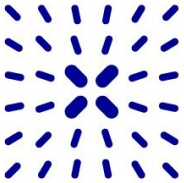
Gaia-X Compliance Document - 25.03 Release



Description	Gaia-X specification to build trusted decentralised digital ecosystems.
Repository	https://gitlab.com/gaia-x/policy-rules-committee/compliance-document
Author(s)	Gaia-X European Association for Data and Cloud AISBL
Copyright(s)	©2024 Gaia-X European Association for Data and Cloud AISBL

Table of Contents

I. About

1 Editorial Information

1.1 Publisher

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

1.2 Authors

GAIA-X European Association for Data and Cloud

1.3 Contact

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

1.4 Other format

For convenience a PDF version of this document is generated here.

1.5 Copyright notice

2 Executive Summary

The Gaia-X Policy Rules define high-level objectives safeguarding the added value and principles of the Gaia-X Ecosystem. To allow for validation, the high-level objectives are underpinned by the Gaia-X Labelling Criteria and the Gaia-X Trust Framework.

The intent of the Gaia-X Policy Rules is to identify clear controls to demonstrate the core European values of Gaia-X: openness, transparency, data protection, security, and portability. The Gaia-X Standard Compliance level defines the minimal set of requirements to be able to participate in the Gaia-X Ecosystem. The optional Label levels define additional criteria and conformance-ensuring measures such as certificates, to achieve additional levels of assurance and trust, with a focus on European values and based on EU/EEA legislation. These initial Labels can be extended, and additional Labels can be added in the future, to accommodate for sectorial or geographical needs. Compliance with these Gaia-X Policy Rules objectives can be achieved via compliance with established standards, certifications, and codes of conduct.

At this stage, the document lists the normative high-level objectives for service offering providers in the following categories: contractual framework, data protection, cybersecurity, European control, and sustainability. The document also defines the mandatory and suggested optional attributes to be used to describe Participants, Services and Resources in the Gaia-X Ecosystem. Furthermore, the document includes a work-in-progress on the requirements towards data exchange services.

The fulfilment of the high-level objectives can be realized in various levels of conformance. The Gaia-X Standard Compliance level includes the set of rules that define the minimum baseline to be part of the Gaia-X Ecosystem. Those rules ensure a common governance and the basic levels of interoperability across individual ecosystems while letting the users in full control of their choices. In other words, the Gaia-X Ecosystem is the virtual set of participants and Service Offerings following the Gaia-X Compliance requirements.

The Trust Framework uses verifiable credentials and linked data representation to build a FAIR (Findable, Accessible, Interoperable, and Reusable) knowledge graph of verifiable claims from which additional trust and composability indexes can be automatically computed. The Labelling Framework extends upon the Gaia-X Standard Compliance level and makes use of verifiable credentials to extend the Trust Framework. Thus, it is ensured that all information required to make a qualified choice between different services is available in a consistent and standardized machine-readable form.

The Labelling Framework itself is further detailed and translated into concrete criteria and measures in this document. The criteria list brings together the policies and requirements from the various Gaia-X Committees – Policy Rules Committee, Technical Committee, and Data Services & Business Committee – along with comprehensive assessments to ensure that these requirements can be met. It allows for further differentiation between services, which is necessary for users wanting to find services for different purposes and based on different needs.

The Gaia-X Labelling Framework is designed using a set of core principles, starting from the high-level objectives which are refined by the labelling criteria. The Labels require consistency among the Gaia-X Ecosystem, scalability and extensibility, composability and modularity mapping, referencing of existing standards, self-assessment and Conformity Assessment Bodies (CAB).

Gaia-X distinguishes 3 levels of Labels, starting from Label Level 1 (the lowest), up to Label Level 3 (the highest), which represent different degrees of compliance with regard to the goals of transparency, autonomy, data protection, security, interoperability, portability, sustainability, and European Control.

II. Introduction

3 Scope

3.1 Preface

Gaia-X Compliance, depending on the specific conformity assessment scheme, can be assessed by technical means and via compliance with established standards, certifications, and codes of conduct. The addition and maintenance of these standards will be defined in this document. Where such tools are not available or approved to demonstrate such compliance, specific methodologies can be further developed and agreed upon within Gaia-X to be included in the attestation of Service Offerings.

In the cybersecurity section we refer, when it is possible, to the current discussions on the European cybersecurity certification scheme for cloud services (the EU Cloud Services Scheme or EUCS). When the EUCS is finalised, Gaia-X may consider adapting the objectives in this document.

Please note that, in general, full adherence to applicable local legislation (e.g., in areas such as data protection and security) is a prerequisite and thus not waived or affected by the following criteria.

It is worth pointing out that participation within Gaia-X by providing Gaia-X compliant services shall not prevent any Provider from also providing non-Gaia-X compliant Service Offerings outside the Gaia-X Ecosystem.

This document is a work in progress, i.e. it will be further worked on to evolve towards a fully clear and complete specification of the Gaia-X Compliance criteria.

Gaia-X will update this document on a regular basis.

Following the publication of the Compliance Document (CD), the previous deliverables of the Policy Rules Committee (Gaia-X Policy Rules and Labelling Document, Gaia-X Trust Framework) are obsolete.

3.2 Design Principles for Gaia-X Standard Compliance and Labels

The Gaia-X Compliance is designed using a set of core principles, starting from the Standard Compliance scheme, which is refined in the Label schemes.

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

*: *not all criteria can be automated.

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

3.2.1 Consistency among the Gaia-X Ecosystem

Gaia-X Compliance reflect the essence of our objectives and concepts. They represent the results of decisions and deliverables introduced by the various Gaia-X Committees and approved by the Gaia-X Board of Directors. The Gaia-X Compliance criteria are always in line with the corresponding concepts and specifications as defined by Gaia-X.

3.2.2 Scalability and extensibility

Based on the four assessment scheme of Gaia-X Standard Compliance and the three (3) Label Levels, further Gaia-X Labels can be created to fit new needs, in particular using extension profiles for country and domain-specific requirements. Extension profiles can also leverage the Label schemes by adding and defining on-top requirements for particular purposes. To ensure the impact and consistency of Gaia-X Compliance, new labels and extensions have to be authorized by the Gaia-X Board of Directors.

3.2.3 Composability and modularity

Gaia-X Compliance schemes are logical groupings of composable service attributes. This results in particular in the assignment of a common set of policies, technical requirements and data space criteria to one or multiple of four schemes. At the same time, Gaia-X Compliance is based upon existing schemes, certifications, and tested and approved codes of conduct where possible to allow the reuse of established standards and thereby simplify the process. Only in areas where no standard has been identified Gaia-X will introduce its own set of attributes and processes to verify the information given.

3.2.4 Standards, self-assessment and Conformity Assessment Bodies (CABs)

Gaia-X Compliance do not normatively reference external documents which are not yet approved (for example the current proposal of the EUCS). Whenever such external documents are approved, Gaia-X may consider adapting its criteria in accordance with them.

Compliance with criteria can be declared by declaration or certification (supported by external Conformity Assessment Bodies), as defined later in this document.

Gaia-X Service Offerings are defined by Provider-generated credentials which include claims that will be validated and verified to prove compliance to the different schemes. The proof of validation of a claim will be also issued as a verifiable credential. The Verifiable Credential can either be issued by a Provider or a CAB directly or it can be created by a trusted Verifiable Credential issuer based on existing documentation (like a signed PDF or paper document).

The Verifiable Credential includes the entity asserting the validity of the claim; the list of trusted Verifiable Credentials issuers is maintained in the Gaia-X Registry.

Users at any time can query the attestation of the Service Offering and for each claim extract the entity and the result of the assessment.

Conformity Assessment Bodies (CABs): Gaia-X reserves its right to choose its own CAB per criteria. A new detailed document will be issued on the process of choosing the relevant CAB. Where the criteria lack reference to established standards, Gaia-X defines a dedicated Assessment Process including a process to appoint adequate CABs (Conformity Assessment Bodies), following internationally recognized good practices, including impartiality, comparability, reliability and accessibility.

3.2.5 Mapping and Referencing of existing standards

It is intended that this document will provide for each criterion a detailed mapping and references to existing standards and certification schemes. This mapping and referencing shall be as detailed as possible, saying that, instead of a generic identification of a standard, the relevant sections in such standards shall be identified.

Example Standard: This document may provide so-called “Example Standards”. Example Standards shall identify potential means of implementation. Gaia-X strives to refer to existing standards and controls to the extent possible. Re-drafting shall be prevented. Nonetheless, Gaia-X and referenced standards may have a different focus and high-level objective. Example standards shall provide for possibilities how criteria may be implemented. Implementation as provided by such standards is not mandatory, and it is required to comply with any such standards. Gaia-X will provide additional notes, if significant differences are identified. Example Standards shall especially help in evaluating compliance with Gaia-X, as Example Standards can be considered “implementation guidance”.

Note: Example Standards will be added after following a thorough assessment by the Gaia-X Working Groups maintaining this document. Such assessment shall follow a transparent process. No Example Standards shall be listed, prior to such process is defined and applied in the determination. The process shall foresee that third-party standards may reach out to Gaia-X and suggest being enlisted.

Permissible Standard: This document may provide so-called “Permissible Standards”. Permissible Standards shall identify standards respectively requirements/controls within such standards, where implementation shall be considered prima facie evidence of conformity with the related Gaia-X criterion. *Note: Permissible Standards can only be added following a thorough assessment by the Gaia-X Working Groups maintaining this document. Such assessment shall follow a transparent process. No Permissible Standards shall be listed, prior to such process is defined and applied in the determination. The process shall foresee that third-party standards may reach out to Gaia-X and suggest being enlisted. The process shall cover both, the material requirements as well as the overarching conformity assessment programme, i.e., the means by which such Permissible Standard determines whether the subject of such assessment is indeed conformant/compliant.*

3.3 Proof of Concept / Bootstrapping

3.3.1 Conformity Assessment Programme and Assessibility

The criteria listed in this document must be and remain assessible at all times. Gaia-X is currently developing accompanying documents outlining the overarching conformity assessment programme and process.

Also, this document will further evolve to enhance the assessibility of its criteria to the extent necessary, e.g. where Gaia-X will not or cannot rely on existing standards and conformity assessment programmes.

Gaia-X anticipates that the requirements outlined in this document are assessible. If comparability of assessment results cannot be guaranteed, or if ambiguities exist, Gaia-X may have to adapt these rules, criteria, or assessment mechanisms in future versions.

In this vein and as mentioned elsewhere in this document, Gaia-X will monitor current regulatory developments as well as developments in the field of standards and conformity assessment programmes. Whilst Gaia-X may consider existing drafts as inspiration, Gaia-X does not endorse any such drafts. Likewise, Gaia-X remains in control of whether to adapt its requirements to future iterations of any such external developments.

3.3.2 Federation of Verification

Gaia-X Labels are issued according to determined criteria and assessments in a federated manner. The concept of modularity also allows Gaia-X to reuse existing certifications for the underlying service attributes whenever possible, hence reducing the cost and complexity of embracing Gaia-X labelling, especially for existing, already certified, services. Assessment Processes defined by Gaia-X itself will also be based on a federation of responsibilities.

3.3.3 Further design principles

The modularity concept requires Gaia-X labelling criteria to describe rather high-level objectives as the detailed requirements are further described in the corresponding standards that are acknowledged. As of today, Gaia-X Labels are issued to a specific Service Offering unless stated otherwise.

3.4 Extendibility of Gaia-X Compliance

Gaia-X Compliance applies to all Gaia-X Service Offerings. And there shall be a Gaia-X Credential for all the entities defined as part of the Gaia-X Conceptual model:

- Participant including Consumer and Provider
- Service Offering
- Resource

The Gaia-X Compliance scheme can be extended by an ecosystem as detailed in the Gaia-X Architecture Document.

3.5 Period of Validity

The targeted updating period of the document is eighteen (18) months. Exceptionally, in case of changes that have become appropriate under applicable laws or standards impacting this document or the Gaia-X Compliance requirements, an update can be made earlier subject to a decision by the Gaia-X Board of Directors.

Upon revisions of the Gaia-X Compliance document, the participants will have the choice of adapting their compliance to the revised requirements or remaining qualified under the former requirements, for a maximum duration of twelve (12) months from the entry into force of the revised Gaia-X Compliance requirements. Exceptionally, in case of changes that have become appropriate under applicable laws or standards impacting the Gaia-X Compliance document, the Gaia-X Board of Directors can determine a grace period that deviates from the maximum twelve (12) months term, when relevant in view of the applicability of the changes of the applicable laws or standards.

III. Compliance Rules

4 Gaia-X Compliance Criteria for Participants

A Gaia-X Participant is a legal or natural person that participate to the Gaia-X ecosytem (consumer, producer, federator, operator, intermediary) and who fullfills conformity level defined in this document and verified by the Gaia-X Participant credential.

4.1 Criteria

Criterion PA1.1: The participant shall agree on GAIA-X Terms and Condition and provide informations detailed in the GAIA-X Ontology. Each participant shall provide an Issuer Verifiable Credential containing the checksum of the Gaia-X terms and conditions as described in the GAIA-X Ontology.
The keypair used to sign Gaia-X Credentials will be revoked where the Gaia-X European Association for Data and Cloud AISBL becomes aware of any inaccurate statements in regards to the claims which result in a non-compliance with the Compliance Document. A Gaia-X participant is compliant if the participant or its power of attorney, provide all mandatory attributes detailed in the Gaia-X Ontology.

Standard Compliance: declaration

Declaration: Using the Gaia-X Ontology, the declaration shall detail the applicable governing laws for the legally binding act, by indicating the ISO 3166-2 code of the respective country.

5 Gaia-X Compliance Criteria for Cloud Services

Note

We use the term 'Provider' throughout this section as the short denominator for a cloud Service Provider or CSP, i.e., the participant who provides cloud Service Offerings in the Gaia-X ecosystem. We use the term 'Customer' in this section to denominate the cloud service Customer, i.e., the participant who consumes a Service Offering from a cloud Service Provider.

Note

We use the term 'Customer Data' throughout this section for all customer provided or generated data, both personal and non-personal data, as processed by a Provider. This is not about the *data-about-the-Customer*, which the Provider needs to administer the service offering, to deploy, meter and bill the service to the Customer. Such *data-about-the-Customer* or *know-my-customer-data* need to be handled according to applicable legislation by the Provider and this falls outside the scope of this document. Please note that additional contractual arrangements, inclusions or exclusions, can be made regarding specific types of data in the scope of a service agreement.

Note

Whereas certain rules have originated from personal data privacy legislation, and other rules are suggested in a non-personal context, in practice, it is in most cases impossible for a Provider to differentiate between these data types. The Provider does not, and in many cases ought not even know which type of data is stored or processed with its services. Still, we have explicitly indicated which rules apply to personal data, where relevant.

Note

The compliance criteria are listed using a hierarchical numbering system, prefixed by a "P" to indicate Provider targeted criteria. The hierarchical numbering allows to assign stable numbers to criteria, also when future additions or deletions are made.

