Geographical and Domain Extension of the Gaia-X Framework

White Paper

Editorial Information

Publisher

Gaia-X European Association for Data and Cloud AISBL
Avenue des Arts 6-9
1210 Brussels
www.gaia-x.eu

Authors

Gaia-X European Association for Data and Cloud

Contact

https://gaia-x.eu/contact/

Other format

The output is published also here

Copyright notice

Disclaimer. This white paper is for informative purposes only and does not constitute a normative document within the Gaia-X Framework. Rather, it's being presented as a space to explore possible scenarios and meaningful ideas for the improvement of the framework regarding industrial requirements from different regions and sectors of the global economy. More specifically, we seek to map ideas and strategies towards the extension of the Gaia-X Compliance Framework for geographical and domain-specific contexts and use cases. The white paper is also meant as a tool for collecting further feedback from stakeholders. Additionally, this document is not proposing final solutions for the issues described. It simply presents some indicative requirements based on user stories, and explores alternatives, highlighting their advantages and disadvantages, for future selection by the Gaia-X Policy Rules Committee (PRC) and further validation by the Gaia-X Board of Directors (BoD). We expect the results of this work to help us produce and improve further documents (e.g., Compliance document, Architecture Document, ontology, and naming, branding and license guidelines), all of which are conditioned to Gaia-X formal review and validation processes.

Table of Contents

Executive Summary

Since its conception, the Gaia-X Framework has been endorsed and adopted by organizations beyond the European region, with the continuing establishment of new hubs and initiatives currently in progress. As the Gaia-X Ecosystem continues to expand globally, it's becoming increasingly clear that the framework must adapt to both geographical- and domain-specific contexts to help ensure regulatory compliance across different industries and international jurisdictions. While the current Gaia-X Compliance Document[1] outlines general criteria applicable to all participants - primarily Cloud Service Providers (CSPs), with a small extension for Data Products - we believe there is significant potential in developing domain-specific extensions to enhance its value.

With this in mind, the Gaia-X Policy Rules Committee (PRC) organized a Working Group (operationalized through the Geographical and Domain Extension Sprint) to write this white paper, seeking to explore possible concepts and scenarios for geographical and domain extensions of the Gaia-X Framework.

In the following chapters, we begin by defining key terms - such as ecosystem and domain - to establish a common understanding. We then examine contexts where extensions may be needed to address new demands while providing additional value to the Gaia-X Ecosystem. Some domain-specific use cases are discussed, including in finance, mobility, and aerospace and defense. The paper also explores governance mechanisms, protocols, and procedures for evaluating whether or not extension initiatives should be pursued. Most importantly, we present four strategic governance scenarios (outlined below), along with potential technical requirements related to the pursuit of geographical and domain extensions.

During the development of this white paper, we identified several key considerations for such extensions. These include questions such as: what kinds of entities or artefacts can be labelled, who defines and maintains these labels, the governance or oversight structures they require, and who is responsible for implementing and operating the necessary tooling. For each of these areas, we outlined plausible options, which were then combined to create the four governance scenarios.

[1] Gaia-X Compliance Document. 24.11 Release. Available at: https://docs.gaia-x.eu/policy-rules-committee/compliance-document/24.11/. Accessed: 12 March 2025.

It’s important to emphasize that the scenarios presented here are not definitive decisions or formal recommendations. Rather, they are intended to inform discussion and invite stakeholder feedback. A brief comparative summary of the scenarios is provided below, with detailed descriptions in the following sections.

Table 1. Summary of suggested governance scenarios

Scenario 1	Scenario 2	Scenario 1	Scenario 4
• Anybody can create a label related to whatever digital artefact they want, for whatever purpose they want, with or without adoption of Gaia-X values. • Whoever creates a label, becomes a label custodian. • The tooling associated with the label is also designed, implemented, deployed and run by the custodian.	• Very strict compliance rules in a single Compliance Document that the PRC reviews. • Labels are designed, maintained and deployed by the Gaia-X PRC, based on requirements established by the Gaia-X Data & Services Business Committee (DSBC). • The criteria are designed by Gaia-X Policy Rules Committee (PRC). If needed, the Gaia-X Ontology is extended by a Working Group under control of the Gaia-X Technical Committee (TC).	• Anybody can create a label related to whatever digital artefact they want, for whatever purpose they want, with or without adoption of Gaia-X values. • If the proposed extension aligns with Gaia-X values and passes a technical check that the source code works as intended, the technical team can integrate it, merge it, and all Gaia-X Digital Clearing Houses (GXDCH) can also run these checks.	• Labels are designed by the custodian and endorsed by Gaia-X after a check has been performed on technical compatibility, but not for content or value of rules. • If the source code works, the Gaia-X technical team can integrate it, merge it, and all the Gaia-X Digital Clearing Houses (GXDCH) can also run those checks.

In **scenario 1** (controlled by custodian), anybody can create and become the custodian of new labels related to any digital artefact they want for whatever purpose they want, with or without adoption of Gaia-X values. The custodian chooses the way to express the label criteria and to check that an artefact fulfills the criteria for that label. Label certificates are issued by tools designed, implemented, deployed and run by the custodian (who might or might not reuse the Gaia-X OSS code). In fact, this scenario is already possible because the Gaia-X source code is open source and anyone can download it from GitHub.

It's important to emphasize that a custodian may choose to reuse existing Gaia-X certified credentials - for example, for infrastructure services - while extending the source code with their own custom credentials or additional options to validate other attributes. This can be done as long as technical compatibility is maintained – that is, by adhering to the same definitions, architecture, and overall structure. The main value for custodians lies in leveraging the Gaia-X brand image - e.g., to support EUC funding applications. For Gaia-X, the value comes from increased visibility and the potential to attract new members, particularly if custodians are required to join.

In **scenario 2** (controlled by Gaia-X), new labels are designed, maintained and deployed by the Gaia-X Policy Rules Committee (PRC), based on requirements established by the Gaia-X Data & Services Business Committee (DSBC). The criteria are designed by the Gaia-X PRC. If needed, the Gaia-X Ontology is extended by a Working Group under control of the Gaia-X Technical Committee (TC). The criteria and the ontology are implemented in the Gaia-X Digital Clearing House (GXDCH) code, developed and maintained by the Gaia-X technical team. Label certificates are issued by the GXDCHs, whose deployment is under Gaia-X control. In this scenario, the market would benefit from a tightly focused Gaia-X brand, supported by centrally managed tools applied to a limited and clearly defined set of labels.

In **scenario 3** (custodian-proposed, Gaia-X validated, and GXDCH-certified), labels are designed by the custodian and are endorsed by Gaia-X after a check has been performed to enable the custodian to use a "Gaia-X endorsed" statement. The custodian may propose source code for the verification of their specific criteria and may suggest source code for the validation and verification of the verifiable credentials. Label certificates are issued by the GXDCHs, whose deployment is under Gaia-X control. The main advantage for custodians would be access to the Gaia-X brand, along with a fully automated compliance tooling to deliver label certificates.

In **scenario 4** (custodian-proposed and validated, and GXDCH-certified), labels are designed by the custodian and are endorsed by Gaia-X after a check has been performed for technical compatibility, but not for content or value of rules (which gives freedom to custodians who might not agree with European values). The custodian may propose source code for the verification of their specific criteria and may suggest source code for the validation and verification of the verifiable credentials. Gaia-X can also act as a custodian and continue to create Gaia-X endorsed labels or labels promoting Gaia-X values. Label credentials are issued by Gaia-X Digital Clearing Houses (GXDCHs). It`s important to note that some custodians or some ecosystems may wish to run their own verification and their own codes on a custodian-owned clearing house and may not want to be involved or depend on the central verification and contracting of GXDCHs. In such cases, these actors will either rely on scenario one, or Gaia-X AISBL will have to develop another governance scenario to respond to such demands.

The main benefit for custodians would be good autonomy for labelling with a fully automated compliance tooling based on Gaia-X open-source GXDCH (hence trustworthy). This alone is a significant advantage, especially for small and medium-sized businesses, considering that even large enterprises struggle with adoption of eIDAS (the EU regulation on electronic identification and trust services), which itself only covers identity of persons. As a result, handling the broader spectrum of Verifiable Credentials remains out of reach for many organizations.

Table 2 below summarizes key aspects of each approach, providing a structured comparison of the four proposed governance scenarios. The table highlights the variables illustrated in the mind map provided in Annex II and described in detail in chapter 3. Stragety and governance options.[2] The variables compared in the table include semantic control, compliance document(s), lexical control, certificate issuance, and tooling. These elements placed side-by-side serve as the basis for understanding how each scenario is structured, facilitating an informed assessment of the distinctions of each scenario and their respective implications for implementation.

As a next step, the White Paper will be presented to the Gaia-X Policy and Rules Committee (PRC) and the Gaia-X Technical Committee (TC). Following more concrete decisions within the PRC, we will initiate a broader consultation with Gaia-X members, including the Gaia-X Lighthouse projects. Based on the feedback received, the document will be iteratively refined, and a final version will be presented to the Board of Directors (BoD). Once the BoD decides on a preferred scenario, a dedicated forum will be established to engage ecosystems in defining potential criteria and progressing toward the alignment of technical requirements.

[2] More specifically, these are found in subchapter 3.1 Considerations for extending the labelling framework and 6.3.5 Variants to be considered.

Table 2. Structured comparison of labelling strategy scenarios

	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Semantic control	Full ecosystem autonomy	Label designed by Gaia-X PRC from DSBC requirements	Label designed by the custodian and validated (endorsed) by Gaia-X with respect to Gaia-X European values	Custodians autonomy according to their core values
Compliance Document(s)	Several independent documents controlled by the custodians	One document written by PRC with one appendix per label	One set of documents (Framework document written by PRC plus label documents written by custodians) in a library managed by Gaia-X	Same as scenario 3
Lexical control	Full ecosystem autonomy	Criteria and artefacts described using Gaia-X syntax and Gaia-X ontology	Criteria expressed in a generic Gaia-X defined syntax (interpretable by the GXDCH code)	Same as scenario 3
Certificate issuance	Controlled by the custodian	Interoperable certificate issued by GXDCH	Same as scenario 2	Same as scenario 2
Tooling	Tooling designed and implemented by the custodian (potentially reusing Gaia-X OSS code)	GXDCH specified by the PRC and coded by the Gaia-X team, labels and ontologies are included in the GXDCH code	GXDCH generic code defined and maintained by Gaia-X team (criteria as parameters)	Same as scenario 3

Introduction

The Gaia-X framework establishes a European-driven next generation data infrastructure focused on creating an interoperable and federated ecosystem for the secure sharing of data and digital services. Our framework has been under constant development since 2019[3] to overcome the critical barriers that prevent organizations from fully exploring the potential economic and social benefits of data and digital infrastructure. In the past years, the Gaia-X framework has been endorsed and adopted by organizations across Europe[4], Asia[5], and North America[6], with the establishment of new Gaia-X Hubs currently in progress across countries in Africa and other regions[7].

In the realm of digital technologies, the flow of data across the globe is often constrained by geographical and political boundaries. Added to this challenge is our increasing awareness of the interdependent nature of our global market and supply chains, conditions which provide us with the strong motivation to continue building the Gaia-X framework not just from a European perspective, but with a global outlook that embraces our core values of transparency and technical compatibility.

