue delay’ in notification will depend on practical circumstances (e.g. urgency, risk) but **does not include factors related to the legal or factual complexity of the case**, which may have influenced the time taken to reach the decision itself. Systemic issues such as insufficient staff resources or internal inefficiencies should not be considered valid reasons for delay in issuing the communication, particularly in light of the Regulation’s requirement that HDABs be adequately resourced to perform their functions effectively.

In addition, the enforcement decision must establish a reasonable period within which the data user or data holder must comply. This period should reflect the nature of the enforcement measure and the complexity or effort required to achieve compliance. For instance, the timeframe for halting an unlawful data processing activity may be short and immediate, while the deadline for implementing corrective organisational measures or submitting overdue data may require more time. Where applicable, the HDAB should also indicate the consequences of failing to comply within the prescribed period, including the possibility of further sanctions or escalation.

To support legal certainty, HDABs are encouraged to use structured templates for enforcement notices and maintain detailed records of when communications are issued and received. This will facilitate transparency, ensure that deadlines are enforceable, and provide clarity for follow-up monitoring.

8.6 Notification and transparency of enforcement measures through the HealthData@EU infrastructure

This notification obligation reflects the inherently cross-border nature of secondary data use within the EHDS framework. Data users operating in one Member State may have access to datasets from others or they may submit applications across multiple jurisdictions. Therefore, it is essential that all HDABs have access to up-to-date information on enforcement actions to avoid regulatory fragmentation and prevent forum shopping by non-compliant actors.

Beyond formal notification through the shared infrastructure, the Regulation also requires HDABs to publish a summary of enforcement measures on their websites pursuant to Article 57(1) points (j) and (iv). While the Regulation does not specify a standard format or level of detail, this mandatory transparency measure plays an important role in enhancing public trust, increasing accountability, and deterring non-compliance by making the consequences of misconduct visible. When publishing enforcement actions, HDABs must ensure that disclosures comply with national and EU-level data protection and transparency requirements, particularly where individuals or entities may be identifiable

To implement this provision effectively, HDABs should establish internal procedures for timely entry of enforcement decisions into the shared IT tool, and for assessing which decisions may be published online. For legal certainty, “timely” should be understood as requiring publication within a clearly defined period following the adoption of the enforcement decision (e.g. within 10 working days), and subsequent updates should take place on a regular schedule, such as monthly, to ensure that information remains accurate and up to date. Coordination among HDABs through the IT platform can also serve as a basis for shared learning, peer support, and harmonisation of enforcement strategies across the EHDS ecosystem. Where the underlying issue is resolved, the entry should be updated to reflect its closure; if a decision is overturned on appeal or by judicial review, the HDAB must promptly update the information in the IT tool, ensuring that it accurately reflects the current legal situation.

8.7 Commission responsibilities: implementing acts and future guidelines on enforcement measures

To ensure coherence, interoperability, and transparency in the enforcement of the EHDS Regulation across all Member States, the European Commission is tasked with establishing a common digital infrastructure to support coordination between HDABs. In accordance with Article 63(7), the Commission will, through implementing acts, define the architecture of a dedicated IT tool that will serve as an integral component of the broader HealthData@EU infrastructure described in Article 75. This tool will enable HDABs to systematically record and share enforcement measures such as periodic penalty payments, revocations of data permits, and exclusions from access to EHDS data. The tool is intended not only to enhance operational support for enforcement but also to promote visibility and transparency among HDABs, particularly in cross-border contexts where coordination is essential.

Until these implementing acts are adopted and the IT tool is operational, HDABs should ensure that their internal systems are able to capture, manage and eventually integrate enforcement-related information in a structured and transferable format.

Furthermore, as outlined in Article 63(8), the Commission will issue detailed guidelines on enforcement measures by 26 March 2032, in close cooperation with the EHDS Board. These guidelines will offer interpretive and operational support on the implementation of enforcement tools, including the application of periodic penalty payments and the criteria for revocation or exclusion. Once issued, these Commission guidelines will serve as a key reference document for HDABs and are likely to influence enforcement methodologies and administrative procedures and national transposition practices.

HDABs are encouraged to actively monitor the development of these implementing acts and guidelines, participate in consultation processes where possible, and prepare their internal workflows and technical systems for alignment with the forthcoming EU-level standards. This proactive engagement will facilitate the seamless adoption of new tools and ensure HDABs are fully equipped to carry out their supervisory responsibilities in a harmonised, efficient, and transparent manner across the EHDS ecosystem.

9 Administrative fines under Article 64

This chapter provides guidance on the principles governing penalties. However, it is important to note that MS have procedural autonomy and may determine their operational arrangements, provided these are in line with the EHDS principles and other applicable EU and national laws.

9.1 General principles: effectiveness, proportionality, and deterrence

HDABs, when determining whether to impose administrative fines under Article 64(1) of the EHDS Regulation, must ensure that their enforcement actions adhere to the fundamental principles of effectiveness, proportionality, and deterrence. These principles serve as the cornerstone for a legitimate and impactful sanctioning regime within the EHDS. Fines must

be effective in addressing and correcting the specific non-compliance observed; proportionate to the nature, scope, and seriousness of the infringement; and dissuasive enough to prevent both the offender and others from committing similar breaches in the future.

In applying these principles, HDABs must conduct a case-by-case assessment that considers all relevant factual and legal circumstances, including the role and responsibilities of the party involved (e.g., whether they are a data user or a data holder), the risks posed to individuals and the EHDS system, and the broader public interest in ensuring responsible secondary use of health data. This approach ensures that fines are not applied mechanically, but rather as part of a calibrated enforcement strategy that promotes compliance while safeguarding procedural fairness and legal certainty.

Ultimately, the goal is to reinforce trust in the EHDS by demonstrating that violations are met with consistent and credible regulatory responses – neither excessive nor lenient – and that HDABs are committed to fostering a data-sharing environment that is legally sound, secure, and ethically governed.

9.2 Criteria for the imposition and quantification of fines

In determining whether to impose an administrative fine, and in setting its precise amount, HDABs must apply the evaluation criteria set out under Article 64(2) of the EHDS Regulation. This provision establishes a framework of qualitative and contextual factors that must guide the enforcement authority's decision-making process. The assessment must be comprehensive, balanced, and well-reasoned, ensuring that each sanction reflects the specific characteristics and impact of the infringement in question.

Key assessment criteria as per Article 64(2) include:

- **Nature, gravity, and duration of the infringement:** HDABs must consider how serious the breach is in terms of its effect on individuals' rights, the EHDS framework, or public trust. Longer-lasting or systemic violations are likely to warrant higher fines.
- **Penalties imposed by other authorities:** HDABs must take into account whether penalties or administrative fines have already been imposed by other competent authorities for the same infringement, in order to ensure proportionality and avoid double sanctioning.
- **Intentionality or negligence:** Whether the violation occurred deliberately or due to a lack of due diligence significantly influences the level of culpability and the appropriateness of a financial penalty.
- **Mitigation efforts:** Actions taken by the infringing party to mitigate or rectify the harm – such as promptly reporting the breach, implementing corrective measures, or offering redress – may justify a reduction in the fine.

- **Degree of responsibility of the health data user:** HDABs must consider the extent of the health data user's responsibility, taking into account the technical and organisational measures implemented pursuant to Article 67(2) point (g), and Article 67(4).
- **Previous infringements:** HDABs must take into account whether the infringing party has committed prior violations of the EHDS Regulation or related EU or national data

protection and health data legislation. Repeated or similar infringements may indicate a pattern of non-compliance or insufficient corrective action, and should therefore be treated as an aggravating factor. However, the absence of prior infringements, may be considered as a mitigating factor.

- **Manner in which the infringement became known:** HDABs must assess how the infringement came to their attention, in particular whether, and to what extent, the health data user proactively notified the HDAB of the infringement.
- **Level of cooperation with the HDAB:** Constructive engagement, transparency, and willingness to comply with regulatory instructions can be considered as mitigating factors.
- **Financial benefit or avoidance of cost:** If the breach resulted in unjust enrichment, financial gain, or the circumvention of obligations, these will weigh in favour of a stronger sanction to remove any benefit from non-compliance.

In applying these criteria, HDABs are required to carry out a holistic and documented analysis, which must be clearly reflected in their reasoning and decision notices. Transparency in how the criteria are applied ensures accountability, promotes consistent enforcement across Member States, and supports legal certainty for all stakeholders operating within the EHDS framework.

9.3 Categorisation of infringements and applicable fine ceilings

The Regulation distinguishes between two levels of infringements:

- Less serious infringements (e.g. failure to comply with Articles 60 or 61) may result in fines up to €10 million or 2% of worldwide annual turnover, whichever is higher.
- More serious infringements (e.g. unauthorised processing, re-identification attempts, or refusal to comply with HDAB enforcement) may attract fines up to €20 million or 4% of worldwide annual turnover, whichever is higher.

9.4 Treatment of multiple infringements and repeat offenders

The EHDS Regulation introduces a tiered structure for administrative fines, distinguishing between less serious and more serious infringements. This classification reflects the need to calibrate enforcement responses based on the severity and impact of non-compliance, in line with the principles of effectiveness, proportionality, and dissuasiveness under Article 64(1).

- **Less serious infringements:** These include breaches such as:
    - failure to fulfil procedural or cooperation obligations under Article 60 (obligations of health data holders)
    - failure to fulfil procedural or cooperation obligations under Article 61 (obligations of health data users).
- **More serious infringements**: These involve violations that directly undermine the core principles of the Regulation, such as:
    - Unauthorised processing of electronic health data in breach of the terms of the data permit;

- Attempts to re-identify individuals, contrary to the strict safeguards on data pseudonymisation or anonymisation;
- Non-compliance with enforcement measures imposed by the HDAB, particularly in cases of persistent or deliberate obstruction.

For such infringements, fines may be as high as €20 million, or 4% of the worldwide annual turnover, depending on which amount is greater.

