DATASPACE 4HEALTH
LUXEMBOURG

Assessment Report: Gaia-X Compliance Status

Document ID: DS4H_WP9_D9.3

Hee Kim and Maximilian Fünfgeld

Luxembourg Institute of Health (LIH)

Date: 24/06/2026

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 Versions

Version n°	Issue Date	Reason for change
0.0	05/06/2026	First draft.
0.1	19/06/2026	Typo corrections and enrichment of references.
0.2	24/06/2026	The target scope is specified to legal participant's onboarding, while leaving other entities for future releases.
1.0	24/06/2026	Final version has been sent to the coordinator.

TABLE OF CONTENTS

TABLE OF FIGURES

Glossary

Abbreviation	Expression
DS4H	Dataspace4Health
Gaia-X	A federated secure data infrastructure initiative
GXDCH	Gaia-X Digital Clearing House
VP	Verifiable Presentation
VC	Verifiable Credential(s)
JSON-LD	JavaScript Object Notation for Linked Data
JWT	JSON Web Token
EEA	European Economic Area
GDPR	General Data Protection Regulation
AI Act	Artificial Intelligence Act
MDR	Medical Device Regulation
EHDS	European Health Data Space
DGA	Data Governance Act
W3C	World Wide Web Consortium
OAuth2	Open Authorization 2.0
OpenID	OpenID Connect

1. INTRODUCTION

Dataspace4Health (DS4H) is a healthcare data exchange ecosystem designed to enable open and secure healthcare data exchange in Luxembourg. DS4H aims to improve clinical insights, accelerate research outcomes, and enhance patient care by enabling healthcare stakeholders in Luxembourg to share healthcare data across two disease areas: diabetes and oncology.

Operating at the intersection of healthcare data exchange, data infrastructures, and advanced analytics, the DS4H ecosystem relies on a technical framework called Gaia-X Trust Framework [1], which ensures three interoperability layers, namely organisational interoperability, semantic interoperability, and technological interoperability.

The objective of this assessment is to evaluate the current compliance status of DS4H and identify gaps in achieving a higher level of compliance, and outlines the necessary steps to bridge the gap. Achieving a higher Gaia-X Compliance label level will add the credibility and trustworthiness of the DS4H ecosystem. The enhanced trust will encourage participation, facilitate data sharing, and support long-term ecosystem growth.

2. GAIA-X COMPLIANCE

Compliance refers to specific guidelines, principles, or regulations that determine how parties operate, makes decisions, and enforces its policies. Likewise, Gaia-X Compliance refers to adherence to a set of guidelines, principles, and governance frameworks that ensure transparency, interoperability, and trust among participants in a digital ecosystem. These rules define how entities share data, and enforce policies in a standard manner.

The Gaia-X Compliance is structured around a core set of principles, such as logical groups of service attributes. Key characteristics of Gaia-X Compliance include:

- Alignment with existing schemes, certifications, and approved codes of conduct wherever possible for simplification.
- Introduction of new criteria only when existing standards are insufficient
- Compliance criteria can be attested by self-declaration or formal certification
- Applicability to three entities, namely: participants, cloud services, and data exchange services
- Extensible to any ecosystem to adapt the framework to their specific needs

2.1. GAIA-X STANDARD COMPLIANCE AND LABELS

Gaia-X Compliance [2] begins with baseline compliance and advanced assurance levels, represented through a structured labelling system. These labels act as a measurable indicator of trust offering transparency to participants in the ecosystem. It structures four assurance levels as shown in Figure 1 and the attestation can be requested for any type of service and product offerings.

- **Gaia-X Standard Compliance:** This is the base assurance. A service or product is compliant with mandatory requirements related to transparency, security, interoperability, portability and sustainability.
- **Gaia-X Label Level 1:** It builds upon the standard requirements and incorporates additional European rules related to data protection regulations. It ensures that personal data is handled according to European privacy standards.