As the Gaia-X ecosystem continues to expand globally and given that legal frameworks and regulatory requirements vary widely across different regions and sectors of the economy, we are invited to consider new possibilities for improvements that can help ensure regulatory compliance across different industries and international jurisdictions. Therefore, to effectively develop a

[3] Federal Ministry for Economic Affairs and Energy (2019) Project Gaia-X: A Federated Infrastructure as the Cradle of a Vibrant European Ecosystem. Available at: https://www.bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.html. Accessed: 14 February 2025.

[4] As of January 2025: Austria, Belgium, Finland, France, Germany, Greece, Hungary, Italy, Slovenia, Netherlands, Poland, Portugal, Romania, Slovakia, Luxembourg, Spain, and Denmark.

[5] As of January 2025: Japan and South Korea.

[6] As of January 2025: United States.

[7] As of January 2025: Ireland, Estonia, Czech Republic, Sweden, Norway, Switzerland, and United Kingdom.

resilient, interoperable, and globally relevant decentralized data infrastructure, our Gaia-X Labelling Framework must be adaptable to both geographical and domain-specific contexts. Our vision is that a geographical and domain extension within this framework should ensure better identity management, interoperability, trust and security, leading to more robustly structured ecosystems integrating different domains and industries across the globe. For this, this paper suggests that the Gaia-X Labelling Framework be extensible to meet the specific needs and regulations of the different ecosystems that wish to adopt the framework.

While the current compliance document focuses on generic criteria for all adopters, and is primarily focused on cloud services, with a small extension for data exchange services, we anticipate that more value can be added with domain-specific extensions. From a user perspective, a geographical and domain extension should ensure an easy way to trustfully identify parties and digital assets that comply with some rules considered as important within the ecosystem. This is a strong foundation for enabling interactions based on trust within and across ecosystems. This is a strong foundation for building a structured ecosystem based on compliance. However, one of the main points for Gaia-X currently is to operationalize and for the market to adopt the labels. Therefore, this document does not aim to question the current labels as they have been developed and adopted. The extension must, therefore, consider the existing labels.

Hence, we believe in the importance of reviewing and understanding the regulations in selected regions so that the proposed solutions enable a model that integrates the globally involved parties under the Gaia-X framework. Otherwise, maintaining silos that restrict the circulation of data is an attitude that would prevent Gaia-X initiatives to develop further.

Due to increasing cross-industry connections, data sharing and integration have become more crucial, increasing the demand for the establishment and expansion of trusted data value chains and data flows between different industries and regions. In this context, it is understood that achieving interoperability between different services from different industries that wish to integrate and collaborate in the data economy requires labelling standardisation in such a way that an ecosystem can trustfully select parties and digital assets based on labels issued by another ecosystem.

Trust in data becomes even more important in the era of rapidly advancing artificial intelligence (AI) technologies and for their use in diverse industries. For this reason, the Gaia-X framework should also consider multi-level integration in its extensions. Overall, we are suggesting that the Gaia-X community consider geographical and domain extensions as one of the key priorities for establishing a trustworthy and user-friendly data ecosystem under the Gaia-X framework. Additionally, we need to define the acceptable impacts of a domain extension on existing Gaia-X products (frameworks, federated services, clearing house, etc.) and how to handle the different impacts. When a new set of rules would impact the code, then we raise the questions of how we reconcile and manage the parallel evolutions of the code and where we limit the domain extensions. Moreover, we believe that it’s too early to come up with concrete naming values, and although some options have been discussed, this part will be worked out after deciding on a scenario to follow.

The main discussion proposed in the white paper begin in chapter 1, which explores the potential contexts and scopes of the labelling framework extensions – who can propose extensions and for which kinds of entities or artifacts, for example. In chapter 2, the reader will find examples of application in the domains of finance, mobility, and aerospace & defence. Chapter 3, in turn, presents fours scenarios for the labelling strategy and governance. Here, it discusses the various alternatives, including pros and cons, related to the Gaia-X labelling strategy (how much constraints are put by Gaia-X on a label extension) and the associated branding schemes. Chapter 4 will then explore technical requirements for the labelling schemes, while taking in consideration issues such as labelling concepts, label extensions (introducing labels as functioning in a stacked configuration that allows adaptations to existing labels), label versioning that provides upward compatibility, and three alternatives for how a GXDCH can decide or not to accept a Verifiable Credential (VC) from a notary. Lastly, for the operationalization of geographical and domain extensions, chapter 5 presents three verification options, each focusing on either Gaia-X Digital Clearing Houses (GXDCHs), Trust Anchors, or notarization. These suggestions are followed by a user story that exemplifies how verification options could work between companies located in different regions.

1. Geographical and domain-specific contexts

Through this white paper, we seek to provide supporting information to our stakeholders to help better understand the concept of geographical and domain extensions, their benefit to the Gaia-X project, and conceptually assist in the decision between different proposed scenarios for the strategic geographical and domain extension of the Gaia-X framework. In this chapter, we will introduce relevant concepts such as ecosystems, domain, and context, explain the nature of targeted entity profiles eventually eligible for Gaia-X label concession, and reasons why geographical and domain extensions are beneficial to the Gaia-X initiative.

The term ecosystems, in a broad sense, refer to networks of interconnected actors – such as organizations, individuals, and technologies – that collaborate within a shared environment. In the context of data spaces, ecosystems facilitate interoperability, enabling data exchange and collaboration across different domains (see definition below). Data ecosystems are characterized by their dynamic and self-organizing nature, where participants both contribute to and derive value from the network according to established governance frameworks.

This governance framework is structured by a common set of rules that participants of the ecosystem need to conform to, and which must be operationalized. Similar to domains, ecosystems can cover a specific economic sector, a subset of an economic sector, subsets of several economic sectors (e.g., aerospace and defence), a geographical region, or an economic sector of a specific region. In the Gaia-X Architecture Document, "the Gaia-X Ecosystem is the virtual set of Service Offerings described by Gaia-X compliant credentials, according to the compliance schemes set by the Gaia-X Association"[8] (see Table 3).

Table 3. Definition of Ecosystem

Broad definition	Gaia-X Architecture Document
Networks of interconnected actors (such as organizations, individuals, and technologies) that collaborate within a shared environment.	The Gaia-X Ecosystem is the virtual set of Service Offerings described by Gaia-X compliant credentials, according to the compliance schemes set by the Gaia-X Association.

The term domain, in turn, generally refers to a specific area of the economy (such as healthcare, mobility, finance, or energy), each representing a structured business environment where opportunities and challenges for innovation can emerge. Beyond this economic perspective, the concept can also extend to broader areas. The Gaia-X Architecture Document states that, in data mesh implementations[9], the term domain "denotes 'bounded contexts' such as spheres of knowledge, influence, activities, or responsibilities within a potentially large single organization (Evans, 2004[10]; Dehghari, 2022[11])"[12] (see Table 4). In the context

[8] Gaia-X Architecture Document. 24.04 Release, pp. 6. Available at: https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/pdf/document.pdf. Accessed: 18 February 2025.

[9] A data mesh is a decentralized data architecture that organizes data by a specific business domain. Source: IBM. What is a Data Mesh? Available at: https://www.ibm.com/think/topics/data-mesh. Accessed: 12 March 2025.

[10] Evans, E. (2004) Domain-Driven Design: Tackling Complexity in the Heart of Software. Addison-Wesley Professional.

[11] Dehghani, Z. (2022) Data Mesh: Delivering Data-Driven Value at Scale. O'Relly Media, Inc.

[12] Gaia-X Architecture Document. 24.04 Release, pp. 40. Available at: https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/pdf/document.pdf. Accessed: 11 March 2025.

of data spaces, domain is often used interchangeably with other terms such as ecosystems, verticals, or sectors. We see this interchangeable use when we say, for example, that Gaia-X facilitates a community of interoperable ecosystems, or domains, where different actors converge to enable data sharing across industries.

Table 4. Definition of Domain

Broad definition	Gaia-X Architecture Document
A specific area of the economy – such as healthcare, mobility, finance, or energy –, each representing a structured business environment where opportunities and challenges for innovation can emerge.	"Bounded contexts” such as spheres of knowledge, influence, activities, or responsibilities within a potentially large single organization.

Lastly, the concept of context refers to the specific conditions (such as environmental, institutional, and regulatory) that shape how data spaces function and evolve. Context involves the unique circumstances and constraints that influence data sharing practices, governance approaches, and value creation opportunities. In geographical contexts, factors such as regulations, infrastructure availability, economic priorities, and cultural attitudes toward data sharing can significantly impact the local development of data spaces. Similarly, domain-specific contexts introduce specialized requirements, terminology, established practices, and stakeholder relationships that must be accounted when building data spaces. In this sense, geographical and domain contexts create distinct conditions and require initiatives to be adaptable rather than following a one-size-fits-all approach (see Table 5). Hence, understanding these contextual dimensions is important for effectively tailoring data space architectures, governance frameworks, and value propositions to meet the specific needs of participants while navigating geographical and domain considerations.

Table 5. Geographical and domain-specific contexts

Context type	Broad definition	Gaia-X Architecture Document
Geographical	Local conditions that influence data spaces based on location.	Regulations / Infrastructure availability / Economic priorities / Political climate / Cultural attitudes
Domain	Unique characteristics of specific sectors or industries that shape data spaces.	Specialized requirements / Industry-specific terminology / Established practices / Market maturity / Stakeholder relationships / Ethical considerations

These definitions provide a background for the kinds of entities that will carry the Gaia-X label. As our white paper exercise is to identify and evaluate a number of scenarios for the geographical and domain extension of the Gaia-X framework, we kept the profile for targeted entity (or object for which parties wish to define criteria) for label concessions fairly open. Under this consideration, we identified scenarios based on current labels for cloud services and data products, but also scenarios with new labels for a party, an IT infrastructure, a software vendor, a specific app (running on a device), an AI agent, and so on. Nonetheless, the proposed scenarios (described in more detail in chapter 3. Strategy and Governance Options) restrict the concession of labels to entities related to the digital environment.

Another key consideration is to question the purpose of creating each geographical and domain extension. We believe this should be the first step into the planning extensions strategically. In this sense, there are two main aspects that would justify our interest. The first is to enable Gaia-X to provide a "ready-to-use" framework for data spaces that is designed for sectors with specific needs (i.e., they provide a better time-to-market for Gaia-X products). The second aspect is having a domain extension for existing lighthouse and/or other projects. In this second case, geographical and domain extensions could (i) facilitate existing lighthouse projects to agree upon common principles with projects in other domains, and (ii) facilitate interoperability of data spaces covering the same or different domains, making it easier for small and medium-sized enterprises (SMEs) and others to migrate from one ecosystem to another. This could also facilitate inter data-space collaboration (see example for the aerospace domain described in chapter 2).

2. Use Case Examples

In this chapter we will focus on different examples from the domains of finance, mobility, and aerospace & defence to help create ideas of how extensions can be organised.

2.1. Finance

The Digital Operational Resilience Act (DORA)[13] for the financial sector is a European regulation that came into force in January 2025. This regulation imposes, for each finance enterprise operating within the EU, a set of cyber security constraints related to their ICT (Information and communications Technology) providers. The regulatory constraints depend on the criticality of the ICT service and/or product in terms of the continuity and/or availability of the financial activity for the finance enterprise, but also for the complete sector. The regulation is based on the concept of CTPP that stands for Critical Third-Party Provider. Therefore, for the extension of the finance domain, it's relevant to complete the Gaia-X labels taking in full consideration the DORA framework (although some of these requirements are already present in CSP[14] label level 1). Note that DORA applies to all ICT providers: cloud services providers, old-fashioned outsourcers, telecom operators, and software providers.

