



# **Guideline for Health Data Access Bodies on international and third country access and transfer of electronic health data**

TEHDAS2 – Second Joint Action Towards the European Health Data Space

27 April 2026

Co-funded by  
the European Union



## 0 Document info

### Disclaimer

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

### 0.1 Authors

Author(s)	Organisation
Cascini Fidelia	UCSC, Italy – Task leader
Valenzano Regina	UCSC, Italy
Arcuri Maria Anastasia	UCSC, Italy
Davidovics Krisztina	OKFŐ, Hungary
Jørgensen, Anne Sofie	Danish Health Data Authority, Denmark
Martin Ana Maria	MS-ES, Spain
Peolsson Michael	Swedish eHealth Agency, Sweden
Petho András	OKFŐ, Hungary
Schlünder Irene	TMF e.V. Germany
Sprengers Vincent	RIVM, the Netherlands
Talvard Dora	Digital Health Delegation, French Ministry of Health
Stuwe Louisa	Digital Health Delegation, French Ministry of Health
Chambon Juliette	Digital Health Delegation, French Ministry of Health
Zdenek Gütter	Ministry of Health, Czech Republic

### 0.2 Keywords

<b>Keywords</b>	TEHDAS2, Joint Action, Health Data, European Health Data Space
-----------------	----------------------------------------------------------------

### 0.3 Document history

Date	Version	Editor	Change	Status
07/11/2025	1.0	Regina Valenzano	Initial document creation	Draft
16/01/2026	2.0	Regina Valenzano	First draft	Draft
13/02/2026	3.0	Regina Valenzano	Second draft	Draft

07/03/2026	4.0	Fidelia Cascini	Final document for review	Deliverable
16/03/2026	5.0	Fidelia Cascini, Regina Valenzano	Integration of final comments	Deliverable
16/03/2026	6.0	Fidelia Cascini	Final reviewed document	Deliverable
26/04/2026		Fidelia Cascini	Integration of comments of the EC	Deliverable

Accepted in Project Steering Group on 27/04/2026

**Copyright Notice**

Copyright © 2026 TEHDAS2 Consortium Partners. All rights reserved. For more information on the project, please see [www.tehdas.eu](http://www.tehdas.eu).

## Contents

1 Executive summary.....	4
2 Introduction .....	5
3 Survey .....	7
3.1 Design process .....	7
3.1.1 Methodological principles .....	8
3.1.2 Expected outcomes .....	8
3.1.3 Structure of the questionnaire .....	8
3.2 Results of the survey .....	9
3.2.1 National governance frameworks.....	10
3.2.2 Technical, organisational and operational measures .....	10
3.2.3 Key challenges identified by the respondents.....	11
3.2.4 Contribution of the survey to this guideline .....	12
4 Scope of the guideline .....	13
5 Access application .....	14
5.1 Scenario 1: The third country/international organisation is an authorised participant....	15
5.1.1 Presentation of the provisions of Article 91(1)(a) combined with Article 75(5):.....	15
5.1.2 Assessment criteria .....	15
5.2 Reciprocity .....	17
5.2.1 Presentation of the provisions of Article 91(1)(b).....	17
5.2.2 Assessment criteria .....	18
6 EHDS provisions on data transfer and data storage.....	19
6.1 Transfer of non-personal electronic health data data .....	19
6.2 Transfer of personal electronic health data.....	19
6.3 EHDS provisions about storage of personal electronic health data by HDAB and SPE. .....	20
6. Interdependencies with other TEHDAS2 deliverables .....	21
6.4 Interdependencies with D4.1 - Guideline for fees and penalties .....	22
6.5 Interdependencies with D6.2 - Guideline for data users on good application and access practice.....	23
6.6 Interdependencies with D8.4 - “Data users’ duties regarding research outcomes” .....	23
6.6.1 Purposes for secondary use.....	24
6.6.2 Prohibited purposes for secondary use of electronic health data.....	25
7 Recommendations .....	26
Annexes .....	29
8 Annex 2 – Methodology .....	30
9 Annex 2: Data user’ journey .....	31
10 Annex 3 – Glossary.....	33
11 Annex 4 – Survey template.....	35
12 Annex 5 – Assessment criteria Scenario 2 – Reciprocity (further details).....	40

## 1 Executive summary

This deliverable provides guidance on the conditions under which electronic health data made available within the European Health Data Space (EHDS) may be accessed by applicants established in third countries or international organisations, and on the rules governing the international transfer of such data within the EHDS framework. In this regard, it has to be specified that the EHDS does not establish a standalone regime for international data transfers: for personal data, transfers remain governed by GDPR Chapter V. Developed within the TEHDAS2 Joint Action, the document analyses the legal framework introduced by the EHDS Regulation, particularly the mechanisms of authorised participation of a third country in HealthData@EU and access based on the principle of reciprocity, as well as the requirements applicable to transfers of personal and non-personal electronic health data. The guideline also examines the interaction between EHDS provisions, the General Data Protection Regulation (GDPR), and the Data Governance Act, taking into account the different roles of these instruments and the related hierarchy: GDPR prevails for personal data protection; EHDS provides sector-specific access/use rules; DGA relevance should be clearly justified to avoid overcomplication. The guideline highlights also the role of EHDS safeguards such as the Secure Processing Environments (SPEs) and other measures in ensuring the protection of sensitive health data. Drawing on insights collected through a survey of Member States and stakeholders, the deliverable identifies key governance challenges, including local differences in the rules' implementation, definitional uncertainties, and the absence of structured reciprocity frameworks. Based on this analysis, the document formulates practical recommendations for Health Data Access Bodies (HDABs) aimed at ensuring a consistent, secure, and transparent approach to international data access, while facilitating responsible global research collaboration and maintaining a high level of protection for EU citizens' health data within the EHDS framework.

## 2 Introduction

### **Advancing health data use in the European Health Union**

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

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

TEHDAS2 focuses on several critical aspects of health data use.

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

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

The development of the European Health Data Space (EHDS) represents a major step toward enabling the secure and trustworthy use of electronic health data across the European Union for research, innovation, policymaking, and public health purposes. By establishing a harmonised framework for the secondary use of electronic health data, the EHDS seeks to unlock the potential of health data while ensuring a high level of protection for individuals' fundamental rights, including privacy and data protection. Within this broader context, the question of access to and transfer of electronic health data involving third countries and international organisations, has become increasingly important. Health research, public health surveillance, and technological innovation often rely on international collaboration, which requires clear rules governing how actors outside the EU may access or process data originating from the EU. However, EHDS regulates access conditions to data within its framework only, while processing and transfers of personal data remain governed by GDPR

(Chapter V). This means that EHDS doesn't provides a complete regulatory framework for third-country data processing.

This guideline has been developed within the framework of the Second Joint Action Towards the European Health Data Space (TEHDAS2) and specifically contributes to Task 4.3 on international access to and transfer of electronic health data. Its objective is to support the interpretation and implementation of the EHDS regulation providing practical guidance to Health Data Access Bodies (HDABs) and other stakeholders in situations involving applicants/users established in third countries or international organisations. The document focuses mainly on the legal mechanisms introduced by the EHDS Regulation to regulate such access, including the authorised participant framework for third-country participation in HealthData@EU, as well as the rules governing transfers of personal and non-personal electronic health data in this context (i.e. this doesn't represent a general regime for international data access)

To facilitate responsible international cooperation while ensuring strong safeguards protecting sensitive health information, intellectual property, and trade secrets, also preventing unlawful access or misuse of European health data, the EHDS regulation introduces specific conditions under which applicants/users from third countries may obtain access to datasets made available through the EHDS infrastructure and clarifies the requirements governing cross-border data transfers.

International access to electronic health data within the EHDS framework is organised around two main legal pathways. The first pathway concerns access by applicants established in authorised third countries or international organisations that have been formally recognised by the European Commission as authorised participants in the HealthData@EU infrastructure. The second pathway is based on the principle of reciprocity only, whereby access may be granted to applicants from a third country that offers EU-based applicants' comparable access to health data. These mechanisms are intended to ensure fairness and mutual benefit in international data sharing while maintaining the regulatory standards established within the EU.

In addition to these access mechanisms, the EHDS Regulation also establishes supplementary safeguards relevant to the international use of electronic health data, without creating an autonomous regime for data transfers. Transfers of personal electronic health data remain governed by Chapter V of the General Data Protection Regulation (GDPR), while the EHDS introduces additional conditions linked to access and processing, including requirements relating to the use of Secure Processing Environments (SPEs) and specific provisions concerning non-personal electronic health data. These provisions are consistent with the need to ensure a high level of protection, given the sensitive nature of health data.

The present guideline therefore aims to support the understanding of the operational implications of these provisions by analysing the relevant legal framework, identifying key implementation challenges, and proposing practical considerations for authorities responsible for granting data access. It also builds on feedback gathered from Member States and stakeholders through a survey conducted as part of the TEHDAS2 activities. The document further explores the interaction between this topic and other TEHDAS2 deliverables addressing related aspects of the EHDS governance model, including guidance on fees and penalties (D4.1), good application practices for data users (D6.2), and the use of secure processing environments (M7.4).

