Gaia-X Labelling Criteria

14 February 2022
Version 0.7

Preface

The Gaia-X Labelling Criteria document links back to the Gaia-X Labelling Framework paper which was published in November 2021. The criteria, and the respective verification process in particular, are subject to a consultation process in Q1 2022.

Introduction

For Gaia-X to ensure a higher and unprecedented level of trust in digital platforms, we need to make trust an easy to understand and adopted principle. For this reason, Gaia-X developed a Trust Framework – formerly known as Gaia-X Compliance - and Labelling Framework that safeguards data protection, transparency, security, portability, and flexibility for the ecosystem as well as sovereignty and European Control.

The Trust Framework is 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 requirements from the Gaia-X Trust Framework.

The Trust Framework uses verifiable credentials and linked data representation to build a FAIR knowledge graph of verifiable claims from which additional trust and composability indexes can be automatically computed.

The Labelling Framework is based on the Trust Framework (named compliance framework in former documents) based on self-descriptions. 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. This Trust Framework is introduced in the Gaia-X Architecture Document, section 4.2.

The Labelling Framework itself is further detailed and translated into concrete criteria and measures in the Gaia-X Labelling Criteria document. The criteria list brings together the policies and requirements from the committees – Policies and Rules Committee, Technical Committee, Data Spaces and Business Committee – along with comprehensive verification means to ensure that these requirements can be met. It allows for further differentiation between services that is necessary for users wanting to find services for different purposes and with different needs. It defines minimum qualification levels for the attributes described in the transparency framework.

Design Principles

The Gaia-X Labelling Framework introduced a set of core principles that are being refined by the criteria.

Consistency among the Gaia-X ecosystem

Gaia-X Labels 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 Board of Directors. Hence, the following key principles for labelling are either directly adopted or derived from our main documents (i.e. the Gaia-X Architecture Document, the Gaia-X Policy Rules Document, or the Gaia-X Principles for Data Spaces) or have been widely adopted by the respective committees and will be published soon. Hence, the labelling criteria are always in line with the corresponding

concepts and papers.

Scalability and extensibility

Based on the three basic labels 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 labelling criteria by adding and defining on-top requirements for particular purposes. To ensure impact and consistency of Gaia-X Labels, new labels and extensions have to be authorized by the Gaia-X Association (Board of Directors).

Composability and modularity

Gaia-X Labels are logical groupings of composable service attributes. This results in particular in the assignment of a common set of policies, technical requirements and data spaces criteria to one or multiple of three levels.
At the same time, Gaia-X labels base upon existing schemes, certifications, testates and approved codes of conduct where possible to allow reuse of established standards and thereby simplifying 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.

Federation of Verification

Gaia-X labels are issued and verified 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. Verification processes defined by Gaia-X itself will also base on a federation of responsibilities.

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. Only the criteria defined by the DSBC apply to data-sharing networks and define the governance, usage policies and obligations among ecosystem partners.

Additional explanation: the ‘T-shirt sizes’ model

The framework contains several sections where the criterion itself is applicable to two or all three levels, while the requirements differ in how they are verified for each of the levels. These criteria can be recognized by the T-shirt sizes S/M/L in the assignment table for the respective criterion instead of the common check mark symbol. The different verification approaches are then further explained in the respective text for verifying entities and verification process.

Gaia-X Labelling Criteria

Data Protection

1. A contract or any other legal binding act under Union or Member State law addressing GDPR requirements is in place.

Source: PRD v2111, Chapter: 1.1.1

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

2. Role and responsibility of each party is defined.

Source: PRD v2111, Chapter: 1.1.2

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

3. Technical and organizational measures are clearly defined in accordance with roles and responsibilities of the parties, including an adequate level of detail.