[13] Regulation (EU) 2022/2554. Available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng. Accessed: 18 February 2025.

[14] Cloud Service Provider (CPS)

2.2. Mobility

The ASAM (Association for Standardization of Automation and Measuring Systems) provides standards for automation and measurement systems.[15] One of these standards is the ASAM OpenX standards that focuses on simulation-based testing. This standard ensures interoperability among the different data and services in the field of simulation. For a Gaia-X-based ecosystem in the field of simulation (e.g. the project Gaia-X 4 PLC-AAD[16]), it is relevant that services offered have the information in the service description and perhaps can also get a label that indicates that they are following the ASAM OpenX standard.

2.3. Aerospace & Defence

The purpose of a domain extension for aerospace and defence is to strengthen the supply chain for production and services, anticipating significant growth within the industry. In addition to the general purpose of the domain extension, some generic and specific use-cases may be identified to fit specific regulations and contexts of the domain. Here are four examples:

1. Traceability throughout the entire supply chain (managing specific objects such as non-quality events and derogations);
2. Facilitation and fostering of co-engineering initiatives while ensuring clarity on intellectual property claims and legal agreements between the parties;
3. Availability of all the technical documentation for the client (exclusively);
4. Provision of sovereign cloud infrastructure services that are immune to non-European regulations for industrial data (beyond GDPR).

Having a domain extension in a given industry, even when there are existing lighthouse and other ongoing data-spaces projects, can benefit these initiatives by

[15] ASAM website available at: https://www.asam.net/standards/. Accessed: 18 February 2025.
[16] Gaia-X 4 PLC-ADD website available at: https://www.gaia-x4plcaad.info/. Accessed: 18 February 2025.

establishing common and reliable basics, thereby fostering interoperability of data spaces within the industry and with other sectors.

Data-spaces interoperability may provide a significant advantage for the aerospace and defence industry, where a significant share of the supply chain is common with the automotive industry. For instance, a major provider of both aeronautics and automotive parts can use the same services to gather planning and scheduling information from their customers and provide delivery forecasts in return as per their contract. Similarly, an aerospace supplier can reach out to its clients and suppliers operating on other aerospace data spaces, ensuring seamless integration and communication. Beyond day-to-day business, this approach also facilitates the migration from one ecosystem to another for SMEs and other entities.

In terms of compliance criteria, the aerospace and defence domain extension could provide an off-the-shelf catalogue compliant with a selected list of standards commonly used in the industry. Amongst domain-specific possible standards, we may include IASA (International Aviation Safety Assessment), EASA (European Union Safety Aviation Agency), AFNOR (Association Française de Normalisation), ITAR (International Traffic in Arms Regulations), and the EU Export Control Regulation Nr. 2021/821. Accordingly, in the aerospace sector, commonly agreed standard-labels for data classification and categorisation, linked to applicable regulations, need to be defined, and proper tagging to be enforced, in order to allow end-to-end compliance traceability. Such standards and regulations may overlap in the same domain extension, as the principle is not to align all players on one standard per use-case but rather provide agnostic enablers for all players.

To be practical, here is an example of a criterion linked to the ASD S-series that could be an off-the-shelf component of the aerospace and defence domain extension. It concerns the S2000M, the material management specification to provide enriched data about in-service parts and services catalogue from an OEM to its customer: "The S2000M[17] syntax used for the interchange of messages is based upon the use of ISO 9735-1. These

[17] S2000M is an international specification used for material management. It defines the processes, procedures and provides the information for data exchange to be used for material management throughout the lifecycle of a product. Source: https://www.s-series.org/s2000m/. Accessed: 18 February, 2025.

require service segments to be wrapped around user data segments for transmission and be supported by special service messages to notify the results of the syntax checks. The following explanation gives the detail contained in the various service segments." This is followed by 21 pages of said service segments.

2.4 Example for geographical extension (Swiss use case)

A European Entity, which is Gaia-X level 3 compliant for their services in EU countries, wants to also obtain a label level 3 for their cloud services hosted in Lausanne, Switzerland. The suggestion is to extend some of the criteria to include Switzerland based services in Gaia-X level 3 labels (in criterion P5.1.2 for instance, add Switzerland at the end "For Label Level 3, the Provider shall process and store all Customer Data exclusively in the EU/EEA or Switzerland"). They would also benefit from a new more restrictive label "level 3 Switzerland only" to reflect the demand from the Swiss market in the following manner: Provider shall process and store all Customer Data exclusively in Switzerland. This would reflect not only what end users are demanding but would also align with local blocking statutes which require certain users to keep data stored within Switzerland (and hence why some Cloud Service Providers such as AWS have set up data centres in the country). For a detailed analysis of criteria, please refer to the dedicated Appendix.

3. Strategy and governance options

This chapter outlines strategic and governance considerations for extending the Gaia-X labelling framework. It presents four governance scenarios intended to guide discussion and support stakeholder feedback around future extension initiatives. These scenarios are informed by a set of key consideration areas, such as how labels are defined, who maintains them, and under what governance structures they operate. To support a deeper understanding of the extension framework, the chapter also introduces the concept of the Digital Clearing House, the central element in the verification function. In addition, it provides detailed insights into label structure, extension entropy, and practical aspects of implementing extension governance across domains and geographies. Together, these components aim to provide a foundation for shaping the strategic direction and operational oversight of future Gaia-X labelling extensions.

3.1. Considerations for extending the labelling framework

The Gaia-X labelling extension strategy must consider a range of options from multiple perspectives. These options can be categorized into different variables. We illustrated this in the mind-map shown in Appendix II and summarized these considerations below:

- **Label extension:** What kind of artefact can be labelled when extending the labelling framework? Such label extension can apply to anything, any digital assets, only artefacts already addressed by a label, etc.
- **Custodian:** This term refers to who can propose, define, and maintain a label extension to the compliance framework. In each scenario, label custodians can be either anybody, any Gaia-X member, only ecosystems with significant market share, only Gaia-X Hubs/Dataspaces or only the Gaia-X PRC (upon requests from the DSBC).
- **Semantic control:** What kind of labels are acceptable in terms of purpose and structure? This can be only extension of existing labels, only labels promoting Gaia-X values, etc.
- **Compliance Document structure:** Is the Gaia-X Compliance Document a unique document, a document with new labels described in appendixes, or a framework document with an associated document per label?
- **Lexical control:** This consideration refers to how the criteria of a new label are expressed. This can be textual description without constraints, predefined syntax within the Gaia-X ontology, predefined syntax with possible ontology extensions, etc.
- **Tooling code control:** This refers to the management of the code used to validate criteria (i.e., the individual rules or claims[18] that participants must comply with). In this case, the tooling code may be either specific to a label, reusable across

[18] A claim is a statement about a subject. A subject is a thing about which claims can be made. Claims are expressed using subject-property-value relationships.

multiple labels and criteria, or tailored (i.e., hard-coded by Gaia-X for specific use cases). The tooling is responsible for verifying individual claims before combining them into a final label[19].

- **Tooling deployment:** This refers to how the tooling is deployed to verify the criteria and assign labels. It can be deployed under Gaia-X control with uniform services for all labels (i.e., all GXDCH can deliver certificates for all labels), under Gaia-X control with basic services for Gaia-X-owned labels (with optional extensions for other labels) or deployed by a custodian with Gaia-X endorsement.
- **Pricing:** The cost elements to be considered for a pricing strategy include the establishment and verification of new extensions. However, it is recommended that the basic certification service for Gaia-X Labels 1 to 3 remain free of charge. Further details are discussed in subchapter 3.2.5 Variants to be considered, item 8. Pricing Strategy.
- **Naming:** Label names should follow a logical naming structure or simply receive a number sequence (such as in ISO standards). Further details are discussed in subchapter 3.2.5 Variants to be considered, item *7. Naming and Branding*.

When extending the labelling framework, business decisions and design choices must be made across these (and potentially more) consideration areas – such as semantic control, tooling deployment, naming, pricing, etc. However, not all choices across these areas are compatible with one another. For instance, granting full lexical autonomy to a custodian is not compatible with the use of a unique tooling code.

To avoid such incompatibilities, our sprint group has designed four coherent governance scenarios (Scenarios 1 to 4), each composed of compatible choices across the consideration areas. Hence, in this chapter, we provide detailed explanations of each scenario (some of which may not align with the current framework), highlighting key advantages, drawbacks, and overall benefits for Gaia-X and custodians. The complete description of each scenario is found in the subchapter 3.3 Governance Scenarios.

[19] A Gaia-X Label is a machine readable, structured and signed document issued by the accredited Gaia-X Compliance services in case of a valid verification and validation of the criteria for a specific assessment scheme.

3.2. Verification Engine

To enable compliance within the Gaia-X ecosystem, an automated mechanism is required to verify that participants and services adhere to established rules and standards. This mechanism is embodied in the Gaia-X Digital Clearing House (GXDCH), which serves as the operational engine for compliance verification. In the subchapters below, we first offer a general definition of a digital clearing house, followed by further details specific to the GXDCH.

3.2.1. Definition of a digital clearing house

A digital clearing house is an online platform or system that facilitates the exchange, settlement, and management of digital transactions or data between various parties, often in a financial, business, or technical context. It acts as an intermediary to ensure that all transactions are properly processed, reconciled, and recorded. Digital clearing houses often have the following purpose:

- Promote secure, transparent, and trustworthy data exchanges.
- Enable decentralized data management and cloud infrastructure.
- Avoid reliance on single points of control and vendor lock-in by promoting decentralized models.
- Support data sovereignty, transparency, and interoperability across different systems and platforms.
- Ensure efficient settlement and reconciliation of transactions (the general purpose of a clearing house).

Examples of digital clearing houses:

- Digital Clearinghouse 1.0: Digital Clearinghouse 1.0 is a platform established by the European Data Protection Supervisor (EDPS) to facilitate the sharing of information and promoting discussions among regulators, industry stakeholders, and policymakers on the enforcement of data protection rules, particularly the General Data Protection Regulation (GDPR).

- Gaia-X Digital Clearing House (GXDCH) is part of the Gaia-X initiative, which aims to establish sovereign, transparent, and secure data spaces across Europe by promoting a decentralized and interoperable data ecosystem. The GXDCH functions as a platform that facilitates the secure exchange of data between organizations, ensuring compliance with data sovereignty and transparency principles.

3.2.2. The Gaia-X Digital Clearing House (GXDCH)

A Gaia-X Digital Clearing House (GXDCH) is defined in the Gaia-X Glossary as follows: The Gaia-X Digital Clearing House operationalizes the Gaia-X mission. A GXDCH makes the various mechanisms and concepts applicable in practice as a ready-to-use service set. The GXDCH contains both mandatory and optional components. All the mandatory components of the GXDCH are open-source software. The development and architecture of the GXDCH is under the governance of the Gaia-X Association.

In sum, a GXDCH is a platform that allows users to get verified against Gaia-X rules to obtain compliance. At the moment, a GXDCH Provider must be a member of the AISBL and must run the 'generic code' as-is provided by Gaia-X as a minimum. Therefore, the GXDCH provider can and needs to issue Gaia-X compliance attestations and labels. In addition, a GXDCH can run other individual services besides and/or on top of the existing code.