By providing a structured overview of the applicable rules and their practical implementation, this guideline aims to support the consistent and coherent application of the EHDS framework across Member States, facilitate responsible international research collaboration, and reinforce trust in the governance of cross-border health data use within the European Health Data Space.

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

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

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

### 3 Survey

The survey was developed under Task 3 of Work Package 4 (WP4) of the TEHDAS2 Joint Action, with the objective of collecting insights on access by international organisations and third countries to, and transfers of, personal and non-personal electronic health data.

The purpose was to support the formulation of guidelines and recommendations for the implementation of the EHDS, focusing on the area of secondary use of health data.

The survey was distributed across three main networks:

- TEHDAS2 partner organisations
- Health Data Access Bodies (HDABs) Community of Practice<sup>i</sup>
- eHMSEG Legal Work Group<sup>ii</sup>

The selection ensured a broad and representative participation from entities directly engaged in data governance, legal compliance, and health data policy at national and EU levels.

#### 3.1 Design process

The design of the survey followed a structured and collaborative process that unfolded through several sequential phases. It began with a clear definition of objectives, during which the T4.3 team identified the key information needs associated with the implementation of the EHDS, paying particular attention to regulatory, legal, and operational dimensions. This was followed by a phase of desk research, which involved an examination of relevant EU legal frameworks, most notably the GDPR.

On the basis of this preparatory work, the team engaged in an iterative drafting process. Several draft versions of the questionnaire were produced, discussed, and progressively refined within T4.3. The refinement process was further enriched by consultations with legal experts from the European Commission, whose feedback contributed to enhancing the

accuracy and coherence of the instrument. Finally, the survey underwent a validation phase during which domain experts reviewed the questionnaire to ensure conceptual clarity, relevance in relation to policy needs, and consistency with established EU terminology in the fields of data protection and health data governance.

### **3.1.1 Methodological principles**

The development of the survey was guided by a set of methodological principles aimed at ensuring the robustness and usefulness of the collected data. A first guiding principle was relevance: each question was formulated to align with the central policy issues identified within T4.3 regarding international data access and governance. Clarity also played a crucial role, leading to the adoption of standardized terminology and the inclusion of a glossary based on definitions from the GDPR and the EHDS regulation.

Another fundamental principle was comparability. The questionnaire was structured to allow consistent comparison of practices across EU Member States, third countries, and international organizations. At the same time, the survey incorporated flexibility by providing open-ended response fields, enabling participants to describe country-specific or organization-specific circumstances in greater detail. Finally, the entire process was informed by strict ethical considerations: no personal data were collected beyond basic contact information for institutional communication purposes, and all responses are processed in compliance with EU data protection rules.

The survey was completed remotely by respondents via a dedicated tool (survey.eu).

### **3.1.2 Expected outcomes**

The data collected through the survey were expected to provide a comprehensive and comparative overview of the current models and practices adopted by EU Member States, third countries, and international organizations in relation to cross-border access to and transfer of health data. By mapping these approaches, the survey aimed to shed light on both common patterns and divergences that might influence the future implementation of the EHDS.

In addition to this comparative perspective, the survey was intended to identify the principal legal and operational challenges that arose in the context of international data exchanges. These challenges could concern, for example, differing interpretations of legal bases, variations in technical safeguards, or inconsistencies in national governance structures. Understanding these obstacles was essential for supporting a coherent and practical approach to cross-border data processing.

Ultimately, the findings served as an evidence base for the development of common guidelines / consistent approaches within the EHDS framework. By capturing the experiences and practices of a broad set of actors, the survey contributed to formulating recommendations that were both actionable and aligned with existing regulatory requirements.

### **3.1.3 Structure of the questionnaire**

The final version consists of eight sections, each addressing a specific thematic area:

- Objective of the survey

- Glossary (defining key terms such as personal data, non-personal data, third country, international organization)
- Respondent information
- General questions on national frameworks and practices
- Specific agreements involving international organizations or third countries
- Legal bases and consent mechanisms
- Security and technical measures adopted in such agreements
- Closing remarks and further information

This structure was designed to allow both qualitative and quantitative analysis, combining multiple-choice questions with open-ended responses.

### **3.2 Results of the survey**

The analysis of the data collected through the TEHDAS2 survey (WP4.3) provides valuable insights into the current European landscape concerning international access to and transfer of electronic health data. The results highlight the diversity of national governance frameworks, the variety of safeguards applied in practice, and the key challenges perceived in view of the implementation of the European Health Data Space (EHDS). The survey therefore played a crucial role in identifying areas where clearer guidance, harmonisation, and operational support are needed.

To address the complexity of the dataset, the survey analysis was conducted through a structured analytical framework combining data normalisation, thematic coding, and comparative assessment. Responses were first standardised to ensure comparability across countries and organisational types. A binary classification system was then applied to distinguish between countries with additional national regulatory frameworks and those relying on the GDPR only; the dimensions related to data access and data transfer were investigated accordingly. Within these categories, responses were further analysed by distinguishing between a) regulatory measures, referring to legal provisions or formal governance frameworks; and b) operational practices, referring to technical and organisational safeguards implemented in practice.

In addition, open-ended responses were analysed using thematic coding. Stakeholder concerns were grouped into five major categories: legal fragmentation, definitional uncertainty, operational costs, reciprocity mechanisms, and governance responsibilities.

Finally, a comparative analysis was carried out to identify discrepancies between declared regulatory frameworks and actual operational practices. This allowed the identification of “de facto governance” systems and the recognition of best practices, such as the Norwegian model, which combines a robust legal framework with advanced technical safeguards.

### 3.2.1 National governance frameworks

One of the primary objectives of the survey was to assess whether Member States already operate regulatory frameworks or infrastructures governing access to health data by third-country entities or international organisations.

The responses reveal two broad categories of national approaches: 1) countries with additional regulatory provisions beyond the GDPR and 2) Countries relying on the GDPR framework only.

#### 1) Countries with additional regulatory provisions beyond the GDPR.

A limited number of countries reported the existence of additional legal frameworks regulating international data access. For example:

- Portugal refers to Article 22 of Law 58/2019, which introduces additional safeguards for international data transfers.
- France relies on provisions within the Public Health Code combined with the Health Data Hosting (HDS) certification scheme.
- Norway operates under the Health Registry Act and the Health Research Act, which provide structured governance mechanisms for data access.
- Germany implements specific technical guidelines such as the System of Hospitals for Innovation in Pediatrics – Medical Devices (SHIP-med) framework, even if they are not widely recognised as a national regulatory framework.

These systems demonstrate a higher degree of institutionalised governance and clearer procedural rules for international data access.

#### 2) Countries relying on the GDPR framework.

A larger group of countries — including Croatia, Cyprus, Czech Republic, Finland, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Slovakia, Spain, Sweden — reported that they have not adopted specific national legislation beyond the GDPR. In these cases, international data access is governed through the general data protection framework and ad hoc institutional practices.

The survey therefore highlights that the EHDS Regulation, is expected to contribute to a more harmonised governance model across Member States and reducing the current fragmentation in national approaches.

### 3.2.2 Technical, organisational and operational measures

The survey revealed that many Member States apply practical safeguards and operational measures. These practices can be analytically distinguished into access conditions—aligned with the emerging logic of the EHDS—and international data transfer safeguards under Chapter V GDPR. With regard to access conditions (EHDS-like practices), several countries have already implemented structured controls governing access to health data. Examples include Portugal (public interest tests and formal validation procedures before granting access), France (certified health data hosting, localisation of data within the EU, and

prioritisation of remote access over physical data transfers), Norway (strict encryption requirements, local key management systems, and comprehensive logging to ensure traceability), Germany (secure download protocols and interoperability standards).

In parallel, other countries rely on GDPR chapter V safeguards, using operational practices such as: Standard Contractual Clauses <sup>iii</sup> (Spain, Luxembourg, Slovakia, Italy, Finland, Sweden); Transfer Impact Assessments (TIA) to evaluate risks related to international data transfers (Ireland); technical/operational restrictions such as the provision of aggregate statistics only or geographical access limitations to the EU/EEA (Lithuania, Czech Republic); case-by-case governance models (Cyprus, Croatia, Netherlands); constitutional or national security reviews for sensitive data transfers (Hungary).

These findings illustrate that several Member States already implement additional safeguards aimed at protecting sensitive health data. In fact, an important analytical improvement emerging from the survey is the identification of situations where countries formally reported the absence of additional regulations but nonetheless operate structured governance practices (“de facto governance” practices). For example, Ireland and the Czech Republic indicated that no additional national legislation exists beyond the GDPR: both countries implement strict operational procedures, including Transfer Impact Assessments and geographical restrictions on data transfers according to EDPB guidance for applying GDPR transfer rules.

