DS4H - RISK ASSESSMENT

Document ID : DS4H_WP1_D1.3

Author

Dataspace4Health Consortium

Date: 05/01/2026

Funding

This project has received funding from the Ministry of the Economy of Grand Duchy of Luxembourg under Grant agreement no 20230505RDI170010392869.

Disclaimer

The documents published by the consortium are intended solely for informational purposes and reflect the views and opinions of the consortium members at the time of publication and within the scope of the Dataspace4Health project (DS4H).

The ideas expressed herein do not necessarily reflect the official policy or position of the funding entity.

Efforts have been made to achieve the relevance of the content; however, the consortium does not make any representation regarding its completeness and accuracy.

This document may be subject to further revision.

This document is intended to be published on the Dataspace4Health website.

TABLE OF CONTENT

LIST OF ABBREVIATIONS

dFMEA	Design Failure Mode and Effect Analysis
DPO	Data Protection Officer
DS4H	Dataspace4Health
EHDS	European Health Data Space
GDPR	General Data Protection Regulation
KPI	Key Performance Indicator
pFMEA	Process Failure Mode and Effect Analysis

EXECUTIVE SUMMARY

- **Purpose of the document:** This document presents the results of a comprehensive risk assessment conducted for the Dataspace4Health (DS4H) project in Luxembourg, focusing on the creation, implementation and operation of a Gaia-X compliant data space in production. The purpose is to provide stakeholders with a clear understanding of the key risks identified, the methodology used for their assessment and the measures proposed to mitigate these risks. The document also serves as an overarching guide to the accompanying risk matrix, which was developed using a structured, Excel-based approach.
- **Key Objectives:**
  - Systematically identify, categorize and assess potential risks across all phases of the DS4H project lifecycle, including design, build and operational stages.
  - Apply a combined Design Failure Mode and Effects Analysis (dFMEA) and Process Failure Mode and Effects Analysis (pFMEA) methodology, ensuring both technical and procedural risks are captured.
  - Prioritize risks based on their likelihood and impact, both before and after mitigation measures, using a transparent and color-coded risk matrix.
- **Strategic Importance:** The DS4H project represents a critical step towards establishing a secure, interoperable and Gaia-X compliant health data ecosystem in Luxembourg. Given the sensitive nature of health data and the complex regulatory environment, a robust risk assessment is essential to ensure compliance, protect patient privacy and maintain stakeholder trust. By leveraging a multidisciplinary team – including experts in data protection, legal compliance, information security, healthcare analytics, software architecture and project management – this assessment delivers a holistic view of the risk landscape.
- **Key Findings:**
  - A total of 59 risks were identified across 8 categories: Consent, Cybersecurity, Data Protection, Data Quality, Ethical, Legal, Project Management and Technical.
  - Before controls: 23 Critical, 19 High, 17 Medium and 0 Critical risks.
  - After controls: 0 Critical, 33 High, 17 Medium and 9 Low risks.
  - The highest concentration of critical risks was observed in Data Protection, Legal & Regulatory, Consent and Cybersecurity.
- **Impact:** Failure to mitigate these risks could result in – amongst others – General Data Protection Regulation (GDPR) non-compliance, reputational damage, operational disruptions and significant financial penalties.
- **Next Steps:**
  - Implement continuous monitoring and updates to the risk matrix accordingly.
  - Conduct regular compliance checks (e.g., through audits) to ensure alignment with Gaia-X, GDPR and emerging regulations such as the AI Act and European Health Data Space (EHDS).
  - Provide ongoing training programs for stakeholders to minimize human-related risks.

1. INTRODUCTION

This deliverable, D1.3, presents the comprehensive risk assessment conducted for the DS4H project, which aims to establish a Gaia-X compliant health data space in Luxembourg. The assessment systematically identifies, evaluates and prioritizes risks associated with the design, implementation and operation of the data space, taking into account both technical and procedural aspects.

The primary objectives of this assessment are to provide a structured and transparent overview of the risk landscape across all phases of the DS4H lifecycle (design, build and run), to ensure that (critical) risks related to compliance, data protection, interoperability (technical) and operational continuity are identified and addressed, as well as to support decision-making by prioritizing risks based on their likelihood and impact, both before and after risk mitigation measures.

This document described the methodology used for the performed risk assessment, as well as provides a summary for the different risk categories and risk items identified – both prior to and after the introduction of risk controls. Furthermore, it highlights greater risk items identified in more detail.

The complete risk matrix is annexed to this deliverable.

2. METHODOLOGY

This chapter outlines the methodology used to conduct the risk assessment for the DS4H project, focusing on the development and operation of the Gaia-X compliant data space in production environment. The approach was designed to ensure a structured, transparent and comprehensive evaluation of risks across all project phases. The chapter is organized into different sections:

- **Purpose and scope of the risk assessment:** Defines the objectives of the risk assessment and outlines the boundaries of the analysis.
- **Risk assessment approach:** Explains the combined use of dFMEA and pFMEA to capture both technical and procedural risks.
- **Risk criteria and scoring methodology:** Details the parameters used to evaluate risks, including the likelihood and severity assessments.
- **Risk matrix structure:** Provides an overview of the Excel-based risk matrix, including its layout, key columns and the scoring methodology used to determine inherent and residual risk levels.
- **Stakeholder involvement:** Describes the multidisciplinary team that contributed to the assessment, ensuring that legal, technical and operational perspectives were fully addressed.
- **Risk mitigation strategy:** Summarizes the planned actions to reduce identified risks, focusing on preventive measures, process improvements and technical safeguards.
- **Residual risk management:** Explains how remaining risks shall be monitored and controlled post-mitigation, including documentation, acceptance criteria and follow-up mechanisms to ensure ongoing safety and compliance.

It will include an explanation of the risk matrix created, that was subsequently used to identify and assess different risk items. Additionally, it will provide a description of the risk matrix lay-out and its key columns. Finally, this chapter will describe the stakeholders who contributed to this risk assessment.

2.1 PURPOSE AND SCOPE OF THE RISK ASSESSMENT

The purpose of this risk assessment is to identify, evaluate, prioritize and mitigate risks associated with the design, implementation and operation of the DS4H platform, ensuring compliance with applicable regulations and maintaining the security and integrity of health data.

Scope includes:

- Phases: Design, Build and Run.
- Domains: Legal and regulatory compliance, data protection, cybersecurity, consent management, technical architecture, data quality, ethical considerations and project management.
- Exclusions: Risks outside the DS4H ecosystem (e.g., unrelated third-party systems).

Assumptions:

- Risk controls described in this document will be implemented as planned.
- Regulatory frameworks (GDPR, AI Act, EHDS, etc.) remain applicable during the assessment period.

This assessment forms part of the DS4H risk governance framework and will be updated periodically to reflect changes in e.g., scope, technology or regulatory requirements.

2.2 RISK ASSESSMENT APPROACH

The approach of this risk matrix combines elements of a dFMEA and pFMEA, adapted to the specific context of data space architecture, governance and operations. This hybrid methodology was chosen to ensure a comprehensive identification and assessment of different risks that may arise both from the structural design of the DS4H platform, as well as from the processes involved in its implementation and (foreseen) operation.

Design Failure Mode and Effects Analysis:

The dFMEA is a structured analytical tool used to identify and evaluate potential failure modes within the design of a system, product or architecture. The dFMEA focuses on how design (decisions) may lead to failures that potentially impact its functionality, safety or compliance. Each failure mode is assessed based on its likelihood of occurrence and foreseen impact, resulting in an inherent risk level. Then, risk controls are introduced to mitigate the identified risks [1] [2].

In the context of Dataspace4Health, the dFMEA methodology was applied to assess risks particularly related to:

- Data space: (technical) architecture and infrastructure
- Interoperability
- Security and privacy
- Scalability and resilience of the system

Process Failure Mode and Effects Analysis:

Complementing the dFMEA, the pFMEA focuses on risk associated with operational and procedural aspects of e.g., a system. It evaluates how processes may fail during execution, leading to inefficiencies, non-compliance or (service) disruptions. Like the dFMEA, the pFMEA uses likelihood of occurrence and foreseen impact to define an inherent risk level. Subsequently, risk controls are defined that (aim to) mitigate these risks from occurring [3] [4]. In DS4H, pFMEA was used to assess risks related to, amongst others:

- Data onboarding and sharing workflows
- Consent management and legal compliance processes
- Governance and stakeholder coordination
- Incident response and operational continuity

Unified risk matrix and scoring

Each identified risk was evaluated using two key dimensions:

- Likelihood of occurrence: The probability that the risk may materialize under given conditions.
- Impact severity: The potential consequences of the risk on e.g., operations, compliance, data integrity or patient safety.

The combination of these two dimensions determines the inherent risk level, which reflects the risk before any mitigation measures are applied. Subsequently, risk controls were defined and assessed for their effectiveness, leading to the calculation of the residual risk level, i.e., the remaining risk after controls are implemented.

To facilitate interpretation and prioritization, a color-coded scale was used:

- Low (Green) – Acceptable risk; minimal impact and low probability.
- Medium (Yellow) – Manageable risk; requires monitoring and possible mitigation.
- High (Orange) – Significant risk; mitigation measures required.
- Critical (Red) – Unacceptable risk; immediate action required.

The decision to integrate both a dFMEA and pFMEA in a single risk matrix was driven by the dual nature of the DS4H project, which encompasses both technical design and anticipated operational process execution. A purely design-focused or process-focused approach would have overlooked critical interdependencies between architecture and actual implementation. Two different risk assessments (a dFMEA as well as a pFMEA respectively) could have resulted in potentially inconsistent or unaligned documentation.

By integrating both methodologies into a single risk matrix:

- It was ensured that design-level risks (e.g., architectural flaws, lack of Gaia-X compliance) were captured alongside process-level risks (e.g., governance failures, data misuse).
- A holistic view of the risk landscape was established, which supports more robust mitigation planning.
- The risk assessment is aligned with best practices in complex system engineering, where both design- and process risks must be managed concurrently.