In determining whether a specific act falls into the “less serious” or “more serious” category, HDABs must consider the substantive impact on data governance, individual rights, and systemic compliance. The level of fine must be aligned with the objective of safeguarding trust in the secondary use of health data within the EHDS and ensuring accountability among both public and private actors.

9.5 Cumulative assessment of multiple infringements

In situations where a health data user or health data holder commits multiple infringements in relation to the same or linked data permit(s), the EHDS Regulation requires a cumulative but proportionate approach to the calculation of fines. Specifically, Article 64(5) establishes that the total administrative fine imposed shall not exceed the maximum amount applicable to the most serious single infringement.

This provision is designed to prevent disproportionate financial penalties where infringements are closely connected or arise from a single act or omission. HDABs must assess whether the breaches are substantively interconnected, such that they form a **single continuous infringement,** or whether they instead constitute **separate, independent breaches**, in which case separate fines may be imposed for each, **up to the applicable maximum per infringement.** This assessment does not depend solely on the presence of systemic or repeated non-compliance, but rather on the **legal and factual distinctness** of the underlying violations.

Furthermore, repeated or systematic violations – especially when they occur despite prior warnings or enforcement actions – are to be regarded as aggravating circumstances. In such cases, HDABs are expected to apply stricter sanctions, both in terms of the amount of the fine and in considering additional enforcement measures, such as revocation of data permits, temporary exclusion from data access, or periodic penalty payments.

HDABs must document the rationale for how multiple infringements are treated in the fine determination process, ensuring transparency, legal certainty, and respect for procedural safeguards. This includes distinguishing between genuinely isolated incidents and behaviours indicative of persistent non-compliance.

9.6 Procedural safeguards and legal remedies

The imposition of administrative fines and any other enforcement action under the EHDS Regulation must strictly respect the principles of due process, as reaffirmed by Article 64(7). This provision ensures that health data users and health data holders subject to sanctions

are fully entitled to procedural safeguards and legal remedies as defined under national and EU law.

Before a decision to impose a fine or take any significant enforcement measure is finalised, the HDAB must inform the concerned party of the findings and provide them with a meaningful opportunity to express their views – typically within a reasonable period that shall not exceed four weeks (per Article 63(2)). This guarantees the right to be heard, a cornerstone of fair administrative proceedings.

In addition, all individuals or entities affected by enforcement actions must have access to effective judicial remedies. This means that they can challenge fines or decisions before competent national courts or authorities, in accordance with the respective procedural rules of the Member State involved. HDABs must facilitate this right by clearly communicating the basis for the enforcement measure, the amount and rationale for any fine, and the available avenues for appeal or redress.

Moreover, HDABs are obliged to maintain detailed and transparent records of their enforcement decisions, including their legal and factual justification, the consideration of aggravating or mitigating factors, and the reasoning applied when determining the type and scale of the measure. These records are essential for ensuring accountability, enabling judicial review, and promoting harmonisation of enforcement practices across the EU.

This procedural framework not only safeguards the rights of stakeholders but also reinforces trust in the regulatory system governing the EHDS.

10 Implementation considerations and recommendations

10.1 Internal decision-making processes for enforcement

HDABs should develop internal protocols for assessing non-compliance and determining appropriate sanctions. This includes clear lines of responsibility, documentation standards, and escalation procedures. While the EHDS Regulation does not prescribe a uniform protocol, guidance may be developed at EU level by the European Commission or the European Health Data Board. In the interim, HDABs may draw on national administrative law frameworks and procedural models used in analogous EU enforcement contexts.

10.2 Use of assessment tools and penalty matrices

To support consistency, HDABs may adopt tools such as penalty matrices or risk assessment frameworks. These can help quantify aggravating and mitigating factors and promote transparency in enforcement decisions. **HDABs are encouraged to document how these tools are applied in individual cases**, including the rationale for the weighting of specific factors and the determination of fine levels. Such documentation enhances the traceability of enforcement reasoning, facilitates internal review and appeals, and supports greater consistency and mutual understanding across Member States

10.3 Integration with national legal frameworks

Each HDAB must align its enforcement activities with the applicable national legal framework. Where the EHDS Regulation is silent, national rules on administrative procedure, appeals, and public sector sanctions will apply.

10.4 Need for capacity building and training

To ensure effective enforcement, HDAB staff must receive ongoing training on the EHDS Regulation, GDPR, administrative law, and investigatory techniques. Capacity building should be a priority, especially in the early phases of implementation.

11 Concluding remarks

11.1 Legal certainty and trust in the EHDS

Consistent and transparent enforcement of the EHDS Regulation is vital to fostering trust among data subjects, health data users, and data holders. This requires HDABs to act with professionalism, impartiality, and legal clarity in the exercise of their supervisory and sanctioning powers. By providing a structured interpretation of Articles 63 and 64, this guideline seeks to enhance predictability for stakeholders, ensure procedural fairness, and strengthen the legitimacy of the EHDS framework. At the same time, enforcement should be seen as part of a broader trust-building strategy, complementing technical, ethical, and participatory safeguards in the governance of secondary health data use.

11.2 Towards a common enforcement culture

This guideline supports the emergence of a shared enforcement culture among HDABs across Member States, grounded in common principles of effectiveness, proportionality, and due process. However, the scope of this Guideline is intentionally focused on the supervisory and sanctioning powers under Articles 63 and 64. Broader enforcement contexts fall under other parts of the EHDS framework and will require separate guidance at EU level.

As implementation progresses, a key challenge will be to reduce divergences in interpretation and practice. Feedback collected through the accompanying stakeholder questionnaire has already highlighted significant differences in national approaches to enforcement – such as in the quantification of fines, the use of exclusion measures, and coordination with data protection authorities. These findings, underscore the need for future EU-level guidance and sustained coordination among HDABs, both bilaterally and through the EHDS Board.

In addition to national divergences, **cross-border enforcement scenarios** will require particular attention. For example, if a data user from **Member State A** commits a serious breach while operating within a **SPE** in **Member State B**, questions may arise regarding which HDAB holds enforcement competence, whether both need to act, and how

responsibilities should be coordinated. Similarly, the **effect of exclusion decisions** (e.g. temporary bans from EHDS access) taken by one HDAB on that user's ability to access data in other Member States **remains unclear**, raising the risk of forum shopping unless mutual recognition mechanisms are established. Cross-border cases shall be assessed on case-by-case basis, as the evaluation of infringements and the imposition of penalties depend on the applicable national law of each involved member state and on the specific nature and circumstances of the infringement.

Looking ahead, continuous dialogue, exchange of case experience, joint training activities, and eventual alignment through implementing acts or Commission guidelines will be essential to maturing the enforcement dimension of the EHDS. Eventually, further alignment through **implementing acts**, **Commission guidelines**, and possibly **mutual recognition procedures** for key enforcement outcomes may be necessary to ensure the credibility and legal coherence of EHDS-wide supervision.

12 References

[1] TEHDAS2 document M6.1 “Guideline for health data holders on making personal and non-personal electronic health data available for reuse”.

[2] TEHDAS2 document M6.3 “Guideline for health data access bodies on the procedures and formats for data access”.

[3] TEHDAS2 document M5.2 “Guideline for health data access bodies on allowed purposes and prohibited secondary use according to EHDS”.

[4] TEHDAS2 document M7.1 “Guideline on how to use data in a secure processing environment”

[5] TEHDAS2 document D5.4 “Short guide for data enrichment for health data access bodies, data holders and data users”

[6] TEHDAS2 Document M7.4 “Draft technical, functional and security specifications of secure processing environments”

13 Annexes

Annex number	Annex title
1	Methodology
2	Public consultation summary
3	User journey
4	Glossary
5	List of costs
6	Illustrative enforcement scenarios under Articles 63 and 64 of EHDS

Annex 1 – Methodology

Two different surveys designed to gather insights on health data fees and penalties practices and benchmarking current fee and penalties structures and policies across EU Member States, were sent in October 2024 to the Competent Authorities of TEHDAS2 covering 29 countries. Respondents completed it remotely via a dedicated tool, and the surveys were closed at the end of January 2025.

For fees, a total of 24 responses were received : 20 from member states (Belgium, Croatia, Cyprus, Denmark, Finland, France, Hungary, Ireland, Italy, Iceland, Lithuania, Malta, Norway, the Netherlands, Poland, Portugal, Romania, Spain-Aragon, Spain and Sweden) 2 from European institutions (EIT Health, ECDC) and 2 from industrial federations (EFPIA, INFARMA). A comparative analysis of the responses was conducted, complemented by targeted interviews with four respondents (Sweden, Poland, Norway, and Denmark), selected on the basis of specific points of interest they had raised in the questionnaire (like some specific aspects in national law, established national pricing models, identified challenges due to a specific economic situation or territorial organisation). Based on this preparatory work, scenarios have been developed and discussed with the WP4.1.1 group members during workshops to converge towards consensual proposals, which form the foundation of the recommendations presented in this guideline. A total of 8 meetings were organised with the WP4.1.1 members and 3 alignment meetings with the DG Santé. Regarding the timelines of the meetings:

- 4 October 2024: Kick off meeting (WP4.1.1)
- 23 October 2024: Presentation of Article 62 (WP4.1.1)
- 8 November 2024: Survey launch (WP4.1.1)
- 17 January 2025: Survey result presentation (WP4.1.1)
- 27 February 2025: Clarification of expectations for guidelines (DG Santé)
- 2, 10 and 14 April 2025: Workshop for scenario definition (WP4.1.1)
- 30 April 2025: Alignment meeting with DG Santé on scenarios (DG Santé)
- 7 May 2025: Feedback from DG Santé presentation and action plan for guidelines drafting (WP4.1.1)

For penalties, a total of 11 responses were received (Netherlands, Czech Republic, Finland, Denmark, Norway, Lithuania, France, Portugal, Ireland, Latvia and Spain).

In order to maintain clarity towards the public and large thematic differences between fees and penalties, the Work Package team decided to split the topics in the public consultation process. This is why these documents were submitted as two separate documents and later merged again after the end of the public consultation.