Consequently, many Member States already implement structured operational safeguards—such as localisation, Transfer Impact Assessments, and access restrictions—even in the absence of additional national legislation beyond the GDPR. This demonstrates that practical governance often precedes formal regulation, allowing the EHDS framework to build on these established practices while introducing a more harmonised and consistent legal structure across Member States.

### 3.2.3 Key challenges identified by the respondents

The survey also revealed several challenges that respondents consider particularly relevant for the future implementation of the EHDS. These can be summarised like that:

- **Legal and regulatory fragmentation.** Several respondents noted that national rules governing access to health data vary significantly between Member States. Countries such as Portugal, Croatia and the Czech Republic highlighted the lack of harmonised procedures for cross-border data access.
- **Complex interaction between EU legal frameworks.** Respondents pointed out the difficulty of interpreting the interaction between the GDPR and the EHDS Regulation, particularly in areas where the EHDS leaves room for national implementation measures.
- **Absence of structured reciprocity frameworks.** Respondents emphasised that, at present – prior to the application of the EHDS, Article 91(2) - there is no established EU-wide framework governing reciprocity with third countries for health data access.
- **Definitional uncertainties.** Several respondents indicated difficulties in distinguishing between anonymised and personal data in practice, which can affect the legal classification of datasets and the applicable safeguards.

- **Governance and liability concerns.** Questions were raised regarding the allocation of responsibility when multiple institutions or countries are involved in cross-border data access requests.
- **Technical and operational costs.** Implementing the necessary technical safeguards—such as cybersecurity infrastructure, secure processing environments, and interoperability standards—was identified as a significant operational challenge.

### 3.2.4 Contribution of the survey to this guideline

Overall, the survey significantly improved the understanding of how international access to health data is currently managed across Europe. By identifying both regulatory gaps and operational practices, the survey provided an evidence base for the development of practical recommendations within this guideline.

The findings highlight the need for:

- clearer governance frameworks for international data access;
- harmonised safeguards across Member States;
- clarity on how reciprocity considerations may be assessed within the EHDS framework;
- guidance on the interaction between EHDS provisions and existing EU legal frameworks.

These insights directly informed the recommendations presented in this guideline and contributed to ensuring that they reflect the practical realities faced by national authorities and data governance stakeholders. In particular, the TEHDAS2 survey has provided an important empirical basis for the development of these guideline recommendations on international access to and transfer of electronic health data. By gathering inputs from national authorities and legal experts interviewed, it offered a comparative overview of existing governance models, safeguards, and challenges related to cross-border health data access. The survey highlights two main regulatory approaches to third-country access to health data: on the one hand, the application of the GDPR complemented by additional technical and organisational safeguards; and, on the other, the existence in some jurisdictions of additional national legislation governing access by third countries. While some Member States rely primarily on general data protection rules and institutional practices, others have developed more tailored legal frameworks. This diversity underscores the need for clearer and more harmonised guidance within the EHDS framework.

Further, the survey identified a wide range of technical and organisational safeguards already implemented in practice (such as secure data hosting, encryption, logging systems, remote access environments, and transfer impact assessments), which have informed the guideline's recommendations to adopt structured security and governance safeguards for international data access.

Where international access involves transfers of personal data, the requirements of Chapter V of the GDPR remain applicable.

The respondents pointed also to legal and interpretative uncertainties, particularly regarding the interaction between the GDPR and the EHDS Regulation, as well as the distinction between anonymised and pseudonymised data. This contributed to the guideline's efforts to clarify the applicable legal framework for international data access and transfers. In addition, the survey has identified operational and governance challenges, including questions related to liability, institutional responsibilities, and the technical costs associated with secure data sharing infrastructures. Overall, the survey has strengthened the guideline by ensuring that its recommendations are grounded in existing practices and stakeholder experiences, thereby supporting a more coherent and practical implementation of data access rules within the EHDS.

## 4 Scope of the guideline

The focus of this guideline is the access and transfer of electronic health data to international actors, such as third countries and international organisations whether they have become authorised participants in HealthData@EU or not. Access and transfer of electronic health data refer to the secondary use within the EHDS framework, according to the purposes listed in Article 53 of the EHDS Regulation. Consequently, it does not cover primary use of electronic health data.

The following Articles of the EHDS Regulation are considered:

- Article 91 (health data access applications and health data requests from third countries),
- Article 75(5) (conditions for third countries and international organisations to become authorised participants),
- Article 87 (storage of personal electronic health data by health data access bodies and secure processing environments),
- Article 88 (third-country transfer of non-personal electronic data),
- Article 90 (additional conditions for transfer of personal electronic health data to a third country or an international organisation).

All these Articles will enter into application on 26 March 2027, except Article 75(5) that will be applicable as of 26 March 2035.

### Topics excluded from the scope of this guideline:

- This guideline does not cover Article 89 of the EHDS Regulation, concerning international governmental access to non-personal electronic health data.
- This guideline does not cover the specific case of ERICs and EDICs.

ERICs and EDICs are entities established under EU law, even if they may include third-country members. As such, they should not be treated as international organisations under Article 75(5).

For ERICs and EDICs, the relevant legal basis is Article 75(4), which applies to entities established under EU law. In detail, health-related research infrastructures (or similar

infrastructures) whose functioning is based on Union law and which provide support for the use of electronic health data for research, policymaking, statistical, patient safety or regulatory purposes may become authorised participants in HealthData@EU and connect to it. Consequently: Article 75(4), rather than Article 75(5), would govern their potential participation to Healthdata@EU and the applicable date of application would be 2029, in line with Article 75(4).

ERICs and EDICs may raise complex legal questions (e.g. resulting from the membership of third-country entities, privileges and immunities), which cannot be fully resolved within the scope of Guideline 4.3. Questions related to privileges and immunities may require case-by-case assessment or future clarification (e.g. through implementing acts or additional guidance).

The scenarios to be considered in this guideline are the following:

- Scenario 1: access by an applicant from a third country that is an authorised participant (Article 91(1)(a) and Art.75(5))
- Scenario 2: access by an applicant from a third country based solely on reciprocity (Article 91(1)(b))

There are three sub-scenarios for each scenario:

- a) the data access involves transfer of personal data, including remote access to the data in the SPE which may amount to a data transfer (=Article 90)
- b) the data access involves transfer of non-personal data (=Article 88)
- c) the data access involves storage in an SPE located outside of the EU (= exception of Article 87(2)).

The rules governing third country access allow protection of sensitive health data concerning EU citizens. It also allows protection of data that is subject to intellectual property rights or trade secrets against unlawful access by third countries.

## 5 Access application

The EHDS Regulation provides for two ways of accessing EHDS data by a health data applicant established in a third country or being an international organisation:

- (1) the third country/international organisation is **an authorised participant** (Art. 91(1)(a) in conjunction with Art. 75(5) EHDS Reg)
- (2) **access based on the reciprocity principle**: the third country/international organisation has been recognised as granting health data applicants from the EU equal access to electronic health data of that third country/international organisation (Art. 91(1)(b)).

While scenario 1 is more demanding, it offers structural incentives compared to scenario 2, notably:

- potential integration with HealthData@EU, including catalogue interoperability;

- a more seamless and stable framework for data access for users from that third country.

Scenario 2, by contrast, provides standing for applicants from third countries to request access, but does not entail infrastructure integration and remains more limited in scope.

Recognition of authorised third countries under Article 75(5) will only be possible as of 2035. In the initial years of the EHDS, third-country access will therefore rely on the reciprocity-based mechanism under Article 91(1)(b). There is not yet any precise timeline available for the adoption of implementing acts on reciprocity under Article 91(1)(b).

## **5.1 Scenario 1: The third country/international organisation is an authorised participant**

### **5.1.1 Presentation of the provisions of Article 91(1)(a) combined with Article 75(5):**

In accordance with Article 75(5), the EU Commission is empowered to, by means of an implementing act, based on the criteria set out in the same Article, grant a third country or international organisation the status of an authorised participant in HealthData@EU (Article 75(5)EHDS Reg). Third countries or international organization may become authorised participants in HealthData@EU if the following conditions are met:

- a national contact point for secondary use of a third country or a system established at international level by an international organisation is compliant with the requirements of HealthData@EU for the purposes of secondary use of health data,
- the third country is compliant with the rules of EHDS Chapter IV,
- and provides access to health data users located in the Union to the electronic health data it has access to, on terms and conditions equivalent to those of HealthData@EU.

Transfers of personal data remain subject to Chapter V of Regulation (EU) 2016/679.

The assessment by the Commission will have to include a verification of compliance with the above-mentioned legal, organisational, technical and security requirements, including with the requirements for secure processing environments provided for in Article 73.