Criteria extract in JSON

A machine readable version of the criteria in JSON is available here. Download JSON

5.1 Nomenclature and Versioning of Referenced Standards

Identified / Term in this Document	Short Description (where necessary)	Version Reference & Access (might be behind a paywall)
SecNumCloud	French Cloud Service Requirements maintained by the Agence nationale de la sécurité des systèmes d'information (ANSSI); further information available at the project's website.	SecNumCloud 3.2.a, as of March, 8th 2022
BSI C5	The C5 (Cloud Computing Compliance Criteria Catalogue) criteria catalogue specifies minimum requirements for secure cloud computing and is primarily intended for professional cloud providers, their auditors and customers. It is published by the German Federal Office for Information Security.	BSI C5:2020
ISO/IEC 27001		ISO/IEC 27001:2022
CISPE (GDPR, Infrastructure & IaaS)	Approved GDPR Code Of Conduct maintained by CISPE, covering Infrastructure and IaaS Cloud Services; further information available at the project's website.	February 9th, 2021
EU Cloud CoC (GDPR, XAAS)	Approved GDPR Code of Conduct maintained by the EU Cloud CoC General Assembly, covering the full cloud stack (XAAS); further information available at the project's website.	EU Cloud CoC v2.11 as of December 2020
SWIPO	SWIPO (Switching Cloud Providers and Porting Data), is a multi-stakeholder group facilitated by the European Commission, in order to develop voluntary Codes of Conduct for the proper application of the EU Free Flow of Non-Personal Data Regulation / Article 6 "Porting of Data". There are two Codes of Conduct available, each independently referred to in this document as "SWIPO IaaS" and "SWIPO SaaS".	SWIPO IaaS: v3.0; SWIPO SaaS:Version 2020 dating 08-07-2020
TISAX	the TISAX® testing and exchange mechanism was founded on the German Association of the Automotive Industry (VDA) catalogue of ISA (Information Security Assessment) requirements, largely established on the basis of the international ISO/IEC 27001 standard. The platform provides members throughout the value chain standardized assessment of their information security status to be shared with partners working in the automotive industry.	TISAX 2017 (Revised Points of Focus 2022)
CSA CCM	CSA Cloud Control Matrix	CSA Cloud Control Matrix v.4

5.2 Assessment procedures

The Gaia-X Standard Compliance and Gaia-X Label are always issued by accredited Gaia-X Compliance services. The Gaia-X Digital Clearing House operates instances of the Gaia-X Compliance service.

Depending on the type of attestation, declaration or certification, different claims and evidences are required.

For declaration, the technical validation of the claims and the evidences is performed by the Gaia-X Compliance service. The claim and evidences are described using the Gaia-X ontology which is available via the Gaia-X Registry services. The Gaia-X Digital Clearing House operates instances of the Gaia-X Registry service.

Gaia-X ontology

An “ontology is a formal, explicit specification of a shared conceptualisation”. (Gruber,1993)

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.

To ensure that an evidence can be verified, a reference to an external document includes a hash value of that document, for future content integrity verification.

Whenever external content is referenced, that content shall be integrity protected using a suitable secure message digest algorithm (e.g. cryptographic hash like SHA512) and the message digest shall be included. The inclusion of the message digest allows to verify the content against the claim at any later time when that referenced content is made available to a verifier (customer or third party e.g. a third party involved in a dispute resolution), including in cases where information contained in such referenced content cannot be made available to the public (e.g. only to customers during or after a contract between the provider and the customer is made).

For certification, the technical or manual verification of the claims and the evidences is performed by external impartial CAB and the Gaia-X Compliance engine verifies the eligibility of the CAB to issue specific certifications based on the ‘Permissible Standards’ information of each criteria.

Validation vs Verification

Based on the ISO/IEC 17000:2020 terms:

- validation: confirmation of plausibility for a specific intended use or application (ISO/IEC 17000:2020)
- verification: confirmation of truthfulness through the provision of objective evidence (ISO/IEC 17000:2020)

5.3 Contractual framework

This section reflects provisions associated with the contractual framework between a ‘Provider’ and a ‘Customer’, required for any Service Offering regardless of its type, purpose, or processed categories of data. It is divided into requirements related to the governance of contract and material aspects that shall be addressed in contracts. This section and subordinate criteria shall not provide exact and exhaustive contractual language. It shall rather allow providers to reflect the requirements subject to their individual needs of structure and language.

Additionally, it is not expected that individual contracts will be subject to an evaluation process by Gaia-X. Gaia-X will rather focus on evaluating a process, reflected by documented internal policies or procedures, that safeguard conformity with the requirements laid out in this section.

Note

To the extent GDPR standards are mapped as permissible standards in this section, i.e., Contractual Governance and General Material Requirements and Transparency: By their very nature, GDPR standards address the processing of personal data. As theoretically implemented technical and organisational measures may differ to the extent personal or non-personal data are affected, this is considered a limited practical concern. Against this background, GDPR standards were mapped as permissible standards accordingly. Consequently, Customers are invited to evaluate if they need any additional assurances.

5.3.1 Contractual governance

Criterion P1.1.1: The Provider shall offer the ability to establish a legally binding act. This legally binding act shall be documented.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, the declaration shall contain either a resolvable identifier pointing to the legally binding act offered by the Provider or a contact form to request more information.

Permissible Standards:

- SecNumCloud: 19.1
- BSI C5: BC-01, OIS-03
- CISPE (GDPR, Infrastructure & IaaS): 4.2
- EU Cloud CoC (GDPR, XaaS): 5.1.A, 5.1.B
- CSA CCM: STA-09
- SWIPO IaaS: FR1, FR2

Example Standards:N/A

Note

The Provider needs to ensure a process that guarantees that a legally binding act is in place before delivering any form of service.

Note

The legally binding act can be a contract.

> **Note**
>
> Documented can be by any means, provided that both parties have the same access to such documentation, including the possibility to technically copy and share such documentation without hindrance. The possibility to technically copy and share without hindrance does not prevent the parties to agree upon any NDA or other means, that might provide for reasonable legal limitations.

Criterion P1.1.2: The Provider shall have an option for each legally binding act to be governed by EU/EEA/Member State law.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, the declaration shall contain the list of ISO 3166-2 codes indicating the EU/EEA/Member States whose law may be applied as governing law for the legally binding act.

Permissible Standards:

- SecNumCloud: 19.1.c
- CISPE (GDPR, Infrastructure & IaaS): 4.2
- EU Cloud CoC (GDPR, XaaS): 5.1.A, 5.1.B, 5.1.C, 5.1.F, 5.4.F

Example Standards:

- BSI C5: BC-01
- CSA CCM: STA-09
- SWIPO IaaS: FR1, FR2

Criterion P1.1.3: The Provider shall clearly identify for which parties the legal act is binding.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: The declaration shall include at least one of the following:

1. Detailed description of the parties using the Gaia-X Ontology.
2. Use of legally relevant or legally binding cryptographic certificates from the Gaia-X Registry (note: this is not applicable in case of manual signature).

Permissible Standards:

- SecNumCloud: 19.1.b
- EU Cloud CoC (GDPR, XaaS): 5.1.C, 5.1.F, 5.1.H

Example Standards:

- BSI C5: BC-01, OIS-03
- CISPE (GDPR, Infrastructure & IaaS): 4.2
- CSA CCM STA-09
- SWIPO IaaS: FR1, FR2

Criterion P1.1.4: The Provider shall ensure that the legally binding act covers the entire provision of the Service Offering.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Detailed description of the service, its components and dependencies using the Gaia-X Ontology.

Permissible Standards:

- SecNumCloud: 19.1, 19.4
- BSI C5: BC-01, BC-02, BC-04
- CISPE (GDPR, Infrastructure & IaaS): 4.2
- EU Cloud CoC (GDPR, XaaS): 5.1.C, 5.1.F, 5.1.H
- CSA CCM: STA-09

Example Standards:

- SWIPO IaaS: FR1, FR2

✓ Rationale

The provisions of the Service Offering may comprise several elements. Increased complexities of individual Service Offerings must not undermine the necessity of a documented legally binding act. To address practical needs, the legally binding act may comprise multiple separate documents, e.g., a master agreement and exhibits such as service level agreements or data protection agreements.

Criterion P1.1.5: The Provider shall clearly identify in each legally binding act the applicable governing law.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, the declaration shall detail the applicable governing laws for the legally binding act, by indicating the ISO 3166-2 code of the respective country.

Permissible Standards:N/A

Example Standards:N/A

Point Of Reference Standards:

- SecNumCloud 3.2.a – 19.1.c

5.3.2 General material requirements and transparency

Criterion P1.2.1: The Provider shall ensure there are specific provisions regarding service interruptions and business continuity (e.g., by means of a service level agreement), Provider's bankruptcy or any other reason by which the Provider may cease to exist in law.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, evidences about the provisions covering the criterion shall be provided, either copied from the legally binding document or in a structured machine-readable format (DSL). The evidence shall detail:

- the nature of the possible disruption (ISO 22301) events identified and the impacts (ISO 22301);
- the conditions for the event to occur;
- the measures which will be implemented to resume normal operation;
- compensation terms;
- the mitigation process to reduce the risks associated with the interruption of the service.

Permissible Standards:

- SecNumCloud: 17.1, 17.2, 19.1.j
- BSI C5: BCM-02, BCM-03
- CISPE (GDPR, Infrastructure & IaaS): 5.5
- CSA CCM: BCR-01, BCR-02, BCR-03

Example Standards:

- EU Cloud CoC (GDPR, XaaS): 6.2.Q
- ISO/IEC 27001: A.5.30, A.8.21
- SWIPO IaaS: DP08
- TISAX: 17.1

Criterion P1.2.2: The Provider shall ensure there are provisions governing the rights of the parties to use the service and any Customer Data therein.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, evidences about the provisions covering the criterion shall be provided, either copied from the legally binding document or in a structured machine-readable format (DSL). The Provider shall indicate the relevant provisions within its agreement. These provisions should consider the following elements:

- how to rectify, erase, restrict, access or port Customer Data and related costs;
- means for the Customer to retrieve and delete Customer Data;
- terms under which the Provider can process Customer Data, also with regard to sub-processors;
- termination of the contract/terms to make available data to the Customer and delete them after the termination of the contract;

Permissible Standards:

- SecNumCloud: 19.1.b, 19.1.d, 19.1.h, 19.1.k

- BSI C5: PI-02
- CISPE (GDPR, Infrastructure & IaaS): 4.7, 4.10, 5.7
- EU Cloud CoC (GDPR, XaaS): 5.1.F, 5.1.H, 5.7.A, 5.10.A, 5.10.B
- CSA CCM: IPY-01, IPY-04
- SWIPO IaaS: TR-04

Example Standards:N/A

Criterion P1.2.3: The Provider shall ensure there are provisions governing changes, regardless of their kind.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X ontology, evidences about the provisions covering the criterion shall be provided, either copied from the legally binding document or in a structured machine-readable format (DSL).
The evidence shall detail:

- issuing of the GaiaXTermsAndCondition verifiable credential. The Participant signing Gaia-X Credentials agrees as follows: “to update its Gaia-X Credentials about any changes, be it technical, organizational, or legal - especially but not limited to contractual in regard to the indicated attributes present in the Gaia-X Credentials.”.
- procedures for monitoring and managing changes to the information processing systems or on the technical and organizational security measures under the Provider’s responsibilities at the effective date of the legally binding agreement;
- procedures detailing how to communicate the following information to the Customer, in the event of operations carried out by the Provider and which may have an impact on the security or availability of the service: scheduled date and time of the start and end of operations, impacts on the security or availability of the service, contact within the provider;
- procedures to notify the Customer of any changes concerning an addition or a replacement of a subprocessor engaged by the Provider based on a general authorization by the Customer.
- criteria for risk assessment, categorisation and prioritisation of changes;
- procedures on how to inform the Customer about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements;
- requirements for the documentation of changes in system, operational and user documentation;
- provisions limiting changes directly impacting Customer’s owned environments/tenants to explicitly authorized requests within service level agreements between the Provider and the Consumer.

Permissible Standards:

- SecNumCloud: 12.2, 14.2a, 15.4.a
- BSI C5: BC-01, OIS-03, DEV-03
- CISPE (GDPR, Infrastructure & IaaS): 4.3
- EU Cloud CoC (GDPR, XaaS): 5.3.F, 6.2.K
- CSA CCM: CCC-01, CCC-05

Example Standards:

- ISO/IEC 27001: A.8.32
- SWIPO IaaS: TR-04
- TISAX: 5.2.1

Criterion P1.2.4: The Provider shall ensure there are provisions governing aspects regarding copyright or any other intellectual property rights.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL).

Permissible Standards:

- SecNumCloud: 7.2.c
- SWIPO IaaS: SCR02
- CISPE (GDPR, Infrastructure & IaaS): 4.8
- EU Cloud CoC (GDPR, XaaS): 5.1.F, 5.2.D, 5.12.A, 5.12.B, 5.12.C, 5.12.D, 5.12.F

Example Standards:

- BSI C5: HR-06
- CSA CCM: HRS-08, HRS-10
- ISO/IEC 27001: A.6.2, A.6.3, A.6.5
- TISAX: 8.2.1, 8.2.2, 8.2.3

Criterion P1.2.5: The Provider shall declare the general location of any processing of Customer Data, allowing the Customer to determine the applicable jurisdiction and to comply with Customer's requirements in the context of its business and operational context.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: The declaration shall include the following details:

1. resources and dependencies of the Service Offering, using the Gaia-X Ontology.
2. country and administrative area of physical resources.
3. management access location

Permissible Standards:

- CISPE (GDPR, Infrastructure & IaaS): 4.4
- CSA CCM: DSP-19

Example Standards:

- SecNumCloud: 19.1.b, 19.2.a
- BSI C5: BC-01
- EU Cloud CoC (GDPR, XaaS): 5.3.E, 5.3.G, 5.4.B

Note

- The general location is a geographical reference, such as a city or city region area.
- Business and operational context shall address elements such as business continuity, by e.g., safeguarding minimum distances between Customer's processing activities.

Criterion P1.2.6: The Provider shall explain how information about subcontractors and related Customer Data localization will be communicated.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL). The evidence shall detail:

- procedures and mechanisms to inform the Customer about the list of all subcontractors involved in the implementation of the Service and related locations where the Customer data is processed, stored and backed up.

Permissible Standards:

- SecNumCloud: 15.1, 15.2, 19.1.b, 19.2.a
- BSI C5: 3.4.4.1, BC-01
- CISPE (GDPR, Infrastructure & IaaS): 4.5
- EU Cloud CoC (GDPR, XaaS): 5.3.C, 5.3.E, 5.3.F, 5.3.G
- CSA CCM: DSP-19, STA-03, STA-09

Example Standards:

- ISO/IEC 27001: A.5.19, A.5.20
- TISAX: 6.1.1

Note

This applies to the subcontractors essential to the provision of the Service Offering, including any sub-processors.

Criterion P1.2.7: The Provider shall communicate to the Customer where the applicable jurisdiction(s) of subcontractors will be.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL). The evidence shall detail:

- Contractual terms to inform the Customer, including notification of any changes, about the jurisdiction(s) of subcontractors applicable to the processing of Customer Data, by providing information on the general location of subcontractors (such as a country or regional area).

Permissible Standards:

- CISPE (GDPR, Infrastructure & IaaS): 4.5
- EU Cloud CoC (GDPR, XaaS): 5.3.A, 5.3.E, 5.3.F, 5.3.G

Example Standards:

- SecNumCloud: 15.1, 15.2, 19.1.b, 19.2.a
- BSI C5: 3.4.4.1, BC-01
- CSA CCM: DSP-19, STA-03, STA-09
- ISO/IEC 27001: A.5.19, A.5.20
- TISAX: 6.1.1

> **Note**
>
> This applies to the subcontractors essential for the provision of the Service Offering, including any sub-processors.