The draft versions of the two documents were in public consultation between the 30th of September and 30th of November 2025. The guideline on fees was commented in total for

83 times, while the guideline on penalties received 48 comments. Following the public consultation, a structured methodology was adopted to review and improve the documents. First, the different sections of the consultation questionnaire were distributed among the main contributors. Second, key feedback was extracted and categorised by section. Third, a summary was prepared for each feedback category, and corresponding changes were discussed and agreed upon. The text was then revised accordingly by the team leader and reviewed by the other contributors to ensure consistency and accuracy. Details of the public consultation analysis and responses are provided in Annex 2, the first section is about fees, and the second section is about penalties, since the documents were submitted separately.

Annex 2 – Public consultation summary

A draft version of each of the draft guideline documents for fees and for penalties was in public consultation from September to November 2025. These documents were commented in total for 83 times regarding fees guidelines and 45 regarding penalties guidelines. 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.

1 – Summary of the public consultation on the section on fees

Respondents answered under different, and sometimes combined, perspectives: as a data holders (67%), public data user (28%), HDAB (25%), and Private data user (23%). The responses came from 17 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: Public organisation (28%), academic and research organisation (22%), private organisation (20%) and non-governmental organisation (8%).

Overall, stakeholders called for clearer and more predictable rules and guidance, along with stronger EU-level harmonisation, to ensure workable fee mechanisms while supporting sustainable data infrastructures and the effective implementation of the EHDS.

A. Classification of comments from the public consultation

Style, language and quality

The style received mixed feedback: some respondents considered it clear and appropriate, while others found the document difficult to understand for non-legal and non-technical audiences. Respondents indicated that key concepts such as "eligible costs" and "data discovery efforts" should be more precisely defined, and that terms in regulation such as "significant findings", "obvious intent" and "systematic non-cooperation" require clarification.

They also stressed that the executive summary should have more clearly articulated the main findings, and several respondents further suggested assessing the internal consistency between the TEHDAS 2 documents and their compliance with the GDPR.

More guidance on eligible costs and operational implementation

While some respondents considered the proposed approach to eligible costs, fee calculation and payment scenarios to be feasible and sufficiently flexible to accommodate different national contexts, many commented that the guideline lacks sufficiently clear, operational and harmonised guidance on how fees should be defined and implemented in practice.

Key concerns included the risk of indirect discrimination arising from differing national cost structures, as well as persistent ambiguity around which costs are eligible or excluded, especially at the boundary between primary-use obligations and secondary-use readiness. Stakeholders also highlight the need to clarify the application of the “no double compensation” rule, notably by distinguishing costs covered by public funding from those financed through private or investment-based sources.

Some respondents felt that the document does not sufficiently reflect the perspectives and practical realities of all relevant stakeholders (researchers, clinical care actors, industrials and microenterprises) and called for stakeholder-specific use cases to be more explicitly addressed. The role, responsibilities and cost implications of intermediaries within the EHDS ecosystem – such as Data Intermediation Entities and data-space operators – were also seen as insufficiently addressed, as was the applicability to third-country HDHs and applicants.

Financial sustainability

Many respondents emphasised that data holders may face substantial additional costs which are not always clearly recoverable under the proposed rules. The exclusion or narrow interpretation of data discovery costs was highlighted as problematic, as it can represent a significant and unavoidable financial burden.

The absence of benefit-sharing mechanisms, incentives for interoperability and standardisation, and co-investment or knowledge-transfer obligations is questioned regarding long-term investment and fair value distribution. At the same time, concerns were raised that allowing recovery of broad fixed or structuring costs could exacerbate inequalities between data holders with different levels of digital maturity or distort access patterns.

Concerns were raised about how reduced fees or exemptions should be financed without disadvantaging data holders, prompting calls for complementary funding or compensation mechanisms at national or Union level.

While the guidelines were recognised as providing a useful baseline for transparency, many argued that the fee structure must better balance cost recovery, proportionality and incentives in order to ensure the economic viability of data sharing and the overall success of the EHDS.

Transparency and predictability of fees

To improve transparency and reduce administrative burden, respondents called for earlier and more indicative cost estimates before application submission, better communication of price ranges or maximum costs, standardised price disclosure tools (such as price lists or simulators), and regular review and updating of national cost models. This need was considered particularly acute in research funding contexts, where cost estimates are required well in advance.

Uncertainty around invoicing, the eligibility of certain costs (e.g. complaint handling, re-extraction due to errors, or IP and trade secret assessments), and the risk of costs being incurred before applicants are informed were identified as major obstacles for both data users and data holders.

While the single-invoice model was generally welcomed for the clarity it could provide, respondents stressed that the early estimates may not reflect actual costs, especially for SPEs, given the challenges of transparent price calculation and managing operational expenses during data exploitation.

Finally, respondents highlighted the need for clearer guidance on appropriate charging models, including predefined rates, usage-based pricing, or bundled approaches. They also warned that smaller or newer actors could face disproportionate implementation burdens unless proportionality and the reuse of existing billing structures were prioritised in national transposition.

EU harmonisation

Respondents strongly called for enhanced EU-level harmonisation of HDAB decision-making and fee policies to support fair and effective cross-border data access. While acknowledging national differences in cost structures, salaries, purchasing power, pricing maturity and legal frameworks, they stressed the need for clearer guidance on which elements should be regulated at EU versus national level, mechanisms to converge fee practices, and safeguards against price dumping or competitive distortions. Questions were raised about how competition neutrality can be ensured in the absence of common fee references, and whether national subsidisation or undercutting could affect intra-EU fairness.

Harmonised definitions of eligible and non-eligible costs, common examples of fee calculations, indicative use cases, and standard invoicing templates were seen as essential to improve transparency, comparability and competition neutrality across Member States. At the same time, contributors emphasised that harmonisation should preserve sufficient national flexibility and suggested a minimum EU baseline or recommended methodology combined with safeguards for public research access.

Burden on stakeholders and related risks

Stakeholders expressed concerns about the administrative and operational burden associated with centralised invoicing at HDAB level, warning that it could create bottlenecks, delays and inefficiencies. Many recommended more decentralised or flexible invoicing approaches aligned with existing workflows and capacity constraints.

Respondents further highlighted the underestimated workload for data holders related to data preparation, anonymisation, coordination, billing and compliance, as well as the cumulative burden on non-profit, academic and smaller actors facing new EHDS-related investments

(like system upgrades, connectors, data normalisation and maintenance). They warned that insufficient recognition of these efforts could discourage participation and slow innovation.

Several responses point to risks arising from unclear responsibilities, notably regarding who must inform data holders at the finalisation stage when results are published, and who bears responsibility for incomplete or late applications. While applicants should be accountable for procedural failures, penalties should not deter good-faith users.

Risk to innovation and competitiveness

The feedback urges Member States to use the flexibility under Article 62(1) to reduce fees for non-commercial users, reflecting the public funding of health data collection. It warns that the proposed approach could discourage data holders from proactively investing in secondary-use infrastructures, risking stagnation of the ecosystem, and suggests incentives such as fee reductions for data holders that invest in data availability.

It also suggests ensuring that entities accessing EHDS data contribute to European research ecosystem through co-investment or knowledge transfer. The responses also highlight the absence of benefit-sharing mechanisms to ensure data holders participate in the societal or economic value generated, and call for clearer guidance on state aid, including full cost recovery or market pricing for commercial users and reduced fees limited to non-economic activities.

General comments on EHDS

Stakeholders raised broader concerns regarding the alignment of the EHDS Regulation with existing national frameworks on data protection, public-sector fees and health data governance, calling for legal clarification to ensure consistent interpretation. The definition of roles and responsibilities within the EHDS, particularly that of “data holder”, was also seen as insufficiently clear.

Several respondents reiterated the need for long-term, dedicated funding mechanisms to support essential registries and pan-European data infrastructures, including proportional contributions from foreign and commercial users, to safeguard continuity, quality and public health value.

B. Focus on specific aspects of the feedback

Detailed taxonomy of eligible costs

While the general need for clear definitions is established, respondents propose that the fee structure should include specific eligible cost categories. These include legal assistance, covering assessments related to GDPR compliance, intellectual property rights, trade secrets, and contract management. Data curation should also be included, encompassing ongoing activities such as updating metadata, standardising formats, and cleaning or quality-assuring data. In addition, user support costs should be recognised, including pre-application dialogue, assistance with defining research variables, and technical training for users. Infrastructure-related costs should reflect the active maintenance of secure channels and the

development of pseudonymisation algorithms. Finally, administrative costs should cover internal coordination efforts as well as targeted staff training.

Complexity and Bespoke Pricing

Additional nuances were raised regarding the nature of the data, highlighting that the fees may need to vary according to dataset complexity, with high-value or complex datasets potentially requiring bespoke pricing models. In particular, data related to rare diseases may involve significantly greater manual effort, which could justify higher associated costs.

Practical Tools for Clarity

To improve the user experience, several practical measures were suggested, including sharing examples of historical costs to help applicants form realistic budget expectations, providing a comprehensive and centralised FAQ to address common scenarios and questions, and establishing clear rules for managing cost changes arising from scope adjustments or errors by the HDAB or the DH.

Technical Standards for Invoicing

A specific framework was suggested for what should and should not appear on an invoice. Invoices should include minimum content such as identification of the invoicing body, a reference to the relevant data permit, and contact details for handling disputes. Costs should be presented using a clear breakdown by high-level categories (administrative, technical processing, or SPE costs), with an indication of whether they are fixed or variable. In addition, invoices should explicitly disclose any applicable discounts, such as those for academic use, and clearly list all non-billable elements, including prohibited margins. To protect sensitive information, invoices should exclude internal hourly calculations, staff effort estimates, and details related to cybersecurity measures or processing algorithms.

2 – Summary of the public consultation on the section on penalties

The responses for this section came from 17 different countries from the EU countries and the European Economic Area countries. The respondents were primarily from three main types of organisations, listed in order of prevalence: public organisations, private organisations, and academic/research organisations.