Article 75(5) EHDS Regulation applies from 26 March 2035 (see Article 105 EHDS Reg.). Therefore, becoming an authorised participant will not be possible before that date while the Article 91(1)(b) route is available earlier (see section 5.2 below)

### **5.1.2 Assessment criteria**

**1st criterion: The Commission has to assess whether a national contact point for secondary use of a third country or a system established at international level by an international organisation is compliant with the requirements of Chapter IV of the EHDS Regulation for the purposes of secondary use of health data.**

A third country applying to be an authorised participant must demonstrate that it has designated a national contact point for secondary use, meeting all the requirements set out in Article 75.

A national contact point corresponds to an organisational and technical gateway, enabling and responsible for making available electronic health data for secondary use in a cross-border context (Article 75(1)).

Notably, the national contact point shall have the technical capability to connect to HealthData@EU and act as joint controller of the processing operations carried out in the infrastructure. The requirements are setting out by the Commission by means of implementing acts, by 26 March 2027 (Article 75(12)):

- the conditions and compliance checks required to be able to join and remain connected to HealthData@EU and conditions for temporary disconnection or definitive exclusion from HealthData@EU, including specific provisions for cases of serious misconduct or repeated infringements;
- the minimum criteria that need to be met by the national contact points for secondary use and the authorised participants in HealthData@EU;
- the responsibilities of the controllers and processors participating in HealthData@EU.
- the responsibilities of the controllers and processors for the secure processing environment managed by the Commission;
- common specifications for the architecture of HealthData@EU and for its interoperability with other common European data spaces.

The Central Platform HealthData@EU hosts the European dataset catalogue, which contains national dataset catalogues, and catalogues of authorised participants, such as research infrastructures, and importantly, international organizations and third countries. It enables the submission of data access and data request applications for review by HDABs. HealthData@EU includes also an IT tool, as part of the infrastructure, aimed at supporting and making transparent to HDABs the enforcement measures as periodic penalty payments, the revoking of data permits and exclusions (Art. 63(7)). Third countries involved as authorised participants are encouraged to regularly consult platform updates, as the system is released in iterative versions. The HealthData@EU Central Platform and its infrastructure are open-source, National Contact points participate in HealthData@EU, which is the cross-border infrastructure for secondary use (Article 75(3)).

Descriptions in the national dataset catalogue, health data access applications and health data requests and all communications between health data user and entities involved in the processes of making data available in third countries shall be possible in at least one official language of the EU.

Further details will be made available through implementing acts of the EHDS regulation.

**2nd criterion: The Commission has to assess whether the third country or international organisation is compliant with the rules of EHDS Chapter IV, including:**

- The minimum categories of electronic health data made available by data holders (Article 51);
- The rules governing intellectual property and trade secrets (Article 52);

- The purposes for which electronic health data can be processed for secondary use (Article 53);
- The prohibited purposes for which electronic health data cannot be processed for secondary use such as (Article 54).
- The governance for secondary use, including the designation of one or more health data access bodies meeting the requirements set out in Article 55 and performing the tasks and complying with the obligations listed in Articles 57 to 59, 63 and 64;
- The duties of data holders (Article 60) and of data users (Article 61);
- The rules governing fees (Article 62);
- The conditions and empowerments for accessing health data for secondary use, including the templates to support access (Art. 70), the requirements concerning HealthData@EU infrastructure (Art. 75), the principle of minimisation and purpose limitation (Article 66); health data access applications (Article 67); data permit (Article 68); health data request (Article 69); rules governing trusted data holders (Article 72); controllership (Article 74);
- The mechanism to opt out (Article 71);
- Secure processing environment (Article 73);
- Rules governing health data quality and utility for secondary use (Article 77 and 78);
- Rules on complaints (Article 81).

Adopted implementing acts that provide details to various provisions of the EHDS Regulation Chapter IV are also applicable.

## 5.2 Reciprocity

### 5.2.1 Presentation of the provisions of Article 91(1)(b)

Article 91(1)(b) provides for a reciprocity requirement as a condition for access to electronic health data: it has to be demonstrated that the third country where the applicant is established allows health data applicants from the EU access to electronic health data in that third country under conditions that are not more restrictive than those provided for in the EHDS Regulation.

Article 91(2) specifies that it is by way of an implementing Act that the Commission will determine that a third country meets the requirement set out in paragraph 1(b).

Recital 94 which elaborates on the reciprocity condition specifies that the safeguards provided in the third country should be taken into account:

- a third country can access EU health data only if it grants equivalent access to its own data for EU users;
- the European Commission must formally confirm this through an implementing act;

- the Commission is responsible for monitoring and periodically reviewing these arrangements;
- the Commission can revoke the authorization if a country no longer provides equivalent access.

Accordingly, both the conditions of access by data users and the safeguards for data users should be equivalent (i.e. “not more restrictive than those provided for in this Regulation”), but not necessarily identical to those in the EU to meet the reciprocity requirement of Article 91(1)(b).

### 5.2.2 Assessment criteria

The assessment criteria required for reciprocity shall, in line with Article 91, focus on ensuring that third countries provide access to electronic health data under conditions -reciprocity conditions - that are not more restrictive than those applicable within the EHDS. These criteria shall include the following non-exhaustive elements (more details are available in Annex 2):

- general requirements ensuring that third countries datasets are discoverable, accessible, interoperable, reusable (FAIR principles);
- standardized metadata, stored in searchable catalogues available in the third country and accessible through transparent procedures;
- guarantees of data quality, equivalent traceability and documentation ensured by the third country;
- requirements and safeguards ensuring that EU datasets are subject to equivalent standards of secure management (including IP rights and trade secret safeguards);
- secure authentication mechanisms, clear licensing conditions, and the use of common data standards.

The objective is not to require identical regulatory structures, but to ensure functional equivalence in data access conditions, so that EU-based applicants are not placed at a disadvantage compared with applicants operating within the EHDS system. Additional checks, coordination, and potential costs may apply.

Third Countries are expected to respect reciprocity mechanisms also regarding purposes for which electronic health data can be processed for secondary use (Art.53) and prohibited purposes for which electronic health data cannot be processed for secondary use (Article 54).

The reciprocity mechanisms is also referred to fees and penalties, process and timeframe for data access: health data holders from the third country shall put the requested electronic health data at the disposal of the HDAB within a reasonable time and no later than three months from the receipt of the request by the HDAB. In justified cases, the HDAB may extend that period by a maximum of three months.

## 6 EHDS provisions on data transfer and data storage

The EHDS Regulations deals with two different transfers scenarios:

1. transfer of non-personal data in Article 88
2. transfer of personal data in Article 90

These Articles must be read in conjunction with horizontal EU data protection and data governance law, i.e. respectively with the Data Governance Act and the GDPR.

### 6.1 Transfer of non-personal electronic health data data

Article 88 EHDS Reg sets out conditions for transfer of non-personal electronic health data, to a data user in a third country, an authorised participant in a third country or an international organisation.

Article 88 applies where the following cumulative conditions are met:

- data are based on a natural person's electronic health data falling within one of the categories referred to in Article 51 of this Regulation,
- data are being considered as non-personal within the EU, and
- data are made available to a user in a third country, an authorised participant in a third country or an international organisation.

Then the data at stake shall be deemed highly sensitive within the meaning of Article 5(13) of Regulation (EU) 2022/868 (i.e. the Data Governance Act) where the transfer of such non-personal electronic data to third countries presents a risk of re-identification through means going beyond those reasonably likely to be used.

In particular, inter alia, the following aspects have to be considered:

- the limited number of natural persons to whom those data relate,
- the fact that they are geographically scattered,
- or the technological developments expected soon.

The protective measures for these categories of data will be detailed by means of a delegated act referred to in Article 5(13) of the Data Governance Act.

### 6.2 Transfer of personal electronic health data

According to Article 90, transfer of personal electronic health data to a third country or an international organisation shall comply with the provisions of Chapter V of the GDPR.

This Article recalls the possibility for Member States to maintain or introduce further conditions on international access to, and transfer of, personal electronic health data, including limitations, in accordance with Article 9(4) of the GDPR.

The scenarios for transfer of personal that can occur in practice are presented below:

#### **a) Remote access to personal data via an EU-based SPE**

Remote access by a third-country user to personal data hosted in a secure processing environment (SPE) operated by an EU Member State or by the Commission may qualify as a transfer of personal data under the GDPR, depending on the concrete circumstances and the design of the SPE, and what information is visible to the health data user.

Where such remote access qualifies as a transfer, the applicable GDPR requirements for transfers to third countries apply.

#### **b) EHDS SPE located in a third country**

The requirements of Article 73 EHDS Regulation and its related implementing act (Based on the TEHDAS2 Guideline D7.4. Technical specification for HDABs on the implementation of Secure processing environment) apply also for the third country hosting the EHDS SPE. An EHDS SPE that just happens to be hosted in a third country has the same requirements as a SPE in the EU. The usage of any SPE located outside the EU should be subject to the compliance check of those SPE with the technical and functional requirements defined in Article 73 (Related Implementing act, for more details see section 6 on Interdependencies with other TEHDAS2 deliverables).