This hybrid approach is thought to be particularly appropriate for data spaces, which are systems involving both (a technical) infrastructure and human-driven processes.

2.3 RISK CRITERIA AND SCORING METHODOLOGY

To ensure consistency and transparency in the evaluation of risks, a standardized scoring methodology was applied across all identified risk items. Each risk was assessed based on two qualitative dimensions: likelihood of occurrence and impact severity. These criteria were used to determine both the inherent risk level (before mitigation) and the residual risk level (after mitigation controls are applied).

Likelihood scale

The likelihood of a risk occurring was assessed using the following qualitative scale:

- Very Rare – Highly unlikely to occur under normal conditions.
- Unlikely – Possible but not expected; may occur under specific circumstances.
- Possible – Could occur under certain conditions; moderate probability.
- Likely – Expected to occur in most circumstances; high probability.

Quantified likelihood reference

To enhance objectivity and consistency, these qualitative ratings were mapped to estimated frequency ranges:

Likelihood level	Estimated frequency	Example interpretation in DS4H context
Very Rare	~1 in 1,000,000 occurrences	May occur only in exceptional cases (e.g., zero-day vulnerability)
Unlikely	~1 in 100,000 occurrences	Could happen if multiple unlikely conditions align
Possible	~1 in 10,000 occurrences	Might happen occasionally under certain conditions
Likely	~1 in 100 occurrences	Expected to happen regularly unless mitigated

Table 1: Quantified likelihood reference

These values are indicative and should be refined over time using real-world data, expert input and incident tracking. They help align qualitative assessments with quantitative reasoning, especially in regulatory or technical contexts.

Impact scale

The following impact categories can be distinguished:

- Minor – Negligible effect on operations, compliance or data integrity.
- Moderate – Limited operational or reputational impact; manageable without major disruption.
- Major – Significant disruption to operations or serious regulatory concern.
- Severe – Critical impact, including legal penalties, patient harm or system failure.

The potential consequences of a risk, if it materializes, were assessed using the following impact categories:

Impact level	Definition	Example in DS4H context	Estimated consequences
Minor	Negligible effect on operations, compliance or data integrity	Temporary delay in data onboarding due to user error	No legal impact, no service disruption, easily recoverable
Moderate	Limited operational or reputational impact; manageable without major disruption	Incorrect metadata tagging affecting data discoverability	Minor reputational concern, localized operational inefficiency
Major	Significant disruption to operations or serious regulatory concern	Failure to validate patient consent before data sharing	Potential GDPR violation, service interruption, stakeholder escalation
Severe	Critical impact, including legal penalties, patient harm or system failure	Unauthorized access to sensitive health data due to system breach	Legal sanctions, loss of trust, possible harm to individuals, full-scale incident response required

Table 2: Impact scale

Risk level matrix

The combination of likelihood and impact determines the overall risk level, which is color-coded for clarity and prioritization. The matrix used in DS4H is as follows:

Impact ↓ / Likelihood →	Very Rare	Unlikely	Possible	Likely
Severe	High	High	Critical	Critical
Major	Medium	High	High	Critical
Moderate	Low	Medium	Medium	High
Minor	Low	Low	Low	Medium

Table 3: Risk level matrix

2.4 STRUCTURE OF THE RISK MATRIX

This section describes the structure, layout and functioning of the risk matrix developed for the DS4H risk assessment. The matrix serves as the central tool for identifying, evaluating and prioritizing risks associated with the design, implementation and operation of a Gaia-X compliant health data space in Luxembourg.

The matrix is designed to be dynamic and iterative, allowing for periodic updates to:

- Incorporate newly identified risks.
- Reassess existing risks.
- Modify, add or remove risk controls based on evolving project conditions.

Matrix layout and organization

The matrix is organized hierarchically to reflect both the lifecycle stage of the data space and the thematic category of each risk. It consists of two levels of risk identification and categorization:

- Risk ID Level 1: High-level grouping of risks by lifecycle phase:
  - R-01: Design / Creation
  - R-02: Build / Implementation
  - R-03: Run / Operations
- Risk ID Level 2: Specific risk items within each group, e.g., R-01-01, R-02-01, etc., where the final two digits represent a consecutive number.
- Risk Category Level 2: Thematic classification of each risk, such as e.g.,:
  - Non-compliance with GDPR
  - Consent not obtained
  - Interoperability
  - Data governance
  - Technical failure

This structure enables clear traceability and facilitates filtering and analysis across different dimensions of the project.

Column descriptions and functions

Each row in the matrix represents a distinct risk item and includes the following columns:

1. **Risk Identification**
   - Risk description: A brief summary of the respective risk item, e.g., “Absence of consent”.
   - Risk example: A detailed scenario describing how the respective risk item could materialize, structured as a sequence of events (e.g., first this happens, then that fails, leading to the risk).

Then, per risk item, the inherent risk is assessed (the assessment before/without taking into consideration the different risk controls):

2. **Inherent Risk Assessment**

   - Risk Applicability: Indicates whether the risk is relevant to the current scope (“Yes” or “No”).
   - Likelihood: Qualitative rating of how likely the risk is to occur:
     - Very Rare
     - Unlikely
     - Possible
     - Likely
   - Impact: Qualitative rating of the potential consequences of the risk, when it occurs:
     - Minor
     - Moderate
     - Major
     - Severe

- Inherent risk level: Overall risk level before mitigation, which is additionally color-coded:
  - Low (Green)
  - Medium (Yellow)
  - High (Orange)
  - Critical (Red)

Then, the different risk controls are introduced per risk item:

3. Risk Controls

- Risk controls: Description of existing or planned mitigation measures.
- Effectiveness of controls: Evaluation of how well the controls address the risk:
  - Not Effective
  - Partially Effective
  - Effective

Finally, taken into consideration the different (foreseen) risk controls, the residual risk is assessed using the same methodology as for the inherent risk assessment:

4. Residual Risk Assessment

- Residual Likelihood: Re-evaluation of likelihood after applying controls, using the same qualitative rating as for the inherent risk assessment.
- Residual Impact: Re-evaluation of impact after applying controls, using the same qualitative rating as for the inherent risk assessment.
- Residual Risk Level: Final risk level, using the same color-coded scale.
- Risk Acceptance: Indicates whether the residual risk is considered acceptable ("Yes" or "No").

2.5 STAKEHOLDER INVOLVEMENT

The DS4H risk assessment was conducted through a collaborative and multidisciplinary approach, ensuring that all relevant perspectives – technical, legal, operational and governance – were considered. This diversity of expertise was essential for identifying risks across the entire lifecycle of the data space and for defining effective mitigation strategies.

Stakeholder groups and roles:

- **Data Protection Officers (DPO) and Legal Advisors:** Ensured compliance with GDPR, Gaia-X principles and other applicable regulations. They assessed risks related to e.g., consent management, data sharing agreements and legal liabilities.
- **Cybersecurity specialists:** Evaluated risks associated with system vulnerabilities, data breaches and security controls. They contributed to defining technical safeguards and incident response measures.
- **Healthcare Business Analysts:** Provided insights into clinical workflows, data usage scenarios and operational dependencies, ensuring that process-related risks were accurately captured.
- **Software Architects:** Assessed risks linked to e.g., system design, interoperability, scalability and resilience. They ensured that architectural decisions aligned with Gaia-X and EHDS requirements.
- **Data and Machine Learning Consultants:** Identified risks related to data quality, algorithmic bias, and ethical considerations in AI-driven processes.
- **Project Managers:** Oversaw the integration of risk management into project governance, ensuring timely updates, documentation and alignment with overall project objectives.

Due to the diverse professional backgrounds of the contributors, the risk matrix benefits from a comprehensive range of perspectives, including legal, technical, data protection, project management and healthcare domains. This multidisciplinary approach ensures that the risk assessment is both robust and well-rounded, adequately addressing the complex and multifaceted nature of risks inherent to the DS4H project. As such, the expertise involved is considered both sufficient and appropriate for the scope and objectives of this assessment.

2.6 RISK MITIGATION STRATEGY

The DS4H risk mitigation strategy was designed to proactively address identified risks across all lifecycle phases, ensuring that both technical- and procedural safeguards were in place.

Categorization and prioritization

Risks were categorized by domain (e.g., legal, technical, operational and ethical) and prioritized based on their potential impact and likelihood. This allowed for targeted mitigation efforts and efficient resource allocation.

Mitigation planning

For each high-priority risk, a mitigation plan shall be defined, including:

- Preventive measures: Actions to reduce the likelihood of occurrence (e.g., training, process redesign, architectural safeguards, etc.).
- Corrective actions: Steps to minimize impact if the risk materializes (e.g., incident response protocols, fallback procedures).
- Monitoring indicators: Metrics and signals to track risk evolution and detect early signs of escalation.

Stakeholder accountability

Each mitigation action shall be assigned to a responsible stakeholder or team, ensuring ownership and follow-through. Roles shall be clearly defined to avoid ambiguity and delays in implementation.

Continuous improvement

Mitigation strategies shall be reviewed regularly and adjusted based on:

- Feedback from stakeholders
- Changes in regulatory or technical context
- Lessons learned from incidents or near misses

This dynamic approach will ensure that risk management remains responsive and aligned with the evolving needs of the DS4H ecosystem.

2.7 RESIDUAL RISK MANAGEMENT

Despite proactive mitigation efforts, certain risks may persist due to technical limitations, regulatory uncertainties or operational constraints. The DS4H framework shall include a dedicated process for managing these residual risks in a transparent and accountable manner.

Identification and documentation

Residual risks shall be explicitly documented following mitigation planning. Each entry shall include:

- A description of the remaining risk
- Justification for its acceptance
- Potential impact and likelihood
- Monitoring mechanisms

Acceptance criteria

Residual risks shall be accepted only if:

- Mitigation measures reduced the risk to a tolerable level
- No feasible alternatives were available
- The Steering Committee validated the acceptance based on impact analysis and stakeholder input

Monitoring and escalation

Accepted residual risks shall be subject to continuous monitoring. Indicators and thresholds shall be defined to detect changes in risk exposure. If a residual risk escalates or new information emerges, it shall be re-evaluated and, if necessary, reclassified for further mitigation.