To implement the public consultation feedback, we established small working groups, feedback was received in an Excel file, with responses from individuals or teams in rows and chapter-specific comments in columns. Working group members reviewed the feedback offline, assessing relevance and feasibility for the guideline:

RELEVANT: Clear to implement – suggest how to reflect the comment in the guidelines;

NEED TO BE DISCUSSED: Uncertain – note what needs to be discussed with the working group;

OUT OF SCOPE: Not to be considered – fall out the scope of the guidelines.

The main challenges in implementing and complying with penalty-related provisions across borders relate to consistency, coordination, and legal clarity, particularly in light of the diversity of national administrative systems. While the EHDS Regulation provides a harmonised legal framework, enforcement will necessarily interact with national authorities, legal traditions, and procedural autonomy. In this context, the guideline could further support a common understanding by offering additional clarification on how similar infringements should be assessed, how sanctions such as suspension or exclusion are applied in practice, and how proportionality is ensured across Member States.

In particular, the guideline could benefit from further elaboration on the methodology for calculating administrative fines, including clarification on the relevant turnover basis (national or worldwide), the weighing of aggravating and mitigating factors, and the use of illustrative numerical examples. Additional guidance on enforcement triggers and escalation thresholds – for example, when to move from warnings to periodic penalty payments, suspension, or exclusion – would further support consistent and predictable application.

Cross-border enforcement scenarios would also benefit from additional operational guidance. The absence of a formal mechanism for mutual recognition of sanction decisions means that coordination between HDABs plays a key role in preventing fragmentation and forum shopping, particularly where data users operate under multiple permits in different Member States. Clarifying how information should be shared, how parallel proceedings may be coordinated, and how proportionality should be assessed in multi-permit situations would strengthen coherence while respecting national competence. Similar clarification could be helpful for enforcement actions involving shared Secure Processing Environments, including practical aspects such as synchronised suspensions, credential management, and verifiable implementation of enforcement measures.

The guideline could also be further strengthened by addressing responsibility allocation in complex processing chains, where data holders rely on processors or technical intermediaries for data extraction and delivery. Additional examples or guidance on how due diligence, contractual safeguards, and effective control should be taken into account would support fair and proportionate enforcement, particularly in cross-border contexts and for smaller actors.

From a procedural perspective, respondents indicated that further clarification could be helpful regarding appeal processes and timelines, especially in cross-border cases. This includes explaining how immediate enforcement interacts with the right to appeal, how the four-week period should be understood as a maximum, and how “reasonable time” may be assessed in practice, including the possibility of extensions where justified. Clarifying these aspects would contribute to procedural fairness and legal certainty.

Transparency and public communication are widely recognised as important elements for building trust in the EHDS. At the same time, stakeholders emphasised that transparency mechanisms would benefit from careful calibration. The guideline could therefore further clarify how publication of sanctions should be handled in a proportionate manner, including

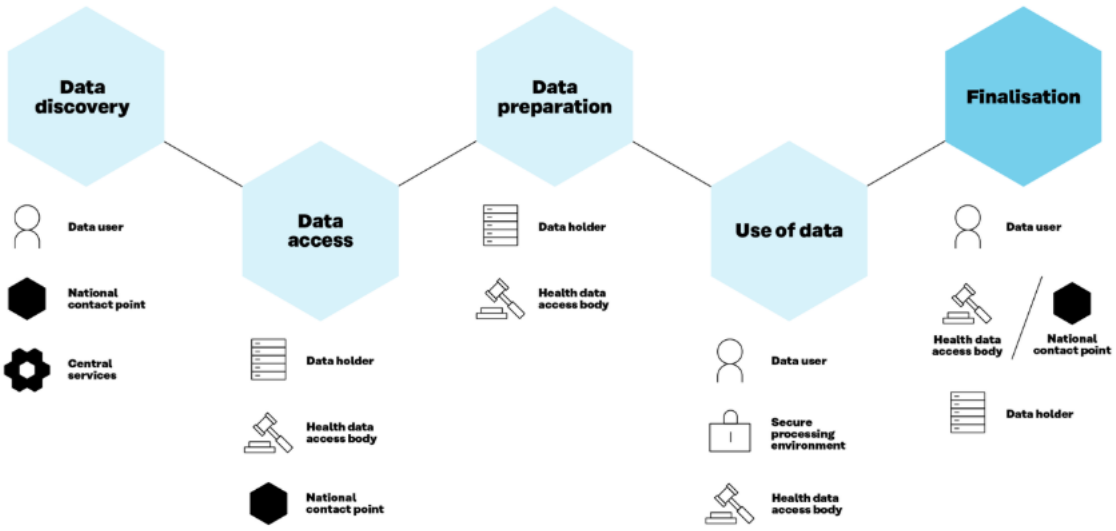
safeguards for confidentiality, trade secrets, ongoing appeals, and the correction or removal of published information where decisions are overturned. Clearer guidance on the role of the HealthData@EU IT tool in this context would also support consistent implementation.

Overall, the guideline provides a strong and well-structured foundation for enforcement under Articles 63 and 64. Its effectiveness could be further enhanced through additional operational guidance, including concrete use cases, harmonised templates, standardised workflows, and illustrative examples. These elements would support convergence across Member States, improve predictability for all actors, and help ensure that cross-border enforcement under the EHDS develops in a consistent, proportionate, and trustworthy manner.

Annex 3 – User journey

When a data user[i] 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)[ii]. 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)[iii] 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 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[iv]. 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 out- comes 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.

Annex 4 – Glossary

Project partners have added key terms and their definitions used in the milestones and deliverables to this glossary. The aim is to ensure harmonised terminology in all the TEHDAS2 deliverables.

Term	Definition
Access permit	Machine-actionable data structure that contains the information from data permit in a standardised format that can be securely transferred and acted on by computer services.
Access point	A component of the HealthData@EU infrastructure that ensures secure, point-to-point message exchange between National Contact Points and the central platform. Access Points exist at both the national and EU levels and enable the technical interconnection required by Articles 36(3d) and 75 of the Regulation.
Additional information (related to pseudonymisation)	Additional information is information whose use enables the attribution of **pseudonymised data** to identified or identifiable persons (EDPB Guideline 01/2025 Glossary, version adopted for public consultation). This term is specific to **pseudonymisation** and related to the "additional information" referred to in Regulation (EU) 2016/679 Article 4(5) (GDPR).
AI system	A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. AI Act – Regulation (EU) 2024/1689, Article 3(1)
Anonymisation	The process by which personal data is altered in such a way that a data subject can no longer be identified directly or indirectly. (Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, Recital 52; EHDS Regulation, Recital 92)

Anonymisation metadata	Where applicable, anonymisation metadata refers to a structured set of detailed information describing (a) the methods and parameters used to anonymise a dataset, and (b) the resulting **quality metrics** used to anonymise a dataset or data processing result, or to assess their anonymisation. It includes details e.g., on applied techniques and transformation logs. This metadata helps assess data protection, track modifications, and ensure compliance with anonymisation criteria.
Anonymisation result	The output of anonymisation, which can be an anonymised dataset or a data processing result including **anonymisation metadata**.
Anonymised statistical format	An anonymised statistical format refers to aggregated data that does not include information on individual data subjects or entities. Aggregation is one possible anonymisation technique.
Areas of occupational health	Areas of occupational health are the main disciplines concerned with protecting and promoting works health and safety in the workplace. It includes: • Occupational medicines: Prevention and management of work-related diseases, • Occupational hygiene: Identification and control of workplace hazards • Occupational safety: Prevention of accidents and injuries • Occupational health nursing: Workplace health services • Ergonomics: adapting work to fit the worker • Occupational psycology: Mental health and well-being at work • environmental healt: Control of enviornmental risks affecting workers A case of occupational disease is defined as a case recognised by the national authorities responsible for recognition of occupational diseases. The data shall be collected for incident occupational diseases and deaths due to occupational disease. Work-related health problems and illnesses are those health problems and illnesses which can be caused, worsened or jointly caused by

	working conditions. This includes physical and psychosocial health problems. A case of work-related health problem and illness does not necessarily refer to recognition by an authority and the related data shall be collected from existing population surveys such as the European health interview survey (EHIS) or other social surveys.
Areas of Public Health	'Public health' shall mean all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Regulation (EU) 2021/2282, Article 2(5).
Attribution of pseudonymised data to data subjects	Process that establishes that **pseudonymised data** relate to an already identified person, or links the data to other information with reference to which the data subjects could be identified. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Authorised user	An authorised natural person or legal person listed in the data permit, giving them the rights to process sensitive data inside a secure processing environment.
Benefits (of data use)	Refers broadly to positive outcomes of data use. It can encompass social, health and environmental aspects, among others.
Central platform	An interoperability platform established by the European Commission, providing services to support and facilitate the exchange of information between national contact points and authorised participants in HealthData@EU for secondary use of electronic health data. (EHDS Regulation, Article 75(8))
Consistent pseudonymisation	Two sets of data are considered to be pseudonymised consistently if data contained in those sets and relating to the same person can be linked on the basis of the **pseudonyms** they contain (EDPB Guideline 01/2025 Glossary, version adopted for public consultation). Consistency is context-specific and may be limited to a **pseudonymisation domain**.

Cross-border gateway	Handles the transmission and reception of communications between one National Contact Point and Central Services in a secure and technically standardised manner. It supports the eDelivery protocol (HD@EU Pilot WP5 – Architecture Definition).
Data access	A phase in the EHDS user journey during which 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). The user must complete the information required in the form, upload necessary documents, and provide justifications as needed.
Data aggregation	A process by which information is collected, manipulated and expressed in summary form (ISO/TR 12300:2014(en), 2.1.4)
Data anonymisation framework	A set of processes and practices designed to ensure data privacy through anonymisation and **privacy risk assessment**.
Data combination	The process of bringing together data from multiple **datasets** that can be processed pursuant to one or multiple data permit(s) or data request(s) (Regulation (EU) 2015/327 (EHDS) Articles 57, 68, 69) or other legal basis (such as consent or permits based on other legislation than EHDS). **Data linkage** can be part of this process.
Data consolidation	A process of combining data from multiple sources, cleaning and verifying them, removing errors so that they can be prepared for provision. Data consolidation may include creation of data subsets, data extraction, duplicates elimination, quality control and data linkage aspects.
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 extraction	Data extraction is the process of retrieving data from its source dataset.

