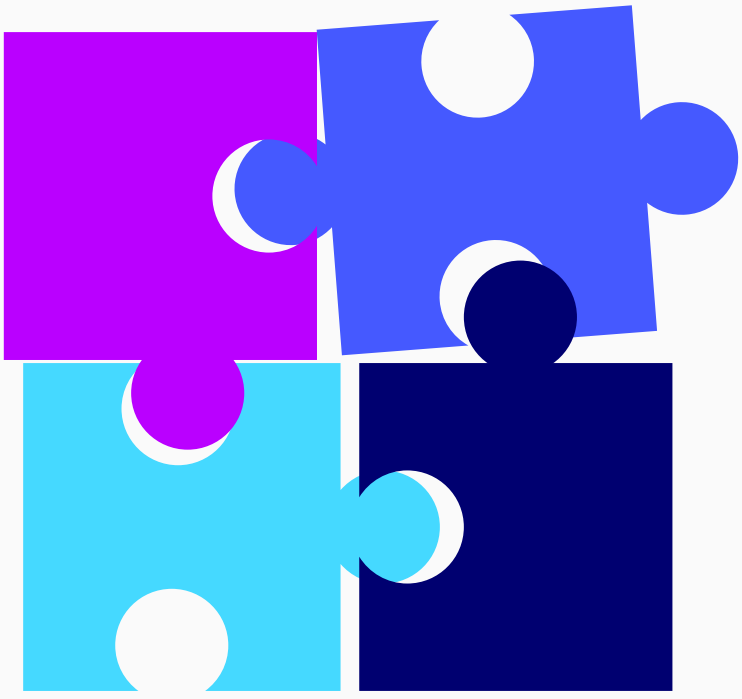
gaia-x

Policy Rules Document

(PRD 21.11)

Table of Contents



Dear all who have commented, contributed and given feedback to the policy rules document (PRD) 21.04,

Thank you very much for your input, which has been viewed and discussed. The result is PRD 21.11 presented herewith. On some topics and paragraphs, we received widely differing views and opinions, while others will require further discussion. These are the topics on the PRC's workstack for the next months that will find their way into the next issue, most likely PRD 22.04.

Meanwhile, please provide any further feedback on this PRD 21.11.

All the best wishes,

Dr. Ulrich Eichhorn, Chair PRC

Alban Schmutz, Vice-Chair PRC

Preamble

The following Policy Rules define High Level Objectives safeguarding the added value and principles of the Gaia-X ecosystem. It intents to identify clear controls to demonstrate European values of Gaia-X, such as Openness, Transparency, Data Protection, Security and Portability. Each service offering to be provided under the Gaia-X framework umbrella shall comply with the following objectives. In general, full adherence to applicable EU legislation (e.g., in areas such as data protection and security) is a prerequisite and thus not waived or affected by the following policies and rules.

Principally, High Level Objectives in section B1 reflect GDPR requirements without extending GDPR's obligations.

It is worth pointing out, that participation within Gaia-X and providing Gaia-X compliant services, shall not prevent any provider from also provide non-Gaia-X service offerings outside the Gaia-X ecosystem.

Compliance with these Policy Rules objectives can be achieved via compliance with standards, certifications, and codes of conduct. Where such tools are not available or approved to demonstrate such compliance, specific methodologies can be developed further and agreed within Gaia-X to be included in the self-description of services.

A. Definitions

There will be a 'Uniform Gaia-X Glossary' to be developed between the TC, the DSBC and the PRC. When available, it will supersede the local definitions. Meanwhile, the following definitions are valid:

1. A **Resource**[2] is an internal building block, not available for order, used to compose Service Offerings. Resource Categories include:

- **Data Resource:** providing for data (which may include derived data) in any form and includes the necessary information for data sharing.
- **Software Resource:** non-physical functions.
- **Node:** a computational or physical entity that hosts, manipulates, or interacts with other computational or physical entities.
- **Interconnection:** details of the connection between two or more Nodes.

Prominent attributes of a Resource are the location - physical address, Autonomous System Number, network segment, and the jurisdiction affiliations.

2. A **Service Offering** is a set of resources bundled into an offering. A Service Offering can be nested with one or more service offerings.

3. A **Provider** is a Participant who provides resources and service offerings in the Gaia-X ecosystem.

Note: The service(s) offered by a Provider are cloud and/or edge services. Thus, the Provider will typically be acting as a Cloud Service Provider (CSP) to their Consumers.