Transparency and governance

All decisions regarding residual risks shall be recorded and made accessible to relevant stakeholders. This ensures that risk acceptance is not only justified but also aligned with the principles of accountability and informed consent.

3. OVERVIEW OF RISKS

This chapter will provide a summary of the number of risks identified, distributed across the different categories. It will summarize the number of low, medium, high and critical risk items identified both prior to, as well as after taking into consideration the (foreseen) risk controls.

The analysis includes:

- The total number of risks identified.
- A breakdown of risks by category (e.g., operational, regulatory, technical, etc.).
- The distribution of risk levels (low, medium, high or critical) before mitigation.
- The residual risk levels after applying the proposed controls.

This summary enables a clear understanding of the overall risk exposure and highlights areas requiring close monitoring or additional mitigation efforts. This is further detailed in subchapter 3.2.

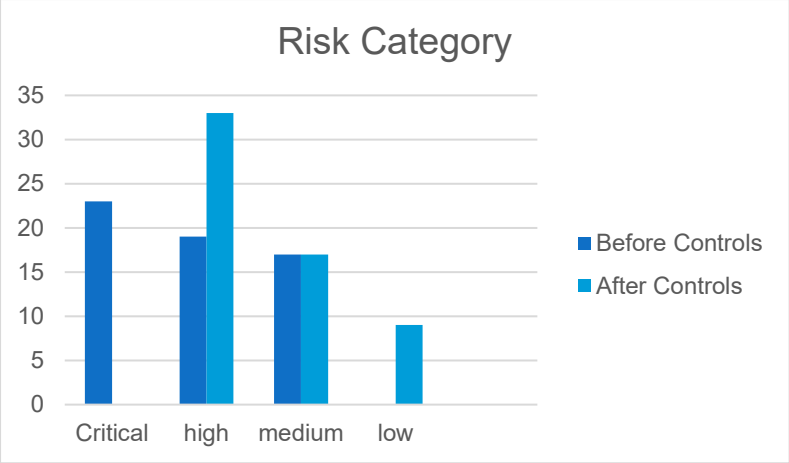

Figure 1: Risk categories – before and after controls

3.1 RISK CATEGORIES

The following risk categories were identified as part of this risk matrix:

- Consent
- Cybersecurity
- Data protection
- Data quality
- Ethical
- Legal
- Project Management
- Technical

3.2 SUMMARY OF RISKS

This subchapter provides a summary of the different risk items that were identified. It will make a distension between the risk level prior to as well as after taking into consideration risk controls.

In total, 59 risk items were identified, divided over the different risk categories as follows:

- Consent: 3
- Cybersecurity: 6
- Data protection: 7
- Data quality: 1
- Ethical: 2
- Legal: 9
- Project Management: 14
- Technical: 17

Prior to risk controls, 17 risk items were categorized as medium risk:

- Data protection: 1
- Legal: 1
- Project Management: 4
- Technical: 11

19 risk items were categorized as high risk:

- Cybersecurity: 3
- Data quality: 1
- Legal: 4
- Project Management: 8
- Technical: 3

Finally, 23 risk items were categorized as critical risk:

- Consent: 3
- Cybersecurity: 3
- Data protection: 6
- Ethical: 2
- Legal: 4
- Project Management: 2
- Technical: 3

After the introduction of the risk controls, this changes as follows:

9 risk items were categorized as low risk:

- Data protection: 1
- Legal: 1
- Technical: 7

17 risk items were categorized as medium risk:

- Cybersecurity: 2
- Legal: 3
- Project Management: 5
- Technical: 7

33 risk items were categorized as high risk:

- Consent: 3
- Cybersecurity: 4
- Data protection: 6
- Data quality: 1
- Ethical: 2
- Legal: 5
- Project Management: 9
- Technical: 3

No critical risk items remained when taking into consideration the risk controls, which demonstrates that the risk controls introduced/foreseen are generally considered/thought to be effective.

The evolution of risk level prior to and after introducing the different risk controls can be summarized in table format as follows:

Risk category	Risk level	Prior to risk controls	After risk controls
Consent	Low	0	0
	Medium	0	0
	High	0	3
	Critical	3	0
Cybersecurity	Low	0	0
	Medium	0	2
	High	3	4
	Critical	3	0
Data protection	Low	0	1
	Medium	1	0
	High	0	6
	Critical	6	0
Data quality	Low	0	0
	Medium	0	0
	High	1	1
	Critical	0	0
Ethical	Low	0	0
	Medium	0	0
	High	0	2
	Critical	2	0
Legal	Low	0	1
	Medium	1	3
	High	4	5
	Critical	4	0
Project Management	Low	0	0
	Medium	4	5
	High	8	9
	Critical	2	0
Technical	Low	0	7
	Medium	11	7
	High	3	3
	Critical	3	0

Table 4: Risk summary

4. HIGH RISKS IDENTIFIED

In this chapter, a few high risks that were identified are highlighted and further detailed.

This chapter highlights a selection of critical risks identified during the initial assessment phase, prior to the implementation of mitigation measures. These risks were considered critical due to their potential impact on e.g., compliance, data protection and operational continuity. For each risk, the following details are provided:

- Risk ID and category
- Description and scenario
- Inherent risk assessment (before controls)
- Mitigation measures
- Residual risk assessment (after controls)

4.1 OVERVIEW OF THE CRITICAL RISK ASSESSMENT APPROACH

A structured risk assessment was conducted using a combined dFMEA and methodology. This approach enabled the identification of both critical technical and procedural risks across the full lifecycle of the DS4H platform – from design to deployment.

As previously described, each risk was evaluated based on two dimensions:

- Likelihood of occurrence
- Impact on the project or stakeholders (severity)

Risks with a combination of high likelihood and severe impact were classified as critical.

4.2 RISK CATEGORIZATION AND PRIORITIZATION

The identified critical risks were grouped into several categories to facilitate analysis and prioritization. These categories include, amongst others:

- Consent and legal basis: Risks related to the absence or invalidity of patient consent.
- Cybersecurity: Risks involving unauthorized access, data breaches or privilege escalation.
- Regulatory compliance: Risks of non-conformity with GDPR, EHDS or Gaia-X requirements.
- Interoperability: Risks that could prevent the platform from integrating with other (e.g., European) data spaces.
- Operational continuity: Risks that could disrupt the availability or reliability of services.

These categories reflect the multidimensional nature of the DS4H project, which operates at the intersection of legal, technical and organizational domains.

4.3 RISK EXAMPLES

A few identified critical risks are further detailed below to illustrate the nature and severity of the threats identified:

- Absence of valid consent: Patient data may be processed without a valid legal basis due to system or process failures in consent verification. This could lead to GDPR violations and reputational damage.
- Unauthorized access to sensitive data: Weak access controls or compromised user accounts could result in data breaches, exposing sensitive health information.

- Non-Compliance with Gaia-X Requirements: Failure to align with Gaia-X specifications could prevent the platform from achieving certification and interoperability with other European data spaces.

Each of these risks was assessed in detail, targeted mitigation measures were proposed to reduce their severity to acceptable levels:

ID	Category	Description	Example	Inherent risk	Controls	Residual risk
R-01-03	Consent - Not obtained	Absence of informed consent	1. Data holder receives data request from requester 2. Data holder requests informed consent from patient to share data 3. Patient does or cannot give informed consent 4. Data holder processes data request and extract data 5. Data holder shares data with data requester without having obtained informed consent	**Critical** (Red) Likeli-hood: Likely Impact: Major	1. For pseudonymized data requests, an informed consent shall be available and approved by the national authorities (e.g., CNER) 2. In hospital EHR, informed consent is attached to respective patient record 3. In hospital EHR, a dedicated field can be added to the form to record that informed consent is obtained (for future) 4. Centralized consent management system 5. Use of (adapted and dedicated) flyers for patient to be informed	**High** (Orange) Likeli-hood: Possible Impact: Major
R-03-02	Cyber-security - Data integrity attack	Un-authorized modification of health data	1. Health data is made accessible through Dataspace4-Health platform and stored within Digital Twin model 2. Health data is stored is tampering with 3. Digital Twin tool is compromised (e.g., biased responses) 4. Potential severe impact on patient	**Critical** (Red) Likeli-hood: Possible Impact: Severe	1. Immutable logs 2. Blockchain audit trails 3. Data validation checks 4. User management (by design, users cannot enter/modify dataset)	**High** (Orange) Likeli-hood: Very rare Impact: Severe

R-03-08	Data protection - Data breach of personal data	Data breach or mishandling of sensitive (personal health) data	1. Data offering contains sensitive (personal health) data 2. There is a data breach 3. There is unauthorized access to sensitive (personal health) data	**Critical** (Red) Likeli-hood: Likely Impact: Severe	1. Data offering (in catalogue) contains only meta-data, no actual personal data 2. Data will be shared either anonymously or pseudonymously 3. Dataspace4Health uses a Secure Processing Environment 4. Data encryption at rest and in transit 5. Regular pen testing 6. Monitoring of platform 7. Regular (security) updates 8. Apply high security standards	**High** (Orange) Likeli-hood: Very rare Impact: Severe
R-03-14	Data quality	Incorrect, incomplete, or non-standardized data	1. Data holders have similar data structure which would allow for interoperability 2. Data holder does not fill the available data fields correctly, partially or entirely 3. Data quality is insufficient for data requestor	**High** (Orange) Likeli-hood: Possible Impact: Major	1. Hospitals in Luxembourg have a Department for Medical Information which are responsible for essential data quality (e.g., ICD coding) 2. Certification within care facilities results in a required level of (structured) health data quality 3. Certification is only obtained after audit by external party 4. Research- and care institute cooperate together to identify essential data elements that can be shared and to improve data quality	**High** (Orange) Likeli-hood: Unlikely Impact: Major

