gaia-x

Gaia-X Labelling Criteria

21 April 2022

Preface

The Gaia-X labelling criteria document links back to the Gaia-X labelling framework paper which was published in November 2021.

Introduction

For the Gaia-X Association 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 standardised 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.

However, it must be clarified that:

- Some of the rules are high level objectives and still need to be more detailed and specified to be implementable. The policy rules committee of Gaia-X with its 3 sub working groups will work on it on further versions. The next version will define the frequency of the updates of this document.
- Redundancies are acknowledged. They shall be resolved to the extent possible in the future iterations. Some redundancies are a result of externalities, such as underlying standards, schemes, laws which cannot be resolved.

- Some of the criteria can be further detailed with the relevant acceptable standards, in that case they are identified. There will be a process to identify additional standards and maintain already listed standards, which will follow good practices defining objective criteria. This shall ensure both quality of accepted standards and neutral and fair access.

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.

The reference numbers of the documents are the following:

- Gaia-X policy rules document – PRD 2204
- Gaia-X Architecture document – TAD2112

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 authorised by the Gaia-X Association (Board of Directors).

Composability and modularity

Gaia-X Labels are logical groupings of composable service attributes. This particularly results 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.

Standards, self-assessment, and Conformity Assessment Bodies (CAB)

Gaia-X labels do not reference text or standards which are not yet approved (example the current proposal of the data act or the EUCS) but tries to align with this moving target. Whenever these standards are approved, Gaia-X will adapt its labels in accordance with these standards. The process to add these new standards will

be detailed in a later version. The verification of the adherence to label criteria can be through self-assessment or external Conformity Assessment Bodies (CAB) as defined later on in this document.

Gaia-X service offerings are defined by provider generated self-descriptions which include claims of adherence to the labelling criteria. The proof of a validation of a claim will be technically realised through 'W3C verifiable credentials'. 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 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 self-description of the service offering and for each claim extract the entity and the result of the assessment.

The process including the possible process of revoking trust to specific CAB or revocation of validity of self-description is described in the Gaia-X 'trust framework;'.

Conformity Assessment Bodies (CAB): The Gaia-X Association reserves its right to choose its own CAB of its own three basic labels. A new detailed document will be issued on the process to choose the relevant CAB. Where the labelling framework lacks reference to accepted standards, Gaia-X will define a dedicated verification process including a process to appoint adequate a CAB (Conformity Assessment Body). Both processes will follow international recognized good practices, including impartiality, comparability, reliability, and accessibility.

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 be based 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.

Gaia-X Labelling Criteria

Contractual governance

Criterion 1: The provider shall offer the ability to establish a legally binding act. This legally binding act shall be documented

Source: PRD v2204, chapter: 1.1.1

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Criterion 2: The provider shall have an option for each legally binding act to be governed by EU/EEA/Member State law

Source PRD v2204, chapter 1.1.2

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Criterion 3: The provider shall clearly identify for which parties the legal act is binding

Source PRD v2204, chapter 1.1.3

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Criterion 4: The provider shall ensure that the legally binding act covers the entire provision of the service offering

Source PRD v2204, chapter 1.1.4

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Transparency

Criterion 5: 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

Source PRD v2204, chapter 1.2.1

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Criterion 6: The provider shall ensure there are provisions governing the rights of the parties to use the service and any data therein

Source PRD v2204, chapter 1.2.2

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

An accepted standard is ISO19944

Criterion 7: The provider shall ensure there are provisions governing changes, regardless of their kind

Source PRD v2204, chapter 1.2.3

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Criterion 8: The provider shall ensure there are provisions governing aspects regarding copyright or any other intellectual property rights

Source PRD v2204, chapter 1.2.4

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Criterion 9: The provider shall declare the general location of physicals Resources at urban area level.

Note: the urban area level is a geographical location more accurate than a country, province, or region.

