D8.1 Guideline for Health Data Access Bodies on implementing opt-out from the secondary use of health data

TEHDAS2 – Second Joint Action Towards the European Health Data Space

24 March 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

Authors	Organisation
János Péter Misek	National Directorate General for Hospitals, Hungary
László Bencze	National Directorate General for Hospitals, Hungary
Roxana Albu	Sciensano, Belgium
Asimina Boumpaki	Ministry of Health, Greece
Krisztina Davidovics	National Directorate General for Hospitals, Hungary
Krisztina Dienes-Horváth	National Directorate General for Hospitals, Hungary
Inge Franki	Health Data Agency, Belgium
Zdenek Gütter	Ministry of Health, Czech Republic
Wannes Van Hoof	Sciensano, Belgium
Richard Hrabčák	National Health Information Centre, Slovakia
Csaba Kiss	National Directorate General for Hospitals, Hungary
Louise Mathieu	Sciensano, Belgium
Bart Motmans	Health Data Agency, Belgium
Azul O'Flaherty	Department of Health, Ireland
Maria Papaioannou	CYENS Research Centre of Excellence, Cyprus
András Pethő	National Directorate General for Hospitals, Hungary
Sam Santosh	Maynooth University, Ireland
Irene Schlünder	TMF e.V., Germany
Anna Szilágyi	National Directorate General for Hospitals, Hungary
Milana Trucl	Sciensano, Belgium

Aurelija Usacova	Centre of Disease Prevention and Control of Latvia
Eva Zvirgzdiņa	Centre of Disease Prevention and Control of Latvia

0.2 Keywords

Keywords	TEHDAS2, Joint Action, Health Data, European Health Data Space, Health Data Access Body, Opt-out

0.3 Document history

Date	Version	Editor	Change	Status
05-5-2025	0.1	Authors and Contributors	First draft	Draft
19-6-2025	0.2	Authors and Contributors	Revisions and additions	Draft
20-6-2025	0.3	Authors and Contributors	Revisions according to EC review	Draft
3-7-2025	0.4	Authors and Contributors	Submission for internal review	Final draft
7-9-2025	0.5	EC review & Consortium review	Revised after internal review	Final
12-9-2025	1.0	Final draft version	Final version after PSG meeting	Final
13-1-2026	1.1	Authors and Contributors	Revisions and additions after public consultation	Draft
02-3-2026	1.2	Authors and Contributors	Submission for internal review	Draft
20-3-2026	1.3	EC review & Consortium review	Revised after internal review	Final
24-3-2026	2.0	Final version	Final version after PSG meeting	Final

Accepted in Project Steering Group on 24 March 2026.

Contents

1 Executive summary

The overall objective of T8.1 of the TEHDAS2 Joint action is to provide guidance to Health Data Access Bodies (HDABs) on their obligations under **Article 71 of the European Health Data Space (EHDS)** Regulation, regarding the right of natural persons to opt out from the secondary use of their personal electronic health data. While this guideline is primarily intended for HDABs, some recommendations may also be relevant to other stakeholders, among others, data holders and data users.

It aims to support HDABs by setting out the requirements and procedures for the effective implementation and administration of the opt-out mechanism, and by providing guidance on citizen engagement and the promotion of public trust to enable data sharing for secondary use. It is important to note that this guideline is not intended to directly inform people of their right to opt out, nor to guide data users on how to manage data impacted by the exercise of this right.

The document outlines the high-level responsibilities of HDABs and gives recommendations for addressing the right to opt-out from secondary use of health data, based on the current legal and policy landscape. More specifically, the guideline:

- Offers a clarification on the scope and implications of the opt-out right from secondary use of health data, under Article 71 EHDS, in contrast to the right to opt-out in primary use [Article 10 (1)].
- Highlights certain important data protection issues, with a focus on the difference between right to opt out, informed consent and the right to object, and the characteristics of personal electronic health data falling under opt-out, as well as the impact of anonymisation on the right to opt-out from secondary use.
- Acknowledges that the Regulation allows Member States (MS) to introduce more granular opt-out mechanisms (as opposed to a general opt-out), acknowledging that differences in legal traditions, cultural expectations, and societal sensitivities across the EU may justify varying levels of granularity at national level.
- Provides recommendations on the national mechanism of opt-out via centralised or decentralised national systems and highlights key legal principles, areas of national discretion, and structural limitations (including cross-border considerations), while clarifying that this guideline does not define detailed national workflows or technical solutions.
- Provides recommendations on how to balance the protection of the rights of individuals with the pursuit of societal benefits, and on how to foster public trust to ensure the success and wide acceptance of the EHDS.

The following areas fall outside the scope of this guideline:

- Does not provide implementation timelines, operational use cases, or country-specific mappings, as such examples or technical architectures would risk pre-empting national choices and future implementing acts.

- Does not offer authoritative legal interpretations of the interactions between the General Data Protection Regulation (GDPR) and the EHDS Regulation.

This guideline aims to better prepare HDABs to fulfil their responsibilities towards natural persons regarding the right to opt-out from the secondary use of personal electronic health data under the EHDS Regulation. The guideline also provides further areas of recommendations to support the alignment of national EHDS structures and to contribute to a harmonised approach to secondary use of health data across Europe.

This document is part of a broader set of TEHDAS2 guidelines aimed at supporting MS readiness and promoting consistent EHDS implementation. This guideline forms part of the initial, foundational layer of the EHDS implementation, providing a harmonised high-level framework to support MS preparedness, while recognising that more detailed operational guidance will emerge through future implementing acts, governance structures, and practical experience.

The methodology applied for the development of this guideline is described in Annex 1.

2 Abbreviations

Abbreviation	Term
D	Deliverable
DGA	Data Governance Act
DH	Data Holder
DPAs	Data Protection Authorities
eIDAS	Electronic Identification, Authentication and trust Services
EHR	Electronic Health Record
EDPB	European Data Protection Board
EHDS	European Health Data Space
EU	European Union
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
HDAB	Health Data Access Body
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
JA	Joint Action
MS	Member State
M	Milestone
SPE	Secure Processing Environment
T	Task
TTP	Trusted Third Party
TEHDAS	Towards the European Health Data Space
WP	Work Package

3 Introduction

3.1 Advancing health data use in the European Health Union

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

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

TEHDAS2 focuses on several critical aspects of health data use.

- Data discovery: findability and availability of health data, ensuring it is accessible for secondary purposes.
- Data access: developing harmonised access procedures and establishing standardised approaches for granting data access across MS.
- 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 MS joint efforts towards the secondary use of health data, while also reducing fragmentation in policies and practices related to secondary use.

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.

3.2 Position of this Guideline within the EHDS Governance Framework

This guideline serves as an initial step to support a consistent interpretation of the Regulation and to help MS prepare for the implementation of Article 71. Further material, operational mechanisms, and detailed guidance will be developed by the EHDS Board, which provides strategic direction, promotes harmonisation, supports implementation, and addresses

cross-border issues. These future elements will also contribute to the preparation of the implementing acts, a legally binding Commission measure that sets out the detailed rules needed to apply the Regulation in practice. Hence, the Joint Action will increase the preparedness of MS for the EHDS implementation and lead to better coordination of joint efforts towards the secondary use of electronic health data, while also reducing fragmentation in policies and practices related to secondary use.

The primary focus of the activities undertaken in TEHDAS2 Work Package 8 is to provide guidance on fulfilling obligations to natural persons and to enhance citizen trust and engagement with the EHDS in the context of the secondary use of electronic health data.

T8.1 addresses obligations towards natural persons through two documents:

- *D8.1 Guideline for Health Data Access Bodies on implementing opt-out from the secondary use of health data*
- *D8.2 Guideline for Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data*.

Article 71 of the EHDS Regulation establishes a clear and enforceable right for all natural persons to opt out of the processing of their personal electronic health data for secondary use. This right applies across the EU and can be exercised at any time, without justification. It is reversible and must be made accessible and easily understandable.

While, like most rights and obligations under EU law, the right itself is established at EU level, its practical implementation is delegated to the MS. This includes the responsibility to define the technical and procedural modalities of the opt-out mechanism and, where relevant, the conditions for narrowly defined exceptions as set out in Article 71(4).

It is important to distinguish between the opt-out provisions for primary and secondary use under the EHDS Regulation. In regulating the primary use of electronic health data, Article 10 allows MS to establish a national right for patients to opt out of the use of their data for healthcare purposes. This primary-use opt-out is entirely subject to national discretion and applies only within the context of healthcare provision and national EHR frameworks. It is therefore not symmetrical with, nor does it affect, the EHDS opt-out for secondary use of electronic health data.

Secondary use of electronic health data under the EHDS (Article 71 of the EHDS Regulation) does not operate on an opt-in basis. The Regulation establishes a default legal framework allowing secondary use for defined purposes, combined with a harmonised, individual right to opt out as a safeguard. This guideline does not prescribe a specific technical solution for implementing the opt out right, nor does it promote the creation of a single centralised opt-out register as a default or preferred approach. The EHDS Regulation requires MS to ensure that the right to opt out can be effectively exercised, while leaving the choice of technical and organisational solutions open.

The EHDS Regulation establishes an EU-wide right to opt out from secondary use of health data, while leaving the practical implementation of that right to the MS. As a result, opt-out mechanisms apply to personal electronic health data generated and held within the MS where care is provided and do not automatically propagate across borders. This legal design

may raise challenges in cross-border healthcare situations, particularly where individuals receive care in a MS other than their country of residence. Differences in national implementation may affect how opt-out choices are applied and communicated, and may complicate the provision of uniform, EU-wide public-facing explanations. These challenges reflect the current balance struck by the Regulation between harmonisation and national responsibility. This guideline cannot resolve such structural tensions but aims to make them transparent and to support coherent national implementation within the limits of the legal framework. Further convergence, where appropriate, will depend on future implementing acts and the work of the EHDS governance bodies.

This guideline is designed to be implementable in MS with very different levels of digital maturity and with pre-existing national secondary use frameworks. It does not require MS to redesign national infrastructures or replace existing statutory secondary use systems (i.e. established permitting authorities, national data services, or long-standing legal obligations to make data available). Instead, the guideline should be read as identifying the EHDS-specific obligations and boundaries relevant to Article 71, which must be integrated into, and, where necessary, aligned with national frameworks. Existing national mechanisms that already comply with the Regulation may remain in place and be further developed, provided that the EHDS opt-out right is effectively supported within the national implementation.

To avoid unnecessary repetition and to support consistent interpretation, all key concepts and legal distinctions relevant to the opt-out (including the relationship between EHDS opt-out, GDPR consent and the right to object) are defined in the Chapter 4. of the guideline and in Annex 4 (Glossary). Other subsequent chapters focus on responsibilities and procedures and do not restate definitions unless strictly necessary.

For clarity, references in this guideline to “data concerning health” should be understood as referring to personal electronic health data within the meaning of the EHDS Regulation. No separate or additional data category is implied.

To support the practical interpretation of this guideline, a set of annexes is provided. Annex 1 describes the methodology used for the development of the guideline, including stakeholder engagement and expert consultation activities. Annex 2 summarises the results of the public consultation process. Annex 3 presents an illustrative user journey related to the exercise of the opt-out right. Annex 4 contains a glossary of key concepts and legal terms used throughout the document. Annex 5 provides an overview of the broader TEHDAS2 deliverable landscape and the relationship of this guideline to other outputs of the Joint Action. Readers are encouraged to consult these annexes for additional context and supporting information.

4 Scope and aim of the guideline

This guideline covers the implementation of the opt-out mechanism established under Article 71 of the EHDS Regulation, within the broader governance framework for the secondary use of electronic health data laid down in Chapter IV of the Regulation.

The scope is limited to the EHDS Regulation and only referring to the GDPR insofar as it is explicitly complemented by the EHDS Regulation [Article 1(2)(a)]. This guideline does not attempt to interpret broader legal frameworks beyond what is necessary to implement Article 71. However national law may define specific circumstances under which exceptions to the opt-out may apply in accordance with Article 71(4) of the EHDS Regulation. No technical specifications can be provided here. The technical means to implement opt-out depend on many factors such as where opt-out is implemented: in a centralised or decentralised way, and how the right can be exercised: through different channels or through one entry point.

The scope is limited to the EHDS Regulation and only referring to the GDPR insofar as it is explicitly complemented by the EHDS Regulation [Article 1(2)(a)]. This guideline does not attempt to interpret broader legal frameworks beyond what is necessary to implement Article 71. However, it is important to note that national law may supplement the Regulation where permitted [i.e., Article 71(4)]. No technical specifications can be provided here. The technical means to implement opt-out depend on many factors such as where opt-out is implemented: in a centralised or decentralised way, and how the right can be exercised: through different channels or through one entry point.

Each MS must establish the measures it considers necessary and appropriate for its national context, while clearly distinguishing between what is mandatory under the Regulation and what may be adapted at national discretion. Many elements already developed at the national level, and aligned with the Regulation, can remain in place and be further built upon. Member States may therefore continue to rely on existing structures, processes, and tools where these are compatible with the EHDS, ensuring continuity while progressively moving toward full compliance. However, it should be noted that the parallel coexistence of different mechanisms at the national level, particularly where they relate to similar categories of health data, may create additional complexity for individuals and could make it more challenging to ensure consistent communication and transparency in the secondary use of health data.

This guideline does not define operational workflows, technical architectures, governance arrangements, or implementation timelines. It does not prescribe national procedures, organisational models, or detailed safeguards, as these depend on decisions to be taken by MS, the European Commission, and future implementing acts. The document does not interpret broader legal frameworks beyond what is necessary to support the implementation of Article 71, nor does it provide an in-depth legal analysis of the interplay between the GDPR and the EHDS Regulation. It also does not set out cross-border procedures, monitoring mechanisms, or enforcement models. Practical examples, case studies, and stakeholder-specific instructions fall outside the scope of this document and will emerge only as national and EU-level implementation advances. This guideline represents an initial, concept- and principles-based contribution to support MS in preparing for the implementation of Article 71 of the EHDS Regulation. It is not intended to serve as a final or exhaustive interpretation of the legal framework. As the European Commission develops the implementing acts foreseen under the Regulation, further technical and procedural

specifications will be issued, and these will be subject to review by the European Data Protection Board and the competent national supervisory authorities. Member States should therefore view this document as a foundation that will evolve over time and ensure that their national approaches remain aligned with subsequent implementing acts, formal guidance from the European Data Protection Board (EDPB), and oversight by their data protection authorities.

Outstanding implementation issues may include interoperability, cross-border recognition of opt-out, and distribution of responsibilities where HDABs are not directly involved.

This guideline provides clarification on how to establish and manage the opt-out mechanism under Article 71 EHDS.

4.1 Audience

This guideline is primarily addressed to HDABs. It may also provide support to data users, data holders and trusted health data holders for contextual understanding of their obligations under Article 71 of the EHDS Regulation, and of how they deliver information duties under Articles 58–59 of the EHDS Regulation.

While this guideline does not provide methodological guidance for data users on the impact of opt-out on analytical results, it supports HDABs in communicating, at a high level, that opt-out may affect dataset representativeness and thus the societal value of secondary use.

4.2 Legal framework

4.2.1 The EHDS opt-out as an autonomous EU right

The EHDS Regulation establishes an EU-wide right to opt out, while the specific mechanisms for exercising that right are implemented at Member State level in accordance with the requirements set out in Article 71. Opt-out is to be implemented at MS level and is applicable to personal electronic health data generated and held in the respective MS. As the EHDS Regulation does not provide for a harmonised approach for the opt-out mechanism across MS, declaring opt-out in one MS will not affect the secondary use of the data in another MS.

