



M4.1 Draft guideline on fees and penalties for non-compliance related to the EHDS regulation

Second section: 4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

TEHDAS2 – Second Joint Action Towards the European Health Data Space

17 September 2025

Co-funded by
the European Union





M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

Disclaimer

Views and opinions expressed in this deliverable represent 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 Document info

0.1 Authors

| Lead Author(s) | Lead organisation |
|---|--|
| Lucrezia Valieri | Ministry of Health, Italy |
| Maya Bucciarelli | Ministry of Health, Italy |
| Reviewers | |
| Katrine Højen Vad | Danish Health Data Authority |
| Eva Zvirgzdiņa | Centre for Disease Prevention and Control Republic of Latvia |
| Inge Franki | Health Data Agency (BE) |
| Emilie Passemard Dora Talvard Louisa Stuwe | Digital Health Delegation, French Ministry of Health |

0.2 Keywords

| Keywords | TEHDAS2, Joint Action, Health Data, European Health Data Space |
|----------|--|
|----------|--|

0.3 Document history

| Date | Version | Editor | Change | Status |
|------------|---------|------------------|--|---------------|
| 16/04/2025 | 0.1 | Lucrezia Valieri | First draft | Draft |
| 26/05/2025 | 0.2 | Lucrezia Valieri | Draft to be reviewed by the Consortium | Draft |
| 10/06/2025 | 0.3 | Lucrezia Valieri | Draft to be reviewed by the | Draft |
| 25/06/2025 | 0.4 | Lucrezia Valieri | Document to be submitted for review to EC | Final |
| 30/06/2025 | 0.5 | Louisa Stuwe | Finalized and submitted to TEHDAS2 consortium and EC | Final version |



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

| Date | Version | Editor | Change | Status |
|------------|---------|------------------|--|--------|
| 5/09/2025 | 0.6 | Lucrezia Valieri | Addressing additional comments from TEHDAS2 Community and DG SANTE | Final |
| 15/09/2025 | 0.6.1 | Lucrezia Valieri | Document for public consultation | Final |

Accepted in Project Steering Group by written procedure on may 2025.

Copyright Notice

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



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

Contents

| | | |
|-----|---|----|
| 1 | Abbreviations | 5 |
| 2 | Executive summary | 6 |
| 3 | Introduction | 7 |
| 3.1 | The Role of Health Data Access Bodies under the EHDS Regulation..... | 7 |
| 3.2 | Target audience..... | 8 |
| 3.3 | Scope..... | 8 |
| 3.4 | Legal framework | 9 |
| 4 | Supervisory Powers of HDABs under Article 63 | 10 |
| 4.1 | Investigative and Monitoring Mandate | 10 |
| 4.2 | Notification Obligations and the Right to Be Heard | 11 |
| 4.3 | Enforcement Measures against data users: Revocation, Suspension and Exclusion | 11 |
| 4.4 | Enforcement Measures Against Health Data Holders | 12 |
| 4.5 | Communication of Enforcement Measures and Compliance Deadlines | 13 |
| 4.6 | Notification and Transparency of Enforcement Measures through the HealthData@EU Infrastructure..... | 14 |
| 4.7 | Commission Responsibilities: Implementing Acts and Future Guidelines on Enforcement Measures | 15 |
| 5 | Administrative Fines under Article 64..... | 16 |
| 5.1 | General Principles: Effectiveness, Proportionality, and Deterrence..... | 16 |
| 5.2 | Criteria for the Imposition and Quantification of Fines..... | 16 |
| 5.3 | Categorisation of Infringements and Applicable Fine Ceilings | 17 |
| 5.4 | Treatment of Multiple Infringements and Repeat Offenders..... | 17 |
| 5.5 | Cumulative Assessment of Multiple Infringements | 18 |
| 5.6 | Procedural Safeguards and Legal Remedies | 18 |
| 6 | Implementation Considerations and Recommendations | 19 |
| 6.1 | Internal Decision-Making Processes for Enforcement..... | 19 |
| 6.2 | Use of Assessment Tools and Penalty Matrices | 19 |
| 6.3 | Integration with National Legal Frameworks..... | 19 |
| 6.4 | Need for Capacity Building and Training | 20 |
| 7 | Concluding Remarks | 20 |
| 7.1 | Legal Certainty and Trust in the EHDS | 20 |
| 7.2 | Towards a Common Enforcement Culture..... | 20 |
| 8 | Annexes | 21 |
| | Annex 1: Glossary | 21 |