3.3. Governance scenarios

The following four governance scenarios outline possible approaches for managing label extensions within the Gaia-X ecosystem. Each scenario illustrates a different level of centralization, oversight, and stakeholder involvement - from open, decentralized models to more structured, centrally governed frameworks. These scenarios are presented in this white paper solely as a basis for discussion and reflection; they do not represent any formal decision or preferred direction. Instead, they are intended to support further deliberation and feedback from the Gaia-X community and stakeholders. The table below provides a comparative summary of the key elements of each scenario, while the details of each scenario are explained in the subsequent subchapters.

Table 6. Summary of governance scenarios (previously shown in Executive Summary)

Scenario 1	Scenario 2	Scenario 1	Scenario 4
• Anybody can create a label related to whatever digital artefact they want, for whatever purpose they want, with or without adoption of Gaia-X values. • Whoever creates a label, becomes a label custodian. • The tooling associated with the label is also designed, implemented, deployed and run by the custodian.	• Very strict compliance rules in a single Compliance Document that the PRC reviews. • Labels are designed, maintained and deployed by the Gaia-X PRC, based on requirements established by the Gaia-X Data & Services Business Committee (DSBC). • The criteria are designed by Gaia-X Policy Rules Committee (PRC). If needed, the Gaia-X Ontology is extended by a Working Group under control of the Gaia-X Technical Committee (TC).	• Anybody can create a label related to whatever digital artefact they want, for whatever purpose they want, with or without adoption of Gaia-X values. • If the proposed extension aligns with Gaia-X values and passes a technical check that the source code works as intended, the technical team can integrate it, merge it, and all Gaia-X Digital Clearing Houses (GXDCH) can also run these checks.	• Labels are designed by the custodian and endorsed by Gaia-X after a check has been performed on technical compatibility, but not for content or value of rules. • If the source code works, the Gaia-X technical team can integrate it, merge it, and all the Gaia-X Digital Clearing Houses (GXDCH) can also run those checks.

3.3.1. Controlled by custodian (scenario 1)

In scenario 1, anybody can create and become the custodian of new labels related to any digital artefact they want for whatever purpose they want, with or without adoption of Gaia-X values. The custodian chooses the way to express the label criteria and to check that an artefact fulfils the criteria for that label. Label certificates are issued by tools designed, implemented, deployed and run by the custodian (who might or might not reuse the Gaia-X OSS code). In fact, this scenario is already possible because the Gaia-X source code is open source, and anyone can download it from GitHub. It's important to emphasize that a custodian may choose to reuse existing Gaia-X certified credentials - for example, for infrastructure services – while extending the source code with their own custom credentials or additional options to validate other attributes. This can be done as long as technical compatibility is maintained – that is, by adhering to the same definitions, architecture, and overall structure. The main value for custodians lies in leveraging the Gaia-X brand image – *e.g.*, to support EUC funding applications. For Gaia-X, the value comes from increased visibility and the potential to attract new members, particularly if custodians are required to join.

Table 7. Pros and cons of scenario 1

Pros	Cons
• Custodians can design labels perfectly suited for their needs. • Custodians benefit from Gaia-X image (e.g., EUC fundings). • Gaia-X gets more visibility and can attract more members	• The Gaia-X brand is diluted. • The Gaia-X ecosystem could have difficulties to understand what Gaia-X is.

3.3.2. Controlled by Gaia-X (scenario 2)

In scenario 2, new labels are designed, maintained and deployed by the Gaia-X Policy Rules Committee (PRC), based on requirements established by the Gaia-X Data & Services Business Committee (DSBC). The criteria are designed by the Gaia-X PRC. If needed, the Gaia-X Ontology is extended by a Working Group under control of the Gaia-X Technical Committee (TC). The criteria and the ontology are implemented in the Gaia-X Digital Clearing House (GXDCH) code, developed and maintained by the Gaia-X technical team. Label certificates are issued by the GXDCHs, whose deployment is under Gaia-X control.

In this scenario, the market would benefit from a tightly focused Gaia-X brand, supported by centrally managed tools applied to a limited and clearly defined set of labels.

Table 8. Pros and cons of scenario 2

Pros	Cons
• The Gaia-X brand is fully controlled by Gaia-X (only Gaia-X decides which labels are added). • Ecosystem labels benefit from the clear Gaia-X brand. • Ecosystems get a fully automated compliance tooling.	• The Gaia-X ontology might become a bit cluttered if it shall include all specificities from various ecosystems. • Limited Gaia-X resources to design new labels will likely create bottlenecks. • Ecosystems which are not selected to have a Gaia-X label (either by Gaia-X choice versus Gaia-X values or by lack of resource to design and implement new labels) might leave Gaia-X.

3.2.3. Custodian-proposed, Gaia-X-validated, and GXDCH certified (scenario 3)

In scenario 3, labels are designed by the custodian and are endorsed by Gaia-X after a check has been performed to enable the custodian to use a "Gaia-X endorsed" statement. The custodian may propose source code for the verification of their specific criteria and may suggest source code for the validation and verification of the verifiable credentials. Label certificates are issued by the GXDCHs, whose deployment is under Gaia-X control. The main advantage for custodians would be access to the Gaia-X brand, along with a fully automated compliance tooling to deliver label certificates.

Table 9. Pros and cons of scenario 3

Pros	Cons
• The Gaia-X brand is controlled by Gaia-X as only Gaia-X decides which labels are endorsed. • Ecosystems have some autonomy to design labels that correspond to their needs. • Enables large scalability for various ecosystems because it requires few Gaia-X resources (the label is fully designed by the custodian and Gaia-X just needs to check technical compatibility of the way criteria are designed). • Ecosystem labels benefit from a clear Gaia-X brand.	• Ability of GXDCH code able to handle ontology extensions in a fully generic way is not granted (at least not in a near future). • This scenario will need to define more precisely the Gaia-X values (to avoid dispute). • The current Gaia-X value might significantly restrict labelling extension with non-European ecosystems. • This approach does not scale.

• Ecosystems get a fully automated compliance tooling.	• The current Gaia-X business and economic model also does not support this scenario.

3.2.4. Custodian-proposed and validated, and GXDCH certified (scenario 4)

In scenario 4, labels are designed by the custodian and are endorsed by Gaia-X after a check has been performed for technical compatibility, but not for content or value of rules (which gives freedom to custodians who might not agree with European values). The custodian may propose source code for the verification of their specific criteria and may suggest source code for the validation and verification of the verifiable credentials. Gaia-X can also act as a custodian and continue to create Gaia-X endorsed labels or labels promoting Gaia-X values. Label credentials are issued by Gaia-X Digital Clearing Houses (GXDCHs).

Important note: Some custodians or some ecosystems may wish to run their own verification and their own codes on a custodian-owned clearing house and may not want to be involved or depend on the central verification and contracting of GXDCHs. In such cases, these actors will either rely on scenario one, or Gaia-X AISBL will have to develop another governance scenario to respond to such demands.

The main benefit for custodians would be good autonomy for labelling with a fully automated compliance tooling based on Gaia-X open-source GXDCH (hence trustworthy). This alone is a significant advantage, especially for small and medium-sized businesses, considering that even large enterprises struggle with adoption of eIDAS (the EU regulation on electronic identification and trust services), which itself only covers identity of persons. As a result, handling the broader spectrum of Verifiable Credentials remains out of reach for many organizations.

Table 10. Pros and cons of scenario 4

Pros	Cons
• The Gaia-X brand is controlled by Gaia-X as only Gaia-X decide which labels can use the Gaia-X name.	• Some custodians might find it difficult to develop the services related to ontology extension.

• Ecosystems have good autonomy to design labels that correspond to their needs. • This scenario enables large scalability for various ecosystems because it requires few Gaia-X resources (the label is fully designed by the custodian and Gaia-X just needs to evaluate compliance with Gaia-X values and to check technical compatibility of the way criteria are designed). • Ecosystem labels benefit from a clear Gaia-X brand. • Ecosystems get an automated compliance tooling.	• In variant 1, this scenario will need to define more precisely the Gaia-X values (to avoid dispute) and the current Gaia-X value might significantly restrict labelling extension with non-European ecosystems.

Table 11 below summarizes key aspects of each approach, providing a structured comparison of the four proposed governance scenarios. The table highlights the variables illustrated in the mind map provided in Annex II and described in detail in this chapter (see 3.1 Considerations for extending the labelling framework and 3.2.5 Variants to be considered). The variables compared in the table include semantic control, compliance document(s), lexical control, certificate issuance, and tooling. These elements placed side-by-side serve as the basis for understanding how each scenario is structured, facilitating an informed assessment of the distinctions of each scenario and their respective implications for implementation.

Table 11. Structured comparison of labelling strategy scenarios (previously shown in Executive Summary)

	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Semantic control	Full ecosystem autonomy	Label designed by Gaia-X PRC from DSBC requirements	Label designed by the custodian and validated (endorsed) by Gaia-X with respect to Gaia-X European values	Custodians autonomy according to their core values
Compliance Document(s)	Several independent documents controlled by the custodians	One document written by PRC with one appendix per label	One set of documents (Framework document written by PRC plus label documents written by custodians) in a library managed by Gaia-X	Same as scenario 3

Lexical control	Full ecosystem autonomy	Criteria and artefacts described using Gaia-X syntax and Gaia-X ontology	Criteria expressed in a generic Gaia-X defined syntax (interpretable by the GXDCH code)	Same as scenario 3
Certificate issuance	Controlled by the custodian	Interoperable certificate issued by GXDCH	Same as scenario 2	Same as scenario 2
Tooling	Tooling designed and implemented by the custodian (potentially reusing Gaia-X OSS code)	GXDCH specified by the PRC and coded by the Gaia-X team, labels and ontologies are included in the GXDCH code	GXDCH generic code defined and maintained by Gaia-X team (criteria as parameters)	Same as scenario 3

3.2.5. Variants to be considered

1. **Accepted custodian:** Any Gaia-X member, any ecosystem with significant market share, and any Gaia-X endorsed Hub or Lighthouse. The primary choice would be any ecosystem with significant market share, and a mechanism for measuring market size would need to be developed.
2. **Label overlap:** Is it accepted to have label overlaps across different ecosystems (e.g., a Cloud Service label for Health, a Cloud Service label for Finance, a Cloud Service label for systemic financial institutions, etc.)? In this case, the principle is that labelling extension overlaps are unavoidable, but we should strive to minimize their occurrence because each overlap reduces their market-share potential.
3. **GXDCH deployment:** Are all GXDCHs delivering certificates for all labels or can a GXDCH focus on specific labels (because other labels might incur access fees to trusted sources)? The recommendation here is to leave clearing houses free to choose which extensions they run so that the market drives adoption.
4. **Label extensions:** See Table 13 below, describing four label extension options and their respective pros and cons.
5. **Functional scope of the ontologies considered for verification in a clearing house:** Today they are limited to the VC (Verifiable Credential) ontologies and the extensions might come with the requirement to add other ontology standards (domain-specific ontologies), which is an item for the road map. For details, see chapter item 3.6 Practical implementation of extensions governance.