Source PRD v2204, chapter 1.2.5

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Criterion 10: The provider shall explain how information about subcontractors and related data localisation will be communicated

Note: this applies to the subcontractors essential to the provision of the service offering, including any sub-processors

Source PRD v2204, chapter 1.2.6

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Criterion 11: The provider shall communicate to the customer where the applicable jurisdiction(s) of subcontractors will be

Note: this applies to the subcontractors essential to the provision of the Service Offering, including any sub-processors

Source PRD v2204, chapter 1.2.7

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Criterion 12: The provider shall include in the contract the contact details where customer may address any queries regarding the service offering and the contract

Note: Queries include request during the pre-contractual state, before coming to an agreement.

Source PRD v2204, chapter 1.2.8

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Criterion 13: The provider shall adopt the Gaia-X trust framework, by which customers may verify provider's compliance

Source PRD v2204, chapter 1.2.9

Applicable to all levels

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: self-assessment through the trust framework

Criterion 14: service offering shall include a policy using a common Domain-Specific Language (DSL) to describe permissions, requirements, and constraints

Source: TAD v2112, chapter: 4.1

Applicable to all levels

Verifying Entity: Gaia-X compliance service provider

Verification Process: Gaia-X trust framework checking the self-description

Criterion 15: service offering requires being operated by service offering provider with a verified identity

Source: TAD v2112, chapter: 4.2 / 4.3

Applicable to all levels

Verifying Entity: Gaia-X compliance service provider

Verification Process: Gaia-X trust framework checking the self-description

Criterion 16: service offering must provide a conformant self-description

Source: TAD v2112, chapter: 4.4 & 4.6.2

Applicable to all levels

Verifying Entity: Gaia-X compliance service provider

Verification Process: Gaia-X trust framework checking the self-description

Criterion 17: self-description attributes need to be consistent across linked self-descriptions

Source: TAD v2112, chapter: 4.4 & 4.6.2

Applicable to all levels

Verifying Entity: Gaia-X compliance service provider

Verification Process: Gaia-X trust framework

Criterion 18: service offering consumer needs to have a verified identity provided by the federator

Source: TAD v2112, chapter: 4.4.1

Applicable to all levels

Verifying Entity: Gaia-X compliance service provider

Verification Process: Gaia-X trust framework checking the self-description

Data Protection

Criterion 19: The provider shall offer the ability to establish a contract under Union or EU/EEA/member state law and specifically addressing GDPR requirements

Source PRD v2204, chapter 2.1.1

Verifying Entity: L1: Gaia-X Association or mandated entity

L2/L3: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process: L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 / L3: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

Criterion 20: The provider shall define the roles and responsibilities of each party

Note: This considers the roles and responsibilities of the parties involved in the scope of this service offering.

Source: PRD v2204, chapter: 2.1.2

Verifying Entity: L1: Gaia-X Association or mandated entity

L2/L3: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process: L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 / L3: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

Criterion 21: 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

Source: PRD v2204, chapter: 2.1.3

Verifying Entity: L1: Gaia-X Association or mandated entity

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

Verification Process: L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 / L3: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

Criterion 22: The provider shall be ultimately bound to instructions of the customer

Source: PRD v2204, chapter: 2.2.1

Verifying Entity: L1: Gaia-X Association or mandated entity

L2/L3: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process: L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 / L3: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

Criterion 23: The provider shall clearly define how customer may instruct, including by electronic means such as configuration tools or APIs

Source: PRD v2204, chapter: 2.2.2

Verifying Entity: L1: Gaia-X Association or mandated entity

L2/L3: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process: L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 / L3: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

Criterion 24: The provider shall clearly define if and to which extent third country transfer will take place

Source: PRD v2204, chapter: 2.2.3

Verifying Entity:

L1: Gaia-X Association or mandated entity

L2: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process: L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

This rule is not applicable to level 3.