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

1 Abbreviations

| Term | Abbreviation |
|--|--------------|
| European Health Data Space | EHDS |
| European Union | EU |
| General Data Protection Regulation | GDPR |
| Health Data Access Body | HDAB |
| Joint Action | JA |
| The Finnish Innovation Fund | Sitra |
| Towards the European Health Data Space | TEHDAS |
| Work Package | WP |



2 Executive summary

The aim of this guideline is to provide practical support to Health Data Access Bodies (HDABs) in exercising their supervisory and enforcement powers under Articles 63 and 64 of the European Health Data Space (EHDS) Regulation. These provisions empower HDABs to monitor compliance, take enforcement actions, and impose administrative fines where appropriate, thereby ensuring the lawful and trustworthy secondary use of electronic health data through the “HealthData@EU” infrastructure.

This guideline is developed from the perspective of the HDABs and is intended to serve as a reference throughout the supervision process—from the early detection of potential non-compliance by health data users or holders, through the application of enforcement measures such as revocation of data permits or exclusions from access, to the imposition and quantification of administrative fines. It provides interpretative guidance on the legal criteria set out in Articles 63 and 64, and offers practical insights on how to ensure that enforcement actions are effective, proportionate and dissuasive, in line with Union and national law. This guidance is non-binding and should be understood as a living document, subject to adaptation as further implementing acts, delegated acts or guidelines are adopted by the European Commission in cooperation with the EHDS Board.



3 Introduction

3.1 The Role of Health Data Access Bodies under the EHDS Regulation

As part of the European Health Union, the European Union (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, 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*



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

responsibilities of national Data Protection Authorities under the GDPR in cases where personal data protection issues are also at stake.

3.2 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.

3.3 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 European Health Data Space (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;



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

- 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 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.

3.4 Legal framework

The principal legal foundation for the supervisory and sanctioning responsibilities of HDABs is the European Health Data Space (EHDS) Regulation, in particular Articles 63 and 64¹. 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 under the General Data Protection Regulation (GDPR); 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 General Data Protection Regulation (GDPR, Regulation (EU) 2016/679). 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 Union 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; 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 Health Data Access Bodies (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,

¹ See paragraph 8. Annexes



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

the present guideline offers a high-level interpretative framework, which will require further specification as national procedures evolve and as additional EU-level guidance and implementing acts are adopted. In

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

4 Supervisory Powers of HDABs under Article 63

4.1 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 General Data Protection Regulation (GDPR).



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

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.

4.2 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 General Data Protection Regulation (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 Union 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.

4.3 Enforcement Measures against data users: Revocation, Suspension and Exclusion



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

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 Secure Processing Environment (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 Secure Processing Environment 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.

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.

4.4 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



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

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.

4.5 Communication of Enforcement Measures and Compliance Deadlines

Once a HDAB has decided to take enforcement action under Article 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



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

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.

4.6 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 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)(j)(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



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

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 mark the decision as inactive or withdraw it, ensuring that the IT tool accurately reflects the current legal situation

4.7 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 Health Data Access Bodies (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.



5 Administrative Fines under Article 64

5.1 General Principles: Effectiveness, Proportionality, and Deterrence

Health Data Access Bodies (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 European Health Data Space (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.

5.2 Criteria for the Imposition and Quantification of Fines

In determining whether to impose an administrative fine, and in setting its precise amount, Health Data Access Bodies (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 criteria 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.

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.



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

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.

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.

5.3 Categorisation of Infringements and Applicable Fine Ceilings

The Regulation distinguishes between two levels of infringements:

Less serious infringements (e.g. failure to comply with Article 60 or 61) may result in fines up to €10 million or 2% of worldwide 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 turnover, whichever is higher.

5.4 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 Articles 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 health data access body (HDAB), particularly in cases of persistent or deliberate obstruction.



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

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.

5.5 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.

5.6 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 Union law.

Before a decision to impose a fine or take any significant enforcement measure is finalised, the health data access body (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.



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

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 European Health Data Space.

6 Implementation Considerations and Recommendations

6.1 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.

6.2 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

6.3 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.



6.4 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.

7 Concluding Remarks

7.1 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 Health Data Access Bodies (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.