4. A **Participant** is an entity which is identified, onboarded, and has a Gaia-X Self-Description. A Participant can take on one or multiple of the following roles: Provider, Consumer, Federator.

5. 'Data' is subject to current work in progress. It is expected to provide a definition either in the Uniform Gaia-X Glossary or in the next iteration of the PRD. For the time being, data shall be understood as customer data and meta-data, potentially including personal data. Where personal data is concerned, compliance with relevant provisions in regards of the protection of personal data (Section B) is mandatory.

2 Resource replaces the term 'Asset' in the technical documents of Gaia-X since the last publication of the PRD. The definition is transferred to this version of the PRD acknowledging that the adaptation shall be subject to further analysis. Where necessary, either the uniform definition will be adapted or deviations for the use within the PRD shall be decided.

B. Cloud Service Provider

1. General Data Protection Regulation (GDPR)

1.1 General

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

1.1.2 the Roles and responsibilities of each party are defined.

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

1.2 Art. 28 GDPR

1.2.1 The provider is ultimately bound to customer instructions.

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

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

1.2.4 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.

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

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

1.2.7 Provisions related to a customer audit right exist.

1.3 Art. 26 GDPR

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

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

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

Possible Third Party Verification of Reference for Section 1
Mechanisms pursuant to Art. 40 / 42 GDPR

2. Transparency

2.1 Contract between CSP and Customer

2.1.1 A legally binding contract is in place

2.1.2 General location of Resource is provided at urban area level

2.1.3 Provisions governing the situation of service interruptions exist

2.1.4 Provisions governing Provider's bankruptcy or any other reason by which the Provider may cease to exist in law, exist

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

2.1.6 A Service Level Agreement exists

2.1.7 Provisions governing changes, regardless of their kind, exist

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

2.2 Resource

2.2.1 Contact details where customer may address any queries are being provided

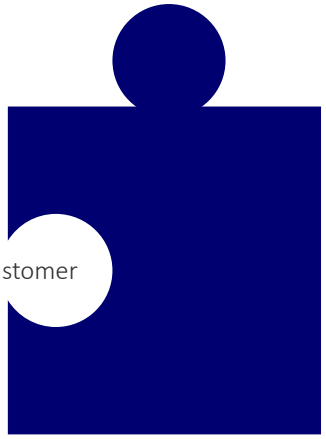
2.3 Compliance

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

2.4 Sub-Contractors

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

2.4.2 Provisions exist how sub-contractors and related data localisation will be communicated.



3. Cyber Security[2]

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

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

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

3.4 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.

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

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

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

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

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

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

3.11 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.

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

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

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

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

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

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

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

3.19 Dealing with information requests from government agencies: Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.

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

Possible Third-Party Verification of Reference for Section 3
Certification according to ENISA Cloud security certification framework can be considered: e.g. ISO 27k certification with appropriate scope, SecNum Cloud certification with appropriate scope, C5 attestation with appropriate scope.

2 The HLO in this section are taken form the ENISA Cloud security certification and will be constantly reviewed until finalization of the ENISA Cloud security certification scheme. Where appropriate the PRD will be updated accordingly. Note: in this section terms are used as defined in the ENISA Cloud security certification scheme.

4. Portability

4.1 Switching and porting of data

The section refers to the application of Art. 6 Free Flow of Data Regulation (FFoDR).

4.1.1 Implemented 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.

4.1.2 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.

Possible Third-Party Verification of Reference for Section 4
Code of Conduct pursuant Art. 6 FFoDR.

5. Contract

5.1 Processing and storing of data in EU/EEA

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

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

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

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

5.2 Access to data

5.2.1 No access to customer data by Provider, unless authorised by customer or required by EU law.*

5.3 Contract governance

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

C. Data Sharing within data spaces

1.1 The data provider shall attach the usage policies including data classification to the data assets to be shared in a machine-readable way according to GaiaX description standards.*

1.2 The data consumer shall respect those usage policies by taking the appropriate technical/organisational means to safeguard secure transfer, integrity, confidentiality and traceability on the use of the data.*

* HLO highlighted with "*" have not been updated based on the contributions received via the consultation in summer 2020. Next iterations of the PRD will consider such contributions and update the HLO where necessary.