Criterion P1.2.8: The Provider shall include in the contract the contact details where Customer may address any queries regarding the Service Offering and the contract.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, evidences covering the criterion shall be provided, either copied from the legally binding document or in a structured machine-readable format (DSL). The evidence shall detail:

- Communications channels or standardised interactive interfaces or Customer Portals available to the Customer to enable cooperation between the Provider and the Customer;
- Contact details available to the Customer to assist him in fulfilling data subject rights requests, including data subject access requests;
- Contact details to enable individual support to the Customer for any questions or requests it may have regarding the data protection measures covered by the Service Agreement;
- Contact data of the Data Protection Officer (as required under the GDPR) or Data Protection Point of Contact.

Permissible Standards:

- EU Cloud CoC (GDPR, XaaS): 5.7, 5.9.A, 5.9.B

Example Standards:

- SecNumCloud: 19.1.b
- BSI C5: BC-02, OIS-03
- CISPE (GDPR, Infrastructure & IaaS): 4.3, 4.6

> **Note**
>
> Queries include requests during the pre-contractual state, before coming to an agreement.

> **Note**
>
> As it is generally foreseen that Lvl2 and Lvl3 will require third-party attestations, for this requirement shall apply the following: For the time being, there exists only one Permissible Standard. Until more Permissible Standards will be identified to this Criterion, Lvl2 and Lvl3 shall only require a declaration.

Criterion P1.2.9: The Provider shall declare the mandatory service and resource attributes in the self-description of each Service Offering.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: The Service Offering credential shall contain the mandatory attributes for services and resources, as they are defined in this document.

Permissible Standards:N/A

Example Standards:N/A

> **Note**
>
> The list of the mandatory attributes to be provided in Gaia-X Credentials to describe Services and Resources is reported in Chapter Services and Resources - Mandatory attributes, while the recommended optional attributes are reported in the Gaia-X Registry.

5.3.3 Technical compliance requirements

Criterion P1.3.1: The Provider shall describe the Permissions, Requirements and Constraints of the Service Offering using a common Domain-Specific Language (DSL) in the self-description.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	declaration	declaration	declaration

Declaration: for Service Offerings and resources, the declaration shall include information on the policies describing Permissions, Requirements and Constraints using a common Domain-Specific Language (DSL).

Permissible Standards:N/A

Example Standards:N/A

Criterion P1.3.2: The Provider shall ensure that the Service Offering is operated by a Gaia-X participant defined by a verified credential.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Using the Gaia-X Ontology, the declaration shall include the following elements:

- Unique registered business identifier identifying the Service Offering Provider. For this purpose, legally relevant or legally binding cryptographic certificates from the Gaia-X Registry shall be used.
- Physical location of the headquarters in ISO 3166-2 format.
- Physical location of legal registration in ISO 3166-2 format.

Permissible Standards:N/A

Example Standards:N/A

Criterion P1.3.3: Not in use

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	N/A	N/A	N/A

Declaration: N/A

Permissible Standards:N/A

Example Standards:N/A

Criterion P1.3.4: Not in use

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	N/A	N/A	N/A

Declaration: N/A

Permissible Standards:N/A

Example Standards:N/A

Criterion P1.3.5: Not in use

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	N/A	N/A	N/A

Declaration: N/A

Permissible Standards:N/A

Example Standards:N/A

5.4 Data Protection

This section only applies in the case of processing personal Customer Data. It reflects GDPR requirements without extending GDPR's obligations, and it cites some of these requirements as they are judged to be explicitly relevant. By principle, this section shall only apply to personal data that are processed and are subject to the commercial relationship between the Customer and the Provider (we call them *'personal Customer Data'*), but not those personal data that are processed by the Provider to establish and maintain such commercial relationship for its own purposes, e.g., contract handling and invoicing. Provided a service offering will not process any personal data in this sense, the requirements as laid down in this section shall not apply.

Note

In this section, Permissible Standards are limited to standards, which have officially passed the Data Protection Supervisory Authorities' approval process. Saying, Permissible Standards must meet the Gaia-X criterion and meet the legal requirements of claiming to be a GDPR standard. Other standards, which might also address the Gaia-X criterion entirely, are listed as Example Standards. Where the Example Standard might address a Gaia-X criterion in its entirety, a (*) has been added. Otherwise, Example Standards remain aligned with the common methodology of this document.

5.4.1 General

Criterion P2.1.1: The Provider shall offer the ability to establish a contract under Union or EU/EEA/Member State law and specifically addressing GDPR requirements.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	declaration	certification	certification

Declaration: The declaration shall include:

1. The list of ISO 3166-2 codes indicating the EU/EEA/Member States whose law may be applied as governing law for the legally binding act.
2. Evidences about the provisions covering the criterion, either by providing a resolvable identifier pointing to the Service agreement offered by the Provider addressing the relevant provision or in a structured machine-readable format (DSL).

Permissible Standards:

- SecNumCloud: 18.1.a, 19.1
- CISPE (GDPR, Infrastructure & IaaS): 4.2
- EU Cloud CoC (GDPR, XaaS): 5.1.A, 5.1.C
- In cases of a Code of Conduct (Art. 40 GDPR): assessment by an accredited monitoring body for the respective Code of Conduct, Art. 41 GDPR. Assessment process as defined by the respective Code of Conduct / accredited monitoring body.
- In case of a Certification (Art. 42 GDPR): assessment by an accredited Certification Body for the respective Certification (Art. 43 GDPR). Assessment process as defined by the respective Certification / accredited certification body.

Example Standards:

- SecNumCloud: 18.1.a, 19.1(*)

Note

GDPR requires EU/EEA or Member State law to be applicable. The Provider needs to ensure a process that guarantees that a legally binding act is in place before delivering any form of service.

Note

The GDPR requires suitable documentation, whilst clarifying, e.g., in Art. 28 (9) GDPR, that such documentation shall be in writing, including electronic form.

Criterion P2.1.2: The Provider shall define the roles and responsibilities of each party.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X ontology, evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL), shall be provided. The evidence shall detail:

- roles and related responsibilities of the Provider and the Customer for the protection of personal data;
- responsibilities of the Provider and the Customer with respect to security measures.

Permissible Standards:

- SecNumCloud: 6.1.e, 19.1
- CISPE (GDPR, Infrastructure & IaaS): 4.3, 5.1
- EU Cloud CoC (GDPR, XaaS): 5.1.C
- In case of a Code of Conduct (Art. 40 GDPR): assessment by an accredited monitoring body for the respective Code of Conduct, Art. 41 GDPR. Assessment process as defined by the respective Code of Conduct / accredited monitoring body.
- In case of a Certification (Art. 42 GDPR): assessment by an accredited Certification Body for the respective Certification (Art. 43 GDPR). Assessment process as defined by the respective Certification / accredited certification body.

Example Standards:

- SecNumCloud: 6.1.e, 19.1 (*)

Criterion P2.1.3: The Provider shall clearly define the technical and organizational measures in accordance with the roles and responsibilities of the parties, including an adequate level of detail.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from the legally binding document/other legally relevant documents or in a structured machine-readable format (DSL). The evidence shall detail:

- a reference to the documentation of the Provider detailing its implemented technical and organisation measures. Such measures should refer to elements such as:
- available documentation and mechanisms to implement a Security Management System, including an internal security organisation;
- documentation regarding a risk assessment covering the scope of the Service;
- technical and organizational measures to ensure a level of security appropriate to the risk;
- technical and organisational measures implemented and maintained for the Provider's data center facilities, servers, networking equipment and host software systems that are within the Provider's control and are used to provide the Service;
- provisions to ensure transparency between the Provider and the Customer regarding their security responsibilities.

Permissible Standards:

- SecNumCloud: 5 to 17
- BSI C5: All Basic Criteria
- CISPE (GDPR, Infrastructure & IaaS): 4.3
- EU Cloud CoC (GDPR, XaaS): Entire Section 6
- In cases of a Code of Conduct (Art. 40 GDPR): assessment by an accredited monitoring body for the respective Code of Conduct, Art. 41 GDPR. Assessment process as defined by the respective Code of Conduct / accredited monitoring body.
- In case of a Certification (Art. 42 GDPR): assessment by an accredited Certification Body for the respective Certification (Art. 43 GDPR). Assessment process as defined by the respective Certification / accredited certification body.

Example Standards:

- SecNumCloud: 5 to 17 (*)
- BSI C5: All Basic Criteria (*)
- CSA CCM: All controls except Domain 'Universal Endpoint Management' (*)
- ISO/IEC 27001: Entire Annex A (*)
- TISAX: All Information Security Requirements (*)

5.4.2 GDPR Art. 28

Criterion P2.2.1: The Provider shall be ultimately bound to instructions of the Customer.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL), shall be provided.
The evidence shall detail:

- The terms under which the Provider shall process Customer Personal Data on behalf of the Customer;
- The scope of Customer's Instructions for the processing of Customer Personal Data;
- The parameters of the Service Offering description within which the Customer can give instructions to the Provider in relation to the processing of personal data.

Permissible Standards:

- CISPE (GDPR, Infrastructure & IaaS): 4.1
- EU Cloud CoC (GDPR, XaaS): 5.1.F, 5.2.D
- In cases of a Code of Conduct (Art. 40 GDPR): assessment by an accredited monitoring body for the respective Code of Conduct, Art. 41 GDPR. Assessment process as defined by the respective Code of Conduct / accredited monitoring body.
- In case of a Certification (Art. 42 GDPR): assessment by an accredited Certification Body for the respective Certification (Art. 43 GDPR). Assessment process as defined by the respective Certification / accredited certification body.

Example Standards:N/A

Criterion P2.2.2: The Provider shall clearly define how Customer may instruct, including by electronic means such as configuration tools or APIs.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X ontology, evidences about the provisions covering the criterion, either copied from the legally binding document or additional manuals or in a structured machine-readable format (DSL), shall be provided. The evidence shall detail:

- format of acceptable Instructions from the Customer to the CSP;
- confirmation of Customer interactions and verification;
- records of completion and actions taken.

Permissible Standards:

- CISPE (GDPR, Infrastructure & IaaS): 4.2
- EU Cloud CoC (GDPR, XaaS): 5.2.A, 5.2.B, 5.2.C
- In cases of a Code of Conduct (Art. 40 GDPR): assessment by accredited monitoring body for the respective Code of Conduct, Art. 41 GDPR. Assessment process as defined by the respective Code of Conduct / accredited monitoring body.
- In case of a Certification (Art. 42 GDPR): assessment by an accredited Certification Body for the respective Certification (Art. 43 GDPR). Assessment process as defined by the respective Certification / accredited certification body.

Example Standards:N/A

Criterion P2.2.3: The Provider shall clearly define if and to which extent third country transfer will take place.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	N/A

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL).

Permissible Standards:

- CISPE (GDPR, Infrastructure & IaaS): 4.4
- EU Cloud CoC (GDPR, XaaS): 5.4.A, 5.4.C, 5.4.E
- In cases of a Code of Conduct (Art. 40 GDPR): assessment by an accredited monitoring body for the respective Code of Conduct, Art. 41 GDPR. Assessment process as defined by the respective Code of Conduct / accredited monitoring body.
- In case of a Certification (Art. 42 GDPR): assessment by an accredited Certification Body for the respective Certification (Art. 43 GDPR). Assessment process as defined by the respective Certification / accredited certification body.

Example Standards:

- CSA CCM: DSP-10, DSP-19 (*)
- SecNumCloud: 5.3.e, 19.1.e
- BSI C5: BC-01
- ISO/IEC 27001: A.5.34

Criterion P2.2.4: The Provider shall clearly define if and to the extent third country transfers will take place, and by which means of Chapter V GDPR these transfers will be protected.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	declaration	certification	N/A

Declaration: Using the Gaia-X Ontology, evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL), shall be provided. The evidence shall detail:

- information regarding the country/countries where the data is stored and processed by or on behalf of the Provider;
- specific safeguards under Chapter V GDPR that the Provider plans to apply in case of third-country transfers and procedures to ensure that no transfer of Customer Personal Data takes place without appropriate safeguards in place;

Permissible Standards:

- CISPE (GDPR, Infrastructure & IaaS): 4.4
- EU Cloud CoC (GDPR, XaaS): 5.4.A, 5.4.C, 5.4.E
- In cases of a Code of Conduct (Art. 40 GDPR): assessment by an accredited monitoring body for the respective Code of Conduct, Art. 41 GDPR. Assessment process as defined by the respective Code of Conduct / accredited monitoring body.
- In case of a Certification (Art. 42 GDPR): accredited Certification Body for the respective Certification (Art. 43 GDPR). Assessment process as defined by the respective Certification / accredited certification body.

Example Standards:

- CSA CCM: DSP-10, DSP-19 (*)
- SecNumCloud: 5.3.e, 19.1.e
- BSI C5: BC-01
- ISO/IEC 27001: A.5.34

Criterion P2.2.5: The Provider shall clearly define if and to which extent sub-processors will be involved.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL), shall be provided. The evidence shall detail:

- Procedures and mechanisms in place to keep up-to-date and communicate to the Customer the list of existing sub-processors involved in the implementation of the service, including the information on the related jurisdictions applicable to the processing of Customer Personal Data and details about the specific contribution of sub-processors to the provision of the service and processing of personal/customer data.

Permissible Standards:

- SecNumCloud: 15.1
- CISPE (GDPR, Infrastructure & IaaS): 4.5
- EU Cloud CoC (GDPR, XaaS): 5.3.E, 5.3.F, 5.3.G
- In cases of a Code of Conduct (Art. 40 GDPR): assessment by an accredited monitoring body for the respective Code of Conduct, Art. 41 GDPR. Assessment process as defined by the respective Code of Conduct / accredited monitoring body.
- In case of a Certification (Art. 42 GDPR): accredited Certification Body for the respective Certification (Art. 43 GDPR). assessment process as defined by the respective Certification/accredited certification body.

Example Standards:

- CSA CCM: DSP-13 (*)
- TISAX: 9.2 (*)
- BSI C5: 3.4.4.1, BC-01
- ISO/IEC 27001: A.5.19

Criterion P2.2.6: The Provider shall clearly define if and to the extent sub-processors will be involved, and the measures that are in place regarding sub-processors management.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, copied from the legally binding document or other legally relevant documents or in a structured machine-readable format (DSL). The evidence shall detail:

- procedures and mechanisms in place to maintain and communicate to the Customer the list of sub-processors involved in the implementation of the service, including the information on the related jurisdictions applicable to the processing of Customer Personal Data and details about their specific contribution to the provision of the service and processing of personal/customer data;
- measures to impose on sub-processors the same or a higher level of data protection than the level ensured by the Provider;
- procedures to regularly monitor the security measures and changes implemented by the sub-processors.

Permissible Standards:

- SecNumCloud: 15.2, 15.3, 15.4, 15.5
- CISPE (GDPR, Infrastructure & IaaS): 4.5
- EU Cloud CoC (GDPR, XaaS): 5.3.C, 5.3.D
- In case of a Code of Conduct (Art. 40 GDPR): Accredited monitoring body for the respective Code of Conduct, Art. 41 GDPR. Assessment process as defined by the respective Code of Conduct / accredited monitoring body.
- In case of a Certification (Art. 43 GDPR): Accredited Certification Body for the respective Certification (Art. 43 GDPR). Assessment process as defined by the respective Certification/accredited certification body.