Once the SPE located outside the EU is compliant with the related implementing act, the actual usage of the data should follow the TEHDAS2 Guideline D7.1 Guideline on how to use data in a secure processing environment (for more details see section 6 on Interdependencies with other TEHDAS2 deliverables.).

#### **c) Other scenarios of personal data transfer**

Personal data must not be extracted from SPEs. Outputs made available to data users must be anonymised or otherwise non-personal, in accordance with the EHDS Regulation. Consequently, beyond remote access scenarios and SPE location considerations, no additional systematic personal data transfer scenarios are foreseen under the EHDS framework.

According to Art. 61 EHDS, health data users must not identify or try to identify the individuals whose electronic health data they access through a permit, request, or authorised access in HealthData@EU. Further, when processing electronic health data within the SPE referred to in Article 73, health data users shall not provide access to the electronic health data, or make those data available, to third parties not mentioned in the data permit.

### **6.3 EHDS provisions about storage of personal electronic health data by HDAB and SPE.**

Article 87 provides, as a matter of principle, that HDABs, trusted health data holders and the Union health data access service shall store and process personal electronic health data in the Union when performing pseudonymisation, anonymisation and any other personal data processing operations through SPEs or through HealthData@EU. That requirement shall apply to any entity performing those tasks on behalf of such bodies, holders, or services.

By way of exception, the data may be stored and processed in a third country, or a territory or one or more specified sectors within that third country, where such country, territory or sector is covered by an adequacy decision adopted pursuant to Article 45 of the GDPR. This is more restrictive than chapter V GDPR as it can only be processed/stored by adequacy decision countries meaning that other transfer mechanisms are excluded. (The aim of this storage requirement is to ensure a high level of data protection, for a large volume of particularly sensitive data, concerning the health of European citizens. This storage obligation is without prejudice to data transfers for other purposes than data hosting and as long as they comply with the relevant provisions of the GDPR.

As explained in recital 93:

*« In order to ensure the full integrity and confidentiality of personal electronic health data under this Regulation, to guarantee a particularly high level of protection and security, and to reduce the risk of unlawful access to those personal electronic health data, this Regulation allows Member States to require that personal electronic health data be stored and processed solely within the Union for the purpose of carrying out the tasks provided for in this Regulation, unless an adequacy decision adopted pursuant to Article 45 of Regulation (EU) 2016/679 applies. »*

Thus, Article 87 establishes a general rule that HDABs, trusted data holders, and the Union health data access service must store and process personal electronic health data within the EU. This includes operations like pseudonymisation, anonymisation, and other processing, which must occur in SPEs or via HealthData@EU. The rule also applies to third parties acting on their behalf. This rule is subject to the exception provided for adequacy decisions under Article 45 GDPR (ensuring an equivalent level of data protection).

Notably, the EHDS Regulation does not prevent Member States from relying on an SPE provider that is not based in the EU, provided that the SPE itself is located within the EU or in a country that benefits from an adequacy decision.

Member States can however decide to impose specific requirements at the national level, to avoid such scenario. Indeed, in application of Article 90 of the EHDS Regulation, Member States can maintain or introduce further conditions on international access to, and transfer of, personal electronic health data, including limitations, in accordance with Article 9(4) of the GDPR.

## **6. Interdependencies with other TEHDAS2 deliverables**

The analysis will explore how the fee structures (D4.1), secure processing environment requirements (D7.1), data user good application (D6.2) and data user duties (D8.3) align with the unique challenges posed by cross-border and international data transfers. Regarding the interdependencies with other TEHDAS2 deliverables, these will be integrated after the public consultation process (in particular, deliverables from wave 2 on datasets, metadata, DAAMS).

## 6.4 Interdependencies with D4.1 - Guideline for fees and penalties

Deliverable D4.1 on fees and penalties is closely interconnected with the analysis carried out under Task 4.3 concerning international access to and transfer of electronic health data. Cross-border and third-country data access scenarios introduce specific legal, technical and governance complexities that may significantly affect the structure and justification of applicable fees.

First, international data transfers may generate additional administrative and compliance costs. These include the assessment of GDPR Chapter V requirements, the verification of adequacy decisions or appropriate safeguards, the conduct of transfer impact assessments where necessary, and the evaluation of national constitutional or security constraints. As identified through the survey responses, some Member States foresee enhanced scrutiny in cases involving third-country entities. Such additional procedural layers may justify differentiated cost-compensation agreements under D4.1.

Second, secure processing environments and enhanced technical safeguards may require higher operational expenditure when international access is involved. Where remote access infrastructures, encryption key management systems, traceability mechanisms or controlled access platforms must be reinforced to mitigate risks associated with extra-EU transfers, fees may need to reflect these additional security burdens in a proportionate manner.

Third, reciprocity concerns may shape the economic aspects of access. Where no formal reciprocity arrangements exist with certain third countries, imbalanced obligations or constraints in enforcement can arise. It may therefore be necessary to assess whether differentiated fee structures are justified in cases where equivalent access conditions are not ensured. Fourth, penalties for misuse or non-compliance acquire particular relevance in international contexts. Enforcement challenges outside the EU/EEA may reduce the practical deterrent effect of administrative sanctions. The interaction between D4.1 and Task 4.3 therefore highlights the importance of designing penalty frameworks that remain effective even when data users are established in third countries.

Overall, the alignment between D4.1 and Task 4.3 requires ensuring that fee structures remain:

- Cost-based and proportionate;
- Non-discriminatory within the EU internal market;
- Transparent in relation to additional compliance and security burdens;
- Consistent with the objectives of the EHDS framework, including facilitating secondary use while safeguarding fundamental rights.

Further refinement of this interdependency will take place following the public consultation phase and in coordination with other Wave 2 deliverables.

## **6.5 Interdependencies with D6.2 - Guideline for data users on good application and access practice**

D6.2 Guideline for data users on good application and access practice – describes how applicants can obtain access to electronic health data for secondary use under EHDS. The guideline first distinguishes between two types of applications:

- Data access application: Access to anonymised or pseudonymised individual-level health data in an SPE.
- Data request: Access to anonymised, aggregated statistics only – no access to raw or individual-level data.

The guideline further outlines the complete process from choosing the correct application pathway, preparing the required documentation, completing the application form, understanding assessment steps and timelines, to working with data in an SPE. It also unfolds the allowed and prohibited purposes for secondary use as well as the obligations that apply once access has been granted.

The guideline states that any natural or legal person in the EU/EEA is eligible to apply. In addition, entities in third countries may apply only under specific conditions:

- Reciprocity (Art. 91(2)): The third country must be recognised by the EU as providing reciprocal access for EU-based applicants
- Authorised participants in HealthData@EU (Art. 75(5)): The third country may obtain authorised participant status within the HealthData@EU infrastructure.

These conditions are briefly introduced in D6.2 and further detailed in this guideline D4.3.

It is stated in D6.2 that recognition under Article 91(2) or designation as an authorised participant under Article 75(5) applies at the country level, not to individual organisations. This means that entities in a third country cannot gain access on their own – the entire country must first be formally recognised by the EU before any organisation established there becomes eligible to apply under the EHDS framework. Further, it would be possible to recognise the third country with limited scope (if e.g. a third country would only make EHRs available, but not the other Art. 51 categories - then we could have them join / be recognised as reciprocal with that limited scope). Further details regarding the designation (including timing) are available in the guideline D6.2).

If a third country is formally recognised for reciprocal access or becomes an authorised participant in HealthData@EU, then the same EHDS procedures, rules, obligations, and application workflows described in D6.2 apply to them as to EU/EEA applicants.

## **6.6 Interdependencies with D8.4 - “Data users’ duties regarding research outcomes”**

The comparison will focus on how data user duties differ when accessing and transferring data across borders, particularly in third-country contexts where different legal frameworks apply.

As established previously, the EHDS Regulation sets out two main scenarios for third-country access under the EHDS regime:

- Scenario 1: access by an applicant from an authorised third country. Under this scenario, a third country or international organisation may be granted authorised participant status if it is formally recognised by the European Commission through an implementing act, based on third country's national contact point for secondary use, full compliance with EHDS Chapter IV, and provide health data on terms and conditions equivalent to those of HealthData@EU (Article 91(1)(a) in conjunction with Article 75(5)).
- Scenario 2: access based on reciprocity. This requires that the third country where the applicant is established grants EU applicants access to electronic health data under conditions that are not more restrictive than those set out in the EHDS Regulation (Article 91(1)(b)).

With regards to the handling of research outcomes, third-country applicants under scenario 1 are directly subject to the full set of EHDS reporting requirements stated in EHDS chapter IV, of which the following two are the most relevant:

- Publication of results (Article 61(4))
- Notification of significant findings (Article 61(5))

Regarding the former obligation, Article 61(4)) requires all health data users to make research results publicly available within 18 months of completing data processing, with possible extensions in justified cases. Results must be anonymised, and all publications must acknowledge the EHDS as the data source.