It is the responsibility of national legislators to ensure that the right to opt out is implemented in a way that ensures compliance not only with the EHDS Regulation, but also with other applicable laws. Among other applicable legal frameworks, the GDPR is particularly relevant. Pursuant to Article 1(2)(a) of the EHDS Regulation, the Regulation complements the rights laid down in the GDPR as regards the processing of personal electronic health data.

The European Health Data Space introduces two distinct opt-out mechanisms that operate in different parts of the electronic health data ecosystem. Although both relate to an individual's control over their electronic health data, they serve different purposes, follow different rules and conditions and have different effects on healthcare delivery and on the reuse of data for research, innovation, policy, and public health. Understanding the distinction between opt-out for primary use and opt-out for secondary use is essential for policymakers, implementers, and citizens alike. The table below provides a clear overview of how these two mechanisms differ in scope, impact, governance, and safeguards.

Primary use opt-out: Article 10 of the EHDS Regulation allows MS the option to provide natural persons the right to opt out from the access to their health data as set up under the EHDS Regulation for primary use. There is no automatic link between opting out in primary or secondary use. A natural person may choose to exercise either opt-out right independently. The two rights function separately: an individual may block the primary exchange of their electronic health data while still allowing its pseudonymised use for secondary purposes, or the reverse. Article 10 limits access to electronic health data but does not prevent its collection nor automatically exclude it from secondary use under the EHDS. Therefore, there is no relationship between the right to restrict access and secondary purposes. If a natural person does not want their electronic health data to be accessed for secondary use, they need to opt-out in accordance with Article 71.

The right to restrict access: Article 8 of the EHDS Regulation allows natural persons to limit the visibility of certain parts of their electronic health data, for primary use. This restriction is limited to the visibility of data in an EHR by healthcare professionals using the health professional access services referred to in Article 12.

Table 1: Summary of the different aspects comparing primary-use and secondary use opt-out under EHDS Regulation.

Item	Primary use Opt-Out (Art. 10, Recital 18)	Secondary use Opt-Out (Art. 71, Recital 54)
What it covers	Sharing electronic health data for primary use in healthcare delivery via EHDS services (e.g., patient summary, ePrescriptions (Art. 10; Recital 18).	Reuse of personal electronic health data for research, innovation, AI training, policymaking, statistics, and other purposes listed in Article 53(1) (Art. 71(1); Art. 53(1); Recital 54).
Who decides if it exists	Optional: MS may introduce it through national law (Art. 10(1)).	Mandatory; all MS must provide this right. (Art. 71(1-2)).
Effect of the opt-out	Once the natural person exercises the opt-out, access to the patient's EHDS-shared data is no longer available to either the patient or health professionals. Local documentation still occurs (Art. 10; Recital 18).	Data excluded from all new secondary-use permits after the natural person has exercised the right to opt out. (Art. 71(1), (6)).
Impact on past uses	Not applicable (primary use is real-time) (Art. 10).	No retroactive effect; existing datasets approved for access remain unchanged. (Art. 71(6)).
Reversibility	Yes, patient may re-allow access (Art. 10).	Yes, patients may reverse their opt-out at any time. (Art. 71(1)).
Emergency access	Possible "breaking the glass" access in emergencies to protect vital interests (Art. 10; Recital 18).	No emergency override. Access to opted-out data is allowed only under strict national exceptions defined pursuant to Article 71(4).

Item	Primary use Opt-Out (Art. 10, Recital 18)	Secondary use Opt-Out (Art. 71, Recital 54)
Exceptions / overrides	Defined by MS (i.e., emergency care) (Art. 10).	Permitted only where national law establishes a specific mechanism under Article 71(4), subject to strict cumulative conditions: – request by a public-sector body or Union institution; – purpose under Article 53(1)(a–c) or important public-interest research; – absence of timely and effective alternative data source (Art. 71(4–7)).
Documentation requirement	Healthcare providers must still record treatment in their own systems (Art. 10).	Already approved data permits or requests may continue using data; future projects must exclude opted-out individuals (Art. 71(6)).
Scope of data	EHR data categories used in care (patient summaries, prescriptions, lab results, imaging, etc.) (Art. 5–6).	Broad categories: EHRs, registries, claims, genomics, clinical trials, device data, person-generated data, etc. Categories listed in Article 51, processed for purposes listed in Article 53.
Legal nature	A MS–defined mechanism for restricting access to care data (EHR) (Art. 10).	A *sui generis* EHDS right, independent of GDPR legal bases (Art. 71(1); Art. 1(2)(a)). It is a new, standalone right created specifically by the EHDS Regulation. It applies regardless of the legal basis used for secondary use of health data. Even if a data user has a valid GDPR legal basis to process health data for secondary use, the natural person can still exercise the EHDS opt-out, and the data cannot be accessed. The opt-out is not an objection under GDPR, not a withdrawal of consent, and not a restriction request. It is a separate regulatory mechanism introduced by the EHDS.
Relation to GDPR	GDPR still applies for processing in care settings.	GDPR applies; EHDS opt-out is independent of GDPR Art. 21 right to object. (Art. 1(2)(a); Art. 65 EHDS).
Who implements it	If a Member State provides for a right referred to in paragraph 1 (opt-out primary use) of this Article, it shall establish the rules and specific safeguards regarding the opt-out mechanism (Art. 10)	Member States shall provide for an accessible and easily understandable opt-out mechanism (Art. 71(2)) to exercise the right established in paragraph 1 (natural persons shall have the right to opt out at any time), whereby natural persons may explicitly state that they do not wish to have their personal electronic health data processed for secondary use; HDABs facilitate and ensure compliance (Art. 57–58).

Item	Primary use Opt-Out (Art. 10, Recital 18)	Secondary use Opt-Out (Art. 71, Recital 54)
Transparency obligations	Patients can see which professionals access their data (Art. 9–12).	HDABs must publish information on data uses, safeguards, permits, and outcomes (Art. 58).
Identifiability requirement	Not applicable.	Opt-out applies only if the person is identifiable in the dataset (Art. 71(8)).
Anonymised data	Not relevant.	Opt-out does not apply to anonymised data; no opt-out is possible after anonymisation. (Art. 71(8); Art. 66).

Scope limitation and interaction with other legal regimes: opt-out rules provided by other legal acts be it on national or EU level are not affected by the opt-out mechanism under the EHDS. Opting out from secondary use through the EHDS infrastructure does not imply opt-out from the use of, for example, cancer registry data based on national law. The use of data under those legal regimes remains unaffected if not explicitly aligned with the EHDS opt-out mechanism by national law.

The GDPR continues to apply fully to all processing of personal electronic health data, and the rights of individuals under the GDPR remain unchanged. Supervisory authorities established under the GDPR retain responsibility for monitoring compliance and handling complaints. The GDPR right to object under Article 21 also remains applicable, but it operates within the GDPR's legal-basis framework and is distinct from the new EHDS mechanism.

The EHDS Regulation does not introduce a new category of lawful basis under the GDPR. Rather, it establishes a sector-specific governance framework for the secondary use of electronic health data, including HDABs, secure processing environments (SPEs), and structured data permits. Where data are made available under the EHDS, the legal obligation laid down in the Regulation may constitute a basis under Article 6(1)(c) GDPR, while the applicable condition under Article 9(2) GDPR depends on the specific purpose pursued (e.g. public health, scientific research, or substantial public interest), in accordance with Union or MS law. The GDPR therefore continues to govern the lawfulness, safeguards, and data protection obligations applicable to secondary use, alongside the specific organisational and procedural requirements introduced by the EHDS.

The EHDS opt-out is a unique legal right (a sui generis right), independent of the GDPR's legal bases and distinct from the GDPR right to object. The EHDS opt-out applies specifically to the secondary use of electronic health data and allows individuals to exclude their data from reuse, regardless of the GDPR legal basis. It complements, rather than replaces, the GDPR framework. Unlike the GDPR right to object, which applies only when processing relies on public interest or legitimate interest as legal basis, the EHDS opt-out applies universally, with exemptions permitted only where national law explicitly defines necessary processing.

The interaction between the GDPR and the EHDS Regulation requires clear communication to ensure that individuals understand when their rights derive from each framework. Under the GDPR, processing for reasons of public interest or for scientific research is permitted under specific conditions, and the definition of what constitutes "public interest" as well as "important reasons of public interest" remains a matter for MS to determine within the

boundaries of EU law. The EHDS does not replace these national determinations; instead, it establishes a harmonised mechanism for secondary use within its own scope, while existing GDPR-based research activities outside the EHDS continue to operate under national rules. Member States should therefore provide citizens with accessible explanations and practical examples that illustrate when processing is carried out under the EHDS and when it relies on GDPR provisions, including how the opt-out under Article 71 interacts with national public-interest or research exemptions. Such clarity helps individuals understand the source of their rights, the limits of each framework, and the circumstances in which their data may be used. In conclusion:

- The GDPR is the foundation, while the EHDS Regulation builds on it for health-specific scenarios.
- The EHDS Regulation introduces real-time digital rights, especially for secondary use, which go beyond GDPR's manual processes.
- For secondary use, the EHDS Regulation defines structured legal bases for the data holders to share the electronic health data, processing rules, and governance mechanisms (including those implemented through tasks assigned to HDABs), in alignment with GDPR.

Table 2: Summary of the relationship between the EHDS Regulation and GDPR (question 56, European Commission FAQ 5 March 2025)

Item	GDPR	EHDS Regulation
Legal role	Core legal framework for data protection in the EU	Sector-specific complement focused on health data
Main focus	Sets out rights for individuals and obligations for data controllers/processors	Adds specific provisions for the use, access, and reuse of electronic health data
Supervisory Authorities	Data Protection Authorities (DPAs) monitor GDPR compliance (Lawfulness of processing in general)	Same DPAs also monitor the EHDS Regulation implementation
Right of access (general)	Individuals can request access to all personal data held by a controller (Article 15 GDPR)	Individuals have immediate access to specific electronic health data (i.e., patient summary) via self-service
Time to respond to the access request	Up to 1 month; can refuse or charge for repetitive/unfounded requests	Immediate access required; no refusal, regardless of frequency
Primary use of data	GDPR applies; access requests must be processed manually	The EHDS Regulation adds real-time, digital access to essential health data

Item	GDPR	EHDS Regulation
Legal basis for processing	Must rely on one of the legal bases under Article 6(1) GDPR	The EHDS Regulation may constitute a legal obligation under Article 6(1)(c), subject to national implementing law.
Processing special categories	Processing health data only allowed under Article 9(2) with safeguards	The EHDS Regulation provides lawful grounds and safeguards (i.e., secure processing, data permits, Chapter IV)
Secondary use of data	Not specifically regulated by GDPR	Structured access for **secondary use** governed by HDABs, permits, secure environments
Safeguards for sensitive data	Requires implementation of appropriate safeguards (Article 9(2)(j))	The EHDS Regulation includes legally binding safeguards in Chapter IV

It is important to highlight that, while according to Article 9(4) of the GDPR, MS may maintain or introduce further conditions, including limitations, regarding the processing of genetic data, biometric data or data concerning health.

The right to opt out under Article 71 of the EHDS Regulation is a separate, EHDS-specific right, operationally implemented and managed at national level, typically by HDABs. Supervision and enforcement of this right remain within the GDPR framework. Article 65 EHDS provides that supervisory authorities established under Regulation (EU) 2016/679 are competent to monitor and enforce the application of the opt-out right, including handling complaints and imposing administrative fines up to the level provided under the GDPR. If a MS provides for the right to opt out pursuant to Article 71 to be exercised through the HDABs, the relevant HDABs shall provide public information about the procedure to opt out and facilitate the exercise of that right [Article 58(2)].

4.2.2 Institutional actors and allocation of responsibilities

The EHDS secondary use opt-out mechanism involves several actors, each with distinct responsibilities to ensure that individuals can meaningfully exercise their rights while maintaining a secure and well-governed data environment. The Regulation distributes obligations across natural persons, data holders, HDABs, data users, MS, supervisory authorities, and the European Commission. Understanding how these roles interact is essential for implementing a coherent, transparent, and trustworthy opt-out system. The table below summarises the key responsibilities of each actor within this framework.

Table 3: Opt-out in the EHDS Regulation: responsibilities of individuals, Data Holders, HDABs, and Others

Actor	Key responsibilities related to Opt-Out
Natural person (Citizen/ Patient: the citizen in healthcare system)	- Exercises the right to opt out from secondary use of personal health data without giving reasons. - May reverse the opt-out at any time. - Must be informed clearly about the opt-out mechanism, including the benefits and drawbacks of exercising that right.
Health Data Holder (hospitals, labs, registries, insurers, etc.)	- Must make electronic health data available to the HDAB when legally required (Art. 6(1)(c) GDPR + Art. 9(2)(i),(j)). - Must apply data minimisation principles and (if their delegated opt-out tasks require it) avoid collecting new identifiers solely to enable opt-out (Art. 61(3)). - Must pseudonymise data during extraction where required. - If the given Member State model allows, must respect the granularity of opt-outs exercised by natural persons when preparing data for secondary use.
HDAB	- Ensures compliance with national opt-out mechanisms while performing its tasks (Art. 57) - Ensures that individuals who opted out are excluded from new data permits. Publishes clear, accessible information on opt-out rights, safeguards, and data uses (Art. 58). - Logs all data access and ensures transparency. - Screens datasets to filter out opted-out individuals when identifiable. - Evaluates and decides on exceptions (public interest with other conditions overrides) based on national law. - Cooperates with Supervisory Authorities for enforcement (Art. 65) - Member States shall provide for penalties; these may be enforced by the HDAB (or another competent authority).
Data User (researchers, public bodies, innovators, etc.)	- Is responsible for comply with data permits and respect opt-out restrictions. - Cannot attempt re-identification of individuals (strictly prohibited). - Is required to establish process data only within the SPE. - Must justify any request falling under national exceptions (public interest, no alternative data source, etc.).
MS (National Legislator / Government)	- Is required to establish an accessible, understandable, reversible opt-out mechanism (Art. 71(2)). - May define national exceptions allowing access to opted-out data (strict conditions in Art. 71(4)). - Is responsible for notify the European Commission of any national override provisions. - Must ensure public information campaigns and respect the transparency obligations.

Actor	Key responsibilities related to Opt-Out
Supervisory Authority (GDPR Regulator)	- Monitors and enforces compliance with the GDPR and is also competent for monitoring and enforcing the application of the right to opt out pursuant to Article 71 (Article 65 EHDS). - Handles complaints from individuals. - Can impose GDPR-level administrative fines (Art. 83. GDPR). - Cooperates with HDABs to ensure consistent enforcement.
European Commission	- Receives notifications from MS on national exceptions (Art. 71(7)). - Evaluates the functioning and impact of opt-out mechanisms by 2033. - Issues guidance on anonymisation and other technical aspects.
SPE Operator	- Within its competence, it ensures that data users access data only within the SPE. - Access-controlled, all actions are logged and an audit trail is ensured. - Ensures no data extraction, copying, or re-identification.

4.2.3 Implementation dimensions arising from the legal framework

When implementing the opt-out mechanism at MS level, particular attention should be paid to the following aspects:

- role, tasks and obligations of HDABs and of (trusted) data holders
- information systems to record, store, manage, check and respect the opt-out decisions of individuals
- centralised or decentralised systems to manage the opt-out mechanism, and how it is coordinated between HDABs and data holders
- whether, and under which national conditions, exceptions to the opt out right may be applied in accordance with Article 71(4)
- The possible granularity of the opt-out mechanism (i.e., full opt-out from all secondary uses or selective exclusion of specific data categories or purposes).
- This guideline supports HDABs in implementing these elements in a manner that respects natural person's fundamental rights, ensures legal compliance, and maintains trust in the EHDS framework. The detailed operational implications of these roles are further elaborated in Chapter 5.