6. **Registry:** We must reflect on whether all labels and criteria would be listed in a common Gaia-X registry. If yes, which would be the case for scenarios 2, 3, and 4, then this common registry would enable the findability or the discoverability of these labels and criteria extensions. This could be implemented in the form of a federated catalogue, allowing decentralized management of all extensions, but securing central visibility or discoverability. The idea here is that we would only create an instance where we can find all extensions, while maintaining the management of extensions decentralized. The pros and cons of this variable relates to how much control there needs to be in this registry function. If labels and criteria are centrally listed, then we would have harmonized labels and criteria. If not centrally listed, then we could end up with multiple variations of the same labels and criteria, which could create confusion in the market.
7. **Naming and branding:** Extensions, according to each scenario, must be clearly named, consistently labelled, and effectively communicated. This is a critical consideration, as clarity in this area is essential to prevent confusion in the market. Nonetheless, the exact details remain to be worked out depending on the scenarios retained. We assume that multiple scenarios and options will remain available, which will make it essential for naming conventions to properly differentiate between the types of extensions developed and the level of Gaia-X control they entail.
8. **Pricing strategy:** The recommendation is that the basic certification service (Gaia-X Labels 1 to 3) remain free to ensure accessibility and lower entry barriers for participants. Nonetheless, the pricing strategy should address two main cost elements: (a) Costs for a custodian to establish a Gaia-X endorsed extension (i.e., a fee paid by the custodian to have their extension formally endorsed); and (b) Costs that the clearing houses are allowed to charge for verification of extensions. This last point, in turn, can be governed by two conditions: (i) the verification of base Gaia-X labels is always free; and (ii) the verification of extensions can either be free or subject to a fee, and such fees may be charged to either the participant requesting the verification or the custodian responsible for the extensions. Table 12 describes pros and cons of establishing a pricing strategy.

Table 12. Pros and cons of establishing a pricing strategy (variable 8)

Pros	Cons
Introducing fees for extensions provides a sustainable revenue stream for Gaia-X (which supports code integration, maintenance, and technical assistance for custodians) and for digital clearing houses (which helps them recover costs).	Introducing fees for extensions may create a financial barrier for custodians – often not-for-profit and resource-limited – potentially slowing down the creation and adoption of extensions.

Table 13. Breakdown of Label Extensions (variable 4)

Extension	Pros	Cons
Whatever the custodian wants	Freedom to custodians.	Beyond existing scope of Gaia-X.
Any digital assets and digital services	Still provides a large scope of freedom to custodians, and resonates better with the purpose of Gaia-X.	The term “digital” is seen as a vague term and therefore this option can potentially lead to option A (whatever the custodian wants).
Any digital assets within the existing scope of Gaia-X[20]	Resonates with the existing scope of Gaia-X values in assets already within the Gaia-X scope.	This option could limit innovation by preventing ecosystems to define novel labels on digital assets that make sense to them, but which are not yet in the Gaia-X conceptual model.
Only extensions of Gaia-X Labels	Resonates with the existing scope of Gaia-X.	Too restrictive for custodian who wants to break from the existing Gaia-X label structure.

3.2.6. Label structure

- Standard Compliance (declaration): Transparency, even if it does not respect the core domain values.

[20] The Gaia-X Architecture Document 5.1.2.2 states that an object can be any entity from the Gaia-X information models, like, and not limited to, a Service Offering, a Data Product, a Participant, and a Data Usage Agreement.

- Level 1 (declaration): Respect of the core domain values (e.g., cyber, SLA, CSP, domain qualification for participants, data quality vs. domain standards for Data Products, etc.).
- Level 2 (certification): Same as Level 1 but certified.
- Level 3 (certification): Full sovereignty and immunity to external policies, i.e., the system under labelling cannot be forced, by an external body, to behave differently than committed (which can typically occur when an actor belongs to several ecosystems, e.g., a CSP from a foreign jurisdiction could be forced to disclose stored data, a banker participating in a medical ecosystem could be forced for AML purpose to declare to ECB some transactions even if related to medical use cases).
- Extension only: The domain can only add new criteria to the Cloud Services criteria defined by Gaia-X, in order to integrate additional domain specific constraints.
    - Pros: Clear message regarding Gaia-X, full automation for the domains, and validation by Gaia-X is easy.
    - Cons: Some business might find it far too constraining, this applies only to Cloud Services, and not compatible with geographical extensions (relating to non-EU jurisdictions).

3.4. The extensions entropy

3.4.1. Domain extensions

The intention is to allow the market to define and propose domain extensions. As a result, these extensions may overlap and become heterogeneous, covering areas such as automotive, manufacturing, intellectual property, and music. We suggest starting with domain experimentation within the 14 sectors of the European Common Data Spaces and initiating pilots with the two or three most promising ones. Additionally, various cross-sector regulations, such as the EU Data Act, AI Act, and the Supply Chain Due Diligence Act, may warrant a common labelling scheme. Given the overlap between sectors, these extensions to the original Gaia-X labelling scope might require overarching governance rather than a dataspace-specific approach.

3.4.2. Geographical extensions

Regarding geographical extensions, the scope should be more stable with joint working groups between Gaia-X and specific countries. However, complexity may also arise in this area, with the aim to open extensions both at national level and regional level (e.g., Japan and APEC).

3.5. The 2 layered governance

The governance process for Gaia-X extensions is crucial to ensure the consistency and stability of the Gaia-X framework and its extensions. For most scenarios, the governance will be structured at two levels: the general governance of all extensions at the Gaia-X level and the specific governance of a given extension.

3.5.1. General governance of extensions at Gaia-X level

For the general governance of extensions at the Gaia-X level, it is essential to ensure the consistency of this Gaia-X "product" with the Gaia-X processes. It is hence considered essential that the tooling associated with the extended labelling framework shall rely on the GXDCH in order to ensure cross-usage among ecosystems. Additionally, a framework for the lifecycle management of domain extensions must be provided, along with a RACI matrix with all the existing bodies of Gaia-X (PRC, TC, DSBC, BoD, etc.).

3.5.2. Specific governance of a given extension

For the specific governance of a given extension, the same basic principles shall apply to all extensions to be compliant with Gaia-X processes, with some specific elements for geographies and for domains. Extensions can have self-determination beyond these basic governance principles. We propose to use the term "extension custodian", who may be a legal person such as an association with fair representing of the given domain or region.

3.6. Practical implementation of extensions governance

To ensure efficient governance, the rules must be based on practical elements such as the ontology and criteria.

Similar to the Gaia-X ontology, an ontology extension should be open-source and made publicly available. Each extension custodian must ensure that their ontology extension complies with the current release of Gaia-X. While the functional scope of ontologies considered for verification in a clearing house is currently limited to VC (Verifiable Credentials) ontologies, future extensions may require the addition of other ontology standards, including domain-specific ontologies, and added as an item in the roadmap.

Another key aspect to implementing practical governance is the criterion unit. An extension criterion can apply to several extensions (e.g., criterion for Digital Product Passport). Like the ontology, extension criteria must be consistent with the evolution of the compliance document's content. This responsibility lies with the extension custodian that provide the extensions encompassing specific criteria.

To meet these expectations of compliance with the Gaia-X framework, several governance schemes can coexist for extensions, depending on their context, use, and lifecycle.

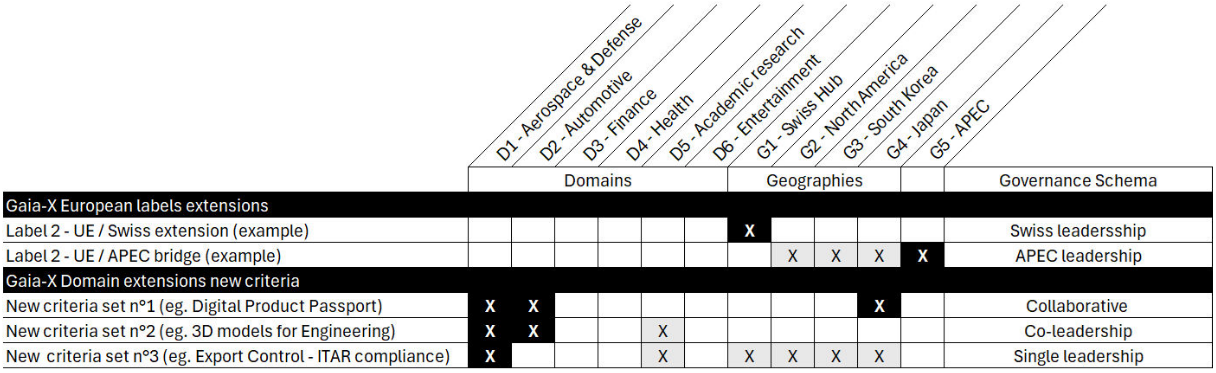
- In the case of a single actor building an extension, for example, within the framework of a data-space project and wanting to make these elements available for other Gaia-X based data spaces, the governance scheme would rely on single leadership, as the actor is doing most of the heavy lifting and is the major user of the extension. This actor is referred to as the sole custodian of the extension.
- For an extension where two actors have a say in the use case and want to create a common model, the governance scheme would rely on co-leadership, with two partners steering the extension and requiring unanimous decisions. These actors are referred as co-custodians of the extension.
- In the case of an extension that is mature and is used or will be used by many actors, it would rely on collaborative governance with quorum voting and specific

rules to access voting rights. A consortium or an association gathering all these actors can be the custodian of the extension.

Regarding criteria, in the current Gaia-X framework, there are three predefined labels. Extensions can add elements to these labels but cannot change them, which remains the exclusive prerogative of the Gaia-X AISBL. Other consistent gatherings of criteria may be created, thereby raising the question of how we name these elements (e.g., labels, set- ups, schemas, etc.).

Below is a figure representing governance scenarios at the intersection of ecosystems (both geographic and domain-oriented) and criteria.

Figure 1. Criteria extensions



	D1 - Aerospace & Defense	D2 - Automotive	D3 - Finance	D4 - Health	D5 - Academic research	D6 - Entertainment	G1 - Swiss Hub	G2 - North America	G3 - South Korea	G4 - Japan	G5 - APEC	
	Domains						Geographies					Governance Schema
Gaia-X European labels extensions												
Label 2 - UE / Swiss extension (example)							X					Swiss leadersship
Label 2 - UE / APEC bridge (example)								X	X	X	X	APEC leadership
Gaia-X Domain extensions new criteria												
New criteria set n°1 (eg. Digital Product Passport)	X	X								X		Collaborative
New criteria set n°2 (eg. 3D models for Engineering)	X	X			X							Co-leadership
New criteria set n°3 (eg. Export Control - ITAR compliance)	X				X		X	X	X	X		Single leadership

4. Technical Requirements

4.1. Important considerations

1. The current discussion supposes that the source code of GXDCH is unique, developed and provided by an OSS community controlled by Gaia-X AISBL (although, this assumption doesn't apply to scenario 1 discussed in Chapter 3. Strategy and governance options). However, specific GXDCH deployments might choose which labels they can provide because access to some admissible issuers (see definition below) might be restricted or costly.
2. The formalization below is independent of the choice to impose or not a predefined label structure (i.e. the 4 scenarios discussed in chapter 3) because this

structuring is not relevant from a pure technical point of view, even if essential from a branding point of view.

3. The formalization below is a generalization of the current scheme. A transition path from the Loire release to Danube can consist in providing in Danube some of the Loire services for Verification Method and in using the Loire GXDCH as an Admissible Issuers (for instance for CSP criteria P1.1.x and P1.2.X).
4. The formalization below to enable definitions of new labels by other ecosystems might seem quite different from the structure of the current Compliance Document (even if we tried to keep full compatibility). If we take this approach, some change management efforts will be necessary to avoid immediate rejection.