Regarding the latter obligation, under Article 61(5), third-country researchers accessing data under Scenario 1 must inform the HDAB of any clinically significant findings that arise during their research. The process for reporting such findings, including respecting individuals' rights not to be informed, must be followed precisely. National implementation measures apply regardless of the researcher's country of origin.

### **6.6.1 Purposes for secondary use**

The purposes for which health data categories referred to in Article 51 may be processed under the EHDS are set out in Article 53 of the EHDS. In line with this Article and JA TEHDAS2 Deliverable 6.2: 'Guideline for data users on good application and access practice', the purposes are as follows:

- Public interest in public and occupational health: this purpose is most relevant if the aim is to monitor, prevent or respond to health threats, such as infectious disease outbreaks or environmental health hazards. It should be noted that access for this purpose is only reserved to public sector bodies and Union institutions, bodies, offices and agencies exercising the tasks conferred on them by Union or national law.
- Policymaking and regulatory activities: this purpose applies where the aim is to support public bodies, including national governments and EU health institutions. It should be selected when the work contributes to policymaking, resource allocation, or other

administrative functions of public health authorities, or when it assists government bodies in designing and implementing evidence-based healthcare policies or initiatives. This purpose is likewise solely reserved to public sector bodies and Union institutions, bodies, offices and agencies exercising the tasks conferred on them by Union or national law.

- (Official) statistics: this purpose applies where the aim is to create health-related statistics. It should be chosen when the work involves generating anonymised health statistics for use in national, multi-national or Union-level official statistics. This purpose is also only reserved for public sector bodies and Union institutions, bodies, offices, and agencies exercising tasks conferred on them by Union or national law.
- Education: This purpose is used where health and care data are used for teaching and training in the health and care sector. It should be chosen when the work involves developing educational materials for healthcare professionals and students or creating case studies for use in academic or professional healthcare programmes.
- Scientific research related to health: this purpose is applicable where the aim is to advance scientific knowledge, develop new health products or services, or improve public health outcomes. It should be chosen in the following contexts:
  - Innovation: Conducting research to create new medical devices, therapies, or healthcare technologies.
  - Algorithm testing: training, validating, or refining machine learning models or other algorithms in healthcare.
  - (Public) health research: performing register-based research to identify disease risk factors, examine social disparities in health, or conduct epidemiological surveillance.
- Personalised healthcare: This purpose is applicable where the aim is to provide tailored healthcare or optimise treatment and care delivery based on the electronic health data of other individuals.

### **6.6.2 Prohibited purposes for secondary use of electronic health data**

Next to lawful purposes for secondary use under the EHDS, the legislation also contains a list of prohibited purposes. These are listed under Article 54. According to this Article and the aforementioned JA TEHDAS2 deliverable, these prohibited purposes are as follows:

- Detrimental decisions: decisions that negatively impact individuals based on their health data.
- Insurance discrimination: decisions to exclude or alter insurance benefits or premiums based on health data.
- Advertising: advertising or marketing to health professionals, organisations or individuals using health data. Scientific dissemination, including publications or presentations at medical or scientific congresses, is allowed if it is non-promotional, evidence-based and aimed at education or scientific exchange.

- Unauthorised access: sharing health data with third parties not specified in the data permit as authorised by the HDAB in question.
- Harmful products: development of products or services that could harm individuals or society, such as illicit drugs or items against public order or morality.

## 7 Recommendations

Health Data Access Bodies (HDABs) should implement a structured and risk-based governance framework when assessing requests for access to or transfer of electronic health data involving applicants established in third countries or international organisations. Such a framework should combine legal eligibility checks, technical safeguards, and organisational controls to ensure that international data access remains consistent with the objectives of the European Health Data Space (EHDS), while maintaining a high level of protection for sensitive health data. It can be summarised in five main points.

First, HDABs should systematically verify whether the applicant's jurisdiction falls under one of the two legally recognised access pathways provided by the EHDS Regulation—either participation as an authorised participant under Article 75(5) in conjunction with Article 91(1)(a), or recognition under the reciprocity mechanism pursuant to Article 91(1)(b). This verification will start from the consultation of implementing acts confirming authorised participant status or reciprocity determinations. Eventually, an updated HDAB internal registry of recognised third countries and international organisations can be created to facilitate consistent application of eligibility criteria. Where reciprocity applies, the HDAB only needs to check data access applications are from a third country that has a decision and that they are in scope. It is, in fact, the European Commission which conducts a proportional assessment of whether the third country provides equivalent—though not necessarily identical—conditions for EU-based applicants regarding data availability, admitted secondary-use purposes, access procedures, fee structures, and safeguards for intellectual property and trade secrets. In the assessment provided by the Commission (whose outcome is an implementing act recognising the third country/international organization as eligible), the attention is also given to whether pseudonymised data access is possible in the third country under conditions comparable to those defined by the EHDS, as exclusive access to fully anonymised data would not meet the equivalence threshold required for reciprocity. In practice, when assessing reciprocity with a third country, the European Commission considers whether EU applicants would be able to access data at a comparable level of detail in that jurisdiction. If the third country only allows access to fully anonymised datasets, while the EHDS allows controlled access to pseudonymised data within secure environments, the conditions for EU applicants would be significantly more restrictive than those provided under the EHDS. In such a case, the reciprocity requirement would not be satisfied because the level of analytical capability offered to EU applicants would be materially reduced. For this reason, the reciprocity assessment should verify that the third country's legal and operational framework permits access to pseudonymised individual-level health data under secure and controlled conditions, similar to those established in the EHDS through the use of Secure

Processing Environments (SPEs), strict purpose limitation, and robust governance mechanisms. The objective is not to require identical regulatory structures, but to ensure functional equivalence in access conditions, so that EU-based applicants are not placed at a disadvantage compared with applicants operating within the EHDS system.

Second, HDABs should apply enhanced scrutiny to international data transfer risks, especially when personal electronic health data may be involved. Any transfer scenario must be compliant with Chapter V of the GDPR and must be assessed by the HDAB considering Article 90 EHDS including verification of the existence of an adequacy decision or other lawful transfer mechanisms where applicable. HDABs should evaluate whether remote access through SPEs constitutes a data transfer considering the technical architecture of the environment, the type of access granted to the user, and the visibility of personal data. As a general rule, HDABs should prioritise solutions where personal electronic health data remain hosted and processed within EU-based. Where SPEs located in third countries are considered, HDABs should ensure that the environment demonstrably complies with the technical and organisational requirements set out under Article 73 EHDS and relevant implementing acts, including strict controls on data export, user authentication, activity logging, and output checking.

Third, HDABs should strengthen operational safeguards for highly sensitive datasets, particularly when dealing with non-personal electronic health data derived from individual-level health records. Even where datasets are classified as non-personal, HDABs should evaluate the risk of re-identification through technological or contextual means, as such data may still qualify as highly sensitive under the Data Governance Act when transferred outside the EU. Risk assessments should therefore consider dataset granularity, the number of individuals represented, geographical concentration, and foreseeable technological developments that could enable re-identification. In high-risk cases, HDABs should implement additional mitigation measures such as stricter output disclosure controls, enhanced aggregation requirements, restricted variable access, or additional contractual safeguards with the data user.

To emphasise the second and third points here mentioned, in addition to legal eligibility checks, HDABs should rely on a reference framework of technical and organisational safeguards meeting minimum operational and security requirements before authorisation is granted. From a technical perspective, safeguards are related to the mandatory use of SPEs - compliant with Article 73 EHDS and the relevant implementing acts - which should include strong authentication mechanisms (e.g. multi-factor authentication), role-based access control, encryption of data both at rest and in transit, strict session monitoring, and comprehensive activity logging to ensure traceability of all user actions. HDABs should also ensure that output checking procedures are implemented to verify that results exported from the SPE are anonymised and cannot lead to re-identification of individuals. Additional technical safeguards may include controlled software environments preventing unauthorised downloads or external connections and secure messaging protocols for cross-border infrastructure communication, such as those used in the HealthData@EU ecosystem. Organisational safeguards should complement technical protections and form an integral part

of the HDAB assessment process. These may include formal data access agreements between the HDAB and the data user specifying permitted uses, security obligations, liability provisions, and penalties in case of misuse; verification of the applicant's data protection compliance; and requirements for data protection impact assessments or transfer impact assessments where international transfers of personal data may occur. HDABs should also ensure that the requesting organisation/user designates responsible data stewards or security officers accountable for compliance with EHDS obligations during the process.

Fourth, HDABs should ensure transparency and procedural consistency in their evaluation processes. Clear internal guidelines should be developed to harmonise the assessment of international access applications across Member States, including GDPR transfer compliance, SPE security validation, and dataset sensitivity analysis. These procedures should be aligned with the operational workflows established in related EHDS guidance for data access applications and SPEs, ensuring that third-country applicants follow the same procedural steps as EU applicants once eligibility has been established. HDABs should also document all the released permits involving third countries and international organizations, including the legal basis relied upon and the safeguards implemented, to facilitate auditability and regulatory oversight.