	Structured data extraction involves extracting data from datasets that are already organised in predefined formats. Unstructured data extraction pertains to extracting data from databases handling unstructured formats such as PDFs, images, or free text. There may be one or more different data sources from which data extraction may be required.
Data holder application (a software linked to a secure processing environment)	A software application that provides the data holder with secure digital access to the secure processing environment (SPE). Its core functions include facilitating the upload and download of data in accordance with the data holder's responsibilities under the EHDS Regulation.
Data linkage	The process of combining **datasets** "from several sources on one topic or data subject" (ISO 5127:2017, 3.1.11.12). This can be done using unique identifiers, probabilistic methods, or a combination of techniques.
Data minimisation	A principle mandating to only collect, store and process personal data in a manner that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. (GDPR Article 5(1)(c)) Access is only provided to electronic health data that is "adequate, relevant and limited to what is necessary in relation to the purpose of processing indicated in the health data access application by the health data user and in line with the data permit issues pursuant to Article 68." (EHDS Regulation, Article 66(1)) Data minimisation applies to all stages of the data lifecycle.
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 EHDS Regulation. (EHDS Regulation, Article 2(2) point (v))
Data preparation	Data preparation is the process in which an organisation (in this case the data holder or the health data access body) transforms and organises raw personal or non-personal health data into one or more datasets (either in

	individual-based or aggregated form), to comply with a data permit or a data request.
Data processing	Any operation or set of operations which is performed on personal/non-personal data or on sets of personal/non-personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (Modified from the GDPR Article 4(2))
Data processing result	Data processing result refers to outputs from data processing activities carried out by the health data user. It may be generated from statistical analysis or machine learning algorithms, including descriptive statistics, model coefficients, performance indicators, visualisations.
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 their behalf. (GDPR, Article 4(1)(8))
Data protection	Processing data respecting the principles laid down in GDPR Article 5(1). The “implementation of appropriate administrative, technical or physical means to guard against unauthorised intentional or accidental disclosure, modification, or destruction of data (ISO/IEC 20944-1:2013(en), 3.6.5.1).
Data provenance	Data provenance means a **description of the source** of the data, including context, purpose, method and technology of data generation, documenting agents involved in the provenance of data, data validation routines, source data verification, traceability of changes, and quality control of data.

Data provision	The stage in the **EHDS user journey** where prepared health data is made accessible to authorised users for secondary purposes.
Data quality	Data quality means the degree to which the elements of electronic health data are suitable for their intended primary use and secondary use; (EHDS Article 2(2) point (z))
Data quality and utility label	Data quality and utility label means a graphic diagram, including a scale, describing the data quality and conditions of use of a dataset. (EHDS Article 2(2) point (aa))
Dataset	A structured collection of electronic health data. (EHDS Article 2(2) point (w))
Dataset catalogue	A collection of dataset descriptions, arranged in a systematic manner and including a user-oriented public part, in which information concerning individual dataset parameters is accessible by electronic means through an online portal. (EHDS Article 2(2) point (y)
Dataset description	A description in the form of metadata of the available datasets and their characteristics (EHDS Article (77(1))
Dataset record	A dataset record is a single, structured unit of data within a dataset, analogous to a row in a table or a record in a database. It contains specific information about a single entity or instance within the broader dataset.
Dataset subset	Dataset subset contains only selected records, variables or elements from a larger dataset while maintaining its key characteristics and relationships.
Data user application (a software linked to a secure processing environment)	A software application that provides the data user with secure, computerised access to their workspace within the secure processing environment. Its primary functions include facilitating the upload and download of data while ensuring robust authentication and authorisation mechanisms to prevent unauthorised access.
Development activities	The concept 'Development activities' is not clearly defined in any legal act. However, there is a definition of the notion of research and development in Directive 2009/81/EC, Article 1(27): 'Research and development' mean all activities comprising fundamental research, applied research and experimental development, where the latter may include the realisation of technological demonstrators, i.e. devices that demonstrate the performance of a new concept or a new technology in a relevant or

	representative environment." Directive 2009/81/EC, Article 1(27)
Direct identifier	A data element (or set thereof) that has been assigned or is being used to distinguish the data subject it refers to from all others in the given context without requiring the use of **additional information**. Examples are passport or social security number, or the set consisting of first and last name as well as date of birth. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Disclosure control	Disclosure control refers to techniques and procedures applied to datasets to reduce the privacy risks for individuals when the data is disclosed to data users.
Dispatcher	A component of the HealthData@EU infrastructure that enables the secure transmission, routing and delivery of structured electronic messages (such as dataset records and access requests) between national and central systems.
European Health Data Space (EHDS) user journey	The path of a data user applying for electronic health data for secondary use purposes within the European Health Data Space (EHDS). A simplified version of a EHDS user journey is included in the annexes of TEHDAS2 Deliverables. It consists of five main phases: data discovery, data access, data preparation, use of data and finalisation.
Electronic health data	Personal or non-personal electronic health data (EHDS Article 2(2) point (c)).
EU dataset catalogue	A dataset catalogue means a collection of dataset descriptions, arranged in a systematic manner and including a user-oriented public part, in which information concerning individual dataset parameters is accessible by electronic means through an online portal. (EHDS Regulation, Article 2(2) point (y))
Federated analysis	A decentralised approach to data analysis where statistical results are computed locally on distributed data resources rather than aggregating raw data centrally. This method enables benchmarking, multi-site research, and collaborative analytics while preserving data privacy and security. Only aggregated insights or summary statistics are shared between nodes, ensuring compliance with data protection regulations.
Federated learning	A decentralised machine learning approach where models are trained and validated on

	distributed data resources without transferring raw data. Instead, only model updates or gradients are exchanged between nodes, enhancing data privacy and security. This method enables collaborative model development across multiple organisations or devices while maintaining local data sovereignty and regulatory compliance.
Federated processing	A decentralised data processing approach where computations occur locally on distributed nodes rather than being centralised. This method enables data to remain on local devices or servers while only aggregated results or model updates are shared, enhancing privacy and security. It is commonly used in machine learning ("federated learning"), analytics ("federated analysis"), and secure data collaborations across multiple organisations.
Fidelity	Fidelity (or resemblance**)** refers to the extent to which processed data – such as anonymised data – retains the statistical properties, relationships, and structural characteristics of the **original/source data**. High fidelity means that distributions, correlations, and key patterns remain unchanged.
Healthcare	'Healthcare' means health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices. Directive 2011/24/EU, Article 3(a)
Health data access application	An application form used to seek access for personal-level electronic health data for secondary use in an anonymised or a pseudonymised format. (EHDS Article 67)
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. (EHDS Article 55 and Recital 52)
Health data applicant	A natural or legal person submitting a health data access application or a data request to a health data access body for the purposes referred to in Article 53 of EHDS 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. For a more detailed definition: EHDS Regulation, Article 2(2) point (t))
Health data request	A request to access data in an anonymised statistical format for the purposes referred to in EHDS Article 53. (EHDS Regulation, Article 69)
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 Regulation, Article 2(2) point (u))
Health technology assessment (HTA)	A multidisciplinary process that summarises information about the medical, patient and social aspects and the economic and ethical issues related to the use of a health technology in a systematic, transparent, unbiased and robust manner. (Regulation (EU) 2021/2282 on health technology assessment and amending Directive 2011/24/EU, Article 2(5))
High performance computing (HPC)	The use of advanced and not commonly available computational infrastructure – such as supercomputers or compute clusters – to solve highly complex and resource intensive computational problems.
Intellectual property (IP)	(a) a trade mark; (b) a design; (c) a copyright or any related right as provided for by national or Union law; (d) a geographical indication; (e) a patent as provided for by national or Union law; (f) a supplementary protection certificate for medicinal products as provided for in Regulation (EC) No 469/2009 of the European Parliament and of the Council of 6 May 2009 concerning the supplementary protection certificate for medicinal products (1); (g) a supplementary protection certificate for plant protection products as provided for in Regulation (EC) No 1610/96 of the European Parliament and of the Council of 23 July 1996 concerning the creation of a

	supplementary protection certificate for plant protection products (2); (h) a Community plant variety right as provided for in Council Regulation (EC) No 2100/94 of 27 July 1994 on Community plant variety rights (3); (i) a plant variety right as provided for by national law; (j) a topography of semiconductor product as provided for by national or Union law; (k) a utility model in so far as it is protected as an intel lectual property right by national or Union law; (l) a trade name in so far as it is protected as an exclusive intellectual property right by national or Union law. (Regulation (EU) No 608/2013 concerning customs enforcement of intellectual property rights and repealing, Article 2(1))
Intermediation entity	A legal person that may be established by national law for the purpose of fulfilling the obligations of certain categories of health data holders and that is able to process, make available, register, provide, restrict access to and exchange electronic health data for secondary use provided by health data holders. (EHDS Regulation, Article 50 (3) and Recital 59)
Interoperability	Ability of organisations, as well as of software applications or devices from the same manufacturer or different manufacturers, to interact through the processes they support, involving the exchange of information and knowledge, without changing the content of the data, between those organisations, software applications or devices. (EHDS Regulation, Article 2(2) point (f))
Invoice	A legally binding commercial document, detailing the complete cost structure with breakdowns by services and data holders. It contains disaggregated cost elements.
Irreversible pseudonymisation	A pseudonymisation method where the **pseudonymising transformation** cannot be reversed. The information necessary to re-establish the link between the **pseudonym** and the **original data** has been permanently destroyed or is otherwise unavailable. If the pseudonymising transformation is truly irreversible and re-identification is no longer reasonably possible, the resulting data qualify as anonymised data rather than pseudonymised data under the GDPR.