Criterion 25: 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

Source: PRDv2204, chapter 2.2.4

Verifying Entity:

L1: Gaia-X Association or mandated entity

L2: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process:

L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

This rule is not applicable for level 3

Criterion 26: The provider shall clearly define if and to which extent sub-processors will be involved

Source: PRD v2204, chapter: 2.2.5

Verifying Entity:

L1: Gaia-X Association or mandated entity

L2/L3: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process:

L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 / L3: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

Criterion 27: 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

Source: PRD v2204, chapter: 2.2.6

Verifying Entity:

L1: Gaia-X Association or mandated entity

L2/L3: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process: L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 / L3: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

Criterion 28: The provider shall define the audit rights for the Customer

Source: PRD v2204, chapter: 2.2.7

Verifying Entity:

L1: Gaia-X Association or mandated entity

L2/L3: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process: L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 / L3: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

Criterion 29: In case of a joint controllership, the provider shall ensure an arrangement pursuant to Art. 26 (1) GDPR is in place

Source: PRD v2204, chapter: 2.3.1

Verifying Entity:

L1: Gaia-X Association or mandated entity

L2/L3: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process: L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 / L3: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

Criterion 30: In case of a joint controllership, at a minimum, the provider shall ensure that the very essence of such agreement is communicated to data subjects

Source: PRD v2204, chapter: 2.3.2

Verifying Entity:

L1: Gaia-X Association or mandated entity

L2/L3: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process: L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 / L3: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

Criterion 31: In case of a joint controllership, the provider shall publish a point of contact for data subjects

Source: PRD v2204, chapter: 2.3.3

Verifying Entity:

L1: Gaia-X Association or mandated entity

L2/L3: CoC Art. 40: competent authority accredited monitoring body or third party; certification: accredited CAB (ISO 17065)

Verification Process: L1: self-verified through internal audit according to an approved CoC/certification scheme and signed Gaia-X self-declaration

L2 / L3: CoC (Art. 40): evaluation by monitoring or third party; certification (Art. 42): inspection/verification/validation based on audit by CAB

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

Security

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 consequently these criteria. Therefore, the terms on the different criteria on this item should be read in the light of EUCS

Criterion 32: Organisation of information security: plan, implement, maintain, and continuously improve the information security framework within the organisation

Source: PRD v2204, chapter: 3.1.1

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognized standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 33: Information Security Policies: Provide a global information security policy, derived into policies and procedures regarding security requirements and to support business requirements

Source: PRD v2204, chapter: 3.1.2

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 34: 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 v2204, chapter: 3.3.3

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 35: Human Resources: Ensure that employees understand their responsibilities, are aware of their responsibilities regarding information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination

Source: PRD v2204, chapter: 3.3.4

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 36: Asset Management: Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.

Source: PRD v2204, chapter: 3.3. 5

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 37: Physical Security: Prevent unauthorised physical access and protect against theft, damage, loss, and outage of operations

Source: PRD v2204, chapter: 3.3. 6

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 38: 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 v2204, chapter: 3.3.7

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 39: identity, authentication, and access control management: limit access to information and information processing facilities

Source: PRD v2204, chapter: 3.3. 8

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 40: cryptography and key management: ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity, or integrity of information

Source: PRD v2204, chapter: 3.3.9

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 41: communication security: Ensure the protection of information in networks and the corresponding information processing systems

Source: PRD v2204, chapter: 3.3. 10

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 42: 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

Remark: this objective should be understood in the context of cybersecurity. Further portability objectives are defined in criteria 52 and 53

Source: PRD v2204, chapter: 3.3.11

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 43: change and configuration management: ensure that changes and configuration actions to information systems guarantee the security of the delivered cloud service

Source: PRD v2204, chapter: 3.3.12

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 44: development of information systems: ensure information security in the development cycle of information systems

Source: PRD v2204, chapter: 3.3.13

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 45: Procurement Management: Ensure the protection of information that suppliers of the CSP can access and monitor the agreed services and security requirements

Source: PRD v2204, chapter: 3.3.14

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 46: incident management: Ensure a consistent and comprehensive approach to the capture, assessment, communication, and escalation of security incidents

Source: PRD v2204, chapter: 3.3. 15

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 47: business continuity: plan, implement, maintain, and test procedures and measures for business continuity and emergency management

Source: PRD v2204, chapter: 3.3.16

This criterion is consistent with criterion 60 (chapter European control)

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA.