4.2. Labelling concepts

A Label is a set of criteria to be fulfilled by an Entity Under Labelling (EUL). An EUL can be a variety of digital related components: a Cloud Service, an Actor, an IT infrastructure, a Software provider, an AI Agent, etc. Each label is “owned” and maintained by one Ecosystem and can be used by several ecosystems. For instance, Gaia-X is an ecosystem which owns some general interest labels. If needed, usage of a label can be restricted to members of an ecosystem by adding a specific membership criterion within the label set of criteria. Each Entity Under Labelling (EUL) must possess a unique identifier, which is included in the certificate delivered by the GXDCH. The scope of this identifier is to be discussed: either global (by means of a directory maintained by Gaia-X AISBL) or per ecosystem. Checking the correspondence between the identifier and the real entity is to be done by the persona using the label and is not guaranteed by Gaia-X. Checking that a service with a Level-3 label is really the one delivered by the provider to a specific consumer is, for instance, outside the scope of Gaia-X.

A Criterion is composed of:

- An Objective which is a high-level textual description of the aim of the criterion;
- A Declaration which is a precise description of the characteristics needed to fulfil the criterion (Open Digital Rights Language with a formal ontology is preferred but text is accepted);

- One or more Verification Methods to automatically check the required characteristics.

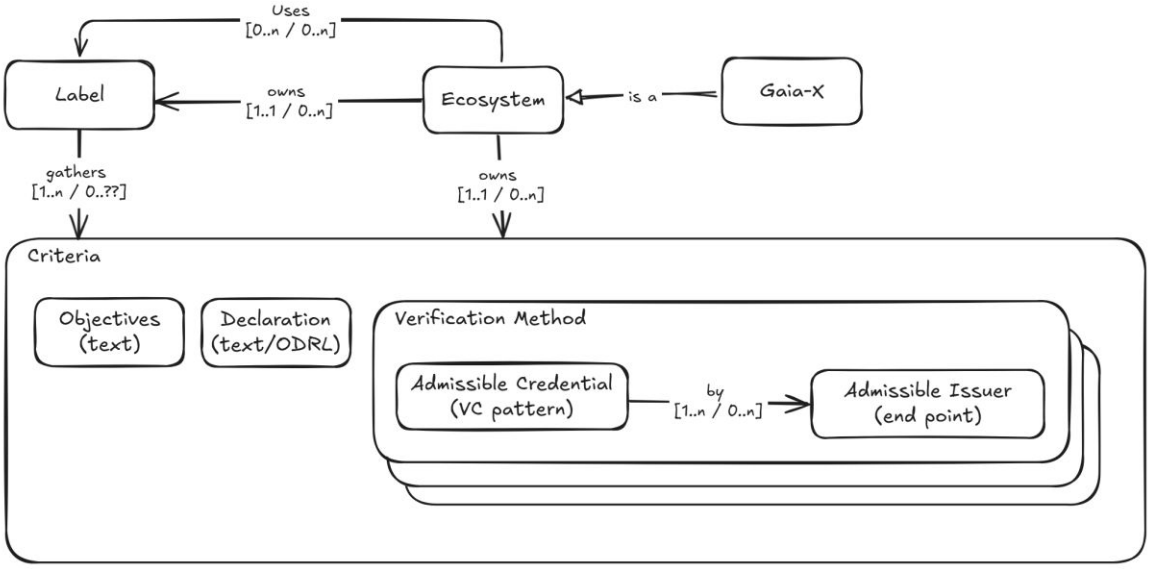


Figure 21. Labelling concepts

To enable a GXDCH to provide labels from different ecosystems, the Verification Method is generic: it specifies an Admissible Credential, which is a Verifiable Credential pattern, and at least one Admissible Issuer. The EUL identifier is part of the Admissible Credential.

To get the EUL stamped for a specific label by a GXDCH, the applicant must provide a Verifiable Presentation containing, for each criterion, the chosen verification method and a verifiable credential (VC) signed by one of the admissible issuers listed in the Verification Method. The role of the GXDCH is “simply” to check that the provided VC matches the Admissible Credential pattern and is valid (i.e., actually signed by an Admissible Issuer and is not suspended or revoked).

An Admissible Issuer listed in a Verification Method must be recognized by the Ecosystem, included in the ecosystem registry and compatible with Gaia-X. It means that the validity of the Issuer signature can be verified by the GXDCH. Being “Gaia-X compatible” is purely technical and is independent from the semantical/trust value that an ecosystem grants to the issuer. A Verification Method might accept the applicant as one of the Admissible Issuer. This corresponds to a self-declaration.

Notaries are discussed in a specific section below. The concept of power of attorney (which are essential) is not described here because we have not identified any significant interaction with label-extension mechanisms; it just impacts the signature verification process.

4.3. Label Extension

Some ecosystems might just need to slightly adapt an existing label and might want to avoid the burden of defining and maintaining a complete label.

From a branding point of view, adapting an existing Label could be useful to benefit from the reputation of the existing label while adding some specificities from the reusing ecosystem. In that purpose, it must be ensured that label extension functions in a stacked configuration, meaning that being certified for the extended label automatically guarantees the respect of the reused label. Hence the possible extensions are either to add a new criterion or to remove a verification method. Other adaptations like removing a criterion, adding a Verification method or adding an Admissible Issuer could weaken the reused label.

If an ecosystem just wants to add some criteria to an existing label and benefit from the new release of this label, then a simple way consists in creating a new label with a first criterion requesting the certification versus the existing label and in using GXDCH as Admissible Issuers.

For all other adaptations, we have not found any technical scheme that brings more value than a simple duplication without significantly increasing the GXDCH complexity. Indeed, label extension mechanisms could be thought to facilitate maintenance when the reused label evolve. This is not the case as any release of the reused label will involve a thorough evaluation by the reusing ecosystem to guarantee that it will not weaken the reusing label. For instance, when adding a Verification Method or an Admissible Issuer which is not trusted by the reusing ecosystem.

Accordingly, we propose to handle label extension as a branding issue: Gaia-X AISBL will manually ensure that the label naming by the different ecosystems make sense, especially for label names owned by Gaia-X.

4.4. Ontology extension

There may still be some technical gaps for how this mechanism can be extended with none or minimal human intervention. Nonetheless, we need to prepare to scale for when many extensions are requested, and we need to (semi-)automatically validate and release such extensions.

4.5. Real time label verification

Some ecosystems might need label verification in "real time". A method to enable that is to include in the Admissible Credential a field specifying a validity period: the VC provided by the Admissible Issuer must be signed within a certain period (for instance less than 30 days). This mechanism could also be used to handle capability evolutions of issuers, for instance to accept only VC signed after a certain date because certificates issued before that date by a particular issuer are not considered safe enough (for example) by the ecosystem.

4.6. Label versioning

From a technical point of view, label versioning is useful to provide upward compatibility, i.e., being certified for a version automatically provides certification for version n+1.

This is rarely the case when the Objective or the Declaration of a criterion is changed or when a Verification Method is removed (for instance, when an issuer is not trustable anymore). Note that from a technical point of view changing a criterion Objectives or Declaration has no impact for the GXDCH but could have an important impact on the way the Admissible Issuers check the compliance before delivering the signed Verifiable Credential.

Label versioning is also important from a marketing point of view for brand continuity. From an operational point of view, it might be convenient to add a new Verification Method (for instance, a new standard is available) or to add a new Admissible Issuer without having to re-certify everything. A way to accommodate these points of view is to consider different label versions as independent from a technical point of view (hence no upward compatibility) and to define the concept of Release. In this case, a release can only add new Verification Methods or Admissible Issuers to the criteria – adding criteria, removing Verification Method or removing Admissible Issuer is forbidden.

As adding a Verification Method and/or an Admissible Issuer can weaken a criterion and consequently a label (if the added method is more permissive), creating a new Release must be limited to the owner of the label.

4.7. Notaries

Notaries are used to convert non-VC attestation (i.e., paper certificate, presence in a register, etc.) into a VC that can be used by a GXDCH. Initially, we can think of three alternatives for how a GXDCH can decide or not to accept a VC from a notary. They are as follows:

Alternative	Description	Pros/Cons
1	Accepted Notaries are listed in the Admissible Issuers for each criterion.	• Pros: easy for the GSDCH • Cons: tedious for label owners
2	Accepted notaries are listed in a register managed by the ecosystem and are recognized for all Verification Methods of the label.	• Pros: easy for label owners • Cons: more complex for Gaia-X OSS team and might not be precise enough (i.e., someone able to understand the specificities of a US standard might not be able to understand the specificities of a Chinees standard).
3	Accepted Notaries are selected by Gaia-X and listed in a general register (independent from labels, ecosystems, labels and verification methods).	• Pros: TBD • Cons: more burden on Gaia-X and might not be precise enough.

Note that there are several ways to implement alternative 1. For example: include the notaries in each Verification Method, list the notaries in a preamble of the Label with the list of VC templates it can provide, and list the notaries in a register managed by the ecosystem with the list of VC templates it can provide. These are second-level optimization choices that can be discussed later.

5. Operationalization

For the operationalization of geographical and domain extensions, we suggest three GXDCH verification options:

- The receiving (verifying) GXDCH only verifies the legitimacy of the issuing GXDCH and fully trusts the VCs, based exclusively on the fact that the source is a verified and hence trusted GXDCH.
- The receiving (verifying) GXDCH verifies the veracity of the VCs by contacting all the original issuers (trust anchors) of the VCs claims (e.g. eIDAS API).
- Notarization: The GXDCH verifies that the credential is properly signed by the notary. No further verification takes place at the GXDCH level. In this case, the notary is legally
- liable for the notarized information and at least one notary for a specific region or regulation (e.g. ecosystem-specific VCs) is required.

A notary service can be provided by a GXDCH. GXDCHs offering notary services due to regional limitation reasons (e.g. Japan) will offer the usage of these notary services to all other GXDCHs, as defined in the GXDCH contract.

5.1. User Story

Company A, delivering services in, but not exclusively for Japan, obtains VCs from a Japanese GXDCH using Japanese Trust Anchors (e.g. VAT API). All other global GXDCHs can recognize, validate and accept these VCs as Gaia-X compliant. Hence when Company B, operating in Europe, intends to consume data services from Company A, they can directly verify Company A's organizational and service VCs using their preferred GXDCH or any GXDCH globally. This use case works in both directions.

This scenario will always work with verification option one, but option two might not be available for all Trust Anchors outside the original GXDCHs region caused by geographical, technical or regulatory limitation to Trust Anchors (service). In this case Company B may either deem verification option 1 as sufficient or can request notarization by a notary for higher veracity.

6. Future Work

As a next step, the White Paper will be presented to the Gaia-X Policy and Rules Committee (PRC) and the Gaia-X Technical Committee (TC). Following more concrete decisions within the PRC, we will initiate a broader consultation with Gaia-X members, including the Gaia-X Lighthouse projects. Based on the feedback received, the document will be iteratively refined, and a final version will be presented to the Board of Directors (BoD). Once the BoD decides on a preferred scenario, a dedicated forum will be established to engage ecosystems in defining potential criteria and progressing toward the alignment of technical requirements.