Legal basis of data processing	The criteria defined in EHDS Regulation Article 68 for health data access bodies to assess whether an applicant can be given a permit to process electronic health data. The conditions under which personal data processing is considered lawful are laid down in GDPR, Article 6. Purposes for which the electronic health data can be processed for secondary use are laid down in EHDS Regulation, Article 53.
Medicinal product	Any substance or combination of substances presented for treating or preventing disease in human beings. Any substance or combination of substances which may be administered to human beings with a view to making a medical diagnosis or to restoring, correcting or modifying physiological functions in human beings is likewise considered a medicinal product. Directive 2011/24/EU referring to Directive 2001/83/EC, Article 1(2)
Medical device	Any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: • diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease • diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability • investigation, replacement or modification of the anatomy or of a physiological or pathological process or state • providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

	The following products shall also be deemed to be medical devices: • devices for the control or support of conception • products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point. Regulation (EU) 2017/745 and (EU) 2017/746, Article 2(1)
Metadata	A structured description of the contents or the use of data facilitating the discovery or use of that data. (Data Act, Article 2)
National contact point (NCP)	A National Contact Point for secondary use is the organisational and technical gateway for making electronic health data available for secondary purposes, including research, innovation, policy-making, and public health. It plays a crucial role in connecting national data infrastructures to the HealthData@EU Central Platform, enabling secure and efficient data sharing across borders. (EHDS Regulation, Article 75(1))
Non-compliance	Any failure to comply with any requirement under the Union harmonisation legislation.
Non-personal electronic health data	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. (EHDS Regulation, Article 2(2b))
Observational Medical Outcomes Partnership (OMOP) common data model (CDM)	A standardised, common data model (CDM) specification originally developed by the Observational Medical Outcomes Partnership (OMOP) and now maintained by the Observational Health Data Sciences and Informatics (OHDSI) community. It defines a consistent structure and a set of standardised vocabularies for observational health data,

	enabling researchers to perform large-scale, reproducible analyses across diverse databases.
Open data	Data in an open format that can be freely used, re-used and shared by anyone for any purpose. Open format means a file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents. (Directive (EU) 2019/1024 on open data, “Open Data Directive”)
Open (data) database	Publicly accessible digital data that anyone can freely use, reuse, and redistribute for any purpose.
Original/source data	Individual-level health data prior to any application of **pseudonymisation, anonymisation**, or **synthetic data generation**. It consists of raw data that directly represent real-world individuals.
Payment	The financial transaction by which the user transfers the requested amount to the health data access body, trusted data holder or the data holder in response to a request for payment.
Payment instalment	One of several scheduled payments made in response to requests for payment. Each instalment corresponds to a portion of the total cost, aligned with the progress of the procedure or delivery of services.
Personal electronic health data	Data concerning health and genetic data, relating to an identified or identifiable natural person, processed in an electronic form. (EHDS Regulation, Article 2(2a))
Privacy (of synthetic or anonymised data)	Privacy measures the extent to which anonymised or synthetic data protects individuals from re-identification, membership inference, or sensitive information leakage. High privacy ensures that no single individual can be traced back to the real dataset, nor can their participation in the **dataset** be inferred.

Privacy risk assessment	Overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information (3.7), framed within an organisation's broader risk management framework (ISO/IEC 29100:2024(en), 3.18). **Re-identification risk assessment** falls under privacy risk assessment, together with attribute inference and group membership, for example.
Pseudonym	Identifier that is added to data during the **pseudonymising transformation** and set in such a way that it can be attributed to data subjects only using **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
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 organisational measures to ensure non-attribution to an identified or identifiable person. (GDPR, Article 4(5))
Pseudonymisation domain	Environment in which the controller or processor wishes to preclude attribution of data to specific data subjects. May incorporate persons acting under the authority of the controller or processor, respectively, other natural or legal persons, public authorities, agencies or other bodies, and their respective technological and informational resources. Does not include persons authorised to process additional data allowing the attribution of the **pseudonymised data** to data subjects. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymisation entity	The entity responsible of processing identifiers into pseudonyms using the pseudonymisation function. It can be a data controller, a data processor (performing pseudonymisation on behalf of a controller), a **trusted third party** or a data subject, depending on the pseudonymisation scenario. It should be

	stressed that, following this definition, the role of the pseudonymisation entity is strictly relevant to the practical implementation of pseudonymisation under a specific scenario. (ENISA, Pseudonymisation techniques and best practices, p. 10)
Pseudonymisation secrets	Data that is used in the application of the **pseudonymising transformation** or is created during that process, for example cryptographic keys or salts, and allows the computation of pseudonyms from certain identifying attributes. Part of **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymised data	Result of applying the **pseudonymising transformation** to some personal data. Cannot be attributed to a specific data subject without **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymising controller or processor	Controller or processor that uses pseudonymisation as a safeguard and modifies **original data** according to Regulation (EU) 2016/679 (GDPR) Article 4(5). (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Pseudonymising transformation	Procedure that modifies **original data** in a way that the result cannot be attributed to a specific data subject without **additional information**. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Public sector body	'Public sector body' means the state, regional or local authorities, bodies governed by public law, or associations formed by one or several such authorities or one or several such bodies governed by public law." Regulation (EU) 2022/868, Data Governance Act, Article 2(17).
Public use file	A **dataset** made available to the public, typically containing anonymised, synthetic or aggregated data to protect individual privacy. These files can be released to data users for information and testing purposes before they apply for a data permit. It is based on **original data**.

Public value (of data use)	For analytical or policy discussion purposes, public value could be understood as a weighted composite of risks and benefits of the data use taking into account the sustainability of benefits, addressing future societal needs, distributing benefits fairly, evaluating potential harm, ensuring stable safeguards through risk assessment, and correcting any harms that may occur.
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. (GDPR, Article 5(1b).
Quality metrics	Quality metrics refer to qualitative and quantitative indicators used to assess the fitness for purpose of a dataset. In the context of synthetic and anonymised data, quality metrics are particularly relevant to evaluate how transformations affect the data's **utility**, **fidelity**, and **privacy**. Quality metrics may also be used to assess pseudonymised or original datasets, particularly when serving as a benchmark or when evaluating fitness for specific secondary use purposes. (Adapted from ISO and EHDS principles; EHDS Regulation, Article 66 and Recital 58)
Quality metrics evaluation	Quality metrics evaluation refers to the calculation or derivation of the **quality metrics**.
Quality metrics tool	Quality metrics tool (or "metrics tool") refers to a software, an algorithm, a processing pipeline, a documented manual process, or a combination of these, designed to perform **quality metrics evaluation**.
Quasi-identifier	A **dataset** attribute that, when considered in conjunction with other attributes are sufficient to attribute at least part of the pseudonymised data to data subjects. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Re-identification	The process of associating data in a de-identified **dataset** with the original data principal

	(i.e., data subject) (ISO/IEC 20889:2018(en), 3.31).
Re-identification risk	The risk of a successful re-identification attack (ISO/IEC 20889:2018(en), 3.33), which describes an action performed on de-identified data by an attacker with the purpose of **re-identification** (ISO/IEC 20889:2018(en), 3.32).
Representational State Transfer Application Programming Interface (RESTful API)	An application programming interface used for building scalable and interoperable web services. RESTful API follows the principles of Representational State Transfer (REST), using standard HTTP methods to perform operations on resources identified by URLs. It emphasises stateless interactions, meaning each request contains all necessary information without relying on server-side sessions.
Request for payment	A formal request submitted to the data user for payment of the actual costs corresponding to work completed during a specific period. It follows the structure defined in the original invoice and refers to the relevant cost components outlined therein.
Reversible pseudonymisation	The **pseudonymisation entity** uses a **pseudonymising transformation** process that allows the pseudonymisation entity to reverse the **pseudonym**, if necessary. For example, by using separately kept matching tables of pseudonyms and identifying data, or computable secrets allowing for calculating back to the original input.
Secondary use	Processing of electronic health data for the purposes set out in Chapter IV of EHDS Regulation, other than the initial purposes for which they were collected or produced. (EHDS Regulation, Article 2(2) point (e))
Secure processing environment (SPE)	An environment in which access to electronic health data can be provided in following a data permit. A secure processing environment is subject to technical and organisational measures and security and interoperability requirements. Specifically allowing access to only those persons listed in the permit, as well as user authentication, authorisation, restricted data handling, logging and the compliance monitoring of respective security measures. (EHDS Regulation, Article 73)
Sensitive data	Data with potentially harmful effects in the event of disclosure (i.e., providing access to data to a third party) or misuse (ISO 5127:2017(en), 3.1.10.16)).