R-01-04	Ethical	Potential impact on privacy, stigma-tization, or patients fairness	1. Data holder receives data request from requester for data 2. Data holder requests informed consent from patients to share data 3. Due to growing ethical concerns in society, all or majority of patients do not consent in sharing data 4. Unavailability of data 5. Data Space concept is not/under utilized	**Critical** (Red) Likeli-hood: Possible Impact: Severe	1. Political acceptance and promotion of benefits of sharing data 2. Citizen education on benefits of access to large data 3. Educate healthcare professionals (HCP) of advantages of sharing data and having access to large datasets for patient care (either directly, or indirectly) 4. Patient education on benefits of sharing data to positively impact patient care (either directly, or indirectly)	**High** (Orange) Likeli-hood: Unlikely Impact: Severe

R-01-09	Legal – Regula-tory	Non-compliance GDPR, data utilization	1. Data holder receives data request from requester 2. Data holder processes data request and extract data 3. Data holder shares data with data requester 4. Data requestor uses data for different/secondary purpose other than original data request	**Critical** (Red) Likeli-hood: Likely Impact: Severe	1. Request to use patient data for different/secon-dary purpose needs to be requested and approved by national authorities (e.g., CNER) 2. Per DSA, data requestor can only utilize data in scope of specific data request and subsequent authorization 3. Per DSA, data holder is allowed to audit data requestor after sharing data to ensure proper use of data 4. Data holder can request declaration of deletion 5. Participants need to comply to applicable law (e.g., GDPR) 6. Use of smart contract to enforce the clauses and obligations within (ODRL)	**High** (Orange) Likeli-hood: Unlikely Impact: Severe
R-01-14	Project Manage-ment - Data governan ce	Lack of clear framework for access control, roles and traceability	1. There is no or insufficient access control 2. Unauthorized individuals / institutions can access (sensitive patient) data or associated tools (e.g., Digital Twin) 3. Non-conformance to GDPR	**Critical** (Red) Likeli-hood: Possible Impact: Severe	1. Identity management to ensure authentication 2. Audit trail 3. Defined roles and related responsibilities (e.g., "Doctor" and "Nurse" profiles for Digital Twin) 4. User training	**High** (Orange) Likeli-hood: Very rare Impact: Severe

R-03-6	Technical - Technical adoption	No or insufficient adoption from targeted participants	1. Technical solution is available 2. Target participant(s) are not or insufficiently able to technically adopt the cloud solution 3. Usage of DS4H is limited due to absence of participants	**Critical** (Red) Likeli-hood: Likely Impact: Severe	1. Possible to provide connector as a service (outsourcing) 2. Top-down change of digital healthcare strategy to provide necessary foundation for adoption for individual participant	**High** (Orange) Likeli-hood: Unlikely Impact: Severe

Table 5: High-risk examples

4.4 COMMON RISK PATTERNS AND DEPENDENCIES

Several cross-cutting patterns emerged from the risk analysis:

- Process gaps: Many risks stemmed from incomplete or manual processes, particularly in consent management and access control.
- Technical dependencies: Some risks were linked to external frameworks or third-party systems, introducing uncertainty and complexity.
- Interconnected risks: Certain risks were found to be interdependent – for example, a failure in consent validation could also trigger compliance and reputational risks.

These patterns highlight the need for integrated controls that address both root causes and downstream effects.

4.5 RESIDUAL RISK LANDSCAPE

Following the implementation of mitigation measures, all critical risks were reassessed. While most were successfully reduced to high or medium residual levels, some risks remain high due to factors such as:

- Limitations in automation or system maturity
- External dependencies (e.g., certification bodies)
- Evolving regulatory requirements

These residual risks are considered acceptable under current conditions, but are subject to continuous monitoring and periodic review.

4.6 IMPLICATIONS FOR GOVERNANCE AND MONITORING

The findings from the risk assessment have direct implications for the project's governance model. To ensure continuous risk control, the following measures shall be integrated into the DS4H governance framework:

- Regular updates to the risk matrix, reflecting changes in the regulatory or technical environment.
- Ongoing compliance checks (e.g., through internal audits).
- Periodic reviews of mitigation strategies, especially for high-residual risks.
- Clear accountability structures, ensuring that risk ownership is defined and monitored.

By embedding risk management into the project's operational and strategic oversight, DS4H aims to maintain a high level of assurance and stakeholder trust throughout the lifecycle of the health data space.

5. RISK MONITORING

Effective risk monitoring is essential to ensure that the DS4H project maintains at an acceptable risk posture throughout its lifecycle. This chapter outlines the monitoring framework, including frequency, responsibilities, tools and escalation procedures.

By implementing such structured approach, DS4H ensures that risk management remains continuous, transparent and aligned with compliance obligations such as GDPR, EHDS and Gaia-X principles.

5.1 OBJECTIVES OF RISK MONITORING

The primary objectives of the DS4H risk monitoring framework are to ensure that risk management remains continuous, proactive and aligned with project goals and regulatory requirements. Specifically, the monitoring process aims to:

- Track the evolution of residual risks and ensure they remain within acceptable thresholds.
- Identify new or evolving risks resulting from changes in the regulatory, technical or operational environment.
- Verify the effectiveness of implemented controls through audits, reviews and performance indicators.
- Support informed decision-making by providing up-to-date risk information to governance bodies.
- Ensure accountability by assigning clear ownership and follow-up responsibilities for each risk.

5.2 MONITORING PROCESS

The risk monitoring process is a structured and continuous activity designed to ensure that (critical) risks remain under control and that new risks are identified and addressed in a timely manner. It shall be fully integrated into the DS4H project governance and include the following key steps:

1. **Regular risk reviews:** Periodic reviews shall be conducted to reassess the status of identified risks, particularly those with high residual levels. These reviews shall evaluate whether the likelihood or impact of a risk has changed and whether existing mitigation measures remain effective.
2. **Dynamic risk matrix updates:** The risk matrix shall be continuously updated to reflect changes in the project environment, such as new regulatory requirements, technical developments or operational incidents. This will ensure that the risk profile remains current and relevant.
3. **Monitoring of Key Risk Indicators:** Quantitative and qualitative indicators shall be used to track early warning signs of risk materialization. These may include audit findings, incident reports, system performance metrics or user feedback.
4. **Audit and compliance checks:** Internal- and external audits shall be conducted to verify compliance with legal, technical and procedural requirements. These audits help validate the effectiveness of risk controls and identify any gaps.

5. **Incident and change management integration:** The risk monitoring process is linked to incident and change management workflows. Any significant incident or system change shall automatically trigger a risk (re)assessment to determine whether new risks have emerged or existing ones have worsened.
6. **Governance oversight and reporting:** Risk monitoring results shall be regularly reported to the project's Steering Committee and relevant stakeholders. This ensures transparency, accountability and timely decision-making regarding risk response strategies.
7. **Continuous improvement:** Lessons learned from risk events, audits and reviews shall be used to refine the risk management framework. This iterative approach supports the continuous improvement of both preventive- and corrective measures.

5.3 KEY PERFORMANCE INDICATORS

The effectiveness of the DS4H risk monitoring framework shall be assessed through a set of measurable indicators (Key Performance Indicators – KPIs) that provide insight into the project's ability to manage and reduce risks over time.

One of the most significant KPI is the number of critical- and/or high-level risks that remain after mitigation measures have been applied. This metric reflects the residual exposure of the project and demonstrates whether the mitigation strategy is achieving its intended effect. Reviews shall be conducted periodically, any significant concentration of critical- or high-level risks shall trigger an escalation process to reassess the adequacy of the controls in place.

Another important KPI is the average time required to implement mitigation measures. This measures the responsiveness of the risk management process and the ability of the project team to act promptly on identified risks. Monitoring this indicator ensures that mitigation actions are not only defined, but also executed within a reasonable timeframe to prevent risks from escalating.

Incident response time for security or compliance breaches is also a key metric. It shall measure the time elapsed between the detection of an incident and the implementation of corrective actions. This KPI is crucial for minimizing the impact of data breaches or regulatory violations. Tracking this indicator helps ensure that incidents are addressed promptly and effectively to maintain compliance and operational continuity.

Finally, the training completion rate for stakeholders involved in risk-related processes shall be monitored to ensure that all relevant personnel are equipped with the knowledge to manage and mitigate risks effectively. This indicator shall measure the percentage of stakeholders who have completed mandatory training programs such as GDPR compliance, cybersecurity awareness and consent management. Maintaining a high level of training completion is essential for reducing human-related risks and ensuring that all parties understand their responsibilities within the risk management framework.

5.4 TOOLS AND PLATFORMS

The DS4H risk monitoring framework relies on a combination of tools and platforms to ensure that risk management activities are efficient, transparent and fully integrated into project governance. The risk matrix is maintained in an Excel-based format, which serves as the central repository for all identified risks, their assessments and mitigation measures. This matrix is not static; it is regularly updated and linked to project governance tools to provide real-time visibility for decision-makers.

Incident management shall be handled through dedicated platforms such as Jira or ServiceNow, which allow for systematic tracking of issues, assignment of responsibilities and escalation when necessary. These tools ensure that incidents are documented, monitored and resolved within the defined response times, reducing the likelihood of operational disruptions or compliance breaches.

Compliance monitoring shall be supported by automated checks that continuously verify adherence to GDPR, EHDS and Gaia-X requirements. These automated processes help detect deviations early, enabling corrective actions before they escalate into significant risks. By combining these tools, DS4H shall ensure a robust, integrated approach to risk governance that aligns with both technical and regulatory expectations.

5.5 ESCALATION PROCEDURE

The escalation procedure within the DS4H risk monitoring framework shall ensure that any significant change in risk exposure is addressed promptly and effectively. When a residual risk increases in severity or when a new critical risk emerges, the process shall begin with an immediate alert to the appropriate governance structure. This alert shall be generated through the incident management system to avoid delays and ensure that all relevant stakeholders are informed in real time.

Once the alert is raised, a review shall be initiated to analyze the root cause of the escalation, evaluate the adequacy of existing controls and define corrective actions. These actions shall be prioritized based on the severity of the risk and its potential impact on compliance, data integrity and operational continuity. The review process shall also ensure that responsibilities for implementing the corrective measures are clearly defined to maintain accountability and prevent ambiguity.