Source: PRD v2111, Chapter: 1.1.3

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

4. Provider is ultimately bound to instructions of customer

Source: PRD v2111, Chapter: 1.2.1

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

5. It is clearly defined how customer may instruct, including by electronic means such as configuration tools or APIs.

Source: PRD v2111, Chapter: 1.2.2

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

6. It is clearly defined if and to which extent third country transfer will take place.

Source: PRD v2111, Chapter: 1.2.3

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

7. If and to the extent third country transfers will take place, it is clearly defined by which means of Chapter V GDPR those will be protected.

Source: PRD v2111, Chapter: 1.2.4

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

8. It is clearly defined if and to which extent sub-processors will be involved.

Source: PRD v2111, Chapter: 1.2.5

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

9. If and to the extent sub-processors will be involved, measures are in place regarding subprocessors management.

Source: PRD v2111, Chapter: 1.2.6

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

10. Provisions related to a customer audit right exist.

Source: PRD v2111, Chapter: 1.2.7

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

11. In case of a joint controllership an arrangement pursuant to Art. 26 GDPR is in place.

Source: PRD v2111, Chapter: 1.3.1

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

12. In case of a joint controllership, at a minimum, the very essence of such agreement is communicated to data subjects.

Source: PRD v2111, Chapter: 1.3.2

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

---

13. In case of a joint controllership, there is a point of contact for data subjects

Source: PRD v2111, Chapter: 1.3.3

Level 1	Level 2	Level 3
M	L	L

Verifying Entity: L1: Gaia-X AISBL or mandated entity (M)

L2/L3: CoC Art. 40: Competent authority accredited monitoring body or third party; Certification: Accredited CAB (ISO 17065) (L)

Verification Process: L1: self-verified through internal audit according to an approved CoC/Certification scheme and signed Gaia-X Self-Declaration (M)

L2 / L3: CoC (Art. 40): Evaluation by monitoring or third party; Certification (Art. 42): Inspection/Verification/Validation based on audit by CAB (L)

Accepted Standards: Codes of Conduct acc. Art. 40 GDPR (currently CISPE, EU Cloud CoC) or certifications acc. Art. 42 GDPR

Transparency

14. A legally binding contract between CSP and customer is in place.

Source: PRD v2111, Chapter: 2.1.1

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

15. General location of Asset is provided at urban area level.

Source: PRD v2111, Chapter: 2.1.3

Level 1	Level 2	Level 3
S	M	M

Verifying Entity: L1: Label Holder self-declares that this requirement is fullfilled (S)

L2 & L3: 3rd party / automatically verified (M)

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

16. Provisions governing the situation of service interruptions exist.

Source: PRD v2111, Chapter: 2.1.4

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

17. Provisions governing provider's bankruptcy or any other reason by which the provider may cease to exist in law, exist.

Source: PRD v2111, Chapter: 2.1.5

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

18. Provisions governing the rights of the parties to use the service and any data therein exist.

Source: PRD v2111, Chapter: 2.1.6

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

19. A Service Level Agreement exists

Source: PRD v2111, Chapter: 2.1.7

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

20. Provisions governing changes regardless of their kind, exist.

Source: PRD v2111, Chapter: 2.1.8

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

21. Provisions governing aspects regarding copyright or any other intellectual property rights, exist.

Source: PRD v2111, Chapter: 2.1.9

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

22. Contact details where customer may address any queries, incl. pre-contractual states, are being provided.

Source: PRD v2111, Chapter: 2.2.1

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

23. It is being defined by which means customer may verify Provider's compliance.

Source: PRD v2111, Chapter: 2.3.1

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

24. Applicable jurisdiction(s) of sub-contractors including sub-processors will be communicated to customer.

Source: PRD v2111, Chapter: 2.4.1

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

25. Provisions exist how sub-contractors and related data localization will be communicated

Source: PRD v2111, Chapter: 2.4.2

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

26. Service Offering shall include a policy using a common Domain-Specific Language (DSL) to describe Permissions, Requirements and Constraints.