Example Standards:

- SecNumCloud: 15.2, 15.3, 15.4, 15.5 (*)
- CSA CCM: DSP-13, DSP-14, DSP-17, STA-01, STA-09, STA-12, STA-13, STA-14
- BSI C5: 3.4.4.1, SSO-01, SSO-02, SSO-03, SSO-04, SSO-05
- ISO/IEC 27001: A.5.19, A.5.20, A.5.34
- TISAX: 6.1.1

Criterion P2.2.7: The Provider shall define the audit rights for the Customer.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL). The evidence shall detail the procedures regarding the audits that the Customer may request to verify the adequacy of the security and data protection controls that apply to the Service Offering, by addressing the following topics:

- how the Provider will contribute to such activity;

- what auditors can be selected by the Customer;
- controls determined by the Provider to avoid risks for other customers/interruption of business operations;
- terms to be accepted by the Customer to protect Provider's confidential information;
- obligations related to the payment of the audit activity.

Permissible Standards:

- SecNumCloud: 19.1.q
- CISPE (GDPR, Infrastructure & IaaS): 4.6
- EU Cloud CoC (GDPR, XaaS): 5.5.C, 5.5.D, 5.5.F
- In case of a Code of Conduct (Art. 40 GDPR): Accredited monitoring body for the respective Code of Conduct, Art. 41 GDPR. Assessment process as defined by the respective Code of Conduct / accredited monitoring body.
- In case of a Certification (Art. 43 GDPR): Accredited Certification Body for the respective Certification (Art. 43 GDPR). Assessment process as defined by the respective Certification/accredited certification body.

Example Standards:

- SecNumCloud: 19.1.q (*)
- BSI C5: COM-02

5.5 Cybersecurity

Safeguarding the appropriate security of service offerings and processed elements is a key and state-of-art principle. Therefore, this section applies to any service offering, regardless of its Provider, type, purpose, or processed category of data. It is acknowledged that implementing cybersecurity-related measures may apply in most cases to the Provider's organisation, rather than the explicit service offering. However, theoretically, measures may deviate between different service offerings. Thus, where measures will be implemented at an organisation-wide level, their inheritance shall suffice for this section. Where measures will be implemented on a per-service offering level, individual evaluation per service offering will be required.

For all the security requirements, the criteria follow as much as possible the current discussions on the European Cloud Scheme (EUCS). When the EUCS is finalised, Gaia-X will adapt these criteria accordingly. Therefore, the terms on the different criteria on this item should be read in the light of EUCS.

Criterion P3.1.1: Organization of information security: Plan, implement, maintain and continuously improve the information security framework within the organisation.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidence about the provisions covering the criterion, either copied from the Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail:

- availability of a service information security policy, approved by the Provider's management;
- procedures to perform a risk assessment covering the entire scope of the service.

Permissible Standards:

- SecNumCloud: 5.2.a, 5.2.b, 5.2.c, 5.2.d, 5.2.e, 5.3.a
- BSI C5: OIS-01, OIS-02, COM-04
- EU Cloud CoC (GDPR, XaaS): 6.1.C
- CSA CCM: GRC-01, GRC-03, GRC-05, GRC-06
- ISO/IEC 27001: Annex A 5.1, Annex A 5.2, Annex 5.4
- TISAX: 1.2.1, 1.2.2, 1.5.2

Example Standards:

- CISPE (GDPR, Infrastructure & IaaS): 4.3
- CSA CCM: GRC-01, GRC-03, GRC-05, GRC-06
- ISO/IEC 27001: Annex A 5.1, Annex A 5.2, Annex 5.4
- TISAX: 1.2.1, 1.2.2, 1.5.2

⚠ Label L2

Onsite assessment following assessment process according to the respective standards.

⚠ Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.2: Information Security Policies: Provide a global information security policy, derived into policies and procedures regarding security requirements and to support business requirements

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidence about the provisions covering the criterion, either copied from the Provider's documentation or in a structured machine-readable format (DSL).
The evidence shall detail:

- availability of a global information security policy;
- availability of policies and instructions derived from the information security policy ;
- procedures to perform at least annually a review of information security policies and instructions.

Permissible Standards:

- SecNumCloud: 5.2
- BSI C5: SP-01, SP-02, OIS-02
- CISPE (GDPR, Infrastructure & IaaS): 4.3
- EU Cloud CoC (GDPR, XaaS): 6.2.A
- ISO/IEC 27001: Annex A 5.1

Example Standards:

- CSA CCM: GRC-01, GRC-03, GRC-05
- TISAX: 1.4.1

⚠ Label L2

Onsite assessment following assessment process according to the respective standards.

⚠ Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.3: Risk Management: Ensure that risks related to information security are properly identified, assessed, and treated, and that the residual risk is acceptable to the CSP.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidence about the provisions covering the criterion, either copied from the Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail :

- availability of policies and instructions for risk management procedures
- procedure to review at least annually the risk assessment;
- acceptance by the management of the Provider of the residual risks identified in the risk assessment;

Permissible Standards:

- SecNumCloud: 5.3.G, 5.3.H
- BSI C5: OIS-06, OIS-07
- CISPE (GDPR, Infrastructure & IaaS): 5.4
- EU Cloud CoC (GDPR, XaaS): 6.1.C
- CSA CCM: GRC-02
- ISO/IEC 27001: 6.1.2, 6.1.3, 8.2

Example Standards:

- TISAX: 1.4.1

⚠ Label L2

Onsite assessment following assessment process according to the respective standards.

⚠ Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.4: Human Resources: Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from Provider's documentation or in a structured machine-readable format (DSL).
The evidence shall detail :

- employment Terms&Conditions requiring compliance with applicable policies and instruction related to information security
- procedures to inform internal and external employees about which responsibilities will remain in place when their employment is terminated or changed and for how long;
- provisions to ensure and document that internal and external employees are committed to the policies and instructions for acceptable use and safe handling of assets and that assets handed over are returned upon termination of employment;
- policies for managing user accounts and access rights for internal and external employees;
- procedures to ensure that access rights are promptly revoked if the job responsibilities of the Provider's internal or external staff change.

Permissible Standards:

- BSI C5: HR-02, HR_03, HR-04, HR-05, HR-06, AM-05, IDM-01, IDM-04
- EU Cloud CoC (GDPR, XaaS): 6.2.C
- SecNumCloud: 7.2, 7.3, 7.4, 7.5
- CISPE (GDPR, Infrastructure & IaaS): 4.3
- ISO/IEC 27001: Annex A 5.2, Annex A 5.11, Annex A 6.2, Annex A 6.3, Annex A 6.6

Example Standards:

- CSA CCM: HRS-02, HRS-03, HRS-04, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, HRS-13
- TISAX: 2.1.1, 2.1.2

⚠ Label L2

Onsite assessment following assessment process according to the respective standards.

⚠ Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.5: Asset Management: Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidence about the provisions covering the criterion, either copied from the Provider's documentation or in a structured machine-readable format (DSL).
The evidence shall detail :

- Procedures for inventorying assets, where in the inventory for each software the information on its version and the equipment on which the software is installed is provided;
- procedures to ensure that software licenses are valid throughout the provision of the service ;
- policies and instructions for acceptable use, safe handling and return of assets;
- processes for hardware commissioning and decommissioning.

Permissible Standards:

- SecNumCloud: 8.1, 8.2, 8.3, 8.4, 8.5, 11.8
- BSI C5: AM-01, AM-02, AM-03, AM-04, AM-05, AM-06
- EU Cloud CoC (GDPR, XaaS): 6.2.D, 6.2.E
- CSA CCM: DCS-01, DCS-02, DCS-04, DCS-05, DCS-06, CCC-01, CCC-04, CCC-06, HRS-05, CEK-04
- ISO/IEC 27001: Annex A 5.9, Annex A 5.12, Annex A 5.15, Annex A 8.3
- TISAX:1.3.1, 1.3.2

Example Standards:N/A

⚠ Label L2

Onsite assessment following assessment process according to the respective standards.

⚠ Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.6: Physical Security: Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from Provider's documentation or in a structured machine-readable format (DSL).
The evidence shall detail:

- security perimeters implemented, with a distinction between different zones and related means of limitation and access control according to the profiles of the stakeholders;
- measures to keep a record of the identity of the visitors;
- measures to prevent and limit the risk of fire departure and spread, water damage, power supply outage and air conditioning failures;
- measures to protect electrical and telecommunications wiring from physical damage and interception;
- means to provide operational redundancy;
- structural, technical and organisational measures to protect the premises and buildings used for the provision of the service.

Permissible Standards:

- SecNumCloud: 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 11.10
- BSI C5: PS-01, PS-02, PS-03, PS-05, OS-07, PS-07
- CISPE (GDPR, Infrastructure & IaaS): 4.3
- EU Cloud CoC (GDPR, XaaS): 6.2.J
- CSA CCM: DCS-07, DCS-09, DCS-10, DCS-12, DCS-13, DCS-14, DCS-15, LOG-12
- ISO/IEC 27001: Annex A 7.1, Annex A 7.2, Annex A 7.3, Annex A 7.4, Annex A 7.5, Annex A 7.6, Annex A 7.7, Annex A 7.8, Annex A 7.9, Annex A 7.10, Annex A 711, Annex A 7.12, Annex A 7.13, Annex A 7.14

Example Standards:

- TISAX: 3.1.1

⚠ Label L2

Onsite assessment following assessment process according to the respective standards.

⚠ Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.7: Operational Security: Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidence about the provisions covering the criterion, either copied from the Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail :

- procedures and technical and organisational safeguards for the monitoring and provisioning and de-provisioning of cloud services;
- policies and instructions with specifications for protection against malware, detailing system-specific protection mechanisms;
- policies and instructions that govern the logging and monitoring of events on system components within the area of responsibility of the Provider and related implementation procedures;
- guidelines and instructions with technical and organisational measures to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the service;
- procedure for controlling the installation of software on the equipment of the service information system.

Permissible Standards:

- BSI C5: OPS-01, OPS-02, OPS-03, OPS-04,OPS-05, OPS-10, OPS-11, OPS-12, OPS-13, OPS-14, OPS-15, OPS-16, OPS-17, OPS-18, OPS-19, OPS-20, OPS-22, OPS-23
- EU Cloud CoC (GDPR, XaaS): 6.2.K
- CSA CCM: IVS-02, IVS-03, IVS-09, LOG-01, LOG-03, LOG-05, LOG-07, LOG-08, LOG-13, SEF-01, SEF-02, SEF-05, SEF-07, TVM-01, TVM-02, TVM-07, UEM-09, UEM-10
- ISO/IEC 27001: Annex A 8.6, Annex A 8.7, Annex A 8.8, Annex 8.9, Annex A 8.15, Annex A 8.16
- SecNumCloud: 6.1.a, 12.1, 12.4, 12.6, 12.7, 12.9, 12.10, 12.11, 16.1, 16.3.a, 17.4.a
- CISPE (GDPR, Infrastructure & IaaS): 4.3

Example Standards:

- TISAX: 5.2.3, 5.2.4, 5.2.5

Label L2

Onsite assessment following assessment process according to the respective standards.

Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.8: Identity, Authentication and access control management: Limit access to information and information processing facilities.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidence about the provisions covering the criterion, either copied from the Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail:

- access control policies and measures, restricting physical access to information processing facilities and technical access to host software and networks to authorised personnel;
- mechanisms for monitoring and detecting unauthorised access to sensitive areas;
- procedures to ensure the allocation, modification, review and removal of access rights to resources from the service's information system;
- mechanisms to implement silos between the customers;
- partitioning measures between the service's information system and other information systems of the Provider.

Permissible Standards:

- SecNumCloud: 9.1, 9.2, 93. 9.4, 9.7, 11.2
- BSI C5: PS-05, IDM-01, IDM-02, IDM-03, IDM-04, IDM-05, IDM-06, IDM-07
- CISPE (GDPR, Infrastructure & IaaS): 4.8
- EU Cloud CoC (GDPR, XaaS): 6.2.F
- CSA CCM: DCS-07, DCS-09, IAM-01, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11
- ISO/IEC 27001: Annex A 5.15, Annex A 5.16, Annex A 5.17, Annex A 5.18, Annex A 8.2, Annex A 8.3

Example Standards:

- TISAX: 4.1.1, 4.1.2, 4.1.3, 4.2.1

Label L2

Onsite assessment following assessment process according to the respective standards.

Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.9: Cryptography and Key management: Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, declaration of adherence to the following standards:

- use FIPS 186-5 and FIPS 180-4 for curves and hash methods
- use RFC9142 or updates for SSH
- use RFC5406 or updates for IPSec
- use RFC7296 or updates for IKEv2
- use RFC8446 or updates for TLS
- use RFC7515 or updated for JOSE

when storing or transferring information afferent to user information and data submitted or generated by the user when using the services.

Permissible Standards:

- SecNumCloud: 10.1, 10.2, 10.3, 10.4, 10.5, 10.6
- BSI C5: CRY-01, CRY-02, CRY-03, CRY-04
- EU Cloud CoC (GDPR, XaaS): 6.2.G, 6.2.Hm 6.2.I
- CSA CCM: CEK-01, CEK-02, CEK-03, CEK-04, CEK-05, CEK-06, CEK-07, CEK-08, CEK-09, CEK-10, CEK-11, CEK-12, CEK-13, CEK-14, CEK-15, CEK-16, CEK-17, CEK-18, * CEK-19, CEK-20, CEK-21

- ISO/IEC 27001: Annex A 8.24

Example Standards:

- TISAX: 5.1.1, 5.1.2

> ⚠ Label L2
>
> Onsite assessment following assessment process according to the respective standards.

> ⚠ Label L3
>
> Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.10: Communication Security: Ensure the protection of information in networks and the corresponding information processing systems.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X ontology, describe in the order of priority:

1. List of IXPs or Transit Providers, or Available Points of Presence (PoPs):
2. List of Datacenters Hosting Infrastructure Services:
3. List of Hardware Equipment Geographic Locations (On-Premises Server Location):

Permissible Standards:

- SecNumCloud: 13.1, 13.2, 13.3
- BSI C5: COS-01, COS-02, COS-03, COS-04, COS-05, COS-06, COS-07, COS-08
- EU Cloud CoC (GDPR, XaaS): 6.2.L
- CSA CCM: IPY-01, IPY-03, IVS-03, IVS-07
- ISO/IEC 27001: Annex A 8.9, Annex A 8.12, Annex A 8.20, Annex A 8.21, Annex A 8.22
- CISPE (GDPR, Infrastructure & IaaS): 4.3

Example Standards:

- TISAX: 5.1.2, 5.2.7

> ⚠ Label L2
>
> Onsite assessment following assessment process according to the respective standards (EUCS Substantial (CKM-03.2, CKM-03.3, CKM-04.2, CKM-04.4)).

> ⚠ Label L3
>
> Assessment process according to the process for EUCS Level High ; ad interim: see Label Level 2 (EUCS High(CKM-03.4, CKM-04.3)).

Criterion P3.1.11: Portability and Interoperability: The CSP shall provide a means by which a customer can obtain their stored customer data, and provide documentation on how (where appropriate, through documented API's) the CSC can obtain the stored data at the end of the contractual relationship and shall document how the data will be securely deleted from the Cloud Service Provider in what timeframe.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidence about the provisions covering the criterion, either copied from the Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail :

- list of methods to export data from the user's account out of the service,
- available protections and known restrictions and technical limitations related to available porting methods and formats;
- information on the means to request data retrieval;
- information on the period during which the Customer is entitled to transfer their data once the contractual relationship is terminated.