- **Gaia-X Label Level 2:** This level introduces additional requirements related to cybersecurity. It also mandates service providers to offer an option for processing and sharing customer data [3] exclusively within the European Economic Area (EEA).
- **Gaia-X Label Level 3:** This is the highest assurance level requiring full compliance with Level 2 criteria and enforces strict geographic constraints such as that data must be processed and shared exclusively within the EEA, as well as that the service provider's headquarter center must be located within the EEA.

property	Standard Compliance	Level 1	Level 2	Level 3
Declaration of Service or Product	✓	✓	✓	✓
Signed with verified method (e.g. eIDAS)	✓	✓	✓	✓
Automated validation by GXDCH	✓	✓	✓	✓
Automated verification by GXDCH*	✓	✓	+	+
Data Exchange Policies	✓	✓	✓	✓
Certified Label Logo		✓	✓	✓
Data protection by EU legislation		✓	✓	✓
Manual verification by CAB			✓	✓
Provider Headquarter within EU				✓

*: *not all criteria can be automated.

+: means automated verification of the evidence issuer (Standard & CAB)

Figure 1. Gaia-X Compliance property and its four assurance levels.

2.2. GAIA-X COMPLIANCE WORKFLOW OVERVIEW

Any legal entities wishing to join a Gaia-X ecosystems need to undergo a compliance process that results in the issuance of Gaia-X Verifiable Credentials. Figure 2 illustrates the Gaia-X Compliance process defined in four steps. The issued Gaia-x credentials enable the user to engage in data exchange activities. Creating a service offering, storing it in a digital wallet, and publishing it to a catalogue were demonstrated and reported in DS4H deliverable 5.5 [4].

The workflow is broken down into four steps for attaining and using the Gaia-X credential:

1. **Provide a Verifiable Presentation:** Participants need to assemble information about their identity, services, and compliance attributes and submit a verifiable presentation (VP). VP must be cryptographically secure and machine-readable.
2. **Call a Gaia-X Digital Clearing House:** The VP is submitted to a Gaia-X Digital Clearing House (GXDCH). GXDCH verifies signatures and credentials, evaluates compliance requirements, and determines whether the participant satisfies the Gaia-X Compliance criteria.
3. **Store the Gaia-X Verifiable Credentials:** If the VP is successfully validated, Gaia-X Verifiable Credentials (VC) [5] are issued and securely stored in the participant's digital wallet. These

credentials are machine-verifiable and can be stored in credential repositories such as digital wallets.

4. **Use the Gaia-X Verifiable Credential:** Participants can use the issued credentials and interact with other participants in data space ecosystems. Example activities include catalogue browsing, service offering publication, establishing digital agreements, etc.

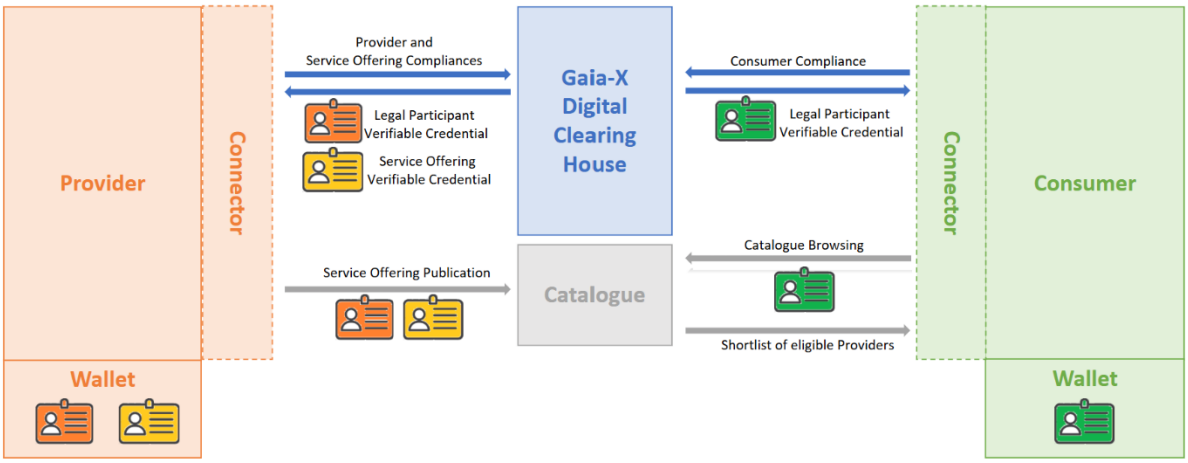

Figure 2. Gaia-X Compliance Workflow Overview.