7.2 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 document is deliberately limited: it focuses on the supervisory and sanctioning powers under **Articles 63 and 64**, and does **not address** broader enforcement contexts, such as obligations under other chapters of the EHDS Regulation, overlapping GDPR enforcement, or national-level health data governance frameworks.

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 **Secure Processing Environment (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 or interoperability rules are established.

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 European Health Data



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

Space. 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.

8. Annexes

Annex 1: Glossary

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

| Term | Description |
|-------------------------------------|---|
| Dataset | Means a structured collection of electronic health data. (EHDS, Article 2(2)(w)) |
| 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)) |
| Anonymisation | The process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party. Anonymised data falls outside the scope of data protection laws such as GDPR. (GDPR Recital 26) |
| Secure Processing Environment (SPE) | ‘Secure Processing Environment’ means the physical or virtual environment and organisational means to ensure compliance with Union law, such as Regulation (EU) 2016/679, in particular with regard to data subjects’ rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, as well as with applicable national law, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms. (DGA, Article 2(20); EHDS, Article 2 (1)(c)) |
| Synthetic Data | Data that is artificially generated rather than obtained by direct measurement. Synthetic data can be created using statistical models, machine learning algorithms, or other generative |

M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

| | |
|--------------------------------|---|
| | processes to reflect the characteristics of real data while ensuring that no real individual can be identified from the data. |
| Data Linkage | The process of combining data from different sources that relate to the same entity (e.g., individual, institution) to create a more comprehensive dataset. This can be done using unique identifiers, probabilistic methods, or a combination of techniques. |
| Re-identification Risk | The potential that anonymised or pseudonymised data could be matched with other data sources to re-identify an individual. Mitigation strategies include robust anonymisation techniques and regular risk assessments. Reference: GDPR Article 6. |
| Data Minimisation | Principle that mandates that only the minimum necessary amount of personal data should be collected and processed for a specific purpose. This principle is fundamental under GDPR and relevant to the tasks outlined in EHDS. (GDPR Article 5(1)(c)) |
| Data Provenance | The history and origins of a dataset, including the methods and transformations applied to the data throughout its lifecycle. Understanding data provenance is crucial for ensuring data quality and integrity. (Relevant to GDPR's accountability principle Article 5(2)) |
| Actors (Roles) | |
| Health data access body (HDAB) | [...] providing access to health data through the involvement of health data access bodies, [...] In addition, the health data access body should assess the information provided by the health data applicant, based on which it should be able to issue a data permit for the processing of personal electronic health data pursuant to this Regulation that should fulfil the requirements and conditions set out in Chapter IV of this Regulation. [...] (EHDS, Recital 52) |
| Health Data holder | 'health data holder' means any natural or legal person, public authority, agency or other body in the healthcare or the care sectors, including reimbursement services where necessary, as well as any natural or legal person developing products or services intended for the health, healthcare or care sectors, developing or manufacturing wellness applications, performing research in relation to the healthcare or care sectors or acting |



M4.1.2 Draft guideline on penalties for non-compliance related to the EHDS regulation

| | |
|------------------------|--|
| | <p>as a mortality registry, as well as any Union institution, body, office or agency, that has either:</p> <ul style="list-style-type: none"> i. the right or obligation, in accordance with [] applicable Union or national law and in its capacity as a controller or joint controller, to process personal electronic health data for the provision of healthcare or care or for the purposes of public health, reimbursement, research, innovation, policy making, official statistics or patient safety or for regulatory purposes; or ii. the ability to make available non-personal electronic health data through the control of the technical design of a product and related services, including by registering, providing, restricting access to or exchanging such data; <p>(EHDS, Article 2(2)(t))</p> |
| Health Data user | <p>‘health data user’ means a natural or legal person, including Union institutions, bodies, offices or agencies, which has been granted lawful access to [] electronic health data for secondary use pursuant to a data permit, a health data request approval or an access approval by an authorised participant in HealthData@EU; (EHDS, Article 2(2)(u))</p> |
| Data life cycle | |
| Data access | <p>Processing by a data user of data that has been provided by a data holder, in accordance with specific technical, legal, or organisational requirements, without necessarily implying the transmission or downloading of such data. (DGA, Article 2(8),(9)&(13))</p> |
| Data permit | <p>‘data permit’ means an administrative decision issued to a health data user by a health data access body [] to process certain electronic health data specified in the data permit for specific secondary use purposes, [] based on conditions laid down in Chapter IV of this Regulation; (EHDS, Article 2(2)(v))</p> |