5 Right to opt out from the processing of personal electronic health data for secondary use

5.1 What is opt-out? Definition.

5.1.1 Legal definition

Secondary use opt-out: Article 71 (1) of the EHDS Regulation obliges MS to establish an opt-out mechanism for the secondary use of personal electronic health data. It states: "*Natural persons shall have the right to opt out at any time, and without providing any reason, from the processing of personal* electronic *health data relating to them for secondary use under this Regulation. The exercise of that right shall be reversible.*" An important element of this provision is that individuals can exercise their right without providing any reason. The mere declaration to not share their data for secondary use, partially or in whole, is sufficient. They can do so at any time; the right is not limited in time and there is no deadline to meet.

The EHDS Regulation does not alter national legal bases for the collection or management of health data, nor does Article 71 introduce new consent requirements. It applies exclusively to secondary use through the EHDS framework.

The Article 71 opt-out mechanism complements, but does not replace, GDPR obligations or national regimes. Where provided under national law, Article 71(4) allows access to opted-out data under strict safeguards for purposes defined in Article 53(1)(a-c) or for important public interest research, including public-health functions carried out by competent national authorities or relevant Union bodies.

The right to opt out is afforded to natural persons, meaning identifiable human individuals. Legal persons, organisations or institutions cannot exercise the opt out right in their own name. How the right is implemented for natural persons without capacity to make their own opt out decision, or who need assistance to do so, (children/minors, persons with limited legal capacity, persons under guardianship) is governed by national legislation. In the case of minors, the age at which they acquire responsibility for their own opt out choice will also vary according to national rules. Before then, their opt out choice is made by the legal guardian. Pragmatically the opt-out status set by legal guardians remains unchanged even after reaching the age of majority. Member States may wish to provide for a one-time communication when control of the opt out decision transitions from the guardian to the individual (child) when they attain the relevant age. This communication could provide information on the opt out right, the current opt-out status and the means by which to set and update their own choices. In this case, the MS should ensure an appropriate legal basis is in place supporting use of the opt-out database for such communications. In respect of persons with limited or no ability to make decisions on their own behalf, the availability of decision-making supports, guardianship arrangements or other frameworks is determined at national level.

5.1.2 Opt-out from secondary use in contrast to opt-out from primary use

The EHDS Regulation clearly distinguishes between opt-out for primary use (Article 10) and opt-out for secondary use (Article 71). The primary-use opt-out is optional for MS and concerns access to electronic health data through EHDS services in the context of healthcare delivery. By contrast, the secondary-use opt-out is a directly granted right that allows natural

persons to exclude their personal electronic health data from future secondary use permits issued under the EHDS framework. The distinction between primary and secondary use opt-out has been explained in Section 4.2, the following section focuses on the specific operational implications of the secondary use opt-out.

The secondary-use opt-out applies prospectively and is reversible at any time. It does not affect datasets lawfully created under previously approved permits, nor does it extend to anonymised data (Article 71(8), Article 66). Where a MS establishes an exception pursuant to Article 71(4), access to opted-out data may be permitted only under strict national conditions.

The secondary use opt-out applies exclusively within the EHDS framework. It does not extend to research or data processing carried out outside the EHDS secondary use system, which continue to rely on their respective legal bases under Union or national law (Articles 1(7) and 1(8)).

Member States must ensure that opt-out decisions are effectively applied at the stage where data are prepared for secondary use. Data-extraction and pseudonymisation workflows should be designed so that opted-out individuals are excluded from new secondary use processing without affecting previously authorised datasets.

HDABs should clearly communicate that primary- and secondary use opt-outs are distinct mechanisms serving different purposes. Individuals should understand that restricting access to data for healthcare delivery does not automatically prevent secondary use, and vice versa.

Operational responsibility for applying the opt-out may lie with HDABs or with data holders, depending on the national model. MS retain flexibility in the design of centralised, federated, or sector-specific solutions, provided that opt-out decisions are effectively respected whenever data are processed under Chapter IV of EHDS.

5.1.3 Opt-out in broader sense and its impact on data availability

Term “opt-out” is not used exclusively by the EHDS Regulation and it is sometimes used also by technology and service providers to refer to a mechanism that allows individuals to withdraw from a service, communication, or data processing they may be included in.

The diversity of healthcare systems and the services provided within them allows, depending on national, regional or even local conditions, the implementation of certain services in which individuals (patients) can choose whether to participate and for how long.

These services usually, but not always, fall under some form of telemedicine or are part of activities such as surveys and questionnaires with a specific healthcare-related purpose. Providers of these services or activities may allow opt-outs, quite independently of opting out of primary or secondary uses of health data under the EHDS Regulation. As a result, there is no data in the datasets made available about these participants who opted out. The theoretically defined cohorts are then incomplete in terms of data.

This is not intended to encourage the above-mentioned providers to use the term ‘opt-out’ from the EHDS Regulation in their services (in fact, it should be the opposite: not to introduce it) but simply reflects the reality as it is. While this is clear, the HDAB should be able to clarify the various opt-outs that individuals may encounter during their healthcare journey. Individuals should therefore not be confused by the term “opt-out” itself into assuming that it

refers to an opt-out that relates, for example, to the secondary use of health data in the EHDS context and should always be sufficiently informed about the scope of the opt-out that they can exercise.

There may also be various mechanisms in existing methods for secondary use of health data in MS that have a similar purpose as opt-out defined by Article 71 of the EHDS Regulation. Member States should make an order in these mechanisms and terms at the national level, in the interest of transparency and clarity for the secondary use of health data.

It should also be noted that some national implementations of the opt-out from the primary use of health data may have the practical effect that data relating to individuals who have opted out are not included in datasets made available for secondary use. This does not affect the exercise of any opt-out under Article 71, but it may be useful information for data users who might not otherwise anticipate such an impact.

5.1.4 Difference between EHDS opt-out and GDPR right to object

According to Article 21(1) of the GDPR, the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. The main difference between opt-out in the EHDS Regulation and the right to object under Article 21 of the GDPR is that no justification is required for the exercise of the right to opt out in EHDS. The right to object under the GDPR is a general data protection right not limited to electronic health data. It allows individuals to object to the processing of their personal data in specific circumstances, including direct marketing and processing based on legitimate interests. The right to opt out within the EHDS is a specific right related to electronic health data, allowing individuals to opt out from the re-use of their electronic health data for secondary purposes within the EHDS framework. It is important to highlight that EHDS opt-out does not require a justification and cannot be overridden by the controller.

For scientific or historic research or statistical purposes the right to object is valid unless the processing is necessary for the performance of a task carried out for reasons of public interest [Article 21 (6)]. In other words, the data subject cannot exercise their right to object unless they give a personal reason to such objection; for scientific or statistical use this may not be enough if the processing is deemed to be necessary for public interest reasons. The right to object is thus conditioned by disclosing personal reasons by the data subject and can be overridden by the compelling interests of the controller. The right to object and the right to opt out are thus cumulative and independent. The exercise of the GDPR right to object does not automatically trigger an EHDS opt-out, nor does an EHDS opt-out preclude the individual from also exercising their GDPR right to object to processing. Controllers must respect both decisions separately and ensure that both objections and opt-outs are recorded and implemented appropriately, according to their respective legal bases and effects.

The EHDS Regulation establishes specific information mechanisms, including an information system referred to in Article 57(1)(j)(vi), intended to comply with the transparency obligations laid down in Article 58. This system is designed to provide continuous, accessible information about the purposes, recipients, and outcomes of secondary use within the EHDS framework.

The EHDS Regulation does not impose an obligation to individually notify data subjects. However, under Article 14 GDPR, general transparency obligations still apply and should be fulfilled through public notices and accessible documentation.

Table 4: Distinguishing GDPR and EHDS data subject rights: a detailed comparison of the right to object and the right to opt out

Aspect	**GDPR – Right to object**	**EHDS: right to opt out from secondary use under EHDS**
Legal source	Article 21 GDPR; Recitals (69–70)	Article 71 EHDS Regulation; Recitals (4), (8), (18)
Nature of the right	A conditional right: the individual must object *on grounds relating to their particular situation* (Article 21(1)).	An unconditional right: individuals may opt out at any time and without giving any reason (Article 71(1)).
Scope of data	Applies only to personal data processed under Art. 6(1)(e) (public interest) or 6(1)(f) (legitimate interest).	Applies to all types of electronic health data processed for secondary use under the EHDS Regulation.
Grounds required	Must provide a personal justification, except for direct marketing (Article 21(2)).	No justification required (Article 71(1)).
Controller's ability to override	Controller may continue processing if it demonstrates compelling legitimate grounds overriding the individual's interests (Article 21(1)).	No individual balancing or controller override is possible. Access to opted-out data is permitted only where national law establishes a specific exception under Article 71(4), subject to strict statutory conditions.
Effect on processing	Processing must stop *unless* the controller proves overriding grounds.	All processing of individual's data for secondary use must stop for that (Article 71(1)).
Applies to pseudonymised data?	Yes, pseudonymised data remain personal data.	Yes, opt-out applies to all personal electronic health data, including pseudonymised data (Article 71(1)).

Aspect	GDPR – Right to object	EHDS: right to opt out from secondary use under EHDS
Applies to anonymised data?	Anonymised data falls outside the GDPR, but the act of anonymising personal data is a GDPR-regulated processing operation that requires a lawful basis.	No. The opt-out does not apply to anonymised data. Article 71(8) explicitly excludes anonymised data from its scope. Once data have been rendered truly anonymised, meaning individuals can no longer be identified, the opt-out right is no longer relevant, as such data fall outside both the GDPR and the EHDS rights framework. When the purposes of the processing of personal electronic health data by a health data holder do not or no longer require the identification of a data subject by the controller, that health data holder shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the right to opt out under the EHDS Regulation Article 71(8).
Which entity is responsible for ensuring compliance with the right?	Responsibility lies with the controller that receives the objection, which must assess and act on it.	The Data Holder may need to apply the opt-out before transmitting data, depending on national rules. HDAB must then enforce the opt-out when preparing datasets for secondary use, in line with Article 71 and Chapter IV of the EHDS Regulation.
Reversibility	GDPR does not define reversibility; objections are situational.	Explicitly reversible at any time (Article 71(1)).
Timing	Can be exercised at any time, but only affects future processing.	Can be exercised at any time, and applies to future secondary use; past uses remain valid (Article 71(6)).
Granularity	Not granular by default; applies to the specific *processing operation* objected to.	MS may allow granular opt-out (e.g., by data category or purpose) (Article 71).

Aspect	GDPR – Right to object	EHDS: right to opt out from secondary use under EHDS
Administrative burden	Requires case-by-case assessment by the controller.	No assessment required; the opt-out is automatic and unconditional. However, implementation of opt-out in practice shall be consistent and timely, which requires efforts with varying degrees of administrative work.
Supervision	Data Protection Authorities (DPAs) (GDPR Chapter VI).	DPAs (for data protection compliance) also enforce and monitor the implementation of the EHDS opt-out (Article 65). Each MS must designate at least an HDAB, which is responsible for ensuring compliance, interoperability, and enforcement of EHDS Regulation (secondary use of data) within their national systems.
Role of European Commission	N/A	By March 2033, performs targeted evaluation on the implementation and use by natural persons of the mechanisms to opt out from secondary use referred to in Article 71, in particular on the impact of those mechanisms on public health, scientific research and fundamental rights (Article 102)
Interaction with legal basis	The right to object is limited to processing carried out under Article 6(1)(e) (task in the public interest) or Article 6(1)(f) (legitimate interests). This can create practical challenges when organisations rely on multiple legal bases or when the legal basis is not clearly communicated.	National decisions determine the level of granularity at which the opt-out is defined. Depending on the Member State, the opt-out may apply to specific categories of data, particular processing activities, or certain stakeholders involved in data reuse. It does not depend on the legal basis under the GDPR; rather, it operates as a sector-specific right overlaying the EHDS framework (see also Section 5.1.3).

In conclusion,

- The GDPR right to object is conditional, requires justification, and can be overridden.
- The EHDS right to opt out is unconditional in its exercise, subject to the exceptions provided for in Article 71(4). It cannot be overridden, except for narrowly defined public-health exceptions set out in national law. It applies specifically to the secondary use of electronic health data.
- Article 71(8) confirms that the opt-out does not apply to anonymised data, aligned with GDPR principles.
- Enforcement differs: GDPR places responsibility on the controller, while EHDS splits responsibilities between data holders and HDABs.
- Although opting out does not require any justification provided by the individual, HDABs could, on voluntary basis for the individual, request information about the reasons for opting out in order to receive valuable information about the motivation behind the decision. This request should clearly indicate that the provision of such information is voluntary and that the opt-out declaration will be valid in any case.

The exercise of the GDPR right to object does not automatically trigger an EHDS opt-out, nor does it invalidate previously issued secondary use permits granted under the EHDS. Conversely, the exercise of the EHDS opt-out does not retroactively affect processing already lawfully carried out under a valid data permit. Where both rights are exercised, each must be assessed and implemented within its own legal framework. The EHDS opt-out applies prospectively to future secondary use permits under Articles 53–71, while the GDPR right to object operates within the legal-basis structure of Article 6 GDPR and may require case-by-case assessment by the controller. The EHDS does not establish an obligation for HDABs to monitor or enforce GDPR objections unrelated to secondary use under the EHDS framework.

5.1.5 Citizen engagement and empowerment as regards the opt-out

This part of the document addresses citizen engagement and societal embedding of the opt-out mechanism as a governance dimension, distinct from the operational communication duties described in Section 5.5.

The EHDS Regulation requires MS to set up an opt-out mechanism regarding the secondary use of personal health data in order to protect data subjects' right to respect for their autonomy. However, its use may hinder the broader objectives of the EHDS. For example, opt-outs can introduce bias into datasets and into the results of data processing, which may reduce the utility, representativeness, and precision of secondary-use analyses. To balance between societal benefits of the secondary use of health data and the opt-out right as a safeguard, this chapter aims at contextualising the opt-out mechanism within the overall goal of the secondary use of health data, and guides HDABs on how to ensure an implementation of the EHDS framework that is trustworthy and respects individual rights.

The necessity to preserve the right for the autonomy of natural persons is explained in Recital 54 of the EHDS Regulation, which provides that "*to balance the need of health data users to have exhaustive and representative datasets with the need for autonomy of natural persons over personal electronic health data of theirs that are considered particularly sensitive,*

natural persons should be able to make the decision as to whether their personal electronic health data can be processed for secondary use under this Regulation, in the form of a right to opt out from having those data being made available for secondary use". This opt-out mechanism is embedded in Article 71 of the EHDS Regulation. Importantly, while this mechanism allows individuals to exclude their identifiable data from secondary use, it is designed in a way that still enables the creation of large, representative datasets for societal benefit, such as research, innovation, and policy.

When engaging citizens on the EHDS and the right to opt out, HDABs and other stakeholders should provide clear, balanced, and practical information that helps individuals understand both the protections in place and the societal value of responsible data sharing. Communication should avoid technical complexity and instead highlight concrete examples of how secondary use of electronic health data contributes to public health, research, and improved care pathways. It is important to emphasise that the national environment for secondary use should be understandable and aligned with the FAIR data principles adopted in the EHDS. This enables communication with citizens that is simple, engaging, and accessible for all target groups, and avoids situations where HDABs cannot clearly answer questions about specific re-uses of an individual's health data.