Permissible Standards:

- BSI C5: PI-01, PI_02, PI-03
- EU Cloud CoC (GDPR, XaaS): 5.2.A, 5.2.B, 5.2.C, 5.7.A, 5.7.B, 5.10.A, 5.10.B, 5.14.A, 5.14.B
- CSA CCM: IPY-01, IPY-02, IPY-03, IPY-04
- SWIPO IaaS: PR01, PR02, PR03, PR06, PR07, DP01, DP02, DP03, DP05, DP06, DP07, DP08, SCR01, TR02, PLR05
- SecNumCloud: 19.1, 19.4
- CISPE (GDPR, Infrastructure & IaaS): 4.7, 4.10, 5.7

Example Standards:N/A

Success

This objective should be understood in the context of cybersecurity. Further portability objectives are defined in criteria P4.1.1 and P4.1.2

Label L2

Onsite assessment following assessment process according to the respective standards.

Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.12: Change and Configuration Management: Ensure that changes and configuration actions to information systems guarantee the security of the delivered cloud service.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail:
- policies and instructions including technical and organisational safeguards for change management of system components of the service;
- procedures to submit changes to a risk assessment with regard to potential effects on the system components concerned;
- mechanisms to ensure logging of changes;
- procedures to submit changes to appropriate testing during software development and deployment;
- provisions limiting changes directly impacting Customer's owned environments/tenants;
- procedures for version control to track dependencies of changes and to restore affected system components.

Permissible Standards:

- BSI C5: DEV-03, DEV-05, DEV-06, DEV-07, DEV-08, DEV-09
- EU Cloud CoC (GDPR, XaaS): 6.2.M
- CSA CCM: CCC-01, CCC-02, CCC-04, CCC-05, CCC-06, CCC-07, CCC-09
- ISO/IEC 27001: Annex A 8.9, Annex 8.32
- SecNumCloud: 12.2, 14.1, 14.2, 14.3, 14.4, 14.6
- TISAX: 5.2.1, 5.2.2

Example Standards:N/A

Label L2

Onsite assessment following assessment process according to the respective standards.

Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.13: Development of Information systems: Ensure information security in the development cycle of information systems.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidence about the provisions covering the criterion, either copied from the Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail:

- rules for the the secure development of software and systems, to be applied to internal developments;
- procedure for supervising and controlling outsourced software and system development activity;
- procedure to maintain the history of the software and systems versions implemented;
- procedures to test all applications before they are put into production;
- mechanisms to implement a secure development environment.

Permissible Standards:

- SecNumCloud: 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7
- BSI C5: DEV-01, DEV-02, DEV-03, DEV-04, DEV-05, DEV-06, DEV-07, DEV-08, DEV-09
- EU Cloud CoC (GDPR, XaaS): 6.2.M

- CSA CCM: DSP-, DSP-08, AIS-04, AIS-05, AIS-06
- ISO/IEC 27001: Annex A 8.25, Annex 8.26, Annex A 8.27, Annex A 8.28, Annex A 8.29, Annex A 8.30, Annex A 8.31
- TISAX: 5.3.1

Example Standards:N/A

> ⚠ Label L2
>
> Onsite assessment following assessment process according to the respective standards.

> ⚠ Label L3
>
> Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.14: Procurement Management: Ensure the protection of information that suppliers of the CSP can access and monitor the agreed services and security requirements.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidence about the provisions covering the criterion, either copied from the Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail:

- procedures to authorize access to the Customer's data by suppliers, in the context of technical support, only after the explicit consent of the Customer;
- procedures to keep up-to-date an exhaustive list of all third parties involved in the implementation of the service;
- requirement to suppliers involved in the implementation of the service to ensure a level of security at least equivalent to that which it undertakes to operationalise its security policy;
- audit clauses enabling a qualifying body to verify that suppliers comply with the security requirements set by the Provider.

Permissible Standards:

- SecNumCloud: 9.7.d, 15.1, 15.2, 15.3, 15.4
- EU Cloud CoC (GDPR, XaaS): 6.2.N
- CSA CCM: STA-09, STA-10, STA-11, STA-12, DSP-13
- ISO/IEC 27001: Annex A 5.19 Annex A 5.20, Annex A 5.21
- TISAX: 6.1.1, 6.1.2

Example Standards:

- BSI C5: SSO-01, SSI-04

> ⚠ Label L2
>
> Onsite assessment following assessment process according to the respective standards.

> ⚠ Label L3
>
> Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.15: Incident Management: Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail:

- procedures to provide prompt and effective response to security incidents, including the means and timelines for communicating security incidents and recommendations to limit their impact to all customers concerned;
- procedures related to the communication of responsibilities of internal and external personnel, third party and customers with regard to the reporting of security incidents ;
- procedures and guidelines for the assessment, classification, prioritisation and escalation of security incidents.

Permissible Standards:

- SecNumCloud: 16.1, 16.2, 16.3, 16.4, 16.5
- BSI C5: SIM-01, SIM-02, SIM-03, SIM-04, SIM-05, OIS-03, OPS-13, OPS-21
- EU Cloud CoC (GDPR, XaaS): 6.2.O, 6.2.P
- CSA CCM: SEF-01, SEF-02, SEF-03, SEF-05, SEF-06, SEF-07, SEF-08, LOG-03, LOG-05

- ISO/IEC 27001: Annex A 5.24, Annex A 5.25, Annex A 5.26, Annex A 5.27
- TISAX: 1.6.1
- CISPE (GDPR, Infrastructure & IaaS): 4.9

Example Standards:N/A

> ⚠ Label L2
>
> Onsite assessment following assessment process according to the respective standards.

> ⚠ Label L3
>
> Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.16: Business Continuity: Plan, implement, maintain and test procedures and measures for business continuity and emergency management.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidence about the provisions covering the criterion, either copied from the Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail :

- availability of business continuity and emergency plans ;
- procedures to maintain or restore the operation of the service and ensure the availability of information according to the terms agreed with the Customer;
- availability of an offline backup procedure for the configuration of the technical infrastructure.
- definition of responsibilities in relation to business continuity and emergency management.

Permissible Standards:

- SecNumCloud: 17.1, 17.2, 17.3, 17.4, 17.5, 17.6
- BSI C5: BCM-01, BCM-02, BCM-03
- EU Cloud CoC (GDPR, XaaS): 6.2.Q
- CSA CCM: BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-09, BCR-10
- ISO/IEC 27001: Annex A 5.29, Annex A 5.30

Example Standards:N/A

> ⚠ Label L2
>
> Onsite assessment following assessment process according to the respective standards.

> ⚠ Label L3
>
> Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.17: Compliance: Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from the Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail:

- procedures and mechanisms to identify and document the security needs relevant to information security of the service;
- procedures and mechanisms to identify the legal, regulatory and contractual requirements applicable to the service and procedures to comply with these requirements;
- procedures to document the choices of technical and organisational measures made to meet the personal data protection requirements in relation to the Provider's role in the processing of data;
- procedures to perform (at least annually) periodical internal audits of the Information Security Management System;
- procedures to provide transparent information on the technical and organisational measures the Provider has in place to protect Customer's data.

Permissible Standards:

- SecNumCloud: 8.3, 18.1, 18.3
- BSI C5: COM-01, COM-03
- EU Cloud CoC (GDPR, XaaS): 6.3.A
- ISO/IEC 27001: Annex A 5.31
- TISAX: 7.1.1

Example Standards:

- CSA CCM: GRC-07, HRS-13, A&A-04

⚠ Label L2

Onsite assessment following assessment process according to the respective standards.

⚠ Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

Criterion P3.1.18: User documentation: Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from the Provider's documentation made available to customers or in a structured machine-readable format (DSL). The evidence shall detail:

- guidelines and recommendations for the secure use of the service provided;
- refer to a register of known vulnerabilities affecting the service offering.

Permissible Standards:

- BSI C5: PSS-01, PSS-03
- EU Cloud CoC (GDPR, XaaS): 6.3.A
- CISPE (GDPR, Infrastructure & IaaS): 5.*

Example Standards:N/A

⚠ Label L2

Onsite assessment following assessment process according to the respective standards.

⚠ Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

✓ LabelL2 & LabelL3

Declaration until additional permissible standards are approved by the Gaia-X Association

---

Criterion P3.1.19: Dealing with information requests from government agencies: Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of Customer Data.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from Provider's documentation or in a structured machine-readable format (DSL). The evidence shall detail:

- procedures to submit to a legal assessment the investigation requests from government agencies ;
- procedures to respond to requests by government agencies in due time and with appropriate detail and quality.
- procedures to inform the Customer when it receives a request from the government agency relating to Customer Data, if permitted by law ;
- procedures to ensure that the agencies submitting investigation requests only gain access to or insight into the data that is the subject of the investigation request. If no clear limitation of the data is possible, procedures to anonymise or pseudonymise the data.

Permissible Standards:

- BSI C5: INQ-01, INQ-02, INQ-03, INQ-04
- EU Cloud CoC (GDPR, XaaS): 5.11.B, 5.11.C

Example Standards:

- CSA CCM: DSP-12, DSP-18

⚠ Label L2

Onsite assessment following assessment process according to the respective standards.

Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

LabelL2 & LabelL3

Declaration until additional permissible standards are approved by the Gaia-X Association

Criterion P3.1.20: Product security: Provide appropriate mechanisms for cloud customers to enable product security.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from the legally binding act/other Provider's documentation made available to the Customer or in a structured machine-readable format (DSL). The evidence shall detail:

- Guidelines and recommendations for the secure use of the service provided;
- Error handling, logging and authentication mechanisms;
- Implementation of a session management system.

Permissible Standards:

- BSI C5: PSS-01, PSS-04, PSS-05, PSS-06, PSS-08, PSS-10, PSS-11, PSS-12
- CISPE (GDPR, Infrastructure & IaaS): 5.1, 5.3, 4.3
- EU Cloud CoC (GDPR, XaaS): 5.1.C

Example Standards:

- CSA CCM: IAM-11

Label L2

Onsite assessment following assessment process according to the respective standards.

Label L3

Assessment process according to the process for EUCS Level High ; ad interim: see Label L2.

5.6 Portability

The section refers to the application of Art. 6 (1) Free Flow of Data Regulation (FFoDR). It applies to any Service Offering, regardless of its Provider, type, purpose, or processed categories of data.

5.6.1 Switching and porting of Customer Data

Criterion P4.1.1: The Provider shall implement practices for facilitating the switching of Providers and the porting of Customer Data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the Customer.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	certification

Declaration: Using the Gaia-X Ontology, evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL), shall be provided. The evidence shall detail:

- Information on the contractual provisions allowing the Customer to retrieve all of its data;
- List of methods to import and export Customer Data in a structured, commonly used and machine-readable format.

Permissible Standards:

- SecNumCloud: 19.1.g, 19.1.h
- SWIPO IaaS: DP01, DP02, DP03, DP04, DP05, DP08

Example Standards:N/A

Note

The switching process involves three parties, the Customer, the exiting Provider and the receiving Provider who should all duly co-operate to execute the transfer.

Note

The Customer Data received by the Customer or the importing Provider could include configuration information as well as information about the software systems used for the Service Offering.

LabelL2, LabelL3

To the extent there is no project with / or no mechanism to receive a third-party attestation, a self-declaration shall suffice; once a mechanism/project including third-party statements exists, and such project/mechanisms is mapped by Gaia-X, the third-party attestation becomes mandatory.

LabelL2, LabelL3

For the time being, for Lvl2 and Lvl3 it must be ensured that at a minimum the self-assessment is formally declared to an independent body as provided by the project - e.g., for SWIPO this is the SWIPO secretariat.

Criterion P4.1.2: The Provider shall ensure pre-contractual information exists, with sufficiently detailed, clear and transparent information regarding the processes of Customer Data portability, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another Provider or port Customer Data back to its own IT systems.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	certification

Declaration: Description based on either 1. or 2.:

1. Using the Gaia-X Ontology, evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL), shall be provided.
   The evidence shall detail:
   - Information on the following elements: documentation, available support and tools, data porting processes and supported capabilities, available porting methods and formats, charges and terms associated with porting, procedures for handling the Customer data on the Provider's infrastructure after termination of the service, third parties that have access to the data through the process, policies and process for accessing data in the event of Provider's bankruptcy or acquisition by another entity;
   - Procedures for initiating and managing switching and porting from/to the Service.
   2. Declaration of compliance to criterion 4.1.2.

Permissible Standards:

- SWIPO IaaS: TR03, PR01, PR02, PR03, PR04, PR06, PR07

Example Standards:N/A

LabelL2, LabelL3

To the extent there is no project with / or no mechanism to receive a third-party attestation, a self-declaration shall suffice; once a mechanism / project including third-party statements exists, and such project / mechanisms is mapped by Gaia-X, the third-party attestation becomes mandatory.

LabelL2, LabelL3

For the time being, for Lvl2 and Lvl3 it must be ensured that at a minimum the self-assessment is formally declared to an independent body as provided by the project - e.g., for SWIPO this is the SWIPO secretariat.

5.7 European Control

This section applies to any service offering, regardless of its Provider, type, purpose, or processed categories of data. However, requirements shall only apply subject to the indicated labels. This section aims to address the Customer's or domain-specific needs, e.g., by limiting storage and/or processing to the area of EU/EEA.

Gaia-X distinguishes 3 levels of Labels, starting from Label Level 1 (the lowest), up to Label Level 3 (the highest), which represent different degrees of compliance with regard to the goals of transparency, autonomy, data protection, security, interoperability, flexibility, and European Control. Some of the following requirements are specific to a respective Label Level.

5.7.1 Processing and storing of Customer Data in EU/EEA

Criterion P5.1.1: For Label Level 2, the Provider shall provide the option that all Customer Data are processed and stored exclusively in EU/EEA.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	N/A	certification	N/A

Declaration: N/A

Permissible Standards:

- SecNumCloud: 19.1, 19.2
- CISPE (GDPR, Infrastructure & IaaS): 4.4

Example Standards:

- BSI C5: PSS-12

✓ LabelL2

Declaration until an external entity is accredited by the Gaia-X Association

---

Criterion P5.1.2: For Label Level 3, the Provider shall process and store all Customer Data exclusively in the EU/EEA.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	N/A	N/A	certification

Declaration: N/A

Permissible Standards:

- SecNumCloud: 19.1, 19.2
- CISPE (GDPR, Infrastructure & IaaS): 4.4

Example Standards:N/A

✓ LabelL3

Declaration until an external entity is accredited by the Gaia-X Association

---

Criterion P5.1.3: 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 statutory order, the Provider shall have verified safeguards in place to ensure that any access request is compliant with EU/EEA/Member State law.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	N/A	N/A	certification

Declaration: N/A

Permissible Standards:N/A

Example Standards:N/A

Note

This is a general principle which is not assessable. The verified safeguards are further specified in subsequent criteria in this section (P5.1.4 - P5.1.7).

Criterion P5.1.4: 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.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	N/A	N/A	certification

Declaration: N/A

Permissible Standards:

- SecNumCloud: 19.6

Example Standards:N/A

✓ LabelL3

Declaration until an external entity is accredited by the Gaia-X Association

---

Criterion P5.1.5: 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 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 for illustrations of decisive control).