Source: TAD v2109, Chapter: 4.1

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X Compliance Service Provider

Verification Process: Gaia-X Compliance Service checking the self-description

Accepted Standards: -

---

27. Service Offering requires being operated by service offering provider with a verified identity.

Source: TAD v2109, Chapter: 4.2 / 4.3

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X Compliance Service Provider

Verification Process: Gaia-X Compliance Service checking the self-description

Accepted Standards: -

---

28. Service Offering must provide a conformant self-description.

Source: TAD v2109, Chapter: 4.4 & 4.6.2

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X Compliance Service Provider

Verification Process: Gaia-X Compliance Service checking the self-description

Accepted Standards: -

---

29. Self-Description attributes need to be consistent across linked Self-Descriptions.

Source: TAD v2109, Chapter: 4.4 & 4.6.2

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X Compliance Service Provider

Verification Process: Gaia-X Compliance Service checking the self-description

Accepted Standards: -

---

30. Service Offering consumer needs to have a verified identity provided by the Federator

Source: TAD v2109, Chapter: 4.4.1

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X Compliance Service Provider

Verification Process: Gaia-X Compliance Service checking the self-description

Accepted Standards: -

Security

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

Source: PRD v2111, Chapter: 3.1

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

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

Source: PRD v2111, Chapter: 3.2

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

33. 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.

Source: PRD v2111, Chapter: 3.3

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

34. 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.

Source: PRD v2111, Chapter: 3.4

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

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

Source: PRD v2111, Chapter: 3.5

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

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

Source: PRD v2111, Chapter: 3.6

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

37. 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.

Source: PRD v2111, Chapter: 3.7

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

38. Identity, Authentication and access control management: Limit access to information and information processing facilities.

Source: PRD v2111, Chapter: 3.8

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

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

Source: PRD v2111, Chapter: 3.9

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

40. Communication Security: Ensure the protection of information in networks and the corresponding information processing systems.

Source: PRD v2111, Chapter: 3.10

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

41. Portability and Interoperability: Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.

Source: PRD v2111, Chapter: 3.11

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

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

Source: PRD v2111, Chapter: 3.12

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

43. Development of Information systems: Ensure information security in the development cycle of information systems.

Source: PRD v2111, Chapter: 3.13

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

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

Source: PRD v2111, Chapter: 3.14

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

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

Source: PRD v2111, Chapter: 3.15

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

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

Source: PRD v2111, Chapter: 3.16

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

47. Compliance: Avoid non-compliance with legal, regulatory, self-imposed or contractual

information security and compliance requirements.

Source: PRD v2111, Chapter: 3.17

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

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

Source: PRD v2111, Chapter: 3.18

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

49. 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 data.

Source: PRD v2111, Chapter: 3.19

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

---

50. Product safety and security: Provide appropriate mechanisms for cloud customers.

Source: PRD v2111, Chapter: 3.20

Level 1	Level 2	Level 3
S	M	L

Verifying Entity: L1: internal + ISO 17065 accredited auditor (S)

L2: ISO 17065 accredited auditor (M)

L3: ISO 17065 accredited auditor (L)

Verification Process: L1: internal audit verified by an ISO 17065 accredited external auditor (S)

L2: onsite assessment by ISO 17065 accredited auditor (M)

L3: L2 plus Critical Requirements for mission critical processes certified ISO 17065 accredited auditor (L)

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27xx, CSA, ENISA EUCS (as soon as available)

Portability

51. Implemented practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the Provider receiving the data.

Source: PRD v2111, Chapter: 4.1.1

Level 1	Level 2	Level 3
S	S	M

Verifying Entity: L1 & L2: Gaia-X AISBL or mandated entity (S)

L3: SWIPO-accredited CAB (M)

Verification Process: L1 & L2: self-verified through internal audit and signed Gaia-X Self-Declaration (S)

L3: SWIPO self-declaration (M)

Accepted Standards: SWIPO IaaS (and SaaS) CoC

---

52. Pre-contractual information exists, with sufficiently detailed, clear and transparent information regarding the processes of data portability, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another Provider or port data back to its own IT systems.