Criterion 48: compliance: avoid non-compliance with legal, regulatory, self-imposed, or contractual information security and compliance requirements

Source: PRD v2204, chapter: 3.3.17

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 49: user documentation: provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers

Source: PRD v2204, chapter: 3.3.18

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 50: 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 v2204, chapter: 3.3.19

Assessing Entity:

L1: internal + authorised entity according to the EUCS Level Basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Criterion 51: product safety and security: provide appropriate mechanisms for cloud customers

Source: PRD v2204, chapter: 3.3.20.

Assessing Entity:

L1: internal + authorised entity according to the EUCS level basic; ad interim: internal+ external confirmation that the internal audit followed recognised standards and/or good practices

L2: Assessing entity authorised according to the respective standards

L3: Assessing entity authorised according to the respective standards

Assessment Process:

L1: internal audit; externally confirmed to be following recognised standards and/or good practices

L2: onsite assessment following assessment process according to the respective standards

L3: According to process for EUCS Level High; ad interim: see Level 2

Accepted Standards: if scope is matching: C5, TISAX, SOC2, SecNumCloud, ISO 27001, CSA

Portability

Criterion 52: The provider shall implement practices for facilitating the switching of 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

Note: The customer can act as an intermediary for transferring data between providers, e.g., by executing the provided tools to execute the transfer.

Note: The 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.

Source: PRD v2204, chapter: 4.1.1

Verifying Entity:

L1 & L2: Gaia-X Association or mandated entity

L3: SWIPO-accredited CAB

Verification Process:

L1 & L2: self-verified through internal audit and signed Gaia-X self-declaration

L3: SWIPO self-declaration

Accepted Standards: SWIPO IaaS, SaaS and merged code CoC

Criterion 53: The provider shall ensure 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 v2204, chapter: 4.1.2

Verifying Entity:

L1 & L2: Gaia-X Association or mandated entity

L3: SWIPO-accredited CAB

Verification Process:

L1 & L2: self-verified through internal audit and signed Gaia-X self-declaration

L3: SWIPO self-declaration (M)

Accepted Standards: SWIPO IaaS, SaaS merged code CoC

European Control

Criterion 54: For label level 2, the provider shall provide the option that all data are processed and stored exclusively in EU/EEA

Source: PRD v2204, chapter: 5.1.1

This criterion is only required for level 2

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: Gaia-X self-declaration through the trust framework

Accepted Standards: -

Criterion 55: For label level 3, the provider shall process and store all data exclusively in the EU/EEA.

Source: PRD v2204, chapter: 5.1.2

This criterion is only required for level 3

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: Gaia-X self-declaration through the trust framework

Accepted Standards: -

Criterion 56: For label level 3, where the provider or subcontractor is subject to legal obligations to transmit or disclose data based on 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

Source PRD 2204, chapter 5.1.3

Note – the safeguards are specified in criteria 57 to 60

Source: PRD v2204, Chapter: 5.1.3

This criterion is only required for level 3

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: Gaia-X self-declaration

Accepted Standards: -

Criterion 57: 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

Source PRD 2204, chapter 5.1.4

This criterion is required only for level 3

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: Gaia-X self-declaration

Accepted Standards: -

Criterion 58: 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 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 PRD2204, chapter 5.1.5

This criterion is required only for level 3

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: Gaia-X Self-Declaration

Accepted Standards: -

Criterion 59: 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-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 compliant under Union law and applicable member states law as provided by Article 48 GDPR

Source: PRD2204, chapter 5.1.6

This criterion is required only for level 3

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: Gaia-X self-declaration

Accepted Standards: -

Criterion 60: For label level 3, the provider 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: PRD2204, chapter 5.1.7

This criterion is only required for level 3

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: Gaia-X self-declaration

Accepted Standards: -

Criterion 61: The provider shall not access customer data unless authorised by the customer or when the access is in accordance with EU/EEA/member state law

Source: PRD2204, chapter 5.2.1

This criterion is required for all 3 levels

Verifying Entity: Gaia-X Association or mandated entity

Verification Process: Gaia-X self-declaration

Accepted Standards: -

Data Protection in Data Spaces

All these criteria will be detailed in a further version of this document.