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	N/A	N/A	certification

Declaration: N/A

Permissible Standards:N/A

Example Standards:N/A

✓ LabelL3

Declaration until an external entity is accredited by the Gaia-X Association

---

Criterion P5.1.6: For Label Level 3, in the event of recourse by the Provider, in the context of the services provided to the Customer, to the services of a third-party company - including a subcontractor - whose registered head office, headquarters and main establishment is outside of the European Union or who is owned or controlled directly or indirectly by another third-party company registered outside the EU/EEA, the third-party company shall have no access over the Customer Data nor access and identity management for the services provided to the Customer. The Provider, including any of its sub-processors, shall push back any request received from non-European authorities to obtain communication of Customer Data relating to European Customers, except if request is made in execution of a court judgment or order that is valid and compliant under Union law and applicable Member States law as provided by Article 48 GDPR.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	N/A	N/A	certification

Declaration: N/A

Permissible Standards:N/A

Example Standards:

- SecNumCloud: 19.6

✓ LabelL3

Declaration until an external entity is accredited by the Gaia-X Association

---

Criterion P5.1.7: For Label Level 3, the Provider must maintain continuous operating autonomy for all or part of the services it provides. The concept of operating autonomy shall be understood as the ability to maintain the provision of the cloud computing service by drawing on the provider's own skills or by using adequate alternatives

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	N/A	N/A	certification

Declaration: N/A

Permissible Standards:

- SecNumCloud: 19.6.d

Example Standards:N/A

✓ LabelL3

Declaration until an external entity is accredited by the Gaia-X Association

5.7.2 Access to Customer Data

Criterion P5.2.1: The Provider shall not access Customer Data unless authorized by the Customer or when the access is in accordance with applicable laws in scope of the legally binding act.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Using the Gaia-X Ontology, the declaration shall include evidences about the provisions covering the criterion, either copied from the legally binding document or in a structured machine-readable format (DSL). The evidence shall detail:

- policies and guidelines to ensure that Customer Data is not accessed by the Provider for any purpose independent of Customer's instructions as provided in the legally binding act, and/or has been explicitly requested by the Customer and/or is necessary to comply with applicable laws in the scope of the legally binding act.

Permissible Standards:

- CISPE (GDPR, Infrastructure & IaaS): 3
- EU Cloud CoC (GDPR, XaaS): 5.4.A, 5.4.B, 5.4.C, 5.12.C

Example Standards:

- SecNumCloud: 9.7
- BSI C5: IDM-07
- CSA CCM: DSP-15

✓ LabelL2 & LabelL3

The verification is done using the permissible standards as they are will cover the criterion.

If access to Customer Data requires customer authorization on a case-by-case basis (e.g. to perform support activities):

- Verification of an exemplary case to determine whether the access to Customer Data was authorized by the Customer in accordance with the requirements in the applicable documentation.

5.8 Sustainability

Criterion P6.1.1: The Provider shall provide transparency on the environmental impact of the Service Offering provided

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: Link to an environmental impact report of the Provider. The report shall describe the consumption of natural resources such as water and energy sources, the carbon footprint, the use of pollutants and other factors.

Permissible Standards:N/A

Example Standards:N/A

Note

The report may be an aggregate statement on a portfolio of services, not necessarily reflecting the impact of an individual Service Offering.

Criterion P6.1.2: The Provider shall ensure that the Service Offering meets or relies on an infrastructure Services Offering which meets a high standard in energy efficiency, meeting an annual target of PUE of 1.3 in cool climates and 1.4 in warm climates

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	declaration	certification	certification

Declaration: Declaration based either on 1. or 2.:

1. Using the Gaia-X Ontology, the declaration shall contain the value of Power usage effectiveness (PUE) met by the Service Offering/by the Infrastructure Services Offering it relies on, meeting an annual target of PUE of 1.3 in cool climates and 1.4 in warm climates.
2. the declaration shall contain the link to the public registered Provider's adherence to one of the Permissible Standards.

Permissible Standards:

- Climate Neutral Data Centre Pact (CNDCP)

Example Standards:N/A

Note

By January 1, 2025, the metric should be met by any new data centre at full capacity used to provide the Service Offering. Pre-existing data centres will achieve these same targets by January 1, 2030. The targets apply to all data centres larger than 50KW of maximum IT power demand.

Note

PUE is a ratio that describes how efficiently a computer data centre uses energy; specifically, how much energy is used by the computing equipment (in contrast to cooling and other overhead that supports the equipment). PUE is the ratio of the total amount of energy used by a computer data centre facility to the energy delivered to computing equipment.

Criterion P6.1.3: The Provider shall ensure that the Service Offering meets or relies on an infrastructure Services Offering for which electricity demand will be matched by 75% renewable energy or hourly carbon-free energy by 31st December 2025, and 100% by 31st December 2030.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	declaration	certification	certification

Declaration: Declaration based either on 1. or 2.:

1. Using the Gaia-X Ontology, the declaration shall contain the percentage of renewable energy or hourly carbon free energy matching the electricity demand of the Service Offering/the infrastructure Services it relies on. The value shall be equal to or greater than 75 by 31st December 2025, and equal to 100 by 31st December 2030.
2. the declaration shall contain the link to the public registered Provider's adherence to one of the Permissible Standards.

Permissible Standards:

- Climate Neutral Data Centre Pact (CNDCP)

Example Standards:N/A

Criterion P6.1.4: The Provider shall ensure that the Service Offering meets or relies on an infrastructure Services Offering that will meet a high standard for water conservation demonstrated through the application of a location and source sensitive water usage effectiveness (WUE)target of 0.4 L/kWh in areas with water stress.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
N/A	declaration	certification	certification

Declaration: Description based either on 1. or 2.:

1. Using the Gaia-X Ontology, the declaration shall contain the value of Water usage effectiveness (WUE) met by the Service Offering/by the infrastructure Services it relies on. By January 1, 2025 the maximum WUE is set to 0.4 L/kWh in areas with water stress for new data centres at full capacity in cool climates that use potable water.
2. the declaration shall contain the link to the public registered Provider's adherence to one of the Permissible Standards.

Permissible Standards:

- Climate Neutral Data Centre Pact (CNDCP)

Example Standards:N/A

> Note
>
> By January 1, 2025 new data centres at full capacity in cool climates that use potable water will be designed to meet a maximum WUE of 0.4 L/kWh in areas with water stress. The limit for WUE can be modified based on climate, stress and water type to encourage the use of sustainable water sources for cooling. By December 31, 2040, existing data centres that replace a cooling system will meet the WUE target applied to new data centres.

> Note
>
> Water usage effectiveness (WUE) is used to measure data centre sustainability in terms of water usage and its relation to energy consumption. It is calculated as the ratio between water used at the data centre (water loops, adiabatic towers, humidification, etc.) and energy delivered to the IT equipment. WUE will be measured using the category 1 site value, per ISO/IEC 30134-9:2022 standard.

6 Gaia-X Compliance Criteria for Data Exchange Services

In Gaia-X, `Data` is at the core of Data Exchange Services. `Data` are furnished by `Data Producers` (for instance data owners or data controllers in the GDPR sense, data holder in EU data acts sense, etc.) to `Data Product Providers` who compose these data into a `Data Product` to be used by `Data Consumers`.

Further details of all the terms used in this section are defined in the section on Data Exchange Services of the Gaia-X Architecture Document and in the Data Exchange Services specifications, and to keep definitions consistent across documents and versions, they won't be duplicated here.

Criteria extract in JSON

A machine readable version of the criteria in JSON is available here. Download JSON

6.1 Criteria

Criterion D1.1.1: The Data Product shall be a Gaia-X compliant Service Offering.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: See P.1.2.9

Permissible Standards:N/A

Example Standards:N/A

Criterion D1.1.2a: The `Data Product Provider` offering the `Data Product` shall be a Gaia-X Participant.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: N/A

Permissible Standards:N/A

Example Standards:N/A

Criterion D1.1.2b: The `Data Product Provider` shall deliver the `Data Product` only to `Data Consumers` with a Gaia-X compliant description

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: N/A

Permissible Standards:

- a conformity assessment scheme which includes the verification of records in the Data Usage Logging Service

Example Standards:N/A

Note

This criterion is important to create trust at the data licensor/data producer level.

Criterion D1.1.3: For each `Data Product`, the `Data Product Provider` shall have the legal authorization from the `Data Producer`(s) to include the data in the `Data Product`.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: The Data Product Description shall include links to authorization documents which are signed through a Gaia-X authorized Trust Service Provider.

Permissible Standards:

- a conformity assessment scheme which includes the verification that the authorization documents are legally valid.

Example Standards:N/A

> **Note**
>
> If the data product aggregates data from several data producers, then the data product provider shall have a legal authorization from each data producer.

> **Note**
>
> The legal authorization will often be subordinated to the data usage agreement from the data licensor(s). Indeed the Data Product will usually be generic (e.g. customer banking transactions) and the real scope (e.g. Jane Doe's transactions) will be defined during instantiation before data usage.

Criterion D1.1.4: For each `Data Product`, the `Data Product Provider` shall provide in the `Data Product Description` a `Data License` defining the usage policy in ODRL for all data in this Data Product.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	declaration	declaration

Declaration: The Data Product Description shall include a data license expressed as a valid ODRL document containing at least indication that the data product contains or not licensed data and, in that case, the template of the Data Usage Agreement to be signed by the data licensor(s) before data usage. The Data license shall contain:

1. the constraints specific to the Data Product Provider.
2. indication that the data product contains or not licensed data and in that case.
3. the template of the Data Usage Agreement to be signed by the data licensor(s) before data usage.

Permissible Standards:N/A

Example Standards:N/A

Criterion D1.1.5: The `Data Product Provider` shall deliver the `Data Usage`, instantiating the `Data Product`, only to `Data Consumer(s)` which have formally accepted the `Data Product Usage Contract`.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Yes/No

Permissible Standards:

- a conformity assessment scheme which includes performing correlation of the records in the Data Usage Logging Service with the Data Product Usage Contracts (either provided by the Data Product Provider or through a Data Product Usage Contract Store) and verifying that each contract is formally accepted by the Data Consumer.

Example Standards:N/A

> **Note**
>
> A `Data Product Usage Contract` is a Ricardian contract: a contract at law that is both human-readable and machine-readable, cryptographically signed and rendered tamper-proof.

> **Note**
>
> A Data Consumer can formally accept the Data Product Usage Contract either through a qualified digital signature or through a record from a Gaia-X Trusted Source (e.g. trusted data intermediary)

Criterion D1.1.6a: For each licensed data element included in the `Data Product`, the `Data Product Provider` shall ensure that each `Data Product Usage Contract` includes `Data Usage Agreement(s)` (DUA) provided by the `Data Licensor(s)` explicitly authorizing the `Data Usage` by the `Data Consumer`.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: In case of data liable to EU regulations (GDPR, EU acts on data ⋯), the provided `Data Usage Agreement` must contain all information required by the regulation (e.g. consent as per GDPR, authorizations/permissions as per EU acts on data, permissions as per the EU Finance Data Access regulation, etc⋯).

Permissible Standards:

- a conformity assessment scheme which includes the verification that the `Data Product Usage Contracts` contain appropriate `Data Usage Agreement(s)`

Example Standards:N/A

> **Note**
>
> A `Data Licensor` is a natural or legal `Participant` who owns usage rights for some `Data`. It can be a data subject as per GDPR for personal data or a primary owner of non-personal data (i.e. not liable to GDPR).

> **Note**
>
> The `Data Licensor(s)` can provide the `Data Usage Agreement(s)` either through a qualified digital signature or through a record from a Gaia-X Trusted Source (e.g. a trusted data intermediary).

> **Note**
>
> The `Data Usage Agreement(s)` gives the `Data Product Provider` the legal authorization for providing the data to the `Data Consumer`. The DUA contains usage terms and conditions associated with these data (permissions, prohibitions, duties ⋯).

> **Note**
>
> Controlling that the `Data Licensor` is legally authorized to give a `Data Usage Agreement` is often domain specific (for instance a farmer can give agreement to use data related to a parcel only if she/he owns or rents this parcel).

Criterion D1.1.6b: The `Data Product Provider` shall deliver the `Data Usage` instantiating the `Data Product` only to `Data Consumer(s)` which fulfill the constraints in the `Data Usage Agreements`.

Standard Compliance	Label Level 1	Label Level 2	Label Level 3
declaration	declaration	certification	certification

Declaration: Yes/No

Permissible Standards:

- a conformity assessment scheme which includes the verification checking that each `Data Consumer` of the `Data Product` has provided appropriate Verifiable Credentials for the constraints in the `Data Usage Agreements`

Example Standards:N/A

> **Note**
>
> Controlling that the `Data Consumer` fulfils the constraints expressed in the `Data Usage Agreement(s)` is often domain specific (for instance a patient might agree to share medical data to non-profit research laboratories from specific countries with defined cyber-security certificates). A generic way to implement this criterion is to request the `Data Consumer` to provide, in the `Data Product Usage Contract`, the appropriate Verifiable Credentials issued by Gaia-X Trusted Data Sources.

IV. Gaia-X Trust Anchors

7 Gaia-X Trust Anchors

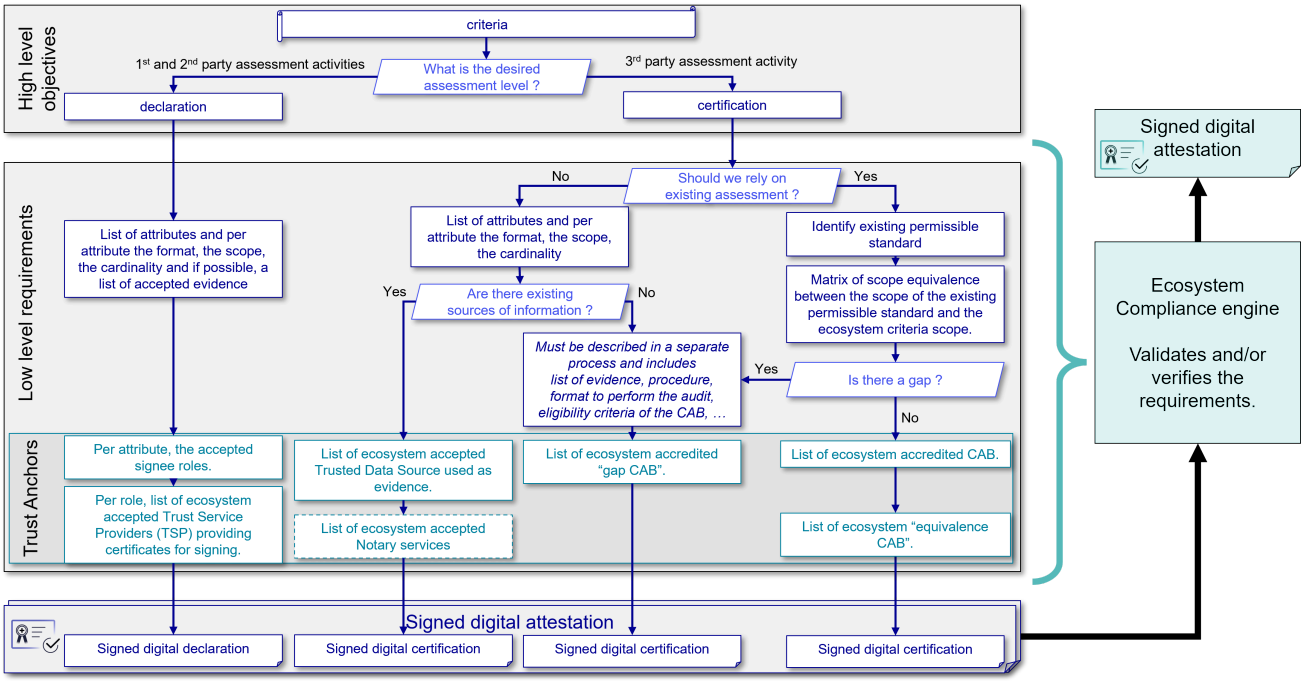
Gaia-X Trust Anchors are bodies, parties, i.e., Conformity Assessment Bodies or technical means accredited by the bodies of the Gaia-X Association to be parties eligible to issue attestations about specific claims.