All decisions taken during the escalation process shall be documented in the risk governance system, including the rationale for the chosen actions and the expected timeline for resolution. This documentation will ensure transparency and provides an auditable trail for future reviews or regulatory inspections. By following this structured approach, DS4H will ensure that critical- and high risks are managed in a timely and effective manner, reducing the likelihood of adverse outcomes.

6. CONCLUSION

This deliverable has provided a structured and transparent overview of the risk landscape associated with the DS4H project, covering the full lifecycle from design and implementation to operational phases. By applying a combined dFMEA and pFMEA methodology, the assessment has captured both technical and procedural risks, ensuring that critical issues related to compliance, data protection, interoperability and operational continuity are systematically addressed.

The results demonstrate that, following the introduction of targeted risk controls, no critical risks remain unmitigated and the risks have been reduced to acceptable levels. This outcome confirms the effectiveness of the proposed controls and highlights the value of a multidisciplinary approach that integrates legal, technical and operational expertise. While the overall risk posture has improved significantly, the presence of residual high-level risks underlines the need for continuous monitoring and proactive governance.

To support continued risk mitigation, the project framework shall include regular updates to the risk matrix, compliance assessments and periodic reviews of mitigation strategies. These activities aim to ensure that the risk management process remains adaptive to regulatory developments, technological evolution and operational demands. Integrating risk monitoring into the project's governance structure is intended to support data integrity, regulatory alignment and stakeholder confidence throughout the lifecycle of the health data space.

7. LITERATURE

1. AIAG & VDA (2019). FMEA Handbook – Failure Mode and Effects Analysis. Automotive Industry Action Group and Verband der Automobilindustrie.
2. IEC 60812:2018. Failure modes and effects analysis (FMEA and FMECA).
3. AIAG (2008). Process FMEA Manual. Automotive Industry Action Group.
4. ISO 31000:2018. Risk Management – Guidelines.

8. TABLES

9. FIGURE

10. ANNEX

						Inherent risk						Residual risk			
Risk ID level 1	Risk category level 1	Risk ID level 2	Risk category level 2	Risk description	Risk example	Risk applicability	Likelihood	Impact	Inherent risk level	Risk Controls	Effectiveness of the controls	Likelihood	Impact	Residual risk level	Risk acceptance
R-01	Design / creation	R-01-01	Consent - No longer obtained	Unexpected withdrawal of consent	1. Data holder receives data request from requester for data 2. Data holder requests informed consent from patient to share data 3. Patient gives informed consent 4. Data holder processes data request and extract data 5. After extracting the data, patient revokes informed consent 6. Data holder does not exclude patient that revokes informed consent from dataset 7. Data holder shares data with data requester without having obtained informed consent	Yes	Possible	Severe	Critical	1. Treating physician is responsible to manage a patient's informed consent and update when applicable 2. In hospital EHR, informed consent is attached to respective patient record 3. In hospital EHR, a dedicated field can be added to the form to record that informed consent is obtained (for future) 4. When the dedicated field for the informed consent is updated, data cannot be extracted and consequently shared (for future)	Effective	Very rare	Severe	High	Yes
R-01	Design / creation	R-01-02	Consent - No longer obtained	Unexpected withdrawal of consent	1. Data holder receives data request from requester for data 2. Data holder requests informed consent from patient to share data 3. Patient gives informed consent 4. Data holder processes data request and extract data 5. Data holder shares data with data requester 6. Patient revokes informed consent after sharing the data with data requestor 7. Data requestor stores/uses data even though patient revoked informed consent	Yes	Possible	Severe	Critical	1. Treating physician is responsible to manage a patient's informed consent and update when applicable, which will prevent data from being re-shared 2. In hospital EHR, informed consent is attached to respective patient record, which will prevent data from being re-shared 3. In hospital EHR, a dedicated field can be added to the form to record that informed consent is obtained (for future), which will prevent data from being re-shared 4. When the dedicated field for the informed consent is updated, data cannot be extracted and consequently shared (for future), which will prevent data from being re-shared 5. Per DSA, data requestor shall destroy data related to patient who revoked consent 6. Data requestor shall have specific procedures to destroy data	Partially effective	Unlikely	Severe	High	Yes
R-01	Design / creation	R-01-03	Consent - Not obtained	Absence of informed consent	1. Data holder receives data request from requester 2. Data holder requests informed consent from patient to share data 3. Patient does or cannot give informed consent 4. Data holder processes data request and extract data 5. Data holder shares data with data requester without having obtained informed consent	Yes	Likely	Major	Critical	1. For pseudonymized data requests, an informed consent shall be available and approved by the national authorities (e.g., CNER) 2. In hospital EHR, informed consent is attached to respective patient record 3. In hospital EHR, a dedicated field can be added to the form to record that informed consent is obtained (for future) 4. Centralized consent management system 5. Use of (adapted and dedicated) flyers for patient to be informed	Partially effective	Possible	Major	High	Yes
R-01	Design / creation	R-01-04	Ethical	Potential impact on privacy, stigmatization, or patients fairness	1. Data holder receives data request from requester for data 2. Data holder requests informed consent from patients to share data 3. Due to growing ethical concerns in society, all or majority of patients do not consent in sharing data 4. Unavailability of data 5. Data Space concept is not/under utilized	Yes	Possible	Severe	Critical	1. Political acceptance and promotion of benefits of sharing data 2. Citizen education on benefits of access to large data 3. Educate healthcare professionals (HCP) of advantages of sharing data and having access to large datasets for patient care (either directly, or indirectly) 4. Patient education on benefits of sharing data to positively impact patient care (either directly, or indirectly)	Partially effective	Unlikely	Severe	High	Yes
R-01	Design / creation	R-01-05	Ethical	Concerns of utilizing AI in regards to sensitive (personal health) data	1. Data holder receives data request from requester for data to be used with AI models 2. Data holder requests informed consent from patients to share data 3. Due to existing ethical concerns in society in regards to using AI on sensitive data such as health data, all or majority of patients do not consent in sharing data 4. Unavailability of data 5. Data Space concept is not/under utilized as well as specifically designed AI models	Yes	Possible	Severe	Critical	1. Political acceptance and promotion of benefits of AI in healthcare 2. Citizen education on benefits of AI in healthcare 3. Educate HCP of advantages of AI in healthcare 4. Patient education on benefits of AI in healthcare	Partially effective	Unlikely	Severe	High	Yes
R-01	Design / creation	R-01-06	Legal - Cross-border regulation conflicts	Different privacy, consent, or retention laws outside EU	1. Dataspace4Health is aligned with EU regulations only 2. Due to misalignment with other jurisdictions, scalability of project is limited 3. Access from data requestors who are not aligned with EU regulations in regards to privacy, consent and retention laws to (complete) data is limited, which limits innovation and subsequent personalized medicine 4. Data Space concept is under utilized, limiting potential added value (for patient)	Yes	Likely	Moderate	High	1. For (sensitive patient) data transfer outside of EU, in addition to CNER approval, national competent authority for data privacy needs to be demonstrated through a risk assessment related to scope of the data sharing (controlling authority is CNPD in Luxembourg) 2. Data holder has DPO and legal team to assess and contribute to non-EU agreement 3. Specific details on data privacy, consent and retention are documented within the contractual agreement between data holder and data requestor	Effective	Very rare	Moderate	Low	Yes
R-01	Design / creation	R-01-07	Legal - Regulatory framework misalignment	Regulatory frameworks may conflict or remain unclear across EU/local jurisdictions	1. Dataspace4Health is aligned with local regulations only 2. Due to misalignment with EU/other jurisdictions, scalability of project is limited 3. Access to (quality) data is limited, which limits innovation and subsequent personalized medicine 4. Data Space concept is under utilized, limiting potential added value (for patient)	Yes	Possible	Moderate	Medium	1. Legal stream to ensure assessment and if applicable harmonization of different regulations 2. Luxembourg, as EU country, adheres to EU regulations 3. Individual Data Sharing Agreements will require specifying the data processing	Effective	Unlikely	Moderate	Medium	Yes
R-01	Design / creation	R-01-08	Legal - Regulatory	Non-compliance GDPR, data minimalization	1. Data holder receives data request from requester 2. Data holder processes data request and extract data 3. Data holder shares data with data requester 4. Data shared contains more data elements than present in data request	Yes	Likely	Severe	Critical	1. Request to share patient data needs to be approved by national authorities (e.g., CNER) 2. Request to share patient data needs to be reviewed and approved by Data Protection Officer (DPO) of data holder in regards to GDPR requirements 3. Data holder assesses data request before sharing to ensure minimally requested data is provided 4. Per Data Sharing Agreement (DSA), data requestor can only utilize data in scope of specific data request and subsequent authorization	Effective	Very rare	Severe	High	Yes
R-01	Design / creation	R-01-09	Legal - Regulatory	Non-compliance GDPR, data utilization	1. Data holder receives data request from requester 2. Data holder processes data request and extract data 3. Data holder shares data with data requester 4. Data requestor uses data for different/secondary purpose other than original data request	Yes	Likely	Severe	Critical	1. Request to use patient data for different/secondary purpose needs to be requested and approved by national authorities (e.g., CNER) 2. Per DSA, data requestor can only utilize data in scope of specific data request and subsequent authorization 3. Per DSA, data holder is allowed to audit data requestor after sharing data to ensure proper use of data 4. Data holder can request declaration of deletion 5. Participants need to comply to applicable law (e.g., GDPR) 6. Use of smart contract to enforce the clauses and obligations within (ODRL)	Effective	Unlikely	Severe	High	Yes
R-01	Design / creation	R-01-10	Legal - Regulatory	Non-compliance GDPR, data storage	1. Data holder receives data request from requester 2. Data holder processes data request and extract data 3. Data holder shares data with data requester 4. Data requestor stores data for longer time than defined in data request	Yes	Likely	Moderate	High	1. Request to use patient data includes a defined storage/retention period which needs to approved by national authorities (e.g., CNER) 2. Per DSA, data requestor can only store data in scope of specific data request and subsequent authorization for defined time period 3. Per DSA, data holder is allowed to audit data requestor after sharing data to ensure storage of data 4. Data requestor shall have specific procedures in place to destroy data after defined storage period is exceeded 5. Data holder can request a formal notice that data was destroyed by data requestor (certificate of destruction and deletion) 6. Participants need to comply to applicable law (e.g., GDPR) 7. Use of smart contract to enforce the clauses and obligations within (ODRL	Effective	Unlikely	Moderate	Medium	Yes