3. GAIA-X COMPLIANCE GAP ANALYSIS FOR DS4H

Achieving higher Gaia-X Compliance label levels strengthens trust in the DS4H ecosystem. By progressing from Gaia-X Standard Compliance to Gaia-X Label Level 1, DS4H can demonstrate stronger alignment with European regulatory principles and improve confidence among ecosystem participants.

3.1. CURRENT STATUS: STANDARD COMPLIANCE (TAGUS RELEASE)

The current DS4H implementation aligns with the Gaia-X Standard Compliance level under the Tagus release. This indicates that the DS4H meets the essential requirements required for participation in a Gaia-X ecosystem. Evidences are based on self-declared descriptions defined in the service metadata and are not mandated through third-party validation.

While aiming the Gaia-X Standard Compliance level could enhance rapid adoption, it is missing higher assurance, in particular, compliance with the European legislations. Moreover, Tagus release is currently deprecated and GXDCH is no longer publishing verifiable credentials.

3.2. TARGET STATUS: COMPLIANCE LABEL LEVEL 1 (DANUBE RELEASE)

The DS4H project aims to achieve Gaia-X Label Level 1 compliance under the Danube release, focusing on legal participants onboarding during the project lifespan, while progressively scale compliance to cloud services and data exchange services for the future release. This target introduces additional requirements, particularly in regards to data protection obligations in the European Union. Attaining Gaia-X Label Level 1 will demonstrate that DS4H not only meets baseline compliance to join a Gaia-X ecosystem, but also adheres to European regulatory standards for handling sensitive data.

Although this level still relies on self-declaration, it reflects a strong commitment of the DS4H ecosystem to guarantee a higher degree of trust and regulatory alignment compared to the standard level. In other

words, Gaia-X Label Level 1 indicates that DS4H provides assurances regarding the lawful processing and protection of health-related data.

3.3. GAP ANALYSIS

In order to achieve the target compliance level of Gaia-X Label Level 1 in the Danube release, two complementary areas require further work as shown in Table 1. The following sections provide further details on each gap area and the corresponding roadmap to achieve the target status.

Table 1. Gap Analysis for the DS4H.

Gap Area	Current Status	Target Status
Regulatory Framework	Gaia-X Standard Compliance	Gaia-X Label Level 1
Technical Framework	JSON-LD-based credential representations	JWT-based credential representations

While Gaia-X Compliance primarily operates at the technical and semantic interoperability layer, higher assurance levels (e.g., Label Level 1) require adherence to regulatory requirements regarding personal data protection. In parallel, the Gaia-X Trust Framework is evolving technically, introducing changes in how credentials are structured and exchanged across ecosystems.

3.3.1. REGULATORY FRAMEWORKS

Regulatory adherence constitutes a critical prerequisite for achieving the targeted assurance level. In other words, attaining Gaia-X Label Level 1 demonstrates accessing and processing healthcare data securely according to the European legal requirements, particularly those governing personal healthcare data. GXDCH performs automated validation of self-declared compliance claims and issues VC, however, it does not provide a manual audit for Gaia-X Label Level 1.. Thus, it requires the DS4H partner to provide transparency and evidence regarding their legal and data protection obligations. The DS4H implementation considers several regulatory regulations reported in deliverable 2.1 [6].