It is helpful to explain that when a person's data is included in research, the resulting evidence, treatments, and innovations are more likely to reflect people like them, supporting better diagnosis, safer medicines, and more effective therapies, particularly in areas such as oncology, rare diseases, and chronic conditions. This communication may also refer to the principles on significant findings (*D8.2 Guideline to Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data*.) and the transparency and publication obligations addressed in D8.3 (*Guideline for Health Data Access Bodies on informing natural persons about the use of health data - "Citizen Information Point"*). At the same time, citizens should be informed that opting out is a legitimate choice, but that widespread opt-out may reduce the representativeness of datasets and introduce biases that can slow scientific progress or limit the development of treatments for specific groups. HDABs may therefore consider providing practical examples, plain-language explanations, and relatable scenarios that illustrate how secondary use works in practice, what safeguards apply, and how individuals benefit indirectly from research that uses population-level health data. Sharing such good practices can help citizens make informed decisions while supporting trust and transparency in the EHDS framework.

To ensure that citizens can meaningfully exercise their right to opt out, MS should complement general awareness efforts with structured education and training delivered by trusted sources. This includes equipping healthcare professionals with the knowledge and communication skills needed to discuss secondary use and the opt-out with patients in an accurate and accessible way. Targeted awareness activities should be developed for people with low digital or health literacy, ensuring that the opt-out mechanism does not inadvertently deepen existing inequalities. Member States are encouraged to design opt-out processes, interfaces, and information materials in close collaboration with patient and citizen representatives, including user testing to verify that the content is understandable and meets people's needs. Citizens should also receive clear explanations of how anonymisation and pseudonymisation work in the EHDS, as well as information on the privacy and cybersecurity safeguards that protect their data. When systems and processes integrate sustainable

educational materials, co-designed solutions, and tailored communication from the outset, MS create the conditions for stronger public trust and genuinely informed, equitable decision-making.

The outcomes of the public consultation informing this guideline are summarised in Annex 2.

5.1.5.1 Balancing societal benefits and individual autonomy in secondary use of health data under the EHDS framework

The EHDS Regulation enables the secondary use of electronic health data for clearly defined purposes in Union law, operating within a robust system of safeguards and governance mechanisms. At its core, the Regulation recognises the transformative societal value that can emerge when health data is reused responsibly, advancing scientific research, driving innovation, strengthening public-health preparedness, and supporting evidence-based policymaking across the European Union.

The Regulation frames secondary use as a means to unlock this broader societal value. Recital 1 explicitly states that the aim of secondary use is "t*o better achieve other purposes involving the use of electronic health data in the healthcare and care sectors that would benefit society (…)*". This vision is carried through the operative provisions: Article 53 outlines the permitted purposes for secondary use, including scientific research in the health and care sectors, which is expected to "*benefit end-users, such as patients, health professionals (…*)". In other words, the Regulation positions secondary use as a mechanism to strengthen health systems and improve outcomes for people and communities across the EU.

Within this regulatory structure, the opt-out mechanism functions not as a form of presumed consent, but as a safeguard measure to uphold individual autonomy within a system that enables data use within a framework that allows secondary use under defined legal. Instead, it functions as a safeguard that allows natural persons to exercise control over the reuse of their personal electronic health data. Secondary use is enabled by the legal framework of the EHDS Regulation and the applicable legal bases under the GDPR, while the opt-out mechanism protects individual autonomy within that framework. It operates not as a form of presumed consent, but as a protective measure within a system that enables secondary use by default under defined legal conditions.

The HDAB bears a crucial responsibility in ensuring that ethical, legal, and societal considerations are fully integrated into the governance of secondary use. This includes not only compliance with the Regulation but also proactive engagement with the public to ensure that citizens are fully informed about the benefits and potential implications of allowing their electronic health data to be reused, particularly regarding who may access the data, for what purposes, and under what safeguards. The long-term success of the EHDS depends on making secondary use the norm rather than the exception. Achieving this requires institutions to commit to transparency, earn trust through consistent practice, and maintain an open, continuous dialogue that strengthens mutual understanding.

5.1.5.2 Promoting awareness of societal benefits

Article 58(1) requires HDABs to inform the public about which entities accessed which datasets, for which purposes, and with what outcomes. This information should be used not

only to comply, but to demonstrate societal benefit clearly and continuously.[1] Information could be both a passive way of engaging the public, while providing insights on what societal benefits are realised and how their achievement could be affected when exercising opt-out.

When promoting health literacy in the context of the EHDS, MS and HDABs should ensure that communication remains value-neutral and does not imply that a better understanding of secondary use should lead to greater acceptance of the EHDS or fewer opt-outs. The purpose of improving health literacy is to equip individuals to engage meaningfully in decisions about how their health data are reused and how such reuse can serve their own interests and broader societal benefits: what health data are, how they are used, and what rights and safeguards apply, regardless of whether they ultimately choose to participate in secondary use. Information provided to citizens should therefore avoid framing the opt-out as detrimental or undesirable and instead focus on supporting informed decision-making. This includes explaining, in an objective manner, the implications of opting out for the individual, the circumstances in which the opt-out may not apply, and the broader societal context in which secondary use operates. By maintaining neutrality and prioritising comprehension over persuasion, MS can strengthen trust and ensure that citizens exercise their rights based on a clear understanding rather than perceived pressure to support the EHDS infrastructure.

For instance, the HDABs' duty to inform includes to provide insights on what benefits have been realised and by whom since the information provided to data subjects will have to cover, among other aspects, "*who has been granted access to datasets of electronic health data and to which datasets they were granted access and details of the data permit regarding the purposes for processing such data as referred to in Article 53(1)*" as well as "*the results or outcomes of the projects for which* the *electronic health data were used*". Even though it could be difficult to understand before EHDS implementation all the factors that could drive the activation of an opt-out mechanism, HDABs can play a key role in ensuring natural persons do not do so as a result of a lack of understanding of the process and benefits of the secondary use of health data. By showing how societal benefits are generated, individuals can better understand how each person's data contributes to achieving those benefits.

5.1.5.3 Digital health literacy, digital health access and diversify communication channels

Member States should ensure that the national implementation of the secondary-use opt-out is supported by clear, accessible, and inclusive communication strategies that reflect the diversity of their populations. This requires investing in practical tools and materials that help citizens understand their rights, including plain-language explanations of the opt-out available in the major languages spoken nationally, as well as formats that comply with recognised accessibility standards such as WCAG 2.1. To reach people with different levels of digital literacy, MS and HDABs should make use of multiple communication channels, printed materials in healthcare settings, digital kiosks, official websites, and social media, so that information is available wherever citizens are most likely to encounter it. Particular attention should be given to vulnerable groups, including older adults, persons with disabilities, and individuals with low literacy, by providing alternative formats such as audio guides or assisted-service options. Developing these materials should involve early and structured engagement with relevant stakeholders, including patient organisations, healthcare

[1] The information portal will be discussed in D8.3 (*Guideline for Health Data Access Bodies on informing natural persons about the use of health data - "Citizen Information Point"*).

professionals, and civil-society groups, to ensure that the content is understandable, culturally appropriate, and responsive to real-world needs. This approach strengthens informed decision-making, supports equitable access to rights, and reinforces public trust in the EHDS framework. Empowerment requires more than informing individuals that the right exists: citizens must understand what opting out means for them personally, what it means for society, when the opt-out may not apply, and how they can activate or reverse it in practice.

Communication strategies should therefore be supported by adequate investment in accessible formats, multilingual materials, and outreach channels that go beyond digital platforms. Ensuring that people have a real capability, not merely a formal right, to control the use of their health data also requires that HDABs and other responsible actors design tools and processes that are easy to use, context-appropriate, and sensitive to different levels of vulnerability and risk. In this way, MS can promote genuine autonomy, reduce the likelihood of uninformed or unnecessary opt-outs.

5.1.5.4 Bottom-up channels - from the public to HDABs

Effective engagement can ensure that natural persons do not opt out due to a lack of understanding of the benefits of sharing health data for secondary purposes. However, it is worth noting that societal benefits are concepts that remain largely undefined. Understandably, defining such a concept at the European level might be irrelevant, as it will apply in culturally different societies.

It is therefore essential to recognise that implementing the EHDS for secondary use at national and regional levels is a decisive exercise: it will shape the nature and extent of the societal benefits that can ultimately be achieved. In practice, implementation choices at national level may influence how the public understands the societal value of secondary use. Member States may consider involving representatives of medical societies, civil societies, patient organisations and other relevant stakeholders in the development and periodic review of national surveys, policies or interpretative frameworks relating to the concept of societal benefit under Article 71. Such involvement can support legitimacy, transparency, and alignment with public expectations.

Indeed, surveys and public consultations across the EU reveal that people are more likely to support the secondary use of their health data when they are involved in and actively engaged in discussions around purpose, safeguards, and oversight. When this engagement is meaningful, individuals can also become ambassadors for the EHDS in their own communities, helping to build trust and understanding around its goals.

In addition, MS and HDABs should be aware that, pursuant to Article 102 of the EHDS Regulation, the European Commission will carry out a targeted evaluation of the Regulation, including the implementation and use by natural persons of the opt-out mechanisms under Article 71 and their impact on public health, research and fundamental rights. Effective national feedback mechanisms may therefore contribute to evidence-based evaluation at Union level.

5.1.5.5 Collaborating and learning from stakeholders

Within the EHDS, the effectiveness of cooperation between parties is facilitated by participatory and responsive implementation processes, as well as by ensuring transparency,

accountability, and public involvement in the governance of health data. Cooperation between the various stakeholders is supported by particularly the following regulations:

I. Stakeholder engagement (Articles 57 and 59 EHDS)

EHDS Regulation establishes mechanisms to ensure that HDABs engage meaningfully with stakeholders. According to Article 57, HDABs are required to "*cooperate with all relevant stakeholders, including patient organisations, representatives of natural persons, health professionals, researchers, and* ethics *committees, where applicable in accordance with EU or national law*." While the regulation does not impose specific modalities or procedures for such cooperation, it creates space for HDABs to engage with these groups in ways that reflect social expectations and ethical standards regarding the secondary use of health data. Such engagement is essential for building public trust and for understanding what is considered socially acceptable in terms of data access and reuse.

II. EHDS Stakeholder Forum (Articles 93 EHDS)

In addition to the above, the EHDS Regulation establishes a Stakeholder Forum under Article 93 (1), designed "to facilitate the exchange of information and promote cooperation among stakeholders in relation to the implementation of this Regulation." According to Article 93 (2) the stakeholder forum shall be composed of relevant stakeholders, including representatives of patient organisations, health professionals, industry, consumer organisations, scientific researchers and academia, and shall represent their views, and the tasks of the stakeholder forum shall encompass equally primary use and secondary use.

5.1.5.6 Co-building a data culture

HDABs have an obligation to cooperate with relevant stakeholders during the exercise of their tasks (Article 57). However, this should be understood as a minimum requirement rather than a complete model for public engagement. Other initiatives may be taken at the will of these bodies and their respective MS and should be encouraged to complement these cooperative efforts and promote public trust in the secondary use of health data.

To foster trust, HDABS should:

- Inform the public clearly about the societal benefits and safeguards of secondary use;
- Involve, in a timely and meaningful manner, the stakeholders who can genuinely represent the views of natural persons, enabling them to act as credible voices for their communities;
- Where suitable, involve citizens themselves or build on existing channels for public participation.

Insight into public views can help to build trust as well as to understand what such trust us dependent upon. These views can be taken into account in the process of the secondary use of health data in order for HDABs to understand how the public understands societal benefits and what data use means to them at a societal level, as well as to ensure that the EHDS

implementation aligns as much as possible with these perspectives, to ensure its trustworthiness and resulting success.[2]

5.2 Opt-out from what

5.2.1 Characteristics of data falling under the opt-out

The scope of the EHDS opt-out is limited to processing carried out within the EHDS secondary use framework (see Section 5.1). Processing conducted under other legal regimes remains governed by their respective legal bases.

The categories of electronic health data that may be made available for secondary use are set out in Article 51 EHDS. These include:

- Data from electronic health records (such as diagnoses, procedures, prescriptions, laboratory results, and medical imaging).
- Administrative health data (including reimbursement and claims data).
- Data from disease registries, public health registries, and similar structured datasets.
- Genomic and other relevant molecular data.
- Data generated by medical devices and certain wellness applications, where they fall within the scope of the Regulation.
- Other categories of electronic health data listed in Article 51.

The opt out right applies to personal electronic health data within these categories when they are processed for secondary purposes under the EHDS. It does not apply to data processed solely for primary use or to data that have been anonymised in accordance with applicable legal standards. Under the EHDS, the term data user refers broadly to any organisation or entity authorised to access to electronic health data for secondary use under Articles 53–56. This can include a wide range of actors such as universities, public research institutes, national public-health authorities, EU bodies, non-profit organisations, and private companies developing health technologies or AI tools.

The term datasets should be understood in a practical sense as the collection of electronic health data held by data holders and made available through the HDAB. These may include, for example, hospital electronic health records, disease-specific registries, national vaccination or cancer registries, administrative datasets such as hospital discharge or reimbursement data, genomic or laboratory datasets, data from clinical trials, or person-generated data from medical devices and wellness applications. The EHDS does not create new datasets; it provides a harmonised framework through which existing datasets, collected under national law or EU law, can be accessed securely and responsibly for secondary purposes such as research, innovation, public-health monitoring, and regulatory activities.

[2] Such an initiative was carried out in the European Joint Action TEHDAS. Between 2021 and 2023, citizens from different European countries participated in the online Healthy Data Consultation to express their views on the secondary use of health data and how they wish to be engaged in it.

To ensure clarity regarding Article 71(8), it is important to emphasise that the EHDS does not allow any indirect or "backdoor" secondary use of personal electronic health data from individuals who have opted out. Under the Regulation, the opt-out must be effectively applied before personal electronic health data are made available for secondary use under the EHDS. The specific operational responsibility for implementing the opt-out may vary depending on the national model, but it must be ensured that datasets provided for secondary use exclude individuals who have exercised their opt-out. Article 71(8) simply confirms that the opt-out does not apply to anonymised data, which are outside the scope of personal data rights under the GDPR. This provision does not diminish the effectiveness of the opt-out; rather, it reflects the legal distinction between personal and anonymised data and ensures that the opt-out remains fully enforceable for all personal electronic health data still identifiable by the data holder. The EHDS architecture is therefore designed so that neither HDABs nor data users can re-identify individuals or circumvent the opt-out in any manner.

For the avoidance of doubt, the opt-out applies to pseudonymised data only when the entity responsible for implementing the opt-out within the national model can identify or re-identify a natural person using means reasonably available to it. The assessment of identifiability should be made in accordance with applicable EU data protection principles, including relevant Commission guidance (i.e. European Commission FAQ 41[3]), and must reflect the specific technical and organisational context in which that entity operates. Entities responsible for applying the opt-out are not required to process additional personal data or obtain re-identification keys solely for the purpose of applying the opt-out under EHDS in accordance with Article 71(8) which mirrors Article 11 of GDPR (*"If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation."*).

The opt-out also applies to the processing of personal data carried out for the purpose of answering data requests. Although the final output provided to the data user will be non-personal, generating that output may require processing personal data at earlier stages. Once a person has opted out, this downstream processing (preparing data to answer to a data request) can no longer take place, and the HDAB must exclude their data from all steps that involve personal-data handling.