Serious cross-border threats	This Regulation shall apply to public health measures in relation to the following categories of serious cross-border threats to health: (a) threats of biological origin, consisting of: (i) communicable diseases, including those of zoonotic origin; (ii) antimicrobial resistance and healthcare-associated infections related to communicable diseases ('related special health issues'); (iii) biotoxins or other harmful biological agents not related to communicable diseases; (b) threats of chemical origin; (c) threats of environmental origin, including those due to the climate; (d) threats of unknown origin; and (e) events which may constitute public health emergencies of international concern under the International Health Regulations (IHR) ('public health emergencies of international concern'), provided that they fall under one of the categories of threats set out in (a–d) Regulation (EU) 2022/2371, Article 2(1)
Statistics	Quantitative and qualitative, aggregated and representative information characterising a collective phenomenon in a considered population. Regulation (EU) 223/2009, Article 3(1)
Synthetic data	Artificially generated data. The concept of synthetic data generation is to take an original data source (dataset) and create new, artificial data, with similar statistical properties from it.
Synthetic data documentation	Documentation of a synthetic dataset generated automatically or semi-automatically by the **synthetic data generator**. The documentation shall be anonymised so that it can be accompanied with the synthetic data set when released for the data user or for public use.
Synthetic data generator	A synthetic data generator is a software application, model or algorithm designed to generate **synthetic data**. It uses real-world data

	as input and generates a synthetic dataset. It is also possible to use parameters derived from the **original data** as input and/or modify additional parameters entered by the user.
Tabular data	Data organised in a structured format of rows and columns, where each row represents a single record or entity, and each column represents a specific attribute or variable. This structure is commonly found in spreadsheets or relational databases, making it easy to store, query, and analyse. Tabular data is often used for structured datasets where relationships between variables are well-defined.
Trade secret(s)	Information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. (Trade Secret Directive (2016/943), Article 2(1))
Transfer of data outside the EU/EEA	Transfer of data outside of the European Union or European Economic Area according to the three cumulative criteria identified by the European Data Protection Board (EDPB): • ”a controller or a processor is subject to the GDPR for the given processing; • this controller or processor discloses by transmission or otherwise makes personal data available to another organisation (controller or processor); • this other organisation is in a country outside EEA or is an international organisation.”
Trusted health data holder	Member State designated health data holder for whom a simplified procedure can be followed for the issuance of data permits. Trusted health data

	holders leverage their expertise on the data they hold to assist the health data access body by providing assessments of data requests or access applications. Once data permits are authorised, these trusted data holders provide the data within a secure processing environment that they manage. (EHDS Regulation, Article 72 and Recital 76)
Trusted research environment (TRE)	A research environment that aims to create trusted, auditable access to sensitive data, often under national governance frameworks. TREs are not the same as secure processing environments, which are legally defined in the EHDS Regulation. TREs emerged from the UK health research sector, shaped by community-led principles and structured around flexible, function-based zones.
Trusted third party (TTP)	A **pseudonymisation entity** which is independent from the data user and data holder that processes identifiers into pseudonyms. (ENISA, Pseudonymisation techniques and best practices). The TTP needs only to know the identifiers of the data subjects on the basis of which it will compute the **pseudonyms**, and no other data. (EDPB Guideline 01/2025 Glossary, version adopted for public consultation)
Utility	Utility refers to how well the data supports its intended use, such as syntactical testing, analytical tasks, decision-making, or machine learning model performance. In the context of anonymised and synthetic data high utility means that insights, predictions, or outcomes derived from the data closely match those obtained using the **original data**.

Annex 5 – List of costs

Data application/ data request/ both	Eligible to be considered for fees?	TOPICS CATEGORY	Marginal/ Fixed	TOPICS	ACTIVITY	Task related to cost	Type of costs	HDAB	TDH	DH
Both	NO	Data discovery	Fixed	National Metadata catalogue	Quality and utility label	Implement provisions on data quality and utility label	HR			X
Both	NO	Data discovery	Fixed	National Metadata catalogue	Quality and utility label	Supervise DH to ensure implementation of the provisions on data quality a	HR	X		
Both	NO	Data discovery	Fixed	National Metadata catalogue	Implementation	Produce of database documentation	HR			X
Both	YES	Data discovery	Fixed	National Metadata catalogue	Implementation	Database update due to project-specific requirements	HR			X
Both	NO	Data discovery	Fixed	National Metadata catalogue	Administrative overheads	Communicate to HDAB a description of the database	HR			X
Both	NO	Data discovery	Fixed	National Metadata catalogue	Database accuracy	Check accuracy of database in the national dataset catalogue on annual ba	HR			X
Both	NO	Data discovery	Fixed	National Metadata catalogue	Implementation	Make and maintain a national dataset catalogue (internet site)	HR	X		
Both	NO	Data discovery	Fixed	National Metadata catalogue	Implementation	Develop tools to consolidate catalogs from DH	HR	X		
Both	NO	Data discovery	Fixed	National Metadata catalogue	Implementation	Integrate data and update in national catalogue	HR	X		
Both	NO	Data discovery	Fixed	National Metadata catalogue	Implementation	Server sizing and security costs	Infrastructure	X		
Both	NO	Data discovery	Fixed	European Metadata catalogue	Implementation	Synchronize at european level	HR	X		
Both	YES	Submission of Data Access application/request	marginal	Application/request management	Examination of the data application/re	Receive and analyse the file (details in M6.3)	HR	X		
Both	YES	Submission of Data Access application/request	marginal	Application/request management	Public information	Make publicaly available data application and request	HR	X		
Both	YES	Submission of Data Access application/request	Fixed	Application/request management	Public information	Run a management system to record and process health data access applic	Infrastructure	X		
Both	YES	Submission of Data Access application/request	marginal	Application/request management	Examination of the data application/re	Assessment of the datasets to be requested to data holders	HR	X		
Both	YES	Submission of Data Access application/request	marginal	Application/request management	Administrative overheads	Transmit the file to concerned data holders	HR	X		
Both	YES	Submission of Data Access application/request	marginal	Application/request management	Administrative overheads	Coordinate between HDAB at EU and national level	HR	X		
Both	YES	Submission of Data Access application/request	marginal	Project feasibility	Examination of the data application/re	Validate method and protocol	HR			X
Both	YES	Submission of Data Access application/request	marginal	Project feasibility	Feasibility study	Validate regulatory feasibility	HR	X		
Both	YES	Submission of Data Access application/request	marginal	Project feasibility	Feasibility study	Perform feasability study	HR			X
Both	YES	Submission of Data Access application/request	marginal	Fee estimate	Quoting	Draft the quote	HR	X		X
Both	YES	Submission of Data Access application/request	marginal	Fee estimate	Administrative overheads	Transmit the quote to HDAB	HR			X
Both	YES	Submission of Data Access application/request	marginal	Fee estimate	Administrative overheads	Compile and transmit the quote to data user	HR	X		
Data application	YES	Data permit/Data request approval	marginal	Data permit assessment	Permit management	Assess data application	HR	X	X	
Data application	YES	Data permit/Data request approval	marginal	Ethical assessment	Submission to ethical committee	Prepare file for ethical committee	HR	X		
Data application	YES	Data permit/Data request approval	marginal	Ethical assessment	Submission to ethical committee	Ethical committee assessment costs	HR	X		
Data application	YES	Data permit/Data request approval	marginal	Data permit	Permit management	Grant (or refuse) permit and justify	HR	X		
Data application	YES	Data permit/Data request approval	marginal	Data permit	Permit publication	Make publicaly available granted permit and refusal	HR	X		
Data request	YES	Data permit/Data request approval	marginal	Data request approval	Data request management	Assess data request (details in M6.3)	HR	X	X	
Data request	YES	Data permit/Data request approval	marginal	Data request approval	Data request management	Approve (or refuse) data request and justify	HR	X		
Data request	YES	Data permit/Data request approval	marginal	Data request approval	Data request publication	Make publicaly available data request approval/refusal	HR	X		
Both	YES	Data permit/Data request approval	marginal	Data request approval	Risk mitigation	Analyse risks for IP rights and trade secrets	HR	X		X
Both	YES	Data permit/Data request approval	marginal	Data request approval	Risk mitigation	Analyse risk for data protection GDPR	HR	X		
Both	YES	Data permit/Data request approval	marginal	Data request approval	Risk mitigation	Analyse risks for national defence, security, public security and public order	HR	X		
Both	YES	Data permit/Data request approval	marginal	Contracting	Contracting management	Prepare contract and signature	HR	X	X	
Both	YES	Database constitution, infrastructure and quality	Fixed	Compiling	Data extraction	Perform data collection to feed datawarehouse for secondary use	HR			X
Both	YES	Database constitution, infrastructure and quality	Fixed	Compiling	Data extraction	Create of new data pipeline for datawarehouse	HR			X
Both	YES	Database constitution, infrastructure and quality	Fixed	Compiling	Data quality	Monitor data (quality control on data collection)	HR			X
Both	YES	Database constitution, infrastructure and quality	Fixed	Compiling	Data quality	Align terminology (protocol + mapping)	HR			X
Both	YES	Database constitution, infrastructure and quality	Fixed	Compiling	Data quality	Improve data quality (accuracy, completeness, format,...)	HR			X
Both	YES	Database constitution, infrastructure and quality	Fixed	Compiling	Data linkage	Perform internal data linkage	HR			X
Both	YES	Database constitution, infrastructure and quality	Fixed	Compiling	Infrastructure	Depreciation cost of investment for secondary use infrastructure	Infrastructure			X
Both	YES	Database constitution, infrastructure and quality	Fixed	Compiling	Data storage	Disk space and infrastructure costs (running+maintaining+update)	Infrastructure			X
Both	YES	Database constitution, infrastructure and quality	Fixed	Regulatory obligation	Patient information	Drafting and validation of patient information	HR			X
Both	YES	Database constitution, infrastructure and quality	Fixed	Regulatory obligation	Patient information	Dissemination of patient information	HR			X
Both	YES	Database constitution, infrastructure and quality	Fixed	Regulatory obligation	Patient information	Maintain a public information system to comply regulatory obligations	HR	X		
Both	YES	Database constitution, infrastructure and quality	Fixed	Regulatory obligation	Patient information	Run a public information system to comply regulatory obligations	Infrastructure	X		
Both	YES	Data preparation for the request	marginal	Regulatory obligation	Patient information	Draft and validate of patient information	HR			X
Both	YES	Data preparation for the request	marginal	Regulatory obligation	Patient information	Disseminate patient information	HR			X
Both	YES	Data preparation for the request	marginal	Data preparation DH	Data preparation follow up	Monitor project	HR			X
Both	YES	Data preparation for the request	marginal	Data preparation DH	Data selection	Check inclusion/exclusion criteria	HR			X
Both	YES	Data preparation for the request	marginal	Data preparation DH	Data extraction	Develop file/data extraction protocole	HR			X
Both	YES	Data preparation for the request	marginal	Data preparation DH	Data extraction	Extract file/data	HR			X
Both	YES	Data preparation for the request	marginal	Data preparation DH	Data treatment and consolidation	Perform pseudonymisation/ anonymisation	HR			X
Both	YES	Data preparation for the request	marginal	Data preparation DH	Data treatment and consolidation	Data minimisation	HR			X
Both	YES	Data preparation for the request	marginal	Data preparation DH	Data treatment and consolidation	Consolidate table	HR			X
Both	YES	Data preparation for the request	marginal	Data preparation DH	Data storage	Storage and computing resources preparation space	Infrastructure			X
Both	YES	Data preparation for the request	marginal	Data preparation DH	Data transmission	Export data to HDAB	HR			X
Both	YES	Provision of the data	marginal	Data preparation in SPE	Project space preparation	Monitor project	HR	X	X	
Both	YES	Provision of the data	marginal	Data preparation in SPE	Data transmission	Receive data and perform quality control	HR	X	X	
Both	YES	Provision of the data	marginal	Data preparation in SPE	Data quality	Align terminology (protocole + mapping)	HR	X	X	
Both	YES	Provision of the data	marginal	Data preparation in SPE	Data linkage	Define linkage strategy and implement	HR	X	X	
Both	YES	Provision of the data	marginal	Data preparation in SPE	Data linkage	Make linkage report	HR	X	X	
Data Application	YES	Provision of the data	marginal	Data preparation in SPE	Data treatment and consolidation	Perform pseudonymisation/ anonymisation	HR	X	X	
Both	YES	Provision of the data	marginal	Data preparation in SPE	Data treatment and consolidation	Take measures necessary to preserve the confidentiality of intellectual proj	HR	X	X	
Both	YES	Provision of the data	marginal	Data preparation in SPE	Dataset validation	Validate data set	HR	X	X	
Both	YES	Provision of the data	marginal	Data preparation in SPE	Run	Storage and computing resources preparation space	Infrastructure	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	Project space preparation follow up	Monitor project	HR	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	Project space preparation	Prepare project space SPE	HR	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	Project space preparation	Adapt existing tools/create new tools for project space	HR	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	Project space preparation	Validate project space	HR	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	Project space preparation	Licence for tool provision in project space	Licences	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	Project space preparation	Additional services from SPE providers and environment updates	HR	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	Project space preparation	Approve project space on security level	HR	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	Project space preparation	Approve data environment in project space SPE	HR	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	Project space preparation	Data export from preparation space to project space	HR	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	Project space preparation	Project space access	Infrastructure	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	SPE access	Project and analysis space provision (user training and support)	HR	X	X	
Data application	YES	Provision of the data	marginal	Project environment SPE	SPE access	Initial disk space in project space	Infrastructure	X	X	
Data request	YES	Provision of the data	marginal	Data request implementation	Data aggregation	Prepare and validate analysis plan	HR	X	X	
Data request	YES	Provision of the data	marginal	Data request implementation	Data aggregation	Develop analysis method	HR	X	X	
Data request	YES	Provision of the data	marginal	Data request implementation	Data aggregation	Generate aggregated statistical report	HR	X	X	
Data request	YES	Provision of the data	marginal	Data request implementation	Data aggregation	CPU for aggregation	Infrastructure	X	X	
Both	YES	Provision of the data	marginal	Invoice	Administrative overheads	Consolidate fee from contributors and send invoice	HR	X		
Both	YES	Provision of the data	marginal	Invoice	Administrative overheads	Reception of fees and redistribution to contributors	HR	X		
Both	YES	Use of the data	marginal	Regulatory obligation	Patient information	Maintain an information system to make public the results or output of sec	HR	X		
Both	YES	Use of the data	Fixed	Regulatory obligation	Patient information	Run an information system to make public the results or output of seconda	Infrastructure	X		
Data application	YES	Use of the data	marginal	Project running	Computation capacity	Computing resources in project space	Infrastructure	X	X	
Data application	YES	Use of the data	marginal	Project running	Disk space capacity	Disk space in project space	Infrastructure	X	X	
Data application	YES	Use of the data	marginal	Project running	Project extension	Infrastructure costs related to an extension of the data permit	Infrastructure	X	X	
Data application	YES	Use of the data	marginal	Project running	Project extension	HR costs related to an extension of the data permit	HR	X	X	
Both	YES	Use of the data	marginal	Project Closure	Project closure and archiving	Monitor project closure and database archiving	HR	X	X	
Both	YES	Use of the data	marginal	Project Closure	Project closure and archiving	Provide technical support for project closure and database archiving	HR	X	X	
Both	YES	Use of the data	marginal	Project Closure	Project closure and archiving	Perform all task for data archiving	HR	X	X	
Both	YES	Use of the data	marginal	Project Closure	Project closure and archiving	Data storage and archiving	Infrastructure	X	X	
Both	YES	Use of the data	marginal	Project Closure	Project closure and archiving	Close the project space	HR	X	X	
Both	YES	Use of the data	marginal	Project Closure	Project closure and archiving	Perform data destruction	HR	X	X	
Both	YES		Fixed	Overhead		Administration		X		X
Both	YES		Fixed	Overhead		Electricty bill		X		
Both	YES		Fixed	Overhead		Location costs		X		
Both	YES		Fixed	Overhead		Employer's social insurance contributions		X		
Both	YES		Fixed	Overhead		Equipment (PC, Telephone,...)		X		
Both	YES		Fixed	Overhead		Infrastructure		X		
Both	YES		Fixed	Overhead		Back office activities		X		