						Inherent risk						Residual risk			
Risk ID level 1	Risk category level 1	Risk ID level 2	Risk category level 2	Risk description	Risk example	Risk applicability	Likelihood	Impact	Inherent risk level	Risk Controls	Effectiveness of the controls	Likelihood	Impact	Residual risk level	Risk acceptance
R-01	Design / creation	R-01-11	Legal - Regulatory	Non-compliance GDPR, data breach	1. Data holder receives data request from requester 2. Data holder processes data request and extract data 3. Data holder shares data with data requester 4. Data requestor stores data without safeguarding controls 5. Unsecure data storage	Yes	Likely	Severe	Critical	1. Request to use patient data includes data safeguarding which needs to approved by national authorities (e.g., CNER) 2. Per DSA, data requestor specifies how data will be safeguarded 3. Per DSA, data holder is allowed to audit data requestor after sharing data to ensure proper storage of data 4. Data requestor shall have specific procedures in place to store data 5. Gaia-X adds compliance requirements on the storage of data 6. Data requestor needs to be considered as reliable partner to onboard in ecosystem 7. Application and use of recognized standards	Effective	Unlikely	Severe	High	Yes
R-01	Design / creation	R-01-12	Legal - Regulatory	Unethical use of AI on health data	1. AI Act currently does not cover well sensitive (personal health) data 2. AI Act can be modified to better cover handling sensitive (personal health) data utilising AI 3. Change in regulation will impact design of the AI Model and respective functioning within the Data Space (more restrictive) 4. Nonconformance to regulation	Yes	Possible	Severe	Critical	1. Dataspace4Health includes Legal stream to monitor regulatory changes and to adapt where needed 2. Close cooperation as consortium to remain agile 3. Training of users in regards to how and what data to share with the AI tool(s) 4. AI Sandbox assessment (e.g., from CNPD) 5. AI policy is drafted as part of DS4H project 6. New participants need to agree to terms and conditions before onboarding (which should prevent unethical use) 7. Compliance with AI Act and GDPR	Effective	Unlikely	Severe	High	Yes
R-01	Design / creation	R-01-13	Legal - Regulatory	Overlap with European Health Data Space (EHDS)	1. Due to upcoming EHDS, society and/or impacted stakeholders do not see relevance of Dataspace4Health project 2. Lack of engagement and acceptance 3. Data Space concept is not/under utilized	Yes	Possible	Major	High	1. Political acceptance and promotion of benefits of Dataspace4Health 2. Citizen education on difference between EHDS (clear separation between primary- and secondary use of data), as well as the benefits of the Dataspace4Health project (intended data loop between primary- and secondary data) 3. Clear understanding of business strategy regarding Dataspace4Health (complement to upcoming EHDS)	Partially effective	Possible	Major	High	Yes
R-01	Design / creation	R-01-14	Project Management - Data governance	Lack of clear framework for access control, roles and traceability	1. There is no or insufficient access control 2. Unauthorized individuals/institutions can access (sensitive patient) data or associated tools (e.g., Digital Twin) 3. Nonconformance to GDPR	Yes	Possible	Severe	Critical	1. Identity management to ensure authentication 2. Audit trail 3. Defined roles and related responsibilities (e.g., "Doctor" and "Nurse" profiles for Digital Twin) 4. User training	Effective	Very rare	Severe	High	Yes
R-01	Design / creation	R-01-15	Project Management - Incomplete stakeholder	User or healthcare professional needs not adequately captured (availability of data)	1. Dataspace4Health does not onboard all healthcare stakeholders (such as hospitals, labs etc.) 2. Due to absent stakeholders, there is a lack of data availability (quantity) 3. Due to a lack of data availability, data quality may be insufficient for both primary- and secondary use 4. Data Space concept is not/under utilized and/or does not add value	Yes	Possible	Major	High	1. Project is open for new partners to join the consortium 2. Project is (actively) promoting and aiming to onboard new partners in healthcare 3. Stakeholder mapping is performed to have a clear overview of all potential stakeholders	Partially effective	Possible	Major	High	Yes
R-01	Design / creation	R-01-16	Project Management - Incomplete stakeholder	User or healthcare professional needs not adequately captured (usage of data)	1. Sufficient quality and quantity of data is available 2. Healthcare professionals do not utilize available data or associated tools 3. Patient does not benefit from innovative solution	Yes	Possible	Major	High	1. Identification of HPC that can be involved in project 2. Early involvement of HPC into project 3. Demonstrations and workshops with HPC	Partially effective	Unlikely	Major	High	Yes
R-01	Design / creation	R-01-17	Project Management - Incomplete stakeholder	User or researchers needs not adequately captured (usage of data)	1. Sufficient quantity of data is available 2. Data is of insufficient quality for research purposes 3. Researcher can and does not use available data 4. Data Space concept is not/under utilized and/or does not add value	Yes	Possible	Major	High	1. Data requestor will detail the required data elements as well as quantity (e.g., number of patients and/or time period of data) in data request 2. Data pre-processing by data holder 3. Clinical trails will ensure that data provided is of sufficient quality and quantity for meaning research innovation 4. Certifications within hospital aid to improve quality of data available	Effective	Unlikely	Major	High	Yes
R-01	Design / creation	R-01-18	Project Management - Incomplete stakeholder	Governmental bodies' needs not adequately captured	1. Governmental bodies are not or insufficiently involved (e.g., MoH, CNS, CNER etc.) 2. Lack of critical stakeholder engagement 3. Data Space concept is under utilized (e.g., ethical assessment and subsequent authorization can be incorporated and digitalized, but are not, resulting in inefficiencies)	Yes	Possible	Major	High	1. Project is funded by MECO, which ensures credibility and aids in onboarding other governmental bodies 2. Project is open for new partners to join the consortium 3. Project is (actively) promoting and aiming to onboard new partners in healthcare 4. Contact with different governmental bodies is initiated 5. Stakeholder mapping is performed to have a clear overview of all potential stakeholders	Partially effective	Possible	Major	High	Yes
R-01	Design / creation	R-01-19	Project Management - Lack of stakeholder engagement	Failure to involve all relevant stakeholders early on	1. Stakeholders are onboarded 2. Onboarded stakeholders are insufficiently engaged 3. Services offered by onboarded stakeholders are absent or incomplete 4. Data Space concept is under utilized	Yes	Possible	Moderate	Medium	1. Onboarded stakeholders have contractual obligation to project consortium 2. Regular meetings (Steering Board, Stream Leader etc.) ensure project coordination 3. Within project, dedicated workshops/meetings are scheduled to address specific topics	Partially effective	Unlikely	Moderate	Medium	Yes
R-01	Design / creation	R-01-20	Project Management - Unclear roles/responsibilities	Unclear governance or responsibility attribution across entities and sectors	1. Unclear roles and responsibilities between consortium partners 2. Lack of overall engagement/project success 3. Data Space concept is not/under utilized, or gaps within project	Yes	Possible	Major	High	1. Detailed project description (incl. list of deliverables) with roles and responsibilities of each partner defined 2. Regular meetings as consortium with different partners to align	Partially effective	Unlikely	Major	High	Yes
R-02	Build / implementation	R-02-01	Project Management - Delays	Delays in development, integration, or go-live	1. Dataspace4Health go-live is delayed 2. Delay in go-live results in budget exceeding 3. Due to budget issues, consortium partners (or sponsor) decide to terminate the project (before completion)	Yes	Likely	Severe	Critical	1. Dataspace4Health consortium is organized in such a way with different streams (and respective stream leaders), which ensures accountability 2. Dataspace4Health has dedicate project managers to track overall progress and budget consumption 3. Regular meetings with project sponsor (and consortium partners) to present project updates	Effective	Unlikely	Severe	High	Yes
R-02	Build / implementation	R-02-02	Project Management - Delays	Delays in development, integration, or go-live	1. Dataspace4Health go-live is delayed 2. While delayed, technology continues to evolve 3. Technical choices from Dataspace4Health does no longer meet technical requirements from targeted audience 4. Arrival of new projects/other competitors serving the target audience 5. Consortium partners (or sponsor) decide to terminate the project (before completion)	Yes	Possible	Major	High	1. Dataspace4Health consortium is organized in such a way with different streams (and respective stream leaders), which ensures accountability 2. Dataspace4Health has dedicate project managers to track overall progress and budget consumption 3. Regular meetings with project sponsor (and consortium partners) to present project updates 4. Dataspace4Health has dedicated technical stream, in case of delays technological choices can be adapted to remain competitive	Effective	Unlikely	Major	High	Yes
R-02	Build / implementation	R-02-03	Project Management - Funding	No funding to sustain Data Space	1. Dataspace4Health is a sponsored project with defined beginning and end date (and corresponding funding) 2. After end date of the project, there is no funding/insufficient funding to sustain the ecosystem 3. End of life of Dataspace4Health	Yes	Possible	Major	High	1. Project consortium consists of different partners with diverse backgrounds (e.g., governmental, public and commercial entities) which aids in defining a sustainable business model 2. Ecosystem in its entirety or aspects from it (such as Digital Twin use-case) can be commercialized 3. Governmental bodies can fund Dataspace4Health ecosystem due to its added value to the country	Partially effective	Unlikely	Major	High	Yes