5.2.1.1 Legal requirements by the Regulation

Under the GDPR, the term processing is defined very broadly in Article 4(2) to include any operation performed on personal data, including collection, storage, adaptation, use, disclosure, and anonymisation. While anonymised data is no longer considered "personal data" under the GDPR (Recital 26), the act of anonymising data still constitutes processing if it is applied to identifiable data. Hence, anonymisation requires a legal basis, and the controller is subject to the GDPR for such processing activity. The different variables that can be used to identify a person can be found in the document of *D7.2 Guideline for Health Data Access Bodies on data minimisation, pseudonymisation, anonymisation and synthetic data* This document also provides additional context on how data is pseudonymised or anonymised to meet the required legal standards.

[3] Frequently Asked Questions on the European Health Data Space - Public Health (March 2025) - Question 41

In the context of the EHDS Regulation, Article 71(1) and (3) provides individuals with the right to opt out of having their health data made available for secondary use under the EHDS Regulation, which explicitly includes data that is still personal at the time of processing. This would therefore also include processing activities that aim to anonymise or pseudonymise the data to make them available through the EHDS for secondary use. This strict interpretation reinforces the notion that the opt out right applies not just to the use of the electronic health data but to the entire chain of processing activities related to secondary use under the EHDS framework. The opt-out does not apply to datasets that were anonymised before the individual exercised their opt out right, nor to datasets anonymised by the data holder under another lawful basis or for purposes unrelated to EHDS secondary use.

5.2.1.2 Exceptions to the opt-out mechanism

The EHDS introduces narrowly defined exceptions to the right to opt out in Article 71(4). Member States may adopt national laws allowing access to health data of individuals who have opted out, provided that three cumulative conditions are met:

1) The application or request is made by a public sector body, EU institution, carrying out tasks in the area of public health, or on behalf of such an entity, and

2) The data is necessary for public health purposes (i.e., those listed in Article 53(1)(a)-(c)) or for scientific research for important reasons of public interest.
The data cannot be obtained by alternative means in a timely and effective manner under equivalent conditions.

3) The applicant has provided sufficient justification why data for which a right to opt out has been exercised should be made available.

Such a mechanism can be provided for in national law and must include specific and appropriate safeguards to protect the rights and freedoms of natural persons. These include the prohibition of re-identification [Article 61(3)], the use of SPEs [Chapter IV], and the respect of necessity and proportionality in a democratic society [Article 71(5)-(6)].

5.2.2 Are there different levels of opt-out available in EHDS?

5.2.2.1 National discretion

Member States may implement the national opt-out mechanism with as much granularity as they deem appropriate. Member States may provide the option, for example, to allow individuals to opt-out of specific types of secondary use or individual data categories. However, excessive complexity can create significant administrative burdens and may risk undermining the overall coherence and interoperability of the EHDS framework. Greater granularity may enhance individual control, but it also increases the effort required to ensure EHDS compliance, system transparency, and usability. Therefore, it is recommended that where MS implement a granular opt-out, they focus on defining a limited set of essential, meaningful opt-out levels, those that reflect real differences in data sensitivity and public expectations.

It is important to highlight three general characteristics of these levels:

1. the resulting stratification must be legally sound;
2. it must be technically, operationally, and compliance-wise feasible; and
3. it must be socially acceptable.

Illustrative models of granularity within national discretion:

- full opt-out,
- opt-out for specific data types, e.g. genomic data, images,
- per data holder, e.g., cohorts, biobanks, EHR,
- per purpose of data use, e.g., research, innovation, policy development.

Where MS consider purpose-based granularity, particular care should be taken to ensure consistency with the categories of data use purpose defined in Article 53 and with the structure of data-permit applications, especially in cross-border contexts.

While the Regulation allows MS to determine the level of granularity of the opt-out, including differentiated approaches, limiting granular opt-out to national use cases while excluding cross-border access may raise significant technical and interoperability challenges in practice.

For the purpose of this guideline, “full opt-out” refers to the exclusion of a natural person’s personal electronic health data from all secondary use processing under the EHDS framework.

“Granular opt-out” refers to a model in which MS allow individuals to exclude specific categories of data, specific purposes of processing, or specific data holders from secondary use.

“Selective exclusion” is used as a descriptive term for the practical implementation of granular opt-out choices.

5.2.2.2 Recommended good practice

Which opt-out levels constitute “essential” may vary across jurisdictions, often shaped by cultural norms, legal traditions, and the extent of individual autonomy typically granted in health-related decision-making. In designing these systems, policymakers must carefully balance personalisation and practicality: too little granularity may erode trust, while too much may lead to confusion, decision fatigue, and low engagement.

In this context, it becomes essential to design opt-out mechanisms that are citizen-centred but not burdensome, allowing individuals to exercise control informedly and reflectively, without being overwhelmed by fragmented or overly technical choices. Only by achieving this balance can the EHDS foster sustainable, trusted cross-border collaboration while respecting fundamental rights.

It is recommended that HDABs inform individuals that opt-outs do not propagate automatically across borders, and that citizens may need to submit opt-outs for their data stored in each relevant country.

It is also recommended that MS use suitable rules, measures, and tools (i.e. information portals) to help citizens obtain information, make decisions, and to collect and provide the necessary data.

A key consideration is the potential risks associated with fragmentation between MS through national approaches to granular opt-outs. Risks include challenges to citizens in understanding and navigating systems that differ in each country, impacts on public trust, compromised interoperability and comparability of data and administrative burdens. The question of harmonisation of opt-out levels across MS cannot be resolved within the scope of this document. As referenced, the choice of opt-out levels is informed by factors that differ significantly between MS including health literacy levels, cultural expectations and administrative capacities to implement a granular opt-out. Therefore, it is recommended that the MS consider alignment of opt-out levels an unresolved issue requiring further coordination and discussion as they progress EHDS implementation.

5.3 Where to declare opt-out

5.3.1 Legal Requirements by the Regulation

The EHDS Regulation assigns HDABs a central role in governing opt-out from secondary use of electronic health data. However, based on national implementation choices, the data holders also may function as a possible point of contact[4]. It ultimately leaves it to each MS to determine how responsibilities for implementing the opt-out mechanism are allocated, including which entity serves as the primary contact point for individuals exercising their rights.

5.3.2 National discretion

Example of possible step-by-step chain of responsibility:

1) **Initiation by the individual:**
   The data subject initiates an opt-out request via a channel established by the MS (e.g. a national opt-out portal, their healthcare provider, national EHR portal, or eHealth application).

2) **Identity verification (GDPR-compliant):**
   Identity verification is performed through channels designated by the MS (e.g., healthcare provider, data holder, or central system, etc.), using secure and GDPR-compliant mechanisms. It is also worth considering MS the use of provisions and tools for electronic identification and trust services, which can be particularly effective in cross-border data flows. Examples from other EU digital initiatives show that cooperation between Member States can help reduce technical and legal fragmentation. While the EHDS Regulation does not provide for cross-border propagation of the opt-out, this underscores the importance of effective coordination

[4] See Article 71 (8) of the EHDS Regulation: “When the purposes of the processing of personal electronic health data by a **health data holder** do not or no longer require the identification of a data subject by the controller, that **health data holder** shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the right to opt out under this Article.”

between competent entities to ensure consistent application of the technical, operational and legal aspects, including in cross-border contexts.

3) **Transmission to HDAB or another national entity:**
The opt-out status is relayed securely to an opt-out database or registry. The MS may decide whether this is housed at the HDAB or at another national entity.

4) **User confirmation and transparency (GDPR Articles 15 EHDS Articles 58, 71):**
The individual receives a confirmation receipt and can view their status and previous decisions. Based on MS legislation, it can be managed via a centralised public information portal maintained or coordinated by the HDAB or managed in a decentralised way by the data holders.

In case of more than one HDAB per country, MS should ensure coordination mechanisms are in place to prevent fragmentation and ensure consistency in opt-out application across all HDABs and data holders. Possible approaches may include the primary competence of a coordinating HDAB or the sharing of competence between HDABs, or a decentralised management at the level of data holders.

Possible role and responsibilities of data holders:

- Where designated under the national implementation model, data holders are required to respect opt-out statuses communicated via HDABs or other competent authorities and to ensure that personal electronic health data are not made available for secondary use where an opt-out is in effect.
- Before providing data for secondary use, data holders that are responsible under the national framework must ensure that datasets made available for secondary use reflect the applicable opt-out decisions.

5.4 Opt-out declaration and enforcement architecture

5.4.1 Opt-out channels and portals

5.4.1.1 Legal requirements of the Regulation

According to Article 71(2) of the EHDS Regulation:

"*Member States shall provide for an accessible and easily understandable opt-out mechanism to exercise the right established in paragraph 1, whereby natural persons may explicitly state that they do not wish to have their personal electronic health data processed for secondary use*".

Individuals are not required to provide a reason when making their opt-out declaration. However, MS will inevitably be interested in the reasons why individuals opt out as this could reveal why trust is lacking in the EHDS framework and what might be needed to restore trust. While individuals cannot be required to give a reason, MS may provide the possibility to record a reason for opt-out. MS implementing this option should have an explicit legal basis. The possibility to provide a reason must be implemented in a way that avoids misinterpretation by individuals as a mandatory condition before their opt-out can be registered. Therefore, if a MS implements the option to provide a reason, it should happen

sequentially after the opt-out is already registered, for example in the communication confirming the opt-out status.

The opt-out must be reversible at any time, as stated in Article 71(1). Reversing an opt-out decision:

- Must be as simple and accessible as the initial opt-out.
- Must trigger updates of the registry and downstream systems.
- Must be reflected in secondary use authorisations made after the reversal.
- Does not affect past data uses approved before the reversal or ongoing secondary use projects.
- Can apply equally to granular opt-outs and total opt-out.

When an opt-out decision is reversed, the individual's health data will be made available for future secondary use – this includes those data that were recorded during the period when the opt-out was effective. Reversing an opt-out decision does not affect past authorisations or processing already lawfully carried out.

Mechanisms for reversing opt-out should observe the same standards as those for registering the initial opt-out, e.g. identity management, confirmation of status to the individual, etc.

The EHDS also requires transparency: individuals must be clearly informed about how the opt-out works and how their choice is recorded, in line with GDPR obligations.

5.4.1.2 National discretion

Member States could deploy a national online portal where people can exercise their opt-out choice. Such portals must provide secure identity management enabling individuals to log in, view the current status of their opt-out choice, make an opt-out declaration and reverse their current choice.

The portal must comply with national language requirements and accessibility requirements (i.e. Web Content Accessibility Guidelines (WCAG) version 2.1 or above and EN 301 549 Accessibility requirements for ICT products and services). Member States may consider ensuring that opt-out portals provide information in structured, machine-readable formats where appropriate, to support accessibility tools, automated services and emerging AI-based agents, while maintaining compliance with data-protection and security requirements.

A national portal could be co-located with the patient app, meaning individuals could exercise all of their EHDS choices in one place. Or it could be hosted on a dedicated portal hosted by the HDAB, meaning more cohesion with secondary use and more clarity on who is managing opt-out.

As stated in this guideline, the right to opt out is managed at the national level and opt-out decisions do not automatically propagate across borders. Therefore, national opt-out portals could be used by non-residents. Member States may wish to make their portals available in translation to improve accessibility for residents of other EU countries.

The opt-out interface may use neutral, factual language and present balanced information on effects and limitations; broader awareness-raising on societal benefits of secondary use could be provided through separate public communication channels.

Member States could ensure that the opt-out mechanism is non-discriminatory and inclusive, covering the needs of diverse population groups. Digital-first approaches are efficient, but alternative channels may be considered to improve accessibility for citizens with limited digital access or literacy. These channels could include paper-based options, in-person declarations at the point of care or through functional desks (e.g. phone lines).

Whether to deploy secondary channels and which channels requires careful consideration. Unlike an online option, such channels will not enable the individual to view their current opt-out status when updating their decision. Enabling opt-out through engagement with data holders or healthcare professionals is a possibility but might increase the administrative burden on the healthcare system. There are specific challenges with paper-based solutions that would have to be addressed at national level, including how to confirm the identity of the person submitting the declaration and how to provide confirmation that the change in opt-out status has been applied. Further, latency of secondary channels needs to be considered. Whether or not a person's data will be included in a secondary use dataset is dependent on their opt-out choice before permit is issued. MS should establish national rules about when an opt out declaration becomes effective (for example, from the moment the declaration is made or from the time it is reconciled with a central registry etc.).

While not a requirement of the Regulation, MS may consider making the opt-out mechanism available in advance of the HDAB "going live" and accepting applications for data access (for example 1 month before). This would facilitate citizens with a period of time to consider the public information on EHDS and opt-out and how they will exercise their opt-out right.

5.4.1.3 Recommended good practice

Engage citizens in the design process of the opt-out mechanism.

Consider accessibility requirements in terms of design, language requirements and needs of diverse populations.

Require individuals to provide only data necessary to identify them and confirm the opt-out status (in line with GDPR Article 5(1)(c) – data minimisation).

Provide clear plain-language explanations of what the opt-out does and does not do. These explanations should include that it applies only to secondary use under the EHDS, does not affect primary care, access to services, or the existence of the EHR, and that it is reversible at any time. Explanations should avoid technical or legal jargon and could use visuals or infographics, where helpful.

If granular opt-out is offered, each level must be clearly defined and distinguishable with meaningful choices, and they must also be operationally enforceable.

Ensure distinction from other rights (e.g., opt-out for primary use, right not to be informed about significant findings from secondary use, right to restrict access under Article 8) is clearly explained and communicated.

5.4.2 Opt-out registries and enforcement mechanisms

5.4.2.1 Legal requirements of the Regulation

Implementing the EHDS opt-out requires careful attention to data protection challenges that arise when aligning Article 71 of the EHDS Regulation with the broader EU framework for processing personal electronic health data. Because the EHDS allows secondary use unless a natural person opts out, MS must ensure that national opt-out mechanisms operate in a way that is fully compatible with the GDPR's principles of transparency, purpose limitation, and data minimisation, without treating the opt-out itself as a legal basis for processing. The opt-out must remain unconditional and reversible, yet its implementation should not require unnecessary disclosure of identifiable information to HDABs or other actors.

Responsibility for ensuring that the opt-out is effectively applied before personal electronic health data are made available for secondary use rests with the entity or entities designated under the national implementation model prior to dataset transmission for secondary use, ensuring that HDABs do not receive additional identifying data solely for enforcement and that no re-identification or linkage is required at HDAB level.

Any data filtering or granularity of opt-out layers entails an enhanced risk of re-identification which needs to be balanced against the benefits for citizens.

The EHDS does not require a central EU-level opt-out registry, nor does it prescribe how MS must technically record opt-out decisions. Article 71 only requires an accessible opt-out mechanism, while the GDPR continues to apply in full. This means any national system used to store opt-out choices must follow GDPR principles, including strong security measures, data minimisation, and appropriate technical and organisational safeguards. Although the Regulation does not specify pseudonymisation or encryption requirements, its emphasis on a high level of data protection (Recital 4) implies that MS must implement secure, well-controlled and legally justified solutions.

5.4.2.2 National discretion

Opt-out registry – keep tracking of opt-out decisions: the exercise of the opt out right under Article 71 of the EHDS Regulation could entail privacy risks, particularly regarding how opt-out declarations are recorded, stored, and acted upon. The process must ensure that individuals can exercise control over the secondary use of their electronic health data without exposing themselves to additional personal data risks.

Opt-out registry – declaring the decision: to manage and enforce opt-outs consistently across the EU, MS or designated HDABs can maintain a secure opt-out registry.

Where MS establish a centralised registry or equivalent mechanism, strong technical and governance safeguards are essential, as opt-out decisions may indirectly reveal sensitive preferences or vulnerabilities. MS should also assess the data-protection implications of any

registry-based approach, avoiding designs that require linkage between registry identifiers and pseudonymised or encrypted data sources.