For each accredited Trust Anchor, a specific scope of attestation is defined.

The Trust Anchors are not necessarily Root Certificate Authorities as commonly understood, but they can be relative to different properties in a claim.

7.1 Overall decision flowchart

The decision flowchart below is used to determine what type of Trust Anchor must be defined for a given criteria objective.



7.2 Trust Anchors

7.2.1 Signee's role

In the Gaia-X Ontology, for specific attributes which are linked or dependent from each other, a criteria can mandate that an attribute must be signed by the same issuer - or signee - of another attribute.

For example, in the Gaia-X Trust Framework 22.10, it is mandatory for the information whether or not a Data Product contains PII that the attribute `dataProduct.containsPII` is signed by the Producer of this Data Product `dataProduct.produceBy`.

7.2.2 Trust Service Provider

By default, for the claims to be legally relevant, all claims must be signed with one or more cryptographic material which can be traced back to a Trust Anchor, which is in most case a Trust Service Provider (TSP).

The Trust Service Providers (TSP) accredited by Gaia-X must be entities issuing cryptographic material based on documented Know Your Business/Know Your Customer (KYB/KYC) processes. Those processes must verify the identity of the party requesting the digital certificate associated to the cryptographic material, such as, and not limited to:

- Business registration or license verification
- Physical address verification
- Phone number verification

The non-exclusive list of accepted Trust Service Providers belong to these categories: - EEA 🇪🇺, Iceland 🇮🇸, Liechtenstein 🇱🇮, Norway 🇳🇴: eIDAS Regulation (EU) No 910/2014. (Homepage, Trusted Data Source) - India 🇮🇳: eMuhdra (Homepage, Trusted Data Source) - South Korea 🇰🇷: KTNET (Homepage) - United Arab Emirates (UAE) 🇦🇪: PASS (Homepage)

To have a global reach, and only if there is no alternative specified in the Gaia-X Registry for the country of the business registration, Gaia-X allows the use of Extended Validation (EV) Secure Sockets Layer (SSL) certificate to sign attributes. (Homepage, Trusted Data Source)

The accepted TSP categories are determined within the Gaia-X Compliance document, while the detailed list of valid TSP belonging to these categories resides in the Gaia-X Registry.

7.3 Trusted Data Sources and Notaries

When an accredited Trust Anchor is not capable of issuing cryptographic material nor signing claim directly, the Gaia-X Association accredits one or more Notaries which convert "not machine readable" proofs into "machine readable" proofs. A Gaia-X Notary must be a Gaia-X participant capable of translating an unsigned evidence to a signed machine readable evidence. For signing, the Gaia-X Notary must use a cryptographic material issued by a Trust Anchor.

Notaries perform validations and issue attestations based on objective evidences from Trusted Data sources. The Verifiable Credentials issued by the Notaries contain the evidences of the validation process.

The following Trusted Data Sources have been accredited by Gaia-X and are currently used by the Gaia-X Notary Service to validate and issue attestations on the Participant's Legal Registration Number:

- `EORI`: the European Commission API.
- `leiCode`: the Global Legal Entity Identifier (GLEIF) API
- `local`: the OpenCorporate API
  - the returned claim will also contain information about `headquarterAddress.countryCode`
- `vatID`: for the European member states or North Ireland, the VAT Information Exchange System (VIES) API
  - the returned claim will also contain information about `headquarterAddress.countryCode`

The accepted Trusted Data Source categories and Notaries are determined within the Gaia-X Compliance document, while the detailed list of valid Trusted Data Sources and Notaries resides in the Gaia-X Registry.

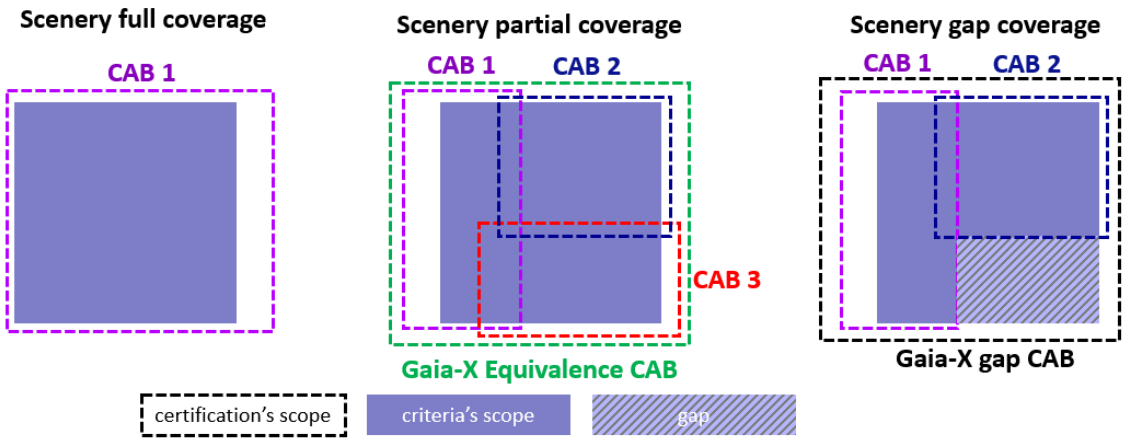
7.4 CAB, "Equivalence CAB", "Gap CAB"

All CABs which are accredited to attestate conformity against a permissable standard by the respective oganizations body are accepted by Gaia-X.

An "Equivalence CAB" is an identified entity approved by Gaia-X to verify that one or more issued certifications cover the entirety of a given criteria scope.

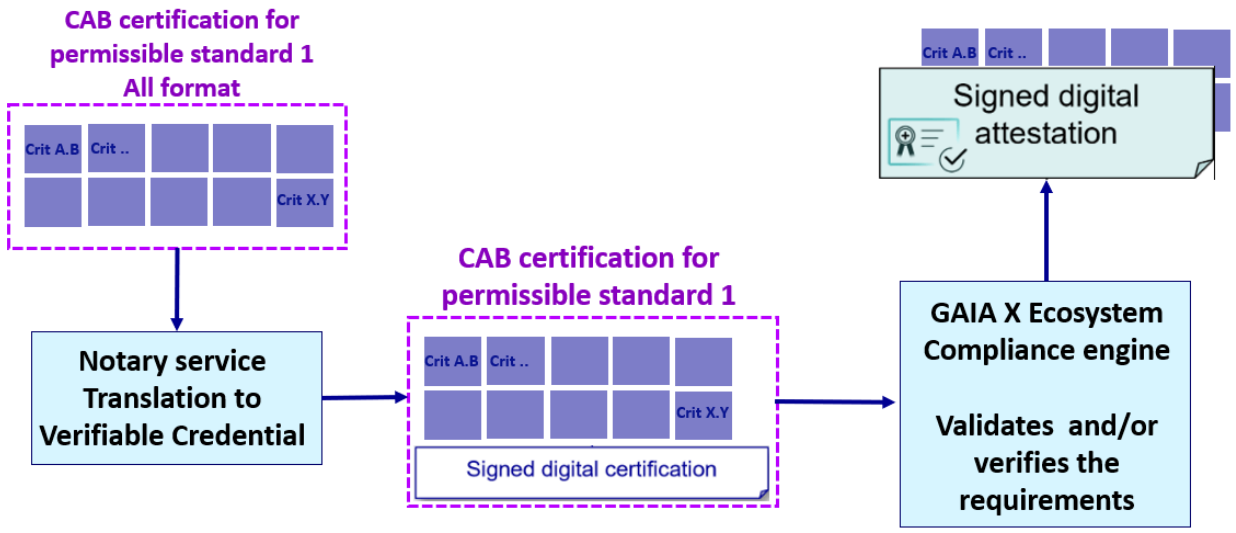
A "Gap CAB" is an identified entity approved by Gaia-X to issue a certification for a scope identified as not covered by an "Equivalence CAB".

The full list of valid CAB, "Equivalence CAB", "Gap CAB" is kept up-to-date and made available via the Gaia-X Registry.



Scenario	The certification covers, at least, the entirety of the criterion's scope.	Overlap of the various certification's scope to be assessed by an equivalence CAB.	The certification(s) don't cover the entirety of the criterion's scope, requiring the gap to be assessed separately.
Trust Anchors type	List of CAB per certification scheme.	List of Gaia-X equivalence CAB	List of Gaia-X gap CAB
## How to use CAB certifications ?			

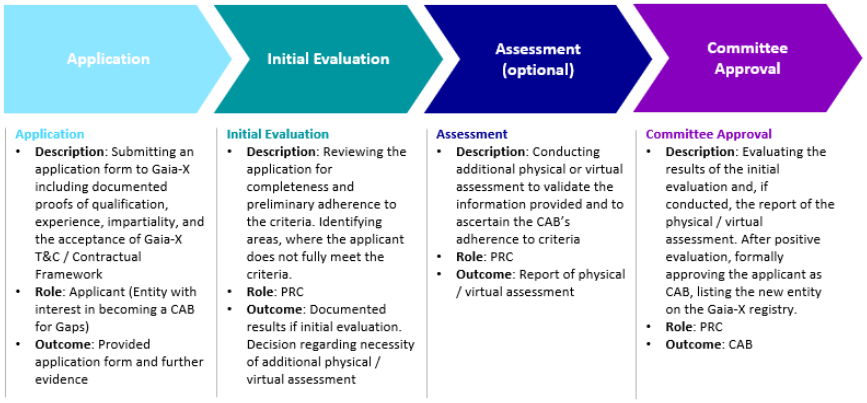
CAB certifications issued by a CAB listed in the GAIA X Registry can be used to validate all criterions fully compliant covered by CAB certificate's perimeter as described in this document.



7.5 GAP CAB Approval Process

The following defines the approval process for GAP CABs (if the CABs are supposed to issue verifiable credentials for Gaia-X Criteria not fully covered by Permissible Standards) to be approved for the verification and final decision. These criteria and proofs will ensure the required competence, a common understanding of the relevant documents, requirements, and procedures for the Gaia-X Labelling.

If Gaia-X criterion are all covered by several international Permissible Standards, this process may not be needed anymore and removed from this document.



7.5.1 Key GAIA-X commitments for the Approval process

Transparency

All processes and approval criteria are publicly disclosed (e.g. on the Gaia-X website), ensuring a transparent and fair approval process which creates reliable trustfullness.

Impartiality

The PRC ensures impartiality for the approval process in line with ISO/IEC 17011 principles.

Competence and experience

The PRC assures that an assessment of competence and experience is performed on Gap CAB applicant in order to demonstrate the required expertise in the domains of Gaia-X criteria and on other permissible standards in line with ISO/IEC 17011 principles.

Quality Assurance

The PRC assures an ongoing quality assurance mechanism, including periodic surveillance assessment and reviews of CABs' continuous improvement plans.

7.5.2 Application

Entities, interested in becoming an approved/listed CAB for Gaia-X Labelling, submit an application form to Gaia-X AISBL including documented proofs of applicable criteria (e.g. qualification, experience, and impartiality).

Along with the application, a checklist that correlates with the criteria for CABs should be provided to aid in documenting the review.

7.5.3 Initial Evaluation

The PRC reviews the application for completeness and preliminary adherence to the criteria. Areas, where the applicant does not fully meet the criteria, are identified.

7.5.4 Assessment

If the criteria are only partial met, additional physical or virtual assessments might be necessary on behalf or by the PRC to validate the information provided and to ascertain the CAB's adherence to criteria.

7.5.5 PRC Approval/Rejection

The final approval is based on the evaluation of the submitted documents and if conducted, the report about the physical or virtual assessments.

After positive evaluation, the CAB will get an Approval Certificate (Statement of Approval) by Gaia-X AISBL and be listed on the Gaia-X Registry.

In case of negative evaluation, the CAB will get a written notification detailing the reasons for refusal to approve and list them. This will include specific references to the applicable criteria for approval.

7.5.6 Criteria for the approval of CABs

This section defines the criteria that CABs shall fulfil to carry out the conformity assessments for verifiable credentials. These criteria and respective proofs will ensure the required competence for all conformity assessments related to the Gaia-X criteria which are relevant for the Gaia-X Labels.

- If a CAB is not yet approved/accredited by the responsible Approval Body for a Permissible Standard, the CAB shall proof adherence to the Gaia-X Criteria as outlined in section "Criteria of approval for CAB that are not yet approved/accredited by an Approval Body for a Permissible Standard" below.
- (Most probably) If a CAB is already active as a CAB for one or more of the Permissible Standards listed in this document and thus is approved/accredited by the responsible Approval Body to issue the corresponding verifiable credential, additional proofs are required with respect to technical competence of the personnel, due to the various domains of the Gaia-X Criteria not covered by each of the Permissible Standards. Which specific proofs are required per Permissible Standard is outlined in section "Proofs of suitability for approval as CAB to remediate gaps" below.

7.5.6.1 Criteria of approval for CAB that are not yet approved/accredited by an Approval Body for a Permissible Standard

7.5.6.1.1 ORGANISATIONAL STRUCTURE AND GOVERNANCE

Legal status

Criteria: Shall be a legally recognized entity capable of entering into contracts and assuming liability. Proof: Current extract from the commercial register

Impartiality and independence

Criteria: Policies should be in place to prevent commercial, financial, or other pressures from compromising impartiality.

Proof: Internal impartiality policy, organizational chart, documented procedures for dealing with conflicts of interest or accreditation certificate issued by a recognized accreditation body listed as a member of the International Accreditation Forum (IAF) or verification of respective statements in the audit firms' Transparency Report issued in accordance with the requirement set forth in European statutory audit regulations (Article 13 of Regulation (EU) 537/2014) or an equivalent approval.

7.5.6.1.2 COMPETENCE AND PERSONNEL

Technical competence

Criteria: Shall have personnel with expertise in the domains of the Gaia-X Criteria.

Proof: Records about existing approvals for Permissible Standards or appropriate evidence to proof the competence with respect to the domains of the Gaia-X Criteria.

Training

Criteria: Should have a continuous professional development programme in place.

Proof: Training plans, attendance records, training content.

Participation in Gaia-X meetings for experience exchange and training

Criteria: Shall participate in annual Gaia-X meetings for experience exchange and training to ensure a common understanding of all rules and procedures within Gaia-X Labelling and a fair competition between the Equivalence CABs.

Proof: Training plans, attendance records, training content.

7.5.6.1.3 ASSESSMENT PROCESS MANAGEMENT

Process documentation

Criteria: Shall have comprehensive and up-to-date documentation for all assessment activities and follow the publication and updates by Gaia-X.

Proof: Process documentation, SOPs (Standard Operating Procedures).

Confidentiality

Criteria: Measures should be in place to protect confidential information.

Proof: Privacy policies, NDAs with employees and subcontractors.

Transparency

Criteria: Processes, criteria and results should be publicly available unless restricted by law or confidentiality.

Proof: Published procedures, public records of statements of conformity issued.

7.5.6.1.4 QUALITY ASSURANCE AND CONTINUOUS IMPROVEMENT

Internal audits

Criteria: Should conduct regular internal audits to assess compliance with processes and standards.

Proof: Internal audit reports, corrective action plans.

Management reviews

Criteria: Should periodically review the effectiveness of the quality management system.