Annex 6 – Illustrative enforcement scenarios under Articles 63 and 64 of EHDS

Purpose of this Annex

This Annex provides illustrative, non-exhaustive scenarios intended to support a common understanding of how supervisory and sanctioning powers under Articles 63 and 64 of the EHDS Regulation may be applied in practice. The scenarios are descriptive in nature and do not create binding obligations. Their purpose is to support proportionality, consistency and legal certainty, while respecting national procedural autonomy.

Scenario 1 – Delay in data delivery due to technical and security constraints

In some cases, a health data holder may fail to deliver data within the initially prescribed timeframe because additional technical measures are required to ensure data protection. This situation may arise, for example, where a dataset relates to a rare disease or a small population and additional pseudonymisation or risk-mitigation measures are necessary to prevent indirect identification.

In such circumstances, a delay should not automatically be interpreted as obstruction. Where the data holder can demonstrate that the delay is objectively justified, proportionate to the risk involved, and has been communicated transparently to the HDAB, enforcement measures should prioritise corrective action and deadline adjustment rather than sanctions. This scenario illustrates the importance of distinguishing between legitimate technical constraints and intentional non-compliance.

Scenario 2 – Repeated failure to meet deadlines by a data holder

By contrast, a different assessment may be warranted where a data holder repeatedly fails to meet delivery deadlines across several permits over an extended period, despite reminders and opportunities to remedy the situation. Even if no single delay appears serious in isolation, a pattern of repeated non-compliance may indicate structural deficiencies or a lack of effective internal controls.

In such cases, HDABs may reasonably escalate enforcement progressively, starting with formal warnings or remedial orders and, where non-compliance persists, moving to periodic penalty payments or administrative fines. This scenario illustrates how repetition and persistence can justify stronger enforcement responses.

Scenario 3 – Misuse of data by a data user

A particularly serious scenario arises where a data user intentionally processes health data beyond the scope of the permit, for example by attempting to re-identify individuals or by using the data for unauthorised commercial purposes. Such conduct directly undermines the trust and safeguards on which the EHDS framework is based.

In these situations, immediate protective measures, such as suspension of access, may be necessary to prevent further harm. Administrative fines and exclusion from EHDS access may also be appropriate, subject to procedural safeguards. This scenario illustrates cases where deterrence and protection of fundamental rights take precedence over corrective approaches.

Scenario 4 – Cross-border enforcement involving multiple HDABs

Cross-border enforcement raises specific challenges where a data user holds permits issued by HDABs in different Member States. If a serious breach occurs under one permit, the HDAB that issued that permit may adopt enforcement measures within its jurisdiction. Other HDABs should be informed through cooperation mechanisms and may assess whether the same conduct affects compliance under permits they have issued.

However, enforcement measures taken by one HDAB do not automatically apply across borders unless national or EU law provides otherwise. This scenario highlights the importance of coordination and information exchange, while recognising the limits of territorial competence.

Scenario 5 – Multiple permits and cumulative penalties

A single operational failure may affect multiple data permits held in different Member States. In such cases, each HDAB remains competent to assess compliance in relation to its own permit. At the same time, proportionality requires that the overall impact of enforcement be considered, so that the same underlying conduct does not result in excessive cumulative penalties.

This scenario illustrates the need for context-aware sanctioning, particularly for actors operating across borders.

Scenario 6 – Responsibility in complex processing chains

In practice, health data holders often rely on processors or technical service providers to extract, transform or transmit data. Where a failure to comply with an obligation is attributable to a processor's technical shortcomings, HDABs should assess whether the data holder exercised appropriate due diligence, including contractual safeguards and oversight.

Where such due diligence can be demonstrated, sanctions should not be imposed automatically on the data holder. This scenario illustrates how responsibility should be linked to effective control, rather than formal roles alone.

Scenario 7 – Overlap between EHDS and GDPR enforcement

Some incidents may simultaneously constitute breaches of the EHDS Regulation and the GDPR, for example where a security incident leads to unauthorised access to personal health

data. In such cases, HDABs should inform the competent data protection authority and coordinate enforcement activities.

The objective should be to ensure coherent outcomes and to avoid duplicative or conflicting sanctions for the same factual conduct. This scenario illustrates the importance of inter-authority coordination and respect for the principle of non bis in idem.

Scenario 8 – Proportionality for small entities and public bodies

Minor, first-time infringements committed by small healthcare providers or publicly funded entities may result from limited resources rather than intent or negligence. In such cases, enforcement measures should focus on guidance, warnings or corrective action plans rather than immediate financial sanctions.

This scenario highlights how proportionality must take into account the nature, size and public role of the entity concerned, in line with Article 64.