They may consider enabling natural persons to record advance directives concerning the EHDS opt-out for situations in which they may later become legally incapable, thereby ensuring that previously expressed wishes, including granular preferences, are respected and consistently applied.

Opt-out registry – keep tracking of opt-out decisions: the exercise of the opt-out right under Article 71 of the EHDS Regulation could entail privacy risks, particularly regarding how opt-out declarations are recorded, stored, and acted upon. The process must ensure that individuals can exercise control over the secondary use of their electronic health data without exposing themselves to additional personal data risks.

5.4.2.3 Recommended good practice

Minimum technical safeguards and audit mechanisms for opt-out registries include but are not limited to:

- Security controls: encryption of opt-out data at rest and in transit, multi-factor authentication for registry access, and regular penetration testing.
- Audit logging: detailed logs of all access and changes to opt-out status, with automated alerts for suspicious activity.
- Compliance: reference to ISO/IEC 27001 and GDPR Article 32 for security management.
- Incident response: breach notification procedures, including timelines and responsible contacts.

The guideline acknowledges that any national opt-out mechanism, including a centralised registry, contains sensitive information about individuals' choices and therefore requires strict safeguards. Implementing an opt-out mechanism raises several data-protection challenges that must be addressed at national level, including ensuring accurate identification and authentication of individuals when recording opt-outs, synchronising opt-out status across multiple data holders without creating new linkage risks, managing retroactive opt-outs in a way that respects GDPR while preserving auditability, preventing unnecessary sharing of identifiable information between institutions, and ensuring consistent propagation of opt-out decisions in multi-centre datasets to avoid re-identification risks.

Record only necessary data to identify the individual and confirm the opt-out status (in line with GDPR Article 5(1)(c) – data minimisation).

Purpose limitation: processing must remain strictly limited to purposes compatible with the registry's function (e.g., verifying opt-out status), and not extend to recontact or analytics unless expressly authorised by law.

Use pseudonymised or encrypted identifiers wherever possible to reduce re-identification risk.

Ensure data subject authentication is robust, possibly via EU digital identification options (eIDAS), national digital ID or healthcare credentials, to confirm whom an opt-out relates to.

Attention should also be paid to the management of individual identities in the opt-out register to ensure the uniqueness of the registration of the person actually exercising the opt-out. This is particularly important in cases where at national level there may be duplicate assignment of one identifier to multiple persons or multiple identifiers to one person. In such cases, registry management should be able to make corrections to match the identifiers to the person who has actually exercised opt-out, or preventive measures should be taken to avoid disputed opt-out registration cases.

The registry must also:

- Provide immediate confirmation of opt-out status to the individual.
- Log the timestamp and source of the declaration.
- Be accessible (via national portal or HDAB interface) so the individual can view, update, or revoke their declaration easily.
- Security and access controls: registry access must be limited to authorised entities with a clearly defined role (e.g., HDABs or designated public authorities) and subject to logging and oversight.

Maintaining a centralised list of opted-out individuals requires particular attention under data protection law, as such registries may, if not properly safeguarded, reveal sensitive individual choices. Member States must ensure this information is processed strictly within the legal purpose and is protected from unauthorised inference or secondary use.

The EHDS Regulation does not require all actors involved in primary or secondary use to access an opt-out registry; its architecture is designed to limit who needs to know about an individual's opt-out decision. Only the HDAB, and in limited cases the data holder preparing extracts, must be aware of a citizen's opt-out status.

Maintaining an opt-out registry is only the first step. The real safeguard lies in ensuring the registry is technically and legally connected to downstream systems so that:

- Data relating to natural persons who have opted out are excluded from any new data permits or health data requests, subject to the exceptional cases referred to in Article 71(4). This may be carried out at dataset, data holder, or HDAB level, as implemented by the MS.
- Data holders (e.g., hospitals, registries) are notified of opt-out status and ensure that relevant electronic health data is not transferred or made available for secondary use.
- This requires interoperable technical standards, national integration with the EHDS infrastructure, and strong governance protocols.

Data filtering in a decentralised system with high levels of integration between the opt-out registry and data holders can be done:

- At the data holder level: as soon as the user exercises their opt-out right and it has been registered in the opt-out registry, healthcare data controllers (e.g., hospitals, clinics, medical records) must be notified immediately. They must ensure that the data concerned is not transferred for secondary use (e.g. for research or statistical purposes). This filtering takes place at the source, minimising the risk.
- At the dataset level: when a researcher or organisation submits a data request, the system releasing the data must put in place a technical barrier to prevent the release of data with opt-out status. This is a secondary line of defence that filters out non-transferable data from the entire dataset.

Table 5: Operational responsibilities for implementing the EHDS opt-out mechanism: what the regulation specifies and what MS could define

Issue raised	What the EHDS Regulation specifies	What the EHDS Regulation leaves to MS decision
1. Where the opt-out should be stored	No requirement for a central registry; Article 71 only requires an "accessible and easily understandable" mechanism.	MS decide storage model (centralised, federated, sector-specific, digital record, etc.).
2. Whether a signature is required	No requirement for a physical or digital signature.	MS choose authentication method (eID, portal login, etc.) consistent with GDPR.
3. Which personal identifiers must be collected	No list of mandatory identifiers in the Regulation.	MS determine the minimum identifiers needed to reliably link the opt-out to the correct person, following GDPR minimisation.
4. Where identifying information is stored or processed	No EU-level repository or trusted third party is created.	MS define storage location and processing arrangements under GDPR security requirements.
5. Who may access opt-out information	Access to opt-out information is limited to the HDAB and, where necessary, to the data holder preparing extracts for secondary use. Data users do not have access to opt-out status information. Supervisory authorities may access relevant information where required for the exercise of their monitoring and enforcement tasks pursuant to Article 65 EHDS and the GDPR.	MS define internal access controls, ensuring strict minimisation.
6. Technical and organisational measures for implementation and cross-country exchange	No specific technical standards for opt-out mechanisms are prescribed. GDPR applies fully (security, confidentiality, minimisation).	MS define technical safeguards, formats, and interoperability arrangements, ensuring HDABs can enforce the opt-out.

5.5 How to implement opt-out with regard to citizens' rights

While Section 5.1.5 addresses engagement and trust-building at governance level, this part of the document focuses on the concrete information and communication obligations necessary to enable the effective exercise of the opt out right.

Effective implementation of the EHDS opt-out requires robust communication and coordination mechanisms between data subjects' points of contact, data holders, and HDABs to ensure that individuals' preferences are correctly captured, transmitted, and enforced.

Without clear and reliable channels, there is a risk that opt-out decisions, including those relating to different categories of personal electronic health data or reversals of previous decisions, may be overlooked or inconsistently applied. As the EHDS operates without prejudice to the GDPR, MS must ensure that obligations under both frameworks are met in a coherent manner, avoiding duplication while preventing gaps in compliance. This includes clarifying how transparency duties are fulfilled when HDAB decisions are published publicly rather than communicated individually and ensuring that any reliance on GDPR exceptions is appropriately justified under national supervision. A centralised or equivalent opt-out mechanism must incorporate strong safeguards, as opt-out decisions may indirectly reveal sensitive preferences or vulnerabilities. Pseudonymisation and anonymisation workflows must also be adapted so that individuals who have opted out are excluded before any processing for secondary use occurs, and these processes should be transparent, documented, and subject to oversight by competent Data Protection Authorities. Ensuring consistent enforcement across multiple data holders, including in multi-centre datasets, requires reliable synchronisation and provenance tracking, while authentication and reversal procedures must verify identity without collecting more data than necessary. Where MS apply narrowly defined exceptions under Article 71(4), they should clearly describe the safeguards and oversight arrangements that ensure compliance with both the EHDS and the GDPR.

5.5.1 How to inform citizens about their right to opt out?

To ensure full respect for patients' rights under the EHDS Regulation, the opt-out mechanism must be implemented in a transparent, understandable, and loyal manner, enabling individuals to make informed decisions about the secondary use of their personal electronic health data. Article 71 grants natural persons an unconditional and reversible right to opt out, and this right must be clearly distinguished from the GDPR right to object to avoid confusion and preserve trust. Opt-out is not a proxy for public acceptance but a rights-based safeguard that protects autonomy within a broader democratic framework of transparency and accountability. Its implementation should therefore avoid unnecessary disclosure of identifiable information to HDABs, in line with the principles of data minimisation and purpose limitation. The Regulation requires that the opt-out be effectively applied before personal electronic health data are made available for secondary use under the EHDS. The allocation of operational responsibility for applying the opt-out depends on the national implementation model. Clear communication, ongoing engagement with citizens, and responsible institutional practice are essential to uphold patient rights, maintain public confidence, and embed opt-out as a meaningful element of the EHDS's rights-centred governance model.

The rules for informing citizens are set out in Article 58 of the EHDS Regulation. Article 58(1) requires HDABs to make information on the legal basis and the conditions under which electronic health data for secondary use may be granted to health data users, publicly available, easily searchable through electronic means, and understandable for natural persons. In addition, Article 58(2) provides that, where a MS has provided for the right to opt out pursuant to Article 71 to be exercised through the HDAB, the relevant HDAB shall make public information available about the opt-out procedure and facilitate the exercise of that right. For the sake of clarity, these provisions set out the general transparency obligations of HDAB and do not create an individual right to verify, for each data permit or specific data-access authorisation, whether an opt-out has been applied.

In the present guideline, information to citizens is discussed in general terms in the chapter on Citizen engagement and empowerment as regards the opt-out. The information portal for citizens will be addressed in detail by D8.3 (*Guideline for informing natural persons about the use of health data - "Citizen Information Point"*).

Before individuals can meaningfully exercise their right to opt out from the secondary use of their health data, they must be clearly and proactively informed of that right. HDABs play a central role in this process. Under the EHDS Regulation, HDABs have specific legal duties when they are entrusted with managing the opt-out mechanism. In addition, HDABs may voluntarily take on broader communication and support functions to strengthen transparency and public trust. HDABs ensure electronic transparency tools, as they are required to maintain a publicly available and electronically searchable register that shows information on data permits, categories of data used, identities of data users, the legal basis for access, and applicable safeguards. This transparency supports accountability and helps build trust in the secondary use system.

Information must be available before any data access is granted to make sure that citizens can effectively exercise their opt-out right.

This section outlines, first, what HDABs must do by law, and second, what they may choose to do as part of a wider role as an information hub.

5.5.1.1 Requirements by the Regulation

Mandatory public information

If a MS has provided for the right to opt out pursuant to Article 71 of the EHDS Regulation to be exercised through the HDAB, the HDAB is legally required to provide public information about the procedure to opt out. This includes clear instructions, available formats, and access points that enable natural persons to exercise their right. However, the general requirement on the opt-out mechanism in Article 71 of EHDS Regulation is that it must be 'accessible', which also means that there must be public information about its existence, so it means, if this right is exercised elsewhere, it's for MS to ensure sufficient publicity.

Facilitation of the opt-out process

Member States, acting as a whole, are responsible for ensuring that an opt-out mechanism is established and maintained. If the MS decides to assign this to HDABs, the HDABs must also ensure that the opt-out mechanism is effectively operational and can be used by individuals. While they are not necessarily required to operate the system themselves, they are responsible for making sure that the opt-out process is clearly defined, accessible, and easy to understand for all users, including people with disabilities and those with limited digital skills. It is important to clarify, that these obligations only apply to HBABs only if they are responsible to implement the opt out, otherwise the responsibility lies with the MS.

Reporting duties

HDABs must publish activity reports every two years. These must include data on permit applications, granted and refused permits, categories of data used, types of applicants, and decisions on exceptional access under article 71(4), including the number of data permit decisions involving individuals who opted out. This ensures that the implementation of the opt-out mechanism is documented and subject to public scrutiny.

5.5.1.2 National discretion

In addition to their legal duties, HDABs may take on supportive roles to enhance awareness and understanding among citizens. While these actions are not mandated by the regulation, they are recommended good practices:

- **Public outreach and awareness**
  HDABs may engage in campaigns to raise awareness about the right to opt out. This could involve developing educational materials, partnerships with civil society groups, or providing public information sessions.
- **Guidance and interpretation**
  HDABs may provide neutral, plain-language explanations about the implications of opting out, including how it affects the availability of data for research, public policy, and innovation.
- **User support services**
  HDABs could establish multichannel support systems, such as helplines, online chats or physical service points to guide citizens through the opt-out process. Multilingual and accessible formats would help reach diverse user groups, including those with limited digital literacy.

Still, Article 84 (1) of the EHDS Regulation provides "*Member States shall promote and support digital health literacy and the development of relevant competences and skills for patients. The Commission shall support Member States in this regard. Awareness-raising campaigns or programmes shall aim, in particular, to inform patients and the public at large about primary use and secondary use in the framework of the EHDS, including the rights arising from it, as well as the advantages, risks and potential gains for science and society of primary use and secondary use.*"

For sake of clarity, given that the EHDS allows each MS to design and operate its own opt-out mechanism, it is important to minimise the risk of fragmentation and inconsistent implementation across the EU. Member States are encouraged to work towards a more harmonised and interoperable approach to opt-out design, including alignment on the structure and granularity of opt-out options, to support cross-border secondary use, particularly in areas such as rare disease research, where data availability across jurisdictions is essential. A consistent framework would also reduce administrative burden for data holders and simplify compliance for organisations operating in multiple MS. In addition, MS should provide clarity on the jurisdictional scope of their national opt-out mechanisms, including how they apply to multinational research settings and datasets that include participants from outside the EU, to ensure that the EHDS opt-out remains practical, predictable, and compatible with broader research governance requirements.

5.5.2 Information to be communicated to citizens regarding the right to opt out

To support citizens in understanding and exercising their right to opt out, it is essential that the national authorities responsible for implementing the EHDS, particularly HDABs, possess the necessary expertise in data protection, health-data governance, and communication. Because the EHDS opt-out and the GDPR right to object operate in parallel and have different legal effects, clear and accurate public information can only be developed when

HDABs coordinate closely with the competent supervisory authorities and, where relevant, ethics committees or advisory bodies. This coordination should take place early in the design of national processes and communication materials to ensure that explanations are legally correct, consistent across institutions, and accessible to people with varying levels of digital and health-data literacy. Member States should also involve affected stakeholders, such as enforcement and regulatory bodies, patient organisations, healthcare professionals, researchers, and civil-society groups, drug or medical devices developing companies, in a timely manner when preparing guidance, so that the language, examples, and level of detail reflect real-world needs and avoid confusion. Such an approach helps ensure that citizens receive trustworthy, comprehensible information about their rights, while also supporting controllers in applying those rights correctly and consistently across different legal frameworks.

The opt-out mechanism described in this section applies exclusively to secondary use of electronic health data under the EHDS framework (Articles 53–71) and does not affect other national or EU legal bases for data processing. This must be reflected in all kinds of knowledge transfer processes towards citizens and different stakeholders, contributors.

5.5.2.1 Legal Requirements by the Regulation

HDABs or other competent national authorities, are responsible for ensuring that individuals are fully informed about the opt out right through clear, accessible, and proactive communication.

Minimum required information

1) **Existence and nature of the right**
   Citizens must be informed that they can opt out of the secondary use of their personal electronic health data. This applies to data used for research, public policy, innovation, and similar purposes.
2) **Voluntary and reversible nature**
   The opt-out is voluntary. It can be exercised at any time and reversed without needing to provide a justification.
3) **Scope of the opt-out**
   The opt-out applies to any secondary use processing based on data permits or health data requests approved after the opt-out is registered, as per Article 71(3) of the EHDS Regulation. It does not apply retroactively to processing authorised before the opt-out was exercised.
4) **How to exercise the right**
   Clear, step-by-step information should be provided on how to opt out. The process should be simple and usable by all individuals, including those with disabilities or limited digital literacy.