						Inherent risk						Residual risk			
Risk ID level 1	Risk category level 1	Risk ID level 2	Risk category level 2	Risk description	Risk example	Risk applicability	Likelihood	Impact	Inherent risk level	Risk Controls	Effectiveness of the controls	Likelihood	Impact	Residual risk level	Risk acceptance
R-02	Build / implementation	R-02-04	Project Management - Insufficient testing	Testing environments not reflecting real-life scenarios	1. Dataspace4Health concept 2. There is no or insufficient testing of its functioning in practice 3. When in production, the ecosystem does not meet user needs 4. Data Space will not, or underutilized	Yes	Possible	Major	High	1. Dataspace4Health is a Proof-of-Concept, research project with ultimate goal to investigate if and how the Data Space concept can be used in practice 2. During PoC, there are different demonstrations to show target audience how it could work (no longer only a concept)	Effective	Very rare	Major	Medium	Yes
R-02	Build / implementation	R-02-05	Technical - Incompatible standards	Difficulty aligning DS4H with other industry standards	1. Dataspace4Health does not consider/is insufficiently aligned with available industry standards 2. Use of the ecosystem is restricted and not scalable 3. Underutilization of Data Space potential	Yes	Possible	Moderate	Medium	1. Dataspace4Health aims to align with industry standard (e.g., for the oncology work package, chose to take into consideration the German MII model for MTB) 2. Dataspace4Health is aligned with different EU regulations	Effective	Unlikely	Moderate	Medium	Yes
R-02	Build / implementation	R-02-06	Technical - Infrastructure limitations	Hosting or technical infrastructure not scalable or redundant	1. Dataspace4Health is build on Gaia-X framework 2. Gaia-X will no longer be utilized for Data Space needs / will be outdated 3. Dataspace4Health ecosystem will no longer be usable	Yes	Possible	Major	High	1. Technical infrastructure can be adapted to other technological choices	Effective	Unlikely	Major	High	Yes
R-02	Build / implementation	R-02-07	Technical - Interoperability	Difficulties integrating with existing systems or non-standard formats (primary & primary)	1. Hospitals in Luxembourg have different hospital information system (or different content within same HIS) 2. There is no harmonization on what and how health data is collected within hospitals 3. Health data between hospitals is not or insufficiently comparable 4. Difficulty when referring a patient to another care facility (lack of data)	Yes	Possible	Moderate	Medium	1. Medical coding in Luxembourg is done following ICD coding, which ensures harmonization of diagnostics and subsequent patient care 2. Certification within care facilities results in a standard way of reporting of (structured) health data 3. In absence of structured data, complementing unstructured data is available for primary purposes	Effective	Very rare	Moderate	Low	Yes
R-02	Build / implementation	R-02-08	Technical - Interoperability	Difficulties integrating with existing systems or non-standard formats (primary & secondary)	1. Hospitals in Luxembourg have different hospital information system (or different content within same HIS) 2. There is no harmonization on what and how health data is collected within hospitals 3. Health data between hospitals is not or insufficiently comparable 4. No access to large dataset required for secondary purposes of health data (research, statics etc.)	Yes	Possible	Moderate	Medium	1. Medical coding in Luxembourg is done following ICD coding, which ensures harmonization of diagnostics and subsequent patient care 2. Certification within care facilities results in a standard way of reporting of (structured) health data 3. Research- and care institute cooperate together to identify essential data elements that can be shared and to improve data quality	Effective	Very rare	Moderate	Low	Yes
R-02	Build / implementation	R-02-09	Technical - Lack of developed standards	No universal interoperability standard in between dataspaces or actors within a single dataspace	1. DS4H is not interoperable with other data spaces (incl. HDAB) 2. Usage of DS4H is limited	Yes	Possible	Moderate	Medium	1. Use of recognized standards 2. DS4H architecture foundation is interoperability by design	Effective	Unlikely	Moderate	Medium	Yes
R-02	Build / implementation	R-02-10	Technical - Lack of developed standards	Upstream change or withdrawal of standards	1. DS4H reference architecture is build following e.g., GAIA-X IDSA standard 2. The Gaia-X IDSA standard is significantly changed/expired 3. DS4H architecture is no longer adaptable with dataspaces using new standards 4. Usage of DS4H is limited	Yes	Possible	Moderate	Medium	1. Dataspace architecture can still run (although support is limited) 2. Required codes can be deployed locally (as they are open source) 3. Architecture and/or implementation can be adapted to new standards	Effective	Very rare	Moderate	Low	Yes
R-02	Build / implementation	R-02-11	Technical - Supply chain	Delays or unavailability of critical components or external services	1. Dataspace4Health ecosystem facilitates data exchange between different institutions 2. For this data exchange, critical components or services are required (e.g., pseudonymization, SPE) 3. Due to unavailable components, there is a delay or absence of requested data exchange	Yes	Possible	Moderate	Medium	1. Services can be performed outside of ecosystem (e.g., in-house pseudonymization, traditional data sharing agreement) 2. Existing SPE	Effective	Unlikely	Moderate	Medium	Yes
R-02	Build / implementation	R-02-12	Technical - Tech debt	Temporary code or architecture causing long-term issues	1. HDAB is not yet implemented in Luxembourg 2. Specific requirement for an HDAB in Luxembourg are not established and available 3. HDAB may imply a different process resulting in new requirement 4. DS4H can not be used within EU context	Yes	Likely	Severe	Critical	1. A PoC is shown to have guidance on how future requirements will be 2. EHDS is published 3. W/o HDAB alignment, DS4H could, in addition to Luxembourg, be used outside EU (e.g., Japan) for cross-border data sharing 4. DS4H can adapt its architecture and implementation to align with future HDAB requirement	Effective	Very rare	Severe	High	Yes
R-02	Build / implementation	R-02-13	Technical - Tech debt	Temporary code or architecture causing long-term issues	1. DS4H reference architecture is defined 2. DS4H reference architecture is not adapted to unique business needs 3. Technical architecture has to be defined prior to establishing all future needs 4. Technical architecture is not fitting to future needs 5. DS4H ecosystem is not or underutilized	Yes	Likely	Major	Critical	1. DS4H can have a translator between external dataspace (legal, technical, business) 2. One-by-one mapping to external request can take place (not scalable) 3. Architecture can be adapted to new business need	Effective	Very rare	Major	Medium	Yes
R-03	Run / operations	R-03-01	Cybersecurity - API Vulnerabilities	Poorly secured APIs allow data leakage	1. Access to health data through Dataspace4Health platform 2. Poorly secured FHIR API exposes sensitive patient metadata	Yes	Possible	Major	High	1. API gateway 2. Rate limiting 3. OAuth2 4. Vulnerability scanning 5. Pen-tests	Effective	Very rare	Major	Medium	Yes
R-03	Run / operations	R-03-02	Cybersecurity - Data integrity attack	Unauthorized modification of health data	1. Health data is made accessible through Dataspace4Health platform and stored within Digital Twin model 2. Health data is stored is tampering with 3. Digital Twin tool is compromised (e.g., biased responses) 4. Potential severe impact on patient	Yes	Possible	Severe	Critical	1. Immutable logs 2. Blockchain audit trails 3. Data validation checks 4. User management (by design, users cannot enter/modify dataset)	Effective	Very rare	Severe	High	Yes
R-03	Run / operations	R-03-03	Cybersecurity - Data Sovereignty Misalignment	Data processed outside approved jurisdictions	1. Dataspace4Health platform contains data 2. Backup of data 3. Backup is hosted outside EU violates GDPR	Yes	Possible	Severe	Critical	1. Data localization policies 2. Automated geo-fencing 3. Legal review 4. Contractual obligations	Effective	Unlikely	Severe	High	Yes
R-03	Run / operations	R-03-04	Cybersecurity - Denial of Service (DoS)	Disruption of data availability via malicious overload	1. Dataspace4Health is hosted on Gaia-X cloud-based servers 2. Dataspace4Health is exposed to the internet 3. Denial of Services attacks 4. Systems are no longer responding	Yes	Likely	Moderate	High	1. Traffic monitoring 2. Autoscaling 3. WAF (Web Application Firewall) 4. Contractual obligations (down-time)	Effective	Unlikely	Moderate	Medium	Yes
R-03	Run / operations	R-03-05	Cybersecurity - Insider threats	Malicious or negligent actors within participating institutions	1. Health data is accessible through Dataspace4Health platform 2. Data requestor requests access to data set 3. Data holder grants access 4. Unauthorized personnel from data requestor accessed datasets	Yes	Possible	Major	High	1. Data loss prevention (DLP) 2. Logging & monitoring 3. Awareness training 4. Contractual obligations and associated responsibilities	Effective	Unlikely	Major	High	Yes
R-03	Run / operations	R-03-06	Cybersecurity - Third-Party Risk	Vendor or digital partner causes vulnerability	1. Cloud partner misconfigures storage and/or is compromised 2. Health data is exposed (confidentiality, integrity & availability)	Yes	Possible	Severe	Critical	1. Third-party risk management 2. Contractual clauses 3. ISO 27001 compliance	Effective	Unlikely	Severe	High	Yes
R-03	Run / operations	R-03-07	Data protection - Data breach	Unauthorized access to sensitive (personal health) data	1. Health data is accessible through Dataspace4Health platform by unauthorized party 2. Dataspace4Health platform is insufficiently secure 3. Unauthorized party identifies vulnerabilities 4. Unauthorized party gains access to patient records (e.g., via weak API security)	Yes	Likely	Severe	Critical	1. Implement strong Identity Access Management (IAM) 2. Data encryption at rest and in transit 3. Regular pen testing 4. Monitoring of platform 5. Regular (security) updates 6. Apply high security standards	Effective	Unlikely	Severe	High	Yes
R-03	Run / operations	R-03-08	Data protection - Data breach of personal data	Data breach or mishandling of sensitive (personal health) data	1. Data offering contains sensitive (personal health) data 2. There is a data breach 3. There is unauthorized access to sensitive (personal health) data	Yes	Likely	Severe	Critical	1. Data offering (in catalogue) contains only meta-data, no actual personal data 2. Data will be shared either anonymously or pseudonymously 3. Dataspace4Health uses a Secure Processing Environment 4. Data encryption at rest and in transit 5. Regular pen testing 6. Monitoring of platform 7. Regular (security) updates 8. Apply high security standards	Effective	Very rare	Severe	High	Yes