Proof: Minutes of management review meetings, action items and follow-up reports.

7.5.6.1.5 SUBCONTRACTING AND OUTSOURCING

Responsibility

Criteria: Remains responsible for all outsourced activities and shall ensure that subcontractors for labeling issuing activities meet the same quality criteria.

Proof: Subcontractor agreements, quality control checks on subcontractor output.

Quality Control

Criteria: Shall have a monitoring system to assess the performance of subcontractors.

Proof: Monitoring reports, subcontractor performance metrics.

7.5.6.1.6 RECORDS AND DOCUMENTATION

Data management

Criteria: Shall securely manage all records and documentation related to labelling activities.

Proof: Data management policies, data security protocols.

Retention policy

Criteria: Shall have a documented retention policy in accordance with relevant laws and regulations.

Proof: Document retention policies, compliance audits.

7.5.6.1.7 MONITORING AND CONTROL

Periodic reviews

Criteria: Shall conduct periodic surveillance reviews to ensure that Gaia-X Service Offerings, for which Gaia-X Statements of Conformity were issued, continue to meet Gaia-X criteria.

Proof: Surveillance review reports, re-assessment records.

Corrective actions

Criteria: Shall have processes to address non-compliance, ranging from corrective action plans to withdrawal of Gaia-X Statements of Conformity.

Proof: Corrective action plans, records of enforcement actions.

7.5.6.1.8 APPEALS AND COMPLAINTS

Appeals procedures

Criteria: Shall provide a mechanism for organizations to appeal Gaia-X Labelling/registration decisions.

Proof: Documented appeals process, records of appeals handled.

Complaints handling

Criteria: Shall have a process for receiving and resolving complaints about its labelling activities.

Proof: Documented complaints procedure, log of complaints received, and action taken.

7.5.6.2 Proofs of suitability for approval as CAB to remediate gaps

CISPE.cloud

No additional proof required.

EU Cloud Code of Conduct

No additional proof required.

BSI C5

- Latest Transparency Report issued in accordance with the requirement set forth in European statutory audit regulations (Article 13 of Regulation (EU) 537/2014) does not indicate material deficiencies with respect to the criteria in section “Criteria for the approval of CABs”.
- Entity has performed at least 2 conformity assessments for Cloud Service Providers in accordance with the programme within 12 months prior to the application (see section “Application”) and can state respective references.

TISAX

Entity has performed at least 2 conformity assessments for Cloud Service Providers in accordance with the programme within 12 months prior to the application (see section “Application”) and can state respective references.

AICPA

- Latest Transparency Report issued in accordance with the requirement set forth in European statutory audit regulations (Article 13 of Regulation (EU) 537/2014) does not indicate material deficiencies with respect to the criteria in section “Criteria for the approval of CABs”.
- Entity has performed at least 2 conformity assessments for Cloud Service Providers in accordance with the programme within 12 months prior to the application (see section “Application”) and can state respective references.

ISO/IEC 27001

- Entity has performed at least 2 conformity assessments for Cloud Service Providers in accordance with the programme within 12 months prior to the application (see section “Application”) and can state respective references.
- Entity has appropriate knowledge and experience of GDPR

CCM v4

No additional proof required.

7.5.6.3 Additional proofs for the criteria on competence and personnel for CABs to remediate gaps

CISPE.cloud

No additional proof required.

EU Cloud Code of Conduct

No additional proof required.

BSI C5

Records for a minimum of 24h of structured training on GDPR requirements for personnel assigned to engagements to issue verifiable credentials with respect to the Gaia-X Criteria in the domain Data Protection.

TISAX

Records for a minimum of 24h of structured training on GDPR requirements for personnel assigned to engagements to issue verifiable credentials with respect to the Gaia-X Criteria in the domain Data Protection.

AICPA

If conformity assessments comprised the “Privacy” category of the Trust Services Criteria: no additional proof required. Otherwise: Records for a minimum of 24h of structured training on GDPR requirements for personnel assigned to engagements to issue verifiable credentials with respect to the Gaia-X Criteria in the domain Data Protection.

ISO/IEC 27001

Records for a minimum of 24h of structured training on GDPR requirements for personnel assigned to engagements to issue verifiable credentials with respect to the Gaia-X Criteria in the domain Data Protection.

CCM v4

Records for a minimum of 24h of structured training on GDPR requirements for personnel assigned to engagements to issue verifiable credentials with respect to the Gaia-X Criteria in the domain Data Protection.

8 List of Gaia-X Conformity Assessment Bodies

All Gaia-X Conformity Assessment Bodies (CABs) which are accredited to attestate conformity against a permissable standard by a respective standards organizations body are accepted by Gaia-X.

Accreditation Bodies: ISO standard definition here

As of 06/06/2024, the list of the accepted accreditation bodies is located at https://www.iafcertsearch.org/search/accreditation-bodies

8.1 SecNumCloud

The list of official assessment bodies for SecNumCloud is located at https://cyber.gouv.fr/voir-les-centres-devaluation.

As of 28/05/2024, the list is the following one:

- AFNOR Certification
- International Certification Trust Services (ICTS)
- LNE
- LSTI

8.2 ISO 27001

The list of official certification bodies for ISO 27001 is located in InternationalAccreditationForum

As of 07/06, 501 CAB are accepted for ISO 27001 worlwide by IAF. They will not be listed in this document. The uptodate list is in the GAIA-X registry.

> Note
>
> In France the accredidation body is located at COFRAC.

As of 03/06/24 the list of COFRAC for France is:

- AFNOR Certification
- International Certification Trust Services France
- LNE
- LSTI
- SGS International Certification Service
- Skill4All
- Vigicert

8.3 EU Cloud CoC

The list of official monitoring bodies able to deliver EU Cloud Code of Conduct assement is located at https://eucoc.cloud/en/public-register/assessment-procedure.

As of 03/06/24 the only one is:

- SCOPE Europe

8.4 CISPE Code of Conduct

The list of official assessment bodies for CISPE is located at https://www.codeofconduct.cloud/monitoring-bodies/.

As of 10/06/2024, the list is the following one:

- Bureau Veritas
- EY CertifyPoint
- LNE (Laboratoire national de métrologie et d'essais)

8.5 Cloud Security Alliance

The list of official CSA certified STAR auditors is located at : https://cloudsecurityalliance.org/star/certified-star-auditors

As of 11/06/2024, more than forty CAB are accepted for CSA STAR so they will not be listed in this document. The up to date list is in the GAIA-X registry.

BSI C5

As of 26/06/2024, BSI C5 doesn't provide the list of official assessment bodies authoristed to issue BSI C5 attestion : BSI. As confirmed by BSI on 3/07/2024: "The BSI often receives enquiries regarding who can perform a C5 audit and whether the BSI can recommend or arrange auditors. The BSI does not as a principle make any such recommendations. The requirements for auditors are specified in Chapter 3 of the C5 and adhering to them should be specified as part of the contract to appoint an auditor." SourceBSI – see the subsection "Recommending or appointing an auditor".

It was found in a personnal website published in an Enisa document CyberSecurity Assessments ver Jan2024

As of 19/06/2024, 8 CAB are accepted for BSI C5 :

- PwC Germany (DEU)
- HKKG (DEU)
- EY (DEU)

- BDO Deutschland (DEU)
- Rödl & Partner (DEU)
- TÜV Nord Group (DEU)
- Schellmann (US)
- Lazarus Alliance (US)

The uptodate list is in the GAIA-X registry.

8.6 SWIPO

As of the 13/06/2024, there is no CAB approved by SWIPO. You can find information regarding SWIPO at SWIPO Certification document.

As there is no SWIPO CAB, SWIPO permissible standard can be used only in case of declaration. SWIPO permissible standard can't be used if certification is needed.

8.7 Climate Neutral Data Center Pact

As of the 17/06/2024 the CNDC Pact is a self assessment. More information : CNDC.

As CNDC Pact is a self assessment, CNDC permissible standard can be used only in case of declaration. CNDC Pact permissible standard can't be used if certification is needed.

8.8 TISAX

The list of official TIXAS audit providers is located at https://enx.com/en-US/TISAX/xap/

As an example, the 11/06/2024 there were 15 assement bodies listed just in Germany. Worldwide accepted CAB will not be listed in this document. The up to date list is in the GAIA-X registry.

V. Annexes

9 Gaia-X Label format

In case of a valid verification and validation of the criteria for a specific assessment scheme, the accredited Gaia-X Compliance services are issuing a Gaia-X Label.

A Gaia-X Label is a machine readable, structured and signed document that comprises at a minimum the following information attributes:

- Label ID, as unique identifier for the label being issued for a specific Service Offering.
- Participant ID, as unique identifier for the Participant that is awarded the Label.
- Participant Business ID, presenting the firm business ID of the Participant.
- Service Offering for which the Label is applicable.
- Conformity assessment scheme, as Gaia-X Standard Compliance, Gaia-X Label Level 1, Gaia-X Label Level 2 or Gaia-X Label Level 3.
- Reference to the assessment scheme version that comprised the Gaia-X criteria for which the claims and evidences were prepared.
- Compliance Service ID, as unique identifier for the Compliance Service that issued the Label.
- Compliance Service version, as the software version that issued the Label.
- Issuance date on which the Label was issued.
- Validity start and end date on which the Label will expire.

> Tip
>
> In technical terms, a Gaia-X Label is a W3C Verifiable Credential and the JSON schema covering the above functional expectations is available via the Gaia-X Registry.

10 Gaia-X Power of Attorney format

To adapt to various organisation structures and introduce a mean for a party to delegate rights to another party, a power of attorney is useful.

A Gaia-X Power of Attorney is a machine readable, structured and signed document that comprises at a minimum the following information attributes:

- Power of Attorney ID, as unique identifier.
- Principal ID, as unique identifier for the Participant that signs the power of attorney.
- Principal cryptographic material reference, to enable the verification of the signature of the power of attorney.
- Authorised Participant ID, as unique identifier for the Participant to whom the powers are granted.
- Authorised Participant cryptographic material reference, to enable the verification of the signature of future claims signed by the Authorised Participant.
- A list of granted powers, either as text or preferably in a machine-readable format using a Domain Specific Language (DSL) like ODRL.
- Issuance date on which the power of attorney was issued.
- Validity start and end dates on which the power of attorney enters into force and will expire.

> Tip
>
> In technical terms, a Gaia-X Label is a W3C Verifiable Credential and the JSON schema covering the above functional expectations is available via the Gaia-X Registry.

11 Process description for how to become a Gaia-X compliant user

Assumed prerequisites:

1. the user is already familiar with the concepts of Gaia-X, like the Verifiable Credential model (digital signatures/using certificates/digital wallets).
2. the user has an EV SSL or an eIDAS certificate and the public part of the certificate is published via DID:WEB method.
3. the user is familiar with the workflow described in the Architecture Document.

A - The user wants to get Gaia-X Compliant Verifiable Credentials

B - The user decides what kind of Gaia-X Compliant Verifiable Credential to obtain from the ones made available by Gaia-X.

E.g.: LegalParticipant.

The list of available VCs can be retrieved from the Gaia-X Registry, using the /v1/api/trusted-shape-registry/v1/shapes/implemented endpoint.

C - The user decides the method to obtain the compliance

1. Through the Gaia-X Wizard: https://wizard.lab.gaia-x.eu/
2. Through direct API calls: https://compliance.gaia-x.eu/

Please note that third-party applications might also be integrated with the Gaia-X Compliance, but they are out of scope for this guide.

D - The user creates first their credential payload

Users create the payload with the mandatory attributes as well as optional attributes needed in their ecosystem. The mandatory attributes vary depending on the type of VC, and the full list of mandatory attributes can be retrieved from the Gaia-X Registry, using the /v1/api/trusted-shape-registry/v1/shapes endpoint.

E - The user signs their credentials with their private key

The https://wizard.lab.gaia-x.eu/ can also be used for this step, but the user is free to choose their preferred signing tool.

F - The user creates a Verifiable Presentation

The Verifiable Presentation includes all the Verifiable Credentials that are required to get the compliance for their Participant or their service. The https://wizard.lab.gaia-x.eu/ can also be used for this step, but the user is free to choose the tool of their choice.

G - The user calls the Gaia-X Compliance Service for their presentation

The Gaia-X Compliance Service is connected in the background with the available Clearing Houses, and the call will go to one of the GXDCH instances. But the experience is seamless for the user. The https://wizard.lab.gaia-x.eu/ can also be used for this step, but the user is free to choose their preferred tool. A direct API call is also possible. If a user wishes to use a specific clearing house instance, this option is available from:

1. the https://wizard.lab.gaia-x.eu/ by selecting a specific Clearing House from the drop-down menu.
2. calling directly the API of the clearing house. More information on how to obtain that can be found in the GXDCH documentation.

H1 - If the verification fails, an error message will be returned to the user to identify the issue

H2 - If the verification is successful, the user will receive a Gaia-X Verifiable Credential.

The Gaia-X Verifiable Credential contains the proof of the verification, signed by the Clearing House which did the verification.

After having received the Gaia-X Verifiable Credential one can claim they are a Gaia-X Conformant Legal Participant, or have Gaia-X Conformant Services based on the proof in the VC returned by the Compliance Service.

The Gaia-X Conformant VCs can be:

1. stored in JSON file format saved on the user's device.
2. stored in a digital wallet.
3. pushed to the Credential Event Service. This service is the base of the creation of Federated Catalogues.

12 Changelog

12.1 2025 March release (25.03)

- Insertion of Chapter 4 Gaia-X Compliance Criteria for Participants
- Restored the specification for criterion P1.1.2, which requires a declaration at the Standard Compliance level, following an editorial error in the previous release.

12.2 2024 November release (24.11)

- Criteria 1.3.2: only allow ISO 3166-2 information for headquarter localisation
- Criteria 3.1.18: add CISPE as permissible standard
- Criteria 3.1.18, 3.1.19: for Label level 2 and 3, allow declarations until additional permissible standards are approved by the Gaia-X Association
- Editorial changes

12.3 2024 June release (24.06)

- The Compliance Document is the new name of the PRC specifications document, which in the previous version was named as Policy Rules Conformity Document (PRCD).
- Consistent use of “Compliance scheme” instead of conformity, labels, and other variations.
- Replace “Conformity”/”Basic Conformity” by “Gaia-X Standard Compliance”.
- Update of the Gaia-X Trust Anchors chapter with the inclusion of the decision flowchart to determine which type of Trust Anchor must be defined for a given criteria and with the requirements for TSPs (Trust Service Providers) and the selection process for CABs.
- Introduction of the new chapter “List of Gaia-X Conformity Assessment Bodies” where all CABs, which are accredited to attest conformity against a permissible standard by the respective organizations body are listed.
- Update of the chapter Gaia-X Compliance Criteria for Cloud Services, with the detail of the required evidence for the first two compliance levels (Declaration evidence).
- Update of the chapter “Proposed Compliance for Data Exchange Services” with the specification of the conformity assessment required for the different schemes.

12.4 2024 April release (24.04)

- The PRCD is a combination of the previous Policy Rules and Labelling Document (PRLD) and Trust Framework, which are now obsolete.
- New “Executive Summary” chapter.
- New chapter on the Process description for how to become a Gaia-X conformant user.
- New chapter on the Self-Declaration of Conformity.
- Definition of Conformity and related criteria.
- New criteria and attributes (mandatory and optional) on “Sustainability”.
- New chapter on Proposed Data Exchange Criteria.
- Update and refinement of Permissible and Example Standards for Gaia-X Labels.