5.5.2.2 Recommended good practice

Possible communication channels include:

- Online channels - official websites of HDABs and DHs, personal digital health accounts, e-health portals.

- Channels at point of care - printed materials made available at hospitals and clinics, digital information kiosks in healthcare facilities.
- Official health insurance websites and other authorities in healthcare.
- Mass media channels - public service messaging, official social media accounts.
- Direct interaction with individuals - information hotlines, in person assistance at local authority offices.
- Stakeholder engagement - engagement with patient organisations and healthcare professional networks; development of information materials for distribution through these channels.

Impact of the opt-out

Citizens must be told that opting out means their data will not be used pursuant to future secondary use applications that involve identifiable information. However, opting out does not stop their data from being stored or used for delivering healthcare, nor does it prevent reporting obligations under public health law.

Identity and contact of the HDAB/authority

Citizens must be informed which authority is responsible for managing opt-out declarations. Contact details, including email, website, and service hours, should be published.

Transparency and visibility of data use

Citizens should know that public web portals exist where they can see who has received data permits, for what purpose, and under what legal basis. They should also be able to access information about whether their opt-out has been respected. The existence and purpose of opt-out registries must also be communicated clearly to individuals, e.g., in the contact channels for declaring the opt-out. In addition, individuals should be informed that appropriate technical and organisational measures are in place to protect their identity, restrict access to authorised entities only, and prevent unauthorised access, disclosure or misuse of opt-out registry information.

Where MS law provides for a mechanism to implement an exception from the right to opt out [referred to in Article 71(4)], information about this should be included in the HDAB's information duties. The information provided should include explanations of the structure of the mechanism, how decisions to make opted-out data available are made and information about applications that have been granted/refused in respect of this exception. Further, where national opt-out implementation includes both an exception and a granular opt-out, clear and understandable explanations should be provided on the difference between these elements, how they operate separately and cumulatively.

Citizens should be informed that, while they can view their opt-out status and history of decisions, they will not be able to see a list of individual secondary use projects from which their data was filtered.

General public awareness

Member States are responsible for ensuring that the public is broadly aware of the opt-out right. This can include collaboration with patient associations, educational campaigns, or integration into digital health literacy programs.

When informing citizens about their right to opt out, it is important to explain that people may express their preferences in simple or general terms, without knowing whether their request relates to the EHDS Regulation or to the GDPR. For example, a person may say that they do not want their data used beyond what is necessary for their healthcare. Citizens should therefore be clearly told that the EHDS opt-out applies only to the secondary use of their electronic health data within the EHDS framework, while other types of research or processing outside the EHDS continue to rely on the GDPR and national laws. They should also understand that the EHDS opt-out does not automatically replace or trigger the GDPR right to object, and that both rights may coexist.

To avoid confusion or unnecessary burden on individuals, MS should ensure that information is presented in an accessible and easily understandable way, helping citizens recognise which right applies to their situation and how to exercise it. Clear explanations also support data controllers, who must interpret and implement individuals' preferences consistently across different legal frameworks. By providing transparent, practical guidance, MS and HDABs can help citizens make informed choices while ensuring that their rights are respected throughout the processing of their electronic health data.

Reversibility of opt-out

Member States should ensure that communication materials explicitly highlight the reversibility of the opt-out decision, including practical guidance on how revocation is recorded and when it becomes effective in national data-access workflows.

5.6 Data use before opt-out

The following chapters address data processing in three scenarios: (1) before individuals exercise their right to opt out, (2) after they have opted out, and (3) after a previous opt out has been revoked.

The following description applies equally to natural persons who do not opt out at all or who have not opted out until a given point in time but will exercise this right in the future.

In respect of natural persons who do not exercise or have not yet exercised their right to opt out, personal electronic health data relating to such natural persons shall be made available or otherwise processed (pragmatically means to cover all secondary use processing) based on data permits issued pursuant to Article 68 or health data requests pursuant to Article 69 of the EHDS Regulation.

According to Article 58 (1)(f) of the EHDS Regulation, HDABs shall make information on the conditions under which electronic health data are made available for secondary use publicly available, easily searchable through electronic means and accessible for natural persons, which information shall cover "*who has been granted access to datasets of electronic health data and to which datasets they were granted access and details of the data permit regarding the purposes for processing such data as referred to in Article 53(1)*".

5.7 Data use after opt-out

5.7.1 Legal Requirements by the Regulation

The opt-out prohibits the processing of identifiable personal electronic health data under any new permits/requests approved after opt-out declaration.

Temporal effect: the exercise of the right of opt-out by natural persons shall not affect the processing for secondary use of personal electronic health data relating to those natural persons pursuant to data permits or health data requests that were issued or approved before the natural persons exercised their right to opt out. In other words, the right to opt out does not have a retrospective effect: it only applies to processing operations approved after the opt-out has been exercised [Article 71(3)].

As discussed in Section 5.4 in relation to reconciliation delays and latency of secondary channels, the legal effect of an opt-out must be clearly linked to its registration in the relevant technical system. For the purposes of determining the temporal effect, an opt-out shall be considered effective from the moment it has been recorded in the relevant technical system that records all opt-out decisions so that the information is available to authorised users of the system (HDAB, DH).

The opt-out applies to new permits and decisions issued after the decision to opt out has been registered. The list of people who have opted out is not static; it changes each day as new decisions to opt-out or to reverse opt-outs are made. Verification of opt-out status does not need to be performed in real time and may be handled at an operational level (for example, through a daily cut-off mechanism or comparable technical solution). For this reason, HDABs will have to consider deploying technical systems (secure opt-out registry) to record opt-out decisions with sufficient functionality to retrieve the list of opted out persons as it existed the date a particular permit was issued.

Reversing an opt-out decision should act in the same manner. The reversal of opt-out decision produces legal effects from the moment it is recorded in the system. A person's data may therefore be processed in respect of permits and decisions issued after the reversal has been recorded.

It means, if the data of a natural person are made available pursuant to a permit issued and this person opts out on a day later than the day of issue of the permit, the content of the SPE will not change. Without this rule, which was made for policy/scientific reasons, and with a retroactive opt out right, the scientific integrity of results would be jeopardised, and it would be impossible to check the correctness of analyses.

Deceased persons and the opt-out: The scope of the EHDS extends to personal electronic health data relating to deceased persons, insofar as such data fall within the material scope of the EHDS Regulation. Accordingly, where a natural person has exercised the right to opt out during their lifetime, that opt-out should continue to produce legal effects after their death.

5.7.2 National discretion

It is important to add that using the opt-out from secondary use under the EHDS does not affect other reporting obligations, e.g. for health professionals.

Where a MS establishes an exception under Article 71(4), as explained in Section 5.2.1.2, the practical implementation must ensure traceability, time-stamping and transparency. HDABs and/or designated authorities should therefore ensure that the opt-out registry allows historical retrieval of status at the time of a permit decision.

This exception applies only to personal electronic health data held in a dataset accessible in or falling under the legislation of that MS. It is therefore important to emphasise about the conditions for application for electronic health data, that the Article 71 (4) (a-c) state, it must involve a public institution, be necessary for listed purposes, not obtainable otherwise, and include appropriate safeguards. While MS may define exceptions in accordance with Article 71(4), excessive divergence may undermine legal certainty and public trust. Transparency and coordination are therefore essential.

HDABs and/or designated national authorities should ensure a registry or functionally equivalent recording mechanism that supports time-stamping and historical retrieval of opt-out status as of the date of a permit/decision, in order to operationalise the non-retroactivity rule.

Additionally, the national authorities responsible for implementing the EHDS Regulation should inform citizens about the exceptions to the opt-out under certain secondary data use purposes with a strong link to the public interest to promote transparency and citizen trust. More recommendations about communication with citizens can be found in section 5.5. 'How to implement opt-out with regard to citizens' rights' of this guideline.

Deceased persons and the opt-out: The scope of the EHDS extends to personal electronic health data relating to deceased persons, insofar as such data fall within the material scope of the EHDS Regulation. Accordingly, the default legal position is that where a natural person has exercised the right to opt out during their lifetime, that opt-out should continue to produce legal effects after their death.

The continued application of the opt-out does not constitute the creation of a new right for deceased persons; rather, it reflects the underlying logic and continuity of the EHDS framework, which attaches legal effects to the exercise of the opt-out at the time it was recorded.

However, the EHDS regulation does not clearly harmonise the post-mortem effect of an opt-out, and national law may need to address this. Therefore, MS may establish clear national rules addressing the post-mortem effect of opt-out decisions, provided that transparency and legal certainty are ensured.

5.8 Data use after the revocation of opt-out

The exercise of the opt out right is reversible meaning that natural persons can reverse their opt-out decision any time and without providing any reason or justification.

The reversal takes effect for data permits and health data requests approved after the reversal has been registered. From that day on, the personal electronic health data of the natural person accessible and identifiable in a dataset can be included into new processing activities, provided that all other conditions under the EHDS Regulation are met. In practice,

it will apply to future data permits and decisions including ongoing data access applications and data requests under assessment.

5.9 Reaction to opt-out

National discretion

If designated by the MS, the HDAB may also act as a contact point, though this presupposes a role in managing opt-out decisions.

Responses to opt-out declarations must be lawful, minimal, and strictly in service of the individual's rights, not institutional convenience or persuasion. The aim must be to uphold informational self-determination without overburdening or alienating the data subject.

A further point of clarification concerns the relationship between pseudonymisation, anonymisation, and national responsibilities. In line with the EHDS Regulation, any transformation of personal electronic health data, whether pseudonymisation or anonymisation, takes place under the control of the MS before data are made available for cross-border secondary use. This ensures that identifiable data are not shared across borders unless a separate legal basis under national law applies.

Member States could clearly communicate this framework to maintain public trust and avoid misconceptions, particularly in systems where societal expectations around data protection are high. In addition, where Article 77(4) allows narrowly defined exceptions, MS should transparently describe the safeguards they apply, including which national authority is responsible for verifying that the conditions are met and for intervening if they are not.

In practice, natural persons may express their preferences regarding the use of their electronic health data in general terms, without distinguishing whether their request concerns the EHDS Regulation or the GDPR. Because both frameworks apply to the processing of electronic health data, and because Article 71 EHDS establishes a sector-specific opt-out that operates alongside, rather than replacing, existing GDPR rights, MS could provide clear guidance on how such general expressions of preference are to be interpreted and translated into the appropriate legal mechanisms.

The EHDS opt-out applies only to secondary-use permits issued under the EHDS framework, while research and processing activities outside the EHDS continue to rely on the GDPR and relevant national laws. The guideline's clarification that the GDPR right to object does not automatically trigger an EHDS opt-out, and vice versa, reflects this legal separation but may create practical challenges for individuals who are not familiar with the distinctions between regulatory regimes.

Any use of opt-out registry data beyond its original purpose, such as profiling, targeted outreach, or analytics, would risk breaching key GDPR principles, including purpose limitation and data minimisation, and would therefore be incompatible with the EHDS. The opt-out mechanism is designed to give individuals meaningful control over secondary use, so repurposing this data for re-engagement would not be permissible unless explicitly authorised by law and supported by an appropriate legal basis.

To avoid placing an undue burden on natural persons or data controllers, MS could ensure that information and support services help individuals understand how their preferences can

be exercised effectively under both frameworks, and that controllers have clear procedures for interpreting and implementing such requests consistently. At the same time, it is important to communicate that widespread opt-out may have unintended consequences for research quality, including reduced sample sizes, selection bias, and diminished representativeness, effects that are particularly acute in fields such as oncology, rare diseases, and public-health surveillance, where robust, diverse datasets are essential for scientific validity and equitable outcomes. Highlighting the societal benefits of responsible health-data sharing, while ensuring that individuals' rights are fully respected, can help maintain trust and support a balanced implementation of the EHDS.

6 Annexes

Annex number	Annex title
1	Methodology
2	Public consultation summary
3	User journey
4	Glossary
5	An overview of deliverables in TEHDAS2

Annex 1 – Methodology

This guideline assists HDABs in implementing the right of natural persons to opt out from the secondary use of their personal electronic health data pursuant to Article 71 of the EHDS Regulation. The drafting was carried out through a structured process incorporating initial input from the Task 8.1 group participants and regulatory analysis related to the opt-out mechanism. The contributors participated according to their commitments, ensuring a collaborative and thorough development process.

The structured work described below represents the first phase of delivering the draft guideline as a milestone under TEHDAS2 Task 8.1. It has been organised and implemented along the following main lines:

Desk research was performed by all contributors. During this process, relevant regulatory provisions, national approaches, technical considerations and best practices were collected from the participating MS, organisations, and related projects such as TEHDAS1 and the EHDS2 Pilot. Particular attention was given to the interpretation of Article 71 of EHDS, its interaction with GDPR principles, and the governance role of HDABs in operationalising opt-out mechanisms.

Working meetings – regular working meetings were conducted to discuss and outline the key components and structure of the guideline, address open interpretative questions, clarify the scope of national discretion, and identify implementation challenges likely to arise at MS level.

Drafting meetings – two drafting meetings were held by the major contributors in the final stage of the work to consolidate comments, refine legal interpretations, and finalise the structure and wording of the document.

Exchanges took place **with DG SANTE** services to gather feedback and support the consistency of the document with the EHDS Regulation. Those exchanges do not imply endorsement by the European Commission.

Alignment between related TEHDAS2 guidelines is ensured, as the present guideline has been prepared in close coordination with other deliverables developed under TEHDAS2. In particular, it has been aligned with the guideline for HDABs on implementing the obligation of notifying natural persons of significant findings from the secondary use of health data, which is also part of T8.1.

This coordination ensures conceptual consistency across TEHDAS2 deliverables, particularly in areas concerning governance responsibilities of HDABs, interaction with data holders, transparency duties, and safeguards under the EHDS framework.

For the next phase, this document underwent a formal public consultation process in alignment with the TEHDAS2 Handbook in order to gather structured stakeholder feedback, including from HDABs, national authorities, data holders, research organisations, and other relevant actors. Although this guideline is primarily addressed to HDABs and national implementing authorities, it may also serve as a reference point when structuring information duties toward citizens (as specified in Articles 58 and 71 of the EHDS Regulation).

The feedback obtained through consultations was systematically analysed and integrated into the final guideline version, ensuring the inclusion of legally robust and practically feasible recommendations within the defined scope of this guideline. Particular attention was paid to clarifying the distinction between the EHDS opt-out and the GDPR right to object, the limits of national discretion regarding granularity, the operational implications of reversibility, and the handling of exceptions under Article 71(4).

Ensuring interoperability across national opt-out mechanisms and related registry or portal solutions requires that all MS adopt a minimum set of technical, organisational, and governance capabilities. Achieving an appropriate level of coordination is essential for enabling consistent cross-border secondary use of electronic health data while respecting individuals' rights under Article 71.

The development of such capabilities cannot occur in isolation; it depends on structured collaboration and systematic feedback from stakeholders across all EU countries. For this reason, the preparation of this guideline and any further guiding developments relies on iterative consultation with national experts, HDAB representatives, data holders, data protection authorities, and other contributors from each MS. Their input is critical to identifying practical constraints, aligning legal interpretations, and ensuring that the recommended opt-out procedures can be implemented consistently across diverse national contexts while preserving both fundamental rights and the objectives of the European Health Data Space.