- **General Data Protection Regulation (GDPR)** [7]**:** Governs lawful processing and protection of personal data
- **Artificial Intelligence Act (AI Act)** [8]**:** Defines risk-based requirements for AI systems
- **Medical Device Regulation (MDR)** [9]**:** Regulates safety and performance of medical devices
- **European Health Data Space (EHDS)** [10]**:** Facilitates secure and interoperable health data exchange and access
- **Data Governance Act (DGA)** [11]**:** Establishes mechanisms for trusted data sharing and reuse

3.3.2. TECHNICAL FRAMEWORK EVOLUTION (TAGUS TO DANUBE)

In addition to regulatory adherence, DS4H must address and align to the evolution of the Gaia-X technical trust framework**,** especially regarding the representation and exchange of credentials. In earlier releases (e.g., Tagus), Gaia-X Credentials were typically expressed as JSON-LD documents enriched with Gaia-X ontology contexts, while recent releases (e.g., Loire and Danube) shift from JSON-LD toward JSON Web Token (JWT) [12], while remaining compatible with the W3C VC model. These evolutions strengthen interoperability with broader European initiatives, including eIDAS 2.0 and the European Digital Identity Wallet ecosystem [13].

JWT structure is a serialized credential, consisting of three elements: Header (metadata), Payload (claims), and Signature (cryptographic proof ensuring integrity and authenticity). The Gaia-X credential eases to transmit and integrate with existing web infrastructures such as OAuth2/OpenID.

4. CONCLUSION

This assessment addresses the evolution from Gaia-X Standard Compliance (Tagus) to Label Level 1 (Danube) and encourages filling both regulatory and technical gaps. From a regulatory perspective, DS4H must strengthen its regulatory adherence to meet Label Level 1 expectations. It must ensure consistent adherence with European regulations, particularly GDPR, EHDS, DGA, AI Act, and MDR where relevant. From a technical perspective, on the other hand, DS4H must adapt its credential infrastructure to support evolving Gaia-X specifications. In particular, a key change is the transition from JSON-LD-based credential representations to JWT-based verifiable credentials, improving compatibility with other European trust infrastructures and supporting long-term sustainability of the platform.

The DS4H ecosystem operates in a highly regulated environment. By addressing these two dimensions in this assessment, DS4H will enhance its level of trust, improve its interoperability, and position itself as a trustful and robust healthcare data ecosystem.

REFERENCES

1. Gaia-X European Association. Gaia-X Trust Framework (latest version). Retrieved June 2026, from https://docs.gaia-x.eu/
2. Gaia-X Standard Compliance and Labels. Retrieved June 2026, from https://docs.gaia-x.eu/policy-rules-committee/compliance-document/2.5.0/Introduction_and_scope/
3. Gaia-X Glossary: Cusromer Data. Retrieved June 2026, from https://gaia-x.gitlab.io/glossary/customer_data/?utm_source=chatgpt.com
4. Dataspace4Health Deliverable 5.5 POC Demonstration Report: Interconnect Data Provider and Data User. Dataspace4Health February. 2026.
5. W3C. Verifiable Credentials Data Model 1.1. Retrieved June 2026, from https://www.w3.org/TR/vc-data-model/
6. Dataspace4Health Deliverable 2.1 Create a Minimal legal framework to enable the success of the new Data Space. Dataspace4Health July. 2025.
7. European Commission. General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679. Retrieved June 2026, from https://eur-lex.europa.eu/eli/reg/2016/679/oj
8. European Commission. Artificial Intelligence Act (AI Act). Retrieved June 2026, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689
9. European Commission. Medical Device Regulation (MDR) – Regulation (EU) 2017/745. Retrieved June 2026, from https://eur-lex.europa.eu/eli/reg/2017/745/oj
10. European Health Data Space Regulation (EHDS). (2025). REGULATION (EU) 2025/327 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500327
11. European Commission. Data Governance Act (DGA) – Regulation (EU) 2022/868. Retrieved June 2026, from https://eur-lex.europa.eu/eli/reg/2022/868/oj
12. Jones, Michael B.; Bradley, John; Sakimura, Nat (May 2015). JSON Web Token (JWT). IETF. doi:10.17487/RFC7519. ISSN 2070-1721. RFC 7519.
13. European Commission. eIDAS 2.0 and European Digital Identity Wallet. Retrieved June 2026, from https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/915931811/The+European+Digital+Identity+Regulation