Finally, HDABs should promote a precautionary yet enabling approach that balances international scientific collaboration with the protection of EU citizens' health data. By fostering these practices, HDABs can reinforce trust in cross-border health data sharing while maintaining the high standards of security, accountability, and ethical governance that underpin the European Health Data Space.

## Annexes

Annex number	Annex title
1	Methodology
2	User journey
3	Glossary
4	Survey template
5	Assessment criteria Scenario 2 (further details)

## 8 Annex 2 – Methodology

The work towards this deliverable followed a structured, mixed-methods approach combining targeted desk research, stakeholder consultation, and iterative drafting of the guideline. The overall process was organised in sequential but partially overlapping phases (analysis, design, data collection, synthesis), with regular coordination among task partners to ensure coherence with the wider TEHDAS2 work plan and deliverables.

In the first phase, the team carried out a focused desk review of the EHDS Regulation, GDPR, the Data Governance Act and other EU-level instruments, as well as existing TEHDAS2 outputs relevant to international access and transfer of electronic health data. This review was used to identify the key legal provisions, governance arrangements and technical safeguards that frame secondary use of health data in cross-border contexts, and to map open questions and implementation gaps that the milestone should address.

Based on this analytical groundwork, the team designed a detailed survey instrument to collect comparative information from Member States, third countries and relevant organisations. The questionnaire was developed through an iterative drafting process within the task team and subsequently refined following discussions with legal and technical experts from partner institutions and EU-level fora. Particular attention was paid to conceptual clarity, alignment with established EU terminology and the balance between closed and open questions to allow both comparability and richer qualitative input.

The final survey was disseminated through key TEHDAS2 networks, including Health Data Access Bodies and specialised communities of practice, using a secure online tool that enabled remote completion by respondents. Participation was encouraged through targeted invitations and follow-ups, with the aim of ensuring broad geographical coverage and representation of different governance models. Responses were collected over a defined period, then exported and prepared for analysis, including basic quality checks and standardisation of selected variables to facilitate comparison across jurisdictions.

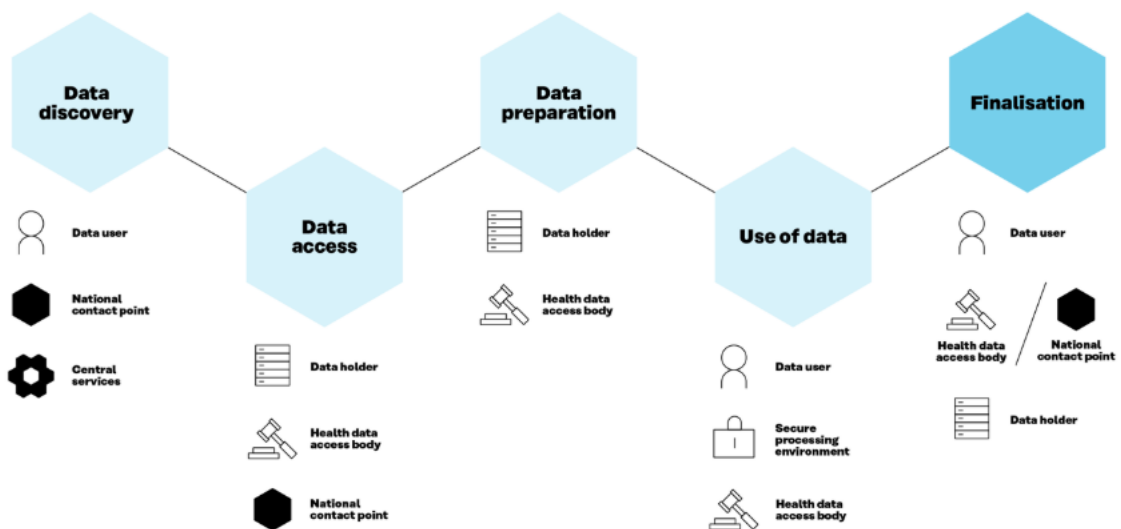
Data analysis combined quantitative and qualitative techniques. At quantitative level, descriptive statistics and simple classifications were applied to distinguish between countries with explicit national frameworks and those relying primarily on general data protection rules, and to map the prevalence of different types of safeguards. At qualitative level, open-ended responses were coded thematically to identify recurring issues such as legal fragmentation, definitional uncertainties, reciprocity mechanisms and operational constraints. This dual approach made it possible to link high-level patterns to concrete examples and practices.

In the final phase, insights from the legal desk analysis and survey results were synthesised through internal drafting rounds within the task team. Draft texts were iteratively revised to ensure internal consistency, traceability to the collected evidence and alignment with the broader EHDS governance architecture. Particular emphasis was placed on translating findings into operational guidance and recommendations that are both legally sound and practically implementable by Health Data Access Bodies and other stakeholders. Where relevant, cross-references to other TEHDAS2 milestones and deliverables were introduced to support a coherent and harmonised interpretation of the EHDS framework.

## 9 Annex 2: Data user' journey

When a data user<sup>i</sup> 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)<sup>ii</sup>. The user must complete the information required in the form, upload necessary documents, and provide justifications as needed.

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

### Data preparation

During this phase, the data holder(s)<sup>iii</sup> 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<sup>iv</sup>. The duration of this phase is specified in the Regulation (Art 68(12)).

### Finalisation

The 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.

## 10 Annex 3 – Glossary

Term	Definition
<b>Electronic health data</b>	Personal or non-personal electronic health data. paste.txt
<b>Health data access application</b>	An application form used to seek access for personal-level electronic health data for secondary use in an anonymised or a pseudonymised format. paste.txt
<b>Health data access body (HDAB)</b>	Member state-designated authority that facilitates the secondary use of electronic health data. HDABs assess applications and requests, issue data permits, obtain data from data holders and make data available in secure processing environments. paste.txt
<b>Health data applicant</b>	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 the EHDS Regulation. paste.txt
<b>Health data holder</b>	Any person, organisation or public body that has the right to process data for health care provision or for public health purposes, reimbursement, research, policymaking, official statistics or patient safety, including hospitals, insurers, research institutes and EU institutions. paste.txt
<b>Health data request</b>	A request to access data in an anonymised statistical format for the purposes referred to in EHDS Article 53. paste.txt
<b>Health data user</b>	A natural or legal person 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. paste.txt
<b>Intellectual property (IP)</b>	Rights such as trade marks, designs, copyright and related rights, patents, supplementary protection certificates, plant variety rights, semiconductor topographies, utility models and protected trade names, as listed in Regulation (EU) No 608/2013. paste.txt
<b>Non-personal electronic health data</b>	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 and data that have never related to a data subject. paste.txt

<b>Personal electronic health data</b>	Data concerning health and genetic data, relating to an identified or identifiable natural person, processed in an electronic form. paste.txt
<b>Secondary use</b>	Processing of electronic health data for the purposes set out in Chapter IV of the EHDS Regulation, other than the initial purposes for which they were collected or produced. paste.txt
<b>Secure processing environment (SPE)</b>	An environment in which access to electronic health data can be provided following a data permit, subject to technical and organisational measures and security and interoperability requirements, allowing access only to authorised persons, and ensuring user authentication, authorisation, restricted data handling, logging and compliance monitoring. paste.txt
<b>Trade secret(s)</b>	Information that is secret, has commercial value because it is secret, and has been subject to reasonable steps to keep it secret, as defined in the Trade Secret Directive. paste.txt

*This glossary is intended to support consistent terminology within TEHDAS2 deliverables. It does not create legal obligations, does not interpret Union law, and does not prejudge the content of implementing acts, guidelines, or national implementation measures under the EHDS Regulation.*

## 11 Annex 4 – Survey template

### Survey on health data access and transfer models involving third countries

**Networks involved in the survey:** TEHDAS2 partners organizations, EHDS2 HDABs Community of Practice, eHMSEG legal work group

**To:** Officers involved in personal data and/or health data processing agreements with third countries

**Objective of the survey:** as a goal of the WP4 (task 3) of the TEHDAS 2 Joint Action, we are collecting insights on international organizations and third country access and transfers of personal and non-personal electronic health data, to support the development of guidelines for the implementation of the European Health Data Space (EHDS) in particular Articles 87–91 on international access and reciprocity for the secondary use of health data.

Section 2

### Glossary

**PERSONAL DATA:** any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Article 4(1) of the GDPR);

**NON-PERSONAL DATA:** 'non-personal electronic health data' meaning 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

**THIRD COUNTRY:** any state that is not part of the European Economic Area (EEA), which includes the 27 EU Member States plus Norway, Iceland, and Liechtenstein;

**INTERNATIONAL ORGANIZATION:** An organization and its bodies governed by public international law, or any other body that is set up by, or based on, an agreement between two or more countries. (Article 4(26) of the GDPR);

**MODEL:** a structured approach or template (e.g. agreement or procedure) used to regulate third-country access or transfers of health data, which may vary depending on national and EU-level requirements.