Source: PRD v2111, Chapter: 4.1.2

Level 1	Level 2	Level 3
S	S	M

Verifying Entity: L1 & L2: Gaia-X AISBL or mandated entity (S)

L3: SWIPO-accredited CAB (M)

Verification Process: L1 & L2: self-verified through internal audit and signed Gaia-X Self-Declaration (S)

L3: SWIPO self-declaration (M)

Accepted Standards: SWIPO IaaS (and SaaS) CoC

European Control

53. Provide mandatory option that data are processed and stored exclusively in EU/EEA for Level 2.

Source: PRD v2111, Chapter: 5.1

Level 1	Level 2	Level 3
	✓	

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

54. Data must be processed and stored exclusively in EU/EEA for Level 3.

Source: PRD v2111, Chapter: 5.1

Level 1	Level 2	Level 3
		✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

55. For Level 3 where the Provider or subcontractor is subject to legal obligations to transmit or disclose data on the basis of a non-EU statutory order, verified safeguards need to be in place that ensure that any access request is compliant with EU law.

Source: PRD v2111, Chapter: 5.1

Level 1	Level 2	Level 3
		✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

56. No access to customer data by provider, unless authorized by customer or required by EU law.

Source: PRD v2111, Chapter: 5.2

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

57. Provide option for each contract to be governed by EU Member State law.

Source: PRD v2111, Chapter: 5.3

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

58. The CSP's registered head office, headquarters and main establishment shall be established in a Member State of the EU.

Source: v2202, Chapter:

Level 1	Level 2	Level 3
		✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

59. Shareholders in the CSP, whose registered head office, headquarters and main establishment are not established in a Member State of the EU 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).

Source: v2202, Chapter:

Level 1	Level 2	Level 3
		✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

60. In the event of recourse by the CSP, in the context of the services provided to the CSC, 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 European Union, the third-party company shall have no access over the CSC data nor access and identity management for the services provided to the CSC. The CSP, including any of its sub-processor, shall push back any request received from non-European authorities to obtain communication of personal data relating to European Customers, except if request is made in execution of a court judgment or order that is valid and legally binding under Union law and applicable member states law as provided by Article 48 GDPR.

Source: v2202, Chapter:

Level 1	Level 2	Level 3
		✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

61. The CSP must guarantee continuous 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

Source: v2202, Chapter:

Level 1	Level 2	Level 3
		✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

Data Protection in Data Spaces

Subject of the following criteria are data sharing ecosystems rather than Cloud Service Offerings as applied for all previous criteria.

62. The contract or any other legal binding act under Union or Member State law shall address data exchange capabilities.

Source: DSBC EWG v2112, Chapter:

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

63. The contract for Data Exchange shall be, at a minimum, in textform.

Source: DSBC EWG v2112, Chapter:

Level 1	Level 2	Level 3

✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

64. The contract shall define the roles and responsibilities of the parties involved, in particular addressing data exchange.

Source: DSBC EWG v2112, Chapter:

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

65. According to the roles and responsibilities, technical and organizational measures are clearly defined including an adequate level of detail and explicitly addressing the data exchange.

Source: DSBC EWG v2112, Chapter:

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

66. Means shall, in particular, address usage policies (including data classification) and purpose conditions of use, limitations confidentiality, IP.

Source: DSBC EWG v2112, Chapter:

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

67. Measures to ensure data security (technical and legal security) are clearly defined in accordance with roles and responsibilities of the parties, including an adequate level of detail.

Source: DSBC EWG v2112, Chapter:

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

---

68. It is defined which party shall fulfill transparency obligations towards third parties.

Source: DSBC EWG v2112

Level 1	Level 2	Level 3
✓	✓	✓

Verifying Entity: Gaia-X AISBL or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -