Dear Gaia-X contributors, friends and fellows,

We are pleased to announce that a new draft version of the Policy Rules Document is now available. We invite you to comment and give feedback on the document. The **consultation phase** starts on 26 April 2021 and runs **until 10 June 2021**.

Please find the link to all relevant documents for the consultation in this folder: https://community.gaia-x.eu/s/q47ZfYEJCzzWCMC

After you have made your comments, you can upload the feedback documents here: https://community.gaia-x.eu/s/33gGq3WG6rc7AZM

We thank you in advance for your feedback and look forward to hearing from you.

Yours sincerely,

Policy Rules Committee Gaia-X AISBL

Policy Rules Document

(PRD 21.04)

22 April 2021

Preamble

The following Policies Rules define High Level Objectives safeguarding the added value and principles of the Gaia-X ecosystem. Gaia-X's Policy Rules intend is to identify clear controls to demonstrate European values of Gaia-X, such values including Openness, Transparency, Data Protection, Security and Portability. Each and every service offering to be provided under the umbrella / via the Gaia-X framework shall comply with all of 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.

It is worth pointing out, that participation within Gaia-X and providing Gaia-X compliant services, shall not prevent any provider to 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 definitions document to be developed between the TC and the PRC when available it will supersede the local definitions. For the time being this document, the following definitions are valid:

1. An Asset is an element used to compose the Service Offering, which does not expose an endpoint.

2. A Service Offering is a set of Assets and Resources, which a Provider bundles into an offering. A Service Offering can be nested with one or more Service Offerings.

3. A provider is a Participant who provides Assets and Resources in the Gaia-X ecosystem.

4. A Participant is an entity, as defined in ISO/IEC 24760-1, 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.

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 Role and responsibility of each party is defined.

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

1.2 Art. 28 GDPR

1.2.1 Provider is ultimately bound to instructions of customer.

1.2.2 It is clearly defined how 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

2.1.1 A legally binding contract is in place.

2.1.2 Foreign applicable laws outside EU/EEA are defined and transparency must be provided.

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

2.1.4 Provisions governing the situation of service interruptions exist.

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

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

2.1.7 A Service Level Agreement exists.

2.1.8 Provisions governing changes regardless of their kind, be it e.g., legally, technically, organisationally, exist.

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

2.2 Asset

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

2.3 Compliance

2.3.1 It is being defined by which means customer may verify providers 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 localization will be communicated.

3 Cyber Security[1]

3.1 Organization 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 with regard to 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 their 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.

[1] Certification according to ENISA Cloud security certification framework (when available); this process have to be reviewed.

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

3.11 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: Provide 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: also taken into consideration can be e.g. ISO 27k certification with appropriate scope, SecNum Cloud certification with appropriate scope, C5 attestation with appropriate scope

4 Portability

4.1 Art. 6 Free Flow of Data Regulation (FFoDR)

4.1.1 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 service 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 service 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 Option to process and store data exclusively in EU/EEA.

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

5.3 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 Gaia-X description standards.

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

./.