**REGULATORY FRAMEWORK:** the set of legal provisions applicable to health data access and transfers, in particular the European Health Data Space Regulation (EU) 2025/327, complemented where relevant by other EU and national laws

Section 3

**Personal Information**

**Type of Organization:** \_\_\_\_\_

**Country:** \_\_\_\_\_

**Network invited to the survey:**

TEHDAS2 partner

EHDS2 HDABs CoP member

eHMSEG legal work group

Other ...

**Role of the respondent in the organization:** \_\_\_\_\_

**Email:** \_\_\_\_\_

Section 4

**GENERAL QUESTIONS**

Does your country apply any specific regulatory or practical requirements for health data access by international organisations or third countries, in addition to the GDPR framework?

Yes

No

- If yes, could you cite the relevant texts references and websites?

\_\_\_\_\_

- If not, is there a **national** practice specific for international organizations or third country health data access and transfer?

\_\_\_\_\_

**Based on your experience**, what challenges (main points) do you foresee **to align third countries with an EU-wide framework** under the EHDS for health data access and transfer?

---

Section 5

**Existing agreements with international organisations and/or third countries on the access and transfer of personal health data**

Does your organization currently have personal health data access and transfer agreements in place with third countries and/or international organizations?

Yes

No

*(If your answer is “yes”, continue the survey by moving on to the next question and section (6); if your answer is “no”, the survey is finished – go to section 7 thank you )*

Section 6

**Elements of existing agreements relevant for future EHDS reciprocity (Articles 87–91)**

**According to these agreements:**

In your organisation’s agreements with third countries or international organisations, under which conditions is the access and transfer of personal health data authorised? (e.g. legal obligation, explicit consent, public interest, research purpose, etc.) \_\_\_\_\_

Which categories of health data are typically included in such agreements? (e.g. EHR data, registries, genomic data, administrative/claims data, etc.)

Beyond GDPR, are there any specific national rules or requirements that affect such agreements (e.g. additional safeguards for health data, restrictions on certain categories, mandatory approvals)? Yes

No

Other ...

If yes, which ones

---

Do such agreements define clear purposes for secondary use of health data, and are these purposes consistent with the permitted purposes under Articles 53–54 of the EHDS Regulation?

Yes / No / Partially – please specify.

---

Are there, in your country, **purpose limitations** for the access and transfer of personal health data in case of international organisation or third countries are involved?

Yes

No

Other  ...

If yes, which ones?

---

Section 7

**Further information : Security and procedural safeguards in agreements – relevance for EHDS**

Which types of security measures are included in existing agreements with international organisations or third countries? (e.g. data traceability, restricted processing, secure remote access, auditing capabilities, cybersecurity standards, other) To the best of your knowledge, is there - in the international organisations/third countries involved in the agreements with your country - an **obligation to inform natural persons about the results** of the secondary use of their health data?

Yes

No

Other  ...

If yes, which ones?

To your knowledge, do these agreements provide procedural safeguards relevant for EHDS reciprocity (Article 91), such as:

- obligation to inform natural persons about secondary use and its results
- complaint or redress mechanisms
- limitations on onward use of data/results

- independent oversight or auditing provisions

From your perspective, are existing measures functionally equivalent to the EHDS minimum requirements, or would stricter alignment be necessary?

---

Do these agreements with international organisations and/or third countries include fees for accessing or transferring such data? If yes, please indicate briefly how these fees are structured (e.g. flat fee, cost-compensation, commercial pricing).

Note: please upload any files you believe are important to provide a thorough response to this survey.

Section 8

**Thank you!**

Thank you for taking the time to share your valuable insights and feedback. We are committed to carefully reviewing and analysing your responses.

Your participation is essential in building a collaborative and impactful European Health Data Space, and we look forward to continuing our partnership in the future.

Please don't hesitate to reach out if you have any questions or need further information.

## 12 Annex 5 – Assessment criteria Scenario 2 – Reciprocity (further details)

### General requirements

- Criteria for ensuring data findability:
  - The electronic health data that is made available are described by metadata with basic characteristics of the datasets allowing users to select the desired datasets;
  - Metadata are registered or indexed in a searchable resource. The searchable resource is continuously accessible for users from the EU for free;
  - The resource (e.g. metadata catalogue) has a formal governance and the entries in it are regularly maintained;
  - Metadata are assigned a globally unique and persistent identifier.
  
- Criteria for ensuring data availability:
  - Metadata are retrievable by their identifier;
  - Health data may be either provided and if not, e.g. due to their sensitivity, they shall be made accessible based on defined conditions;
  - A mechanism or protocol for making data available or accessing the data (datasets) is described and made publicly known;
  - Processes for access to the data are open to users from the EU and are based on transparent, consistently applied rules;
  - Authentication and authorisation methods for access to the processes and data are available to the users from the EU;
  - Principles for fee policies and fee structure are transparent.
  
- Criteria for ensuring data interoperability:
  - Metadata use a formal, accessible, shared, and broadly applicable language for knowledge representation;
  - Metadata inform about the standards (formats and vocabularies) used by the datasets;
  - Datasets use standards that are defined and the definition is made publicly available.
  
- Criteria for ensuring data reusability:
  - Metadata are published with a clear and accessible data usage license;

- Data sets that cannot be provided should be made available for analyses or other processing to EU users using common information technologies and tools in an appropriate and accessible environment.

### **Other important aspects**

Considering the system that is established by the EHDS Regulation for access to health data, its performance in case of data users based in third countries introduces certain differences that should be taken into account by HDAB, TDH and also SPE because they may influence pertinent processes for most of the elements of user journey in the EHDS.

These differences may manifest themselves in (may not be an exhaustive list):

- languages used;
- the duration of the assessment of a request for data or access to data by HDAB or TDH;
- coordination of multicountry data access application;
- methods for verification of the information provided by the data user in the application and its credibility;
- the assessment of the application for access to data considering context of the third country, including safeguards planned by the applicant in order to prevent any misuse of the electronic health data;
- solvency of the data user, identification methods of the (non-EU) users;
- extra explanatory sessions with the data user due to various differences in processes and standards that the user is not prepared for;
- higher costs calculation;
- amount of fees (see also TEHDAS2 M4.1 Guideline on fees and penalties for non-compliance related to the EHDS regulation);
- criteria for reduced fees for certain types of health data users, if a MS decides to introduce discounts applicable for third countries;
- communication with the data user (incl. time zones and communication means);
- in case a health data applicant intends to bring own datasets into the SPE, assessment of these datasets;
- improvements of health data, such as correction, annotation or enrichment proposed by data users, which may be marked by a non-EU context and may deserve special attention;
- invoicing and payment;
- currency exchange rates and their development over time (may have adverse effects on user side);

- verification of publication of results of the analyses made by the data user (incl. e.g. relevance);
- fines and their enforcement;
- assistance or support and their possible scope provided to a public sector body from a third country by HDAB pursuant Article 57(3 and 4).

It should be finally recalled that one of the goals of the EHDS and the establishment of common data spaces is to increase the EU's competitiveness on a global scale. Furthermore, the level and depth of international cooperation with various countries of the world is continuously developing, which may also have some impact on cooperation in the use of data.

---

<sup>i</sup> The HDAB Community of Practice has been established by the Member States with the support of the European Commission to facilitate the interaction between HDABs and relevant competent authorities from different EU Member States through a common structured platform enabling the sharing of best practices, challenges, and concerns, as well as the strengthening of collaborations, agreement on common procedures, and convergence on practical solutions to build and manage their tasks. ( details are available here: [https://health.ec.europa.eu/ehealth-digital-health-and-care/ehds-action/projects-supporting-ehds/health-data-access-bodies-community-practice\\_en](https://health.ec.europa.eu/ehealth-digital-health-and-care/ehds-action/projects-supporting-ehds/health-data-access-bodies-community-practice_en))

<sup>ii</sup> The eHMSEG Legal Work Group is a division of the eHealth Member States Expert Group (eHMSEG) which coordinates the

technical and organisational implementation of the National Contact Points for eHealth to ensure that they are fully interoperable. The members of eHMSEG participate in the deployment and operation of eHealth cross border infrastructure and are responsible for setting up National Contact Points for eHealth. (more details are available here: [https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services\\_en](https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en))

<sup>iii</sup> contractual templates adopted by companies to ensure adequate safeguards when transferring data to countries *without* an adequacy decision. They should be valid for the parties signing the agreement (usually an agreement between a controller and a processor).

An adequacy decision is a formal EU commission ruling declaring a country's data laws equivalent to the GDPR, allowing free data flow.

(more details are available here: [https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview\\_en](https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en))