Annex I. Detailed analysis of extension of criteria to Switzerland

Control No.	Comments	Control Description Proposal
Control P.1.1.2.	Contract governed to include Switzerland	• **Control Proposal:** The Provider shall have an option for each legally binding act to be governed by EU/EEA/Member State and Switzerland Law. • **Permissible standards:** N/A
Control P.2.1.1.	Applicable Law to include Switzerland.	• **Control Proposal:** The Provider shall offer the ability to establish a contract under Union/EU/EEA/ Member State Law and Switzerland specifically addressing local privacy requirements. • **Permissible standards:** N/A
Control P.2.2.3.	Third country transfer to mirror Switzerland adequacy decision.	• **Control Proposal:** Current description is ok. • **Permissible standards:** Federal Act on Data Protection. Section 3 Cross-Border Disclosure of Personal Data.
Control P.2.2.4.	Third country transfer to mirror Switzerland adequacy decision.	• **Control Proposal:** The Provider shall clearly define if a to the extend third country transfers will take place, and by which transfer mechanism, contemplated in EU/EEA/ Member State Law and Switzerland law will apply. • **Permissible standards:** Federal Act on Data Protection. Section 3 Cross-Border Disclosure of Personal Data.
Control P.5.1.1.	Data to be processed to include Switzerland.	• **Control Proposal:** For Label Level 2, the Provider shall provide the option that all Customer Data are processed and stored exclusively in EU/EEA or Switzerland. • **Permissible standards:** Lex Generalis (e.g. Federal Act on Data Protection) does not contain limitation (same as GDPR). However, lex specialis (e.g. Blocking statutes) sets limitations. An example can be found under Art. 47* of the Swiss Federal Act on Banks and Saving Banks Blocking statutes which highlights the principle “over the border out of control”.

Control P.5.1.2.	Disclosure of data to include Switzerland regulatory requirements.	• **Control Proposal:** For Label Level 3, the Provider shall process and store all Customer Data exclusively in the EU/EEA or Switzerland. • **Permissible standards:** Lex Generalis (e.g. Federal Act on Data Protection) does not contain limitation (same as GDPR). However, lex specialis (e.g. Blocking statutes) sets limitations. An example can be found under Art. 47* of the Swiss Federal Act on Banks and Saving Banks Blocking statutes which highlights the principle "over the border out of control".
Control P.5.1.3.	HQ to also include Switzerland.	• **Control Proposal:** For Label Level 3, where the Provider or subcontractor is subject to legal obligations to transmit or disclose Customer Data on the basis of a non-EU/EEA or Switzerland statutory order, the Provider shall have verified safeguards in place to ensure that any access request is compliant with EU/EEA/Member State and Switzerland law. • **Permissible standards:** Federal Act on Data Protection. Section 3 Cross-Border Disclosure of Personal Data.
Control P.5.1.4.	Provider main establishment to also include Switzerland.	• **Control Proposal:** For Label Level 3, the Provider's registered head office, headquarters and main establishment shall be established in a Member State of the EU/EEA or Switzerland. • **Permissible standards:** N/A
Control P.5.1.5.	Switzerland to be included for shareholders that are ok to exercise decisive control.	• **Control Proposal:** For Label level 3, shareholders in the Provider, whose registered head office, headquarters and main establishment are not established in a Member State of the EU/EEA nor in Switzerland, shall not, directly or indirectly, individually or jointly, hold control of the CSP. Control is defined as the ability of a natural or legal person to exercise decisive influence directly or indirectly on the CSP through one or more intermediate entities, de jure or de facto (cf. Council Regulation No. 139/2004 and Commission Consolidated Jurisdictional Notice under Council Regulation (EC) No. 139/2004 and Commission Consolidated Jurisdictional Notice under Council

		Regulation (EC) No. 139/2004 for illustrations of decisive control). • **Permissible standards:** N/A

*ARTICLE 47 1. Whoever intentionally does the following shall be imprisoned up to three years or fined accordingly:

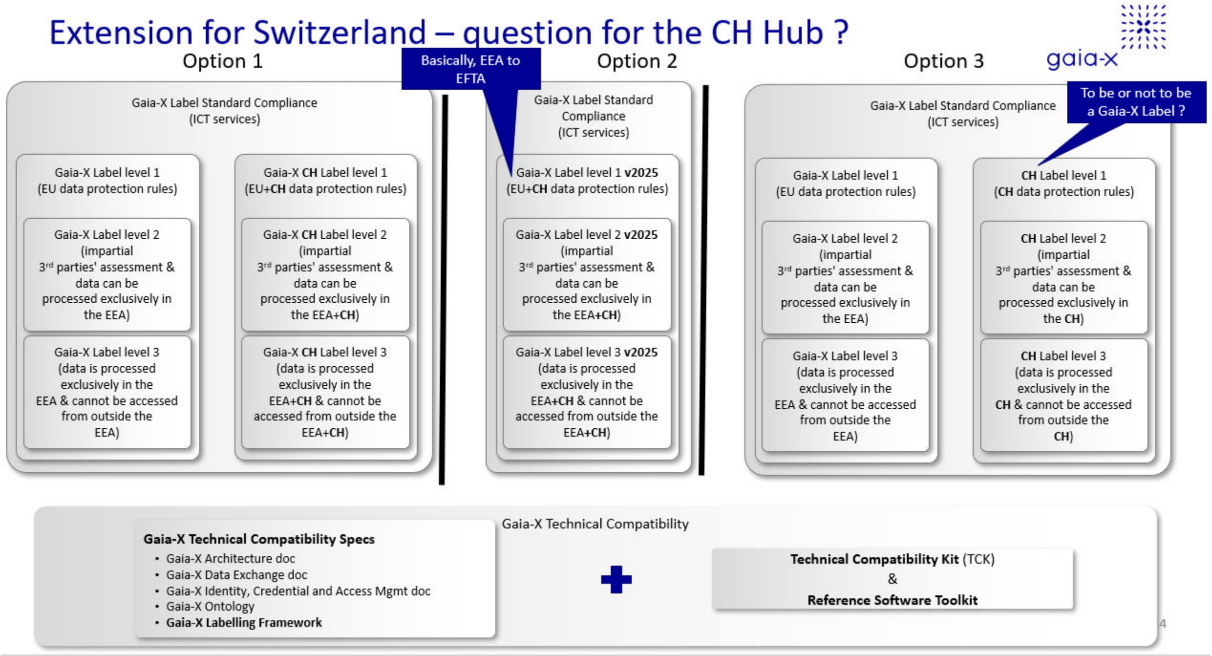
a. Disclose confidential information entrusted to them in their capacity as a member of an executive or supervisory body, employee, representative, or liquidator of a bank or a person in accordance with Article 1b, as member of a body or employee of an audit firm or that they have observed in this capacity.

b. Attempt to induce an infraction of the professional secrecy.

c. Disclose confidential information to third parties or use this information for own benefits or the benefit of others.

1bis. Whoever enriches themselves or others with an action in accordance with (1)(a) or © shall be punished with imprisonment for up to five years or fined accordingly.

1. Whoever acts in negligence shall be penalized with a fine of up to CHF 250,000.
2. … (repealed)
3. The violation of the professional confidentiality shall remain punishable even after a bank license has been revoked or a person has ceased his/her official responsibilities.
4. The federal and cantonal provisions on the duty to provide evidence or on the duty to provide information to an authority shall be exempted from this provision.
5. Prosecution and judgment of offenses pursuant to these provisions shall be incumbent upon the cantons. The general provisions of the Swiss Penal Code shall be applicable.



Extension for Switzerland – question for the CH Hub ?

Option 1

Gaia-X Label Standard Compliance (ICT services)

Gaia-X Label level 1 (EU data protection rules)

Gaia-X Label level 2 (impartial 3rd parties' assessment & data can be processed exclusively in the EEA)

Gaia-X Label level 3 (data is processed exclusively in the EEA & cannot be accessed from outside the EEA)

Gaia-X **CH** Label level 1 (EU+**CH** data protection rules)

Gaia-X **CH** Label level 2 (impartial 3rd parties' assessment & data can be processed exclusively in the EEA+**CH**)

Gaia-X **CH** Label level 3 (data is processed exclusively in the EEA+**CH** & cannot be accessed from outside the EEA+**CH**)

Basically, EEA to EFTA

Option 2

Gaia-X Label Standard Compliance (ICT services)

Gaia-X Label level 1 **v2025** (EU+**CH** data protection rules)

Gaia-X Label level 2 **v2025** (impartial 3rd parties' assessment & data can be processed exclusively in the EEA+**CH**)

Gaia-X Label level 3 **v2025** (data is processed exclusively in the EEA+**CH** & cannot be accessed from outside the EEA+**CH**)

Option 3

Gaia-X Label Standard Compliance (ICT services)

To be or not to be a Gaia-X Label ?

Gaia-X Label level 1 (EU data protection rules)

Gaia-X Label level 2 (impartial 3rd parties' assessment & data can be processed exclusively in the EEA)

Gaia-X Label level 3 (data is processed exclusively in the EEA & cannot be accessed from outside the EEA)

CH Label level 1 (**CH** data protection rules)

CH Label level 2 (impartial 3rd parties' assessment & data can be processed exclusively in the **CH**)

CH Label level 3 (data is processed exclusively in the **CH** & cannot be accessed from outside the **CH**)

Gaia-X Technical Compatibility

Gaia-X Technical Compatibility Specs

- Gaia-X Architecture doc
- Gaia-X Data Exchange doc
- Gaia-X Identity, Credential and Access Mgmt doc
- Gaia-X Ontology
- **Gaia-X Labelling Framework**