Annex 2 – Public consultation summary

A draft version of this document was in public consultation in November 2025. This document was commented in total for 85 times. The number of responses may contain some duplicates as there was no individual identification and verification required to respond to the surveys. Some respondents have also responded both from data holder's and data user's perspective. The responses came from 20 different countries from the EU countries and the European Economic Area countries. Responses from stakeholders based in Bulgaria (BG), Republic of Cyprus (CY), Estonia (EE), Greece (EL), Italy (IT), Latvia (LV), Lithuania (LT), Malta (MT), Poland (PL), Romania (RO), Slovakia (SK), and international organisations were largely missing. The respondents were primarily from three main types of organisations, listed in order of prevalence: public organisations, academic/research organisations, and private organisations.

I. Key gaps identified from public consultation:

1) Timelines: lack of clarity and limits of prescriptiveness

Many respondents noted that timelines and sequencing for implementation are not clearly defined, creating uncertainty for planning and coordination. They highlighted that the guideline cannot fully address this, as detailed timelines depend on alignment with the European Commission and MS. In particular, the EHDS introduces new mechanisms, such as the opt-out and new authorities, without precedent, and the Regulation provides only high-level milestones. Respondents indicated that further clarification on timelines will rely on future decisions during implementation.

2) Evaluation, monitoring, and correction mechanisms

Several respondents highlighted the absence of evaluation frameworks, monitoring indicators, enforcement mechanisms, and processes for learning and improving implementation. The guideline can only address these aspects conceptually, as concrete criteria and procedures depend on authorities, workflows, and operational realities that do not yet exist. Respondents noted that these mechanisms will need to be developed iteratively during implementation, in coordination with the Commission and MS, and informed by practical experience. Further clarification will depend on future decisions during implementation.

3) Level of detail: technical guidance, use cases, and impact on current activities

Stakeholders highlighted the need for more technical detail, practical workflows, examples, and explanations of national impacts. At this stage, such detail cannot be provided, as EHDS introduces new structures and processes without existing cases or systems. Hypothetical scenarios could go beyond the Regulation and pre-empt national choices. The guideline therefore remains high-level, with concrete guidance expected to emerge through implementation, pilots, and shared learning.

4) GDPR–EHDSR interplay: limits of analysis and appropriate referencing

Many respondents requested a more detailed analysis of the interaction between EHDS and GDPR. The guideline addresses this at a high level, but deeper legal interpretation is beyond its remit. Authoritative guidance comes from the European Data Protection Board and supervisory authorities. The guideline therefore refers to ongoing and future work by these bodies, recognising that this area will continue to evolve.

II. How the feedback was addressed in the revised guideline:

In response to the consultation feedback, the task group revised the guideline with a focus on clarification, structure, and proportionality, rather than expanding scope.

1) Timelines: lack of clarity and limits of prescriptiveness

In response to comments requesting clearer allocation of roles and decision-making responsibilities, the guideline was revised to:

- More explicitly describe the governance framework and obligations set out in the EHDS Regulation.
- Clarify the high-level process leading up to the involvement of data holders.
- State clearly that detailed operational responsibilities and workflows depend on national implementation arrangements, which vary significantly across MS.

Rather than prescribing uniform internal structures, the guideline now recommends that MS ensure transparency by publicly describing their national governance setup, including roles, responsibilities, and decision-making processes. The examples provided are explicitly hypothetical, as this is a new regulation and many processes and governing bodies have yet to define their activities and practical workflows. These examples are therefore illustrative only, helping MS explore possible approaches while fully respecting national competence and administrative diversity.

2) Evaluation, monitoring, and correction mechanisms

Stakeholders called for more detailed procedures for cross-border cases. In response, the guideline acknowledges that complex multi-country scenarios, particularly those involving shared datasets, will need to be addressed on a case-by-case basis once concrete situations arise.

The revised text clarifies that:

- The primary point of contact remains the HDAB that granted the data access permit.
- Cross-border questions may require coordination between relevant authorities depending on the specific circumstances.
- Practical arrangements will evolve with implementation of the EHDS framework, including through the HealthData@EU infrastructure.

The guideline therefore adopts a step-by-step and experience-based approach, recognising that it is not feasible to anticipate all possible cross-border configurations at this stage.

3) Level of detail: technical guidance, use cases, and impact on current activities

In light of requests for clearer timelines and monitoring mechanisms, the guideline now explicitly clarifies that:

- The binding deadline for implementation is March 2029, when the relevant provisions of Chapter IV and the infrastructure become applicable and the significant findings mechanism must be operational.
- No intermediate milestones are established at EU level.
- The detailed implementation method, internal sequencing, and supervision arrangements remain the responsibility of MS.

The revised text emphasises the regulatory deadline while clarifying the distribution of responsibilities between EU-level obligations and national implementation.

4) GDPR–EHDSR interplay: limits of analysis and appropriate referencing

Regarding comments on legalistic language and evaluation mechanisms, the guideline clarifies its scope and target audience. It underlines that the document is primarily addressed to MS, HDABs, and data holders, who operate within a legal-regulatory context.

- The level of technical and legal terminology reflects the need for alignment with the EHDS Regulation.
- The guideline represents a first implementation layer under the broader EHDS framework and provides a general and harmonised structure.

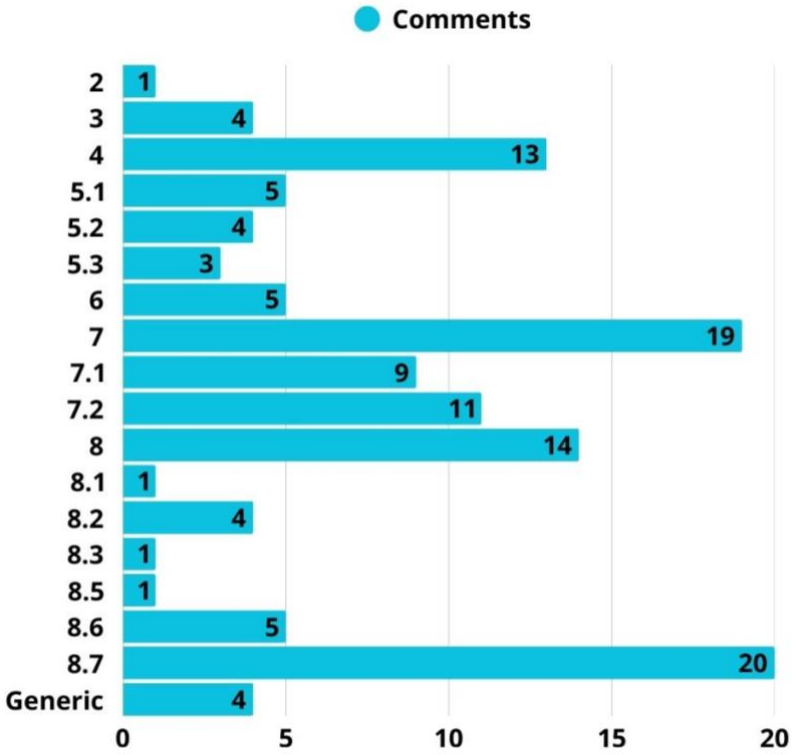
While the document maintains a strong technical level, it also clarifies its role as a foundational instrument. It acknowledges that further national-level impact assessments, communication, decision-making, and practical interpretation may still be required for different stakeholder groups. At the same time, the document calls for joint harmonisation and clarification efforts to avoid inconsistencies across countries.

III. Statistics of integrated comments:

During the processing of the consultation input, the 623 comments received were first allocated to the relevant chapters of the document. Where a single comment addressed multiple chapters, it was split accordingly and assigned new comment IDs. As a result, the total number of comment units increased to 729.

Subsequently, all comments were subjected to a triage process in which they were categorised as out of scope, not applicable, to be implemented, or requiring further discussion. This assessment resulted in 424 comments classified as not applicable or out of scope, representing 58.2% of the total, and 305 comments classified as to be implemented, representing 41.8%.

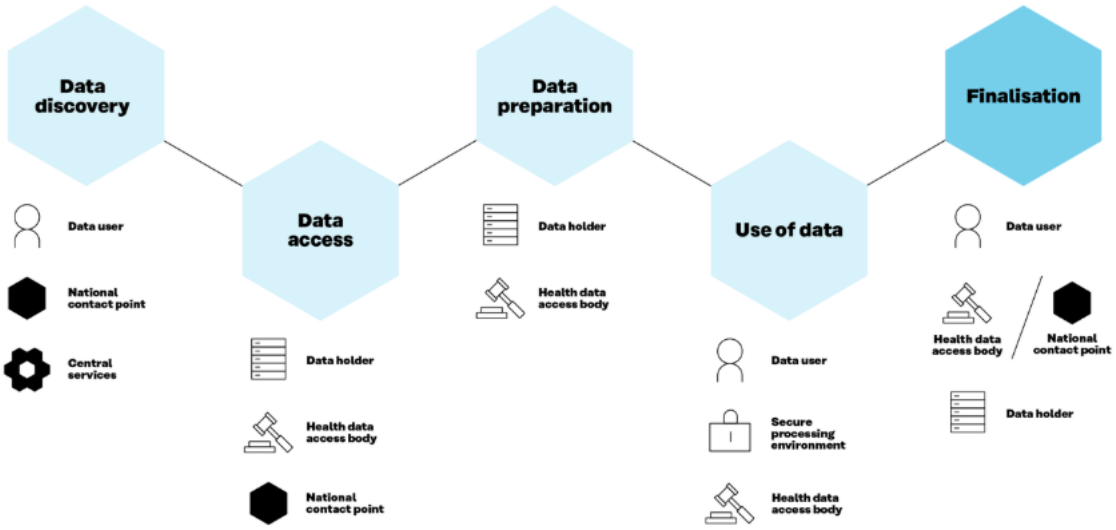
The comments marked for implementation were incorporated into the revised guideline. The distribution of comments by chapter is presented below.



Annex 3 – User journey

When a data user[5] 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)[6]. The user must complete the information required in the form, upload necessary documents, and provide justifications as needed.

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

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

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)[7] 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[8]. The duration of this phase is specified in the Regulation (Art 68(12)).

Finalisation

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

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

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

Annex 4 – Glossary

TERM	DEFINITION
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)
Benefit (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))
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 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)).

TERM	DEFINITION
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 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 & 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)(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)

TERM	DEFINITION
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.
Dataset description	A description in the form of metadata of the available datasets and their characteristics (EHDS Article (77(1))
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))
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.

TERM	DEFINITION
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))
Intermediation entity (Health data 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))

TERM	DEFINITION
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.
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 dataset catalogue	Making public, through electronic means: (i) a national dataset catalogue that includes details about the source and nature of electronic health data, in accordance with Articles 77, 78 and 80, and the conditions for making electronic health data available; (EHDS Article 57(1)(j)(i)).
National contact point (NPC)	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-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))

TERM	DEFINITION
Opt-out	Article 71 (1) EHDS Regulation states: "Natural persons shall have the right to opt out at any time, and without providing any reason, from the processing of personal electronic health data relating to them for secondary use under this Regulation. The exercise of that right shall be reversible."
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))
Pseudonymisation	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)
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.
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).
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))

TERM	DEFINITION
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)
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 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)
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.

Annex 5 – An overview of deliverables in TEHDAS2

D4.1 Guideline for Health Data Access Bodies on fees and penalties for non-compliance related to the EHDS Regulation

This guideline creates guidelines for fees and penalties for non-compliance to facilitate organisational implementation of the EHDS for Health Data Access Bodies (HDABs) and data holders in the EU. The guideline aims to support the convergence of fees and penalties practices across the EU while also reflecting diverse perspectives of involved stakeholders.

D4.2 Guideline for Health Data Access Bodies on collaboration with other parties

This document outlines collaboration models for the EHDS secondary use framework, addressing ethical governance, intellectual property protection, and the role of research infrastructures across EU Member States.

D4.3 Guideline for Health Data Access Bodies on international and third country access and transfer of electronic health data

This guideline serves as a practical legal and operational guidance to Health Data Access Bodies and other stakeholders on how to interpret and implement the EHDS rules governing international access to and transfer of electronic health data by applicants established in third countries or international organisations.

D5.1 Guideline for data holders on data description

This guidance helps health data holders comply with the EHDS Regulation by clarifying which electronic health datasets must be made available for secondary use and providing practical instructions for describing them using the HealthDCAT-AP common metadata model.

D5.2 Guideline for Health Data Access Bodies on minimum categories and limitations on the reuse of health data

This guideline reflects and do recommendations on allowed purposes and prohibited use according to EHDS.

D5.3 Technical specification for Health Data Access Bodies on the national metadata catalogue

The technical specification describes 4 main capabilities of the national Metadata catalogue Metadata input, Metadata management, Metadata output and Metadata access.

D5.4 Guideline for data enrichment for Health Data Access Bodies, data holder and data user

This guideline explains data enrichment approaches and best practices for consideration within the European Health Data Space framework.

D5.5 Guideline for data user navigating the catalogue

A user guide for discovering and evaluating health datasets available through the HealthData@EU Central Platform.

D6.1 Guideline for data holders on making personal and non-personal electronic health data available for reuse

This guideline provides guidance for data holders on how to prepare, structure, and make electronic health data (personal and non-personal) available for secondary use in line with EHDS requirements.

D6.2 Guideline for data users on good application and access practice

This document defines best practices for data users on how to apply for and obtain access to health data, including completing applications and complying with legal, ethical, and procedural requirements.

D6.3 Guideline for Health Data Access Bodies on the procedures and formats for data access

This guideline specifies procedures and standardised formats for Health Data Access Bodies to manage health data access applications, health data requests, data permits, health data request approvals and data handling processes under the EHDS.

D6.4 Data Access Application Management System (DAAMS) - Technical specification for health data access bodies

This guidance defines technical specifications for the Data Access Application Management System (DAAMS) to support interoperable, efficient, and harmonised processing of data access requests across Europe.

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

This guideline aims at helping data users to inform on how to use data in a secure processing environment (SPE) under the EHDS.

D7.2 Guideline for Health Data Access Bodies on data minimisation, pseudonymisation, anonymisation and synthetic data

This document helps HDABs manage data protection considerations and requirements under the EHDS, including hands-on examples.

D7.3 Technical specification for Health Data Access Bodies on the implementation of the common IT infrastructure

These technical specifications provide a policy-level overview and technical guidance to help Member States and Health Data Access Bodies connect to the secure, cross-border HealthData@EU infrastructure for the secondary use of health data.

D7.4 Technical specification for Health Data Access Bodies on the implementation of secure processing environments

These specifications define the core functional and security requirements for SPEs to enable the safe secondary use of health data across the EU. It provides a harmonised framework for Member States to align their high-level design choices with the legal obligations of the EHDS.

D7.5 Guideline for Health Data Access Bodies on linkage of health datasets

This document helps HDABs on various aspects regarding data linkage under the EHDS.

D8.1 Guideline for Health Data Access Bodies on implementing opt-out from the secondary use of health data

This guideline helps HDABs establish practical and legally compliant procedures for implementing individuals' opt-out rights within the EHDS secondary use framework.

D8.2 Guideline for Health Data Access Bodies on implementing the obligation of notifying the natural person on a significant finding from the secondary use of health data

This guidance helps HDABs manage the assessment and communication of clinically significant findings arising from.

D8.3 Guideline for Health Data Access Bodies on informing natural persons about the use of health data - "Citizen Information Point"

This guideline instructs HDABs on what, how and when to inform natural persons and the general public about the secondary use of health data.

D8.4 Guideline for data users on handling research outcomes

This document provides practical and legal guidance for secondary data users on how to identify, assess, and appropriately manage research outcomes within the EHDS framework.