						Inherent risk						Residual risk			
Risk ID level 1	Risk category level 1	Risk ID level 2	Risk category level 2	Risk description	Risk example	Risk applicability	Likelihood	Impact	Inherent risk level	Risk Controls	Effectiveness of the controls	Likelihood	Impact	Residual risk level	Risk acceptance
R-03	Run / operations	R-03-09	Data protection - Data Loss	Accidental deletion or corruption of health data	1. Health data is made accessible through Dataspace4Health platform 2. Health data is deleted or wrongly modified 3. Unavailability/poor quality of data 4. Potential severe impact on patient	Yes	Possible	Severe	Critical	1. Regular backups and go-back scenarios 2. Redundancy 3. BCP/DRP plans	Effective	Unlikely	Severe	High	Yes
R-03	Run / operations	R-03-10	Data protection - Data misuse	Use of data beyond initial purpose (e.g., commercial profiling)	1. Data holder receives data request from requester 2. Data holder processes data request and extract data 3. Data holder shares data with data requester 4. Data requester uses data for different/secondary purpose other than original data request	Yes	Likely	Severe	Critical	1. Request to use patient data for different/secondary purpose needs to be requested and approved by national authorities (e.g., CNER) 2. Request to share patient data needs to be reviewed and approved by Data Protection Officer (DPO) of data holder in regards to GDPR requirements 3. Per DSA, data requestor can only utilize data in scope of specific data request and subsequent authorization 4. Per DSA, data holder is allowed to audit data requestor after sharing data to ensure proper use of data 5. GDPR requirements	Partially effective	Unlikely	Severe	High	Yes
R-03	Run / operations	R-03-11	Data protection - Identity & access management failures	Mismanagement of identities across federated entities	1. Employee and/or third-party has access to system 2. Employee leaves/changes the company 3. Employee's and/or third-party's access rights are not revoked 4. Unauthorized access to sensitive (personal health) data	Yes	Possible	Severe	Critical	1. Role-based access control 2. Federated identity management 3. Continuous access reviews (incl. off-boarding process) 4. Policies and procedures 5. IAM tools 6. Regular process auditing	Effective	Unlikely	Severe	High	Yes
R-03	Run / operations	R-03-12	Data protection - Privacy Re-identification Risk	Risk of data subjects (e.g., patient) re-identification from linked datasets	1. Dataspace4Health platform contains pseudonymized data 2. Table of Correspondence is compromised 3. Pseudonymized datasets reveals identity	Yes	Likely	Severe	Critical	1. Differential privacy 2. K-anonymity 3. Data minimization 4. Third-party control mechanisms (e.g., Lux Trust, LNDS)	Effective	Very rare	Severe	High	Yes
R-03	Run / operations	R-03-13	Data protection - Shadow IT / Uncontrolled Systems	Use of unsanctioned systems by partners	1. Data holder uses Dataspace4Health platform 2. Data is shared through connectors 3. Connector is not, or insufficiently limited (/ protected) 4. Other, non-controlled data can be shared outside approved Gaia-X framework	Yes	Unlikely	Moderate	Medium	1. Enforced access policies 2. Partner training 3. Platform onboarding process 4. Validation of connector set-up and subsequent monitoring	Effective	Very rare	Moderate	Low	Yes
R-03	Run / operations	R-03-14	Data quality	Incorrect, incomplete, or non-standardized data	1. Data holders have similar data structure which would allow for interoperability 2. Data holder does not fill the available data fields correctly, partially or entirely 3. Data quality is insufficient for data requestor	Yes	Possible	Major	High	1. Hospitals in Luxembourg have a Department for Medical Information which are responsible for essential data quality (e.g., ICD coding) 2. Certification within care facilities results in a required level of (structured) health data quality 3. Certification is only obtained after audit by external party 4. Research- and care institute cooperate together to identify essential data elements that can be shared and to improve data quality	Effective	Unlikely	Major	High	Yes
R-03	Run / operations	R-03-15	Legal - Compliance Risk	Failure to meet Gaia-X, GDPR, eIDAS or other regulation/framework requirements	1. Dataspace4Health platform contains data 2. No audit trail of data access by partners 3. Non-compliance with applicable regulations or frameworks 4. No enforcement of the requirements	Yes	Possible	Major	High	1. Continuous compliance auditing 2. Legal oversight 3. DPO function 4. Contractual obligations (incl. audit trail retention period)	Effective	Very rare	Major	Medium	Yes
R-03	Run / operations	R-03-16	Project Management - Governance failure	Governance committees inactive, absent, or ineffective post-deployment	1. Dataspace4Health is available 2. There is a lack of governance 3. Lack of coordination between different consortium partners 4. The solution is not working, or working suboptimal	Yes	Possible	Moderate	Medium	1. Onboarded stakeholders have contractual obligation to consortium 2. Regular meetings (Steering Board, Stream Leader etc.) ensure coordination 3. Dedicated workshops/meetings are scheduled to address specific topics 4. Alternative service providers will be identified	Effective	Unlikely	Moderate	Medium	Yes
R-03	Run / operations	R-03-17	Project Management - Lack of user support	End-users not trained, no onboarding plans or documentation	1. Dataspace4Health is available 2. Target audience is engaged to using the ecosystem 3. Target audience is not trained on how to use the ecosystem 4. Due to lack of knowledge, target audience does not use the ecosystem (correctly)	Yes	Possible	Moderate	Medium	1. Dedicated user training (instructions, helpdesk, FAQ etc.) 2. Following of activity to monitor if target audience is correctly using the solution	Effective	Unlikely	Moderate	Medium	Yes
R-03	Run / operations	R-03-18	Project Management - User adoption	Low uptake or resistance to the solution by end users	1. Dataspace4Health is available 2. Target audience are resistance to the available ecosystem 3. Target audience are not or less confident in the solution 4. Data Space will be not or underutilized	Yes	Possible	Moderate	Medium	1. Political acceptance and promotion of benefits of sharing data 2. Citizen education on benefits of sharing of data 3. Educate healthcare professionals (HCP) of advantages of sharing data and having access to large datasets for patient care (either directly, or indirectly) 4. Patient education on benefits of sharing data to positively impact patient care (either directly, or indirectly)	Effective	Unlikely	Moderate	Medium	Yes
R-03	Run / operations	R-03-19	Technical - Availability of the solution	Temporary or permanent unavailability of the solution	1. Federator is down due to e.g., network or infrastructure issues, cyberattack etc. 2. Discovery and publishing services are no longer working 3. Disruption of the system	Yes	Possible	Major	High	1. Redundancy of the federator can ensure that federator stays up 2. SLA to ensure minimum downtime 3. Adherence to NIS2 4. Federator is run on reliable infrastructure 5. Manual publishing and discovery possible	Effective	Very rare	Major	Medium	Yes
R-03	Run / operations	R-03-20	Technical - Availability of the solution	Temporary or permanent unavailability of the solution	1. One or several services or functionalities of the federator are down 2. Disruption of the system (e.g., metadata is tampered with) 3. Usage of DS4H is limited	Yes	Unlikely	Moderate	Medium	1. Revert to previous version of the working component 2. Robust test incl. unit, integration and end-to-end testing environment before going public	Effective	Very rare	Moderate	Low	Yes
R-03	Run / operations	R-03-21	Technical - Degraded availability of the solution	Degraded availability of the solution for one or multiple partners	1. Connector is down due to e.g., network or infrastructure issues, cyberattack etc. 2. Discovery and publishing services are no longer working for one or multiple partners 3. Usage of DS4H is limited	Yes	Possible	Moderate	Medium	1. Redundancy of the connector can ensure that connector stays up 2. SLA to ensure minimum downtime 3. Adherence to NIS2 4. Connector is run on reliable infrastructure	Effective	Very rare	Moderate	Low	Yes
R-03	Run / operations	R-03-22	Technical - Degraded availability of the solution	Degraded availability of the solution for one or multiple functions	1. One or several services or functionalities are down (e.g., contracting) 2. Disruption of the system 3. Usage of DS4H is limited	Yes	Possible	Moderate	Medium	1. Revert to previous version of the working component 2. Robust test incl. unit, integration and end-to-end testing environment before going public	Effective	Unlikely	Moderate	Medium	Yes
R-03	Run / operations	R-03-23	Technical - Monitoring failure	No mechanism to detect anomalies, errors, or outages	1. Federator, connector or service is down 2. Usage of DS4H is limited	Yes	Possible	Major	High	1. By design, observability of whole dataspace with automatic alerts 2. By design, observability for participants with automatic alerts	Effective	Very rare	Major	Medium	Yes
R-03	Run / operations	R-03-24	Technical - Provider	Failure or service interruption from an external provider	1. One or several services or functionalities from external provider are down (e.g., pseudonymization service, storage provider) 2. Disruption of the system 3. Usage of DS4H is limited	Yes	Possible	Moderate	Medium	1. Redundancy of the services 2. Some services may be handled offline (e.g., pseudonymization) 3. Services from other service provider within ecosystem can be utilized	Effective	Very rare	Moderate	Low	Yes
R-03	Run / operations	R-03-25	Technical - Vendor lock-in	Dependency on a provider	1. Locked with specific provider or solution 2. Locked with specific infrastructure provider 3. Limits flexibility and negotiation power	Yes	Unlikely	Moderate	Medium	1. Open source (Apache 2.0) solution that are publicly available 2. Working according to Gaia-X framework	Effective	Very rare	Moderate	Low	Yes
R-03	Run / operations	R-03-26	Technical - Technical adoption	No or insufficient adoption from targeted participants	1. Technical solution is available 2. Target participant(s) are not or insufficiently able to technically adopt the cloud solution 3. Usage of DS4H is limited due to absence of participants	Yes	Likely	Severe	Critical	1. Possible to provide connector as a service (outsourcing) 2. Top-down change of digital healthcare strategy to provide necessary foundation for adoption for individual participant	Partially effective	Unlikely	Severe	High	Yes