✚

Technical Compatibility Kit (TCK) & **Reference Software Toolkit**

Figure 2. Swiss extension

Annex II. Mind map scenarios

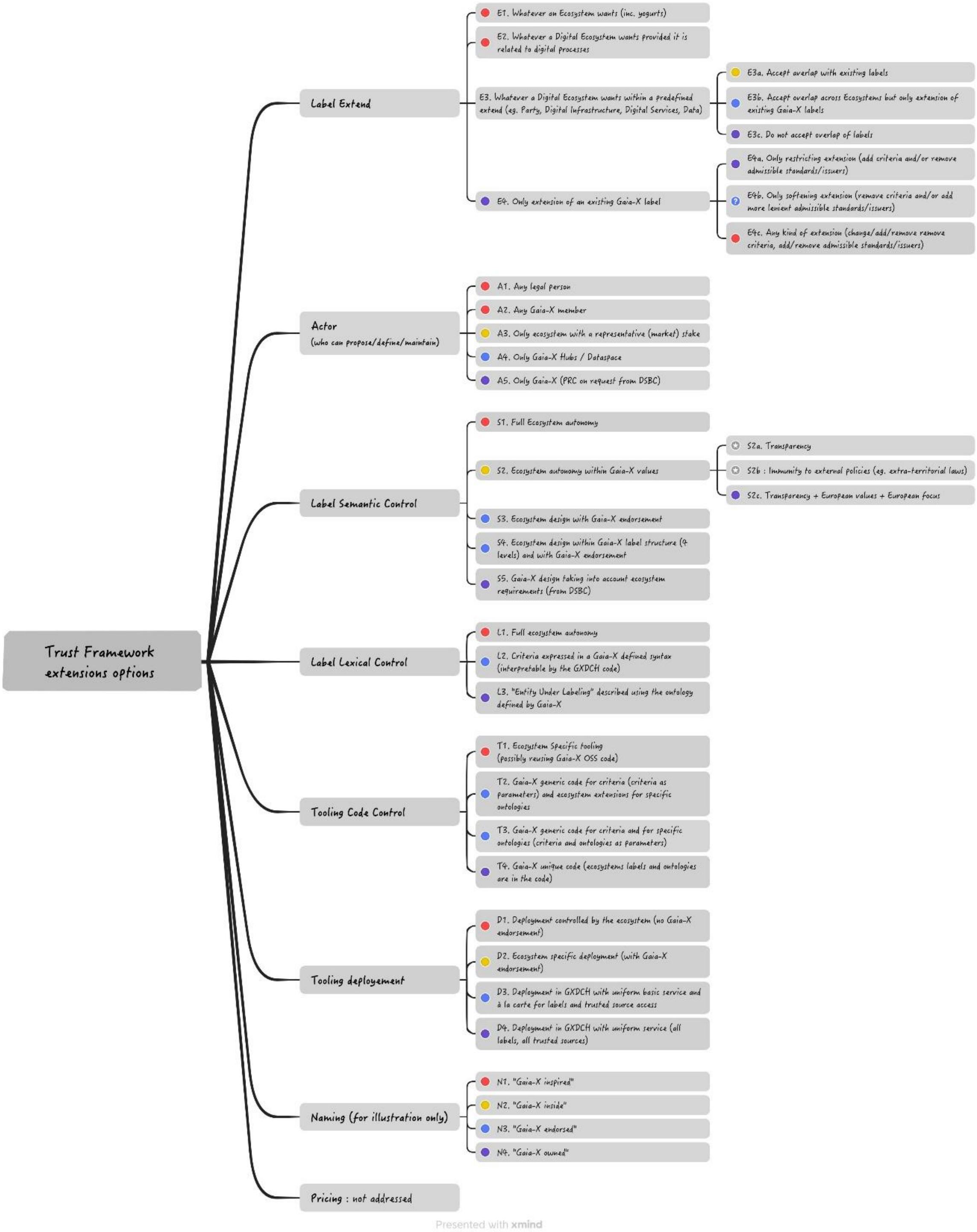

Trust Framework extensions options
Label Extend
E1. Whatever an Ecosystem wants (inc. yogurts)
E2. Whatever a Digital Ecosystem wants provided it is related to digital processes
E3. Whatever a Digital Ecosystem wants within a predefined extend (eg. Party, Digital Infrastructure, Digital Services, Data)
E3a. Accept averlap with existing labels
E3b. Accept overlap across Ecosystems but only extension of existing Gaia-X labels
E3c. Do not accept overlap of labels
E4. Only extension of an existing Gaia-X label
E4a. Only restricting extension (add criteria and/or remove admissible standards/issuers)
E4b. Only softening extension (remove criteria and/or add more lenient admissible standards/issuers)
E4c. Any kind of extension (change/add/remove remove criteria, add/remove admissible standards/issuers)
Actor
(who can propose/define/maintain)
A1. Any legal person
A2. Any Gaia-X member
A3. Only ecosystem with a representative (market) stake
A4. Only Gaia-X Hubs / Dataspace
A5. Only Gaia-X (PRC on request from DSBC)
Label Semantic Control
S1. Full Ecosystem autonomy
S2. Ecosystem autonomy within Gaia-X values
S2a. Transparency
S2b : Immunity to external policies (eg. extra-territorial laws)
S2c. Transparency + European values + European focus
S3. Ecosystem design with Gaia-X endorsement
S4. Ecosystem design within Gaia-X label structure (4 levels) and with Gaia-X endorsement
S5. Gaia-X design taking into account ecosystem requirements (from DSBC)
Label Lexical Control
L1. Full ecosystem autonomy
L2. Criteria expressed in a Gaia-X defined syntax (interpretable by the GXDCH code)
L3. "Entity Under Labeling" described using the ontology defined by Gaia-X
Tooling Code Control
T1. Ecosystem Specific tooling (possibly reusing Gaia-X OSS code)
T2. Gaia-X generic code for criteria (criteria as parameters) and ecosystem extensions for specific ontologies
T3. Gaia-X generic code for criteria and for specific ontologies (criteria and ontologies as parameters)
T4. Gaia-X unique code (ecosystems labels and ontologies are in the code)
Tooling deployement
D1. Deployment controlled by the ecosystem (no Gaia-X endorsement)
D2. Ecosystem specific deployment (with Gaia-X endorsement)
D3. Deployment in GXDCH with uniform basic service and à la carte for labels and trusted source access
D4. Deployment in GXDCH with uniform service (all labels, all trusted sources)
Naming (for illustration only)
N1. "Gaia-X inspired"
N2. "Gaia-X inside"
N3. "Gaia-X endorsed"
N4. "Gaia-X owned"
Pricing : not addressed
Presented with xmind

Figure 3. Scenarios - Mind map

Annex III. Potential label structure

Some scenarios listed in chapter 3 consider using a coherent label structure across all Gaia-X endorsed labels to capitalise on the current 4-levels and to fit with Gaia-X values (mainly transparency and sovereignty). Here is an attempt to generalize the 4-levels to other kind of artefacts (parties, digital assets, …) beyond Cloud Services:

- Standard Compliance (declaration): transparency, even if the artefact does not respect core domain values.
- Level 1 (declaration): respect of the core values of the domain, for instance cybersecurity or SLA for CSP, domain qualification for participants, data quality vs domain standards for Data Products.
- Level 2 (certification): Same as Level 1 but certified by an external Assessment Body accredited by the domain.
- Level 3 (certification): Full sovereignty and immunity to external policies, i.e. the artefact cannot be forced, by an body external to the domain, to behave differently than originally committed (which can typically occurs when an actor belongs to several ecosystems, e.g., a CSP from a foreign jurisdiction could be forced to disclose stored data, a banker participating in a medical ecosystem could be forced for Anti Money Laundering (AML) purpose to declare to the European Central Bank some transactions even if considered as trade secret within some domains, etc.).

Annex IV. Glossary

Disclaimer. Concepts presented in this paper that are not included in the formal glossary are provided solely for the purpose of clarifying information found in this document. Their inclusion does not imply formal concept adoption or standardization beyond the scope of this paper.

Accredited Labelling Body (ALB): An enterprise accredited by Gaia-X and the custodian ecosystem to check EUL against the label criteria and deliver Label Stamps (currently the only ALB accepted by Gaia-X are the GXDCH – opportunity to extend or not is discussed later in the document).

Admissible Credential:

Admissible Issuer:

Aerospace, Security and Defence Industry Association of Europe (ASD):

Association for Standardization of Automation and Measuring Systems (ASAM):

Association Française de Normalisation (AFNOR):

Attestation:

Cloud Service:

Cloud Service Provider (CSP):

Credentials:

Critical Third-Party Provider (CTPP):

Custodian: Custodians (i.e., the actors) is the term used within the scope of this white paper to refer to who can propose, define, and maintain a label extension to the compliance framework. In each scenario, label custodians can be either anybody, any Gaia-X member, only ecosystem with a significant market share, only Gaia-X Hubs/Dataspaces or only Gaia-X PRC (upon requests from the DSBC).

Danube:

Data: Any digital representation of acts, facts or information and any compilation of such acts, facts or information. Data are furnished by Data Producers to Data Providers who compose them into a Data Product to be used by Data Consumers.

Data Exchange Service:

Data infrastructure:

Data product: Data are furnished by Data Producers to Data Providers who compose them into a Data Product to be used by Data Consumers. A Data Products is described by a Data Product Description, which must be a valid Gaia-X Credential and is stored in a (searchable) Federated Data Catalogue.

Data space: Interoperable framework, based on common governance principles, standards, practices and enabling services, that enables trusted data transactions between participants.

Digital Operational Resilience Act (DORA):

Domain:

Ecosystem: A group of interacting participants which have agreed through a formal governance body to a set of Policy Rules that any participant needs to conform to.

Entity Under Labelling (EUL): Specific things that an applicant wants to be checked against the criteria of a specific label.

European Union Safety Aviation Agency (EASA):

Extension:

Federated:

Gaia-X Compliance Document:

Gaia-X Compliance Framework:

Gaia-X Data & Services Business Committee (DSBC): The Data & Services Business Committee (DSBC) collects, shares, and aligns needs and achievements between national

Hubs, Ecosystems, Gaia-X Lighthouses & projects, and Service Providers to support the creation of Data Spaces and accelerate Gaia-X market adoption.

Gaia-X Digital Clearing Houses (GXDCH): The Gaia-X Digital Clearing House operationalizes the Gaia-X mission. A GXDCH makes the various mechanisms and concepts applicable in practice as a ready-to-use service set. The GXDCH contains both mandatory and optional components. All the mandatory components of the GXDCH are open-source software. The development and architecture of the GXDCH is under the governance of the Gaia-X Association.

Gaia-X Ecosystem: The virtual set of participants and Service Offerings following the Gaia-X Compliance requirements.

Gaia-X Framework: The Gaia-X Framework provides an overall view of the Gaia-X Association pillars and deliverables, highlighting the elements that are mandatory to be Gaia-X Compliant and Gaia-X Technical Compatible.

Gaia-X Hub: Gaia-X Hubs bundle user interests across Europe to facilitate the creation of European Data Spaces. They gather use cases, requirements, and standards, to support the Gaia-X Association in setting up and establishing a sovereign data infrastructure via a common Gaia-X architecture as well as policy rules, standards and Federated Services. Gaia-X Hubs are the central contact points for interested parties in each country, and grassroots supporters of the Gaia-X project.

Gaia-X Label: A Gaia-X Label is a machine readable, structured and signed document issued by the accredited Gaia-X Compliance services in case of a valid verification and validation of the criteria for a specific assessment scheme.

Gaia-X Level:

Gaia-X Lighthouse projects: Projects aiming to create a data exchange platform built on transparency, trust, and openness. They target multiple industries and are the front-runners implementing the Gaia-X Framework.

Gaia-X Ontology: An ontology is a formal, explicit specification of a shared conceptualisation.1 In Gaia-X case, it means to create models that are understandable by an algorithm so one can automate rules with a computer. The models are developed by Gaia-X members under the Technical Committee.

Gaia-X Policy Rules Committee (PRC): The Policy Rules Committee (PRC) aims to translate the guiding principles of the Gaia-X initiative, e.g., transparency data protection, cyber security, portability, and openness, into High-Level Objectives to safeguard the added value of the Gaia-X ecosystem. Furthermore, the PRC has the role to monitor, integrate and define the relationship with EU regulations and external standards.

Gaia-X Technical Committee (TC): The Gaia-X Technical Committee defines and implements the technological vision of Gaia-X. It plans, develops, and is accountable for the Gaia-X technology roadmap and its contributors. It further communicates the Gaia-X technological vision and its related objectives to establish trust and credibility with members and third parties.

General Data Protection Regulation (GDPR):

International Aviation Safety Assessment (IASA):

International Traffic in Arms Regulations (ITAR):

Interoperability:

Label: See "Gaia-X Label".

Label Custodian: The ecosystem that defines and maintains the label.

Label Extension:

Label stamp: A secure non-forgeable digital document provided by an Accredited Labelling Body (ALB).

Loire:

Notarization:

Open Digital Rights Language (ODRL):

Permissible Standards:

Release:

Service Offerings:

Specification:

Standards:

Trust Anchors: Gaia-X Trust Anchors are bodies, parties, i.e., Conformity Assessment Bodies or technical means accredited by the bodies of the Gaia-X Association to be parties eligible to issue attestations about specific claims.

Verifiable Credential (VC):

Verification Method:

Working Group: