gaia-x

Policy Rules Document

(PRD 22.04)

A. Preamble

The following policy rules define high level objectives safeguarding the added value and principles of the Gaia-X ecosystem. To allow for validation, the high-level objectives are underpinned by the actual requirements of the suitable criteria catalogues, as further specified in the Gaia-X Label and Trust Framework documents.

The intent of the policy rules is to identify clear controls to demonstrate European values of Gaia-X, such values including openness, transparency, data protection, security, and portability. Each service offering to be provided under the umbrella or via the Gaia-X framework shall comply with all the following objectives. In general, full adherence to applicable EU/EEA 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 compliant services under the Gaia-X framework 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 established standards, certifications, and codes of conduct. The addition and maintenance of these accepted standards will be performed as part of the labeling criteria document (WG labeling) and in the trust framework document (WG compliance). Where such tools are not available or approved to demonstrate such compliance, specific methodologies can be further developed and agreed within Gaia-X to be included in the self-description of service offerings.

For these high-level objectives, we follow the current discussions on the european cybersecurity certification scheme for cloud services (the EU cloud services scheme or EUCS). When the EUCS is finalised, Gaia-X may consider adapting the objectives in this document.

The Association will update this document on a regular basis.

B. Cloud Service Provider

Note: we use the term 'provider' throughout this section as the short denominator for a cloud service provider or CSP, i.e., the participant who provides cloud service offerings in the Gaia-X ecosystem. We use the term 'customer' in this section to denominate the cloud service customer, i.e., the participant who consumes a service offering from a cloud service provider.

1 Contractual Framework

This section reflects provisions associated to the contractual framework between a 'provider' and a 'customer', required for any service offering regardless of its type, purpose, or processed category of data. It divides in requirements related to the governance of contract and material aspects that shall be addressed in contracts. This section, and subordinate criteria shall not provide exact and exhaustive contractual language. It shall rather allow providers to reflect the requirements subject to their individual needs of structure and language.

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

1.1 Contractual governance

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

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

Note: The legally binding act can be a contract.

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

1.1.2 The provider shall have an option for each legally binding act to be governed by EU/EEA/member state law

1.1.3 The provider shall clearly identify for which parties the legal act is binding

1.1.4 The provider shall ensure that the legally binding act covers the entire provision of the service offering

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

1.2 General material requirements and transparency

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

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

1.2.3 The provider shall ensure there are provisions governing changes, regardless of their kind

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

1.2.5 The provider shall declare the general locations of physical resources at an urban area level

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

1.2.6 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.

1.2.7 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

1.2.8 The provider shall include in the contract the contact details where the 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

1.2.9 The provider shall adopt the Gaia-X trust framework, by which customers may verify the provider's service offering

Note: The Gaia-X compliance verification is based on the trust framework and based on self-descriptions validated by verifiable credentials.

2 General Data Protection Regulation (GDPR)

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

2.1 General

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

Note: GDPR requires union or member state law to be applicable. The provider needs to ensure a process that guarantees that a legally binding act is in place before delivering any form of service

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

2.1.2 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

2.1.3 The provider shall clearly define the technical and organisational measures in accordance with the roles and responsibilities of the parties, including an adequate level of detail

2.2 GDPR Art. 28

2.2.1 The provider shall be ultimately bound to instructions of the customer

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

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

2.2.4 The provider shall clearly define if and to the extent third country transfers will take place, and by which means of Chapter V GDPR these transfers will be protected

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

2.2.6 The provider shall clearly define if and to the extent sub-processors will be involved, and the measures that are in place regarding sub-processors management

2.2.7 The provider shall define the audit rights for the customer.

2.3 GDPR Art. 26

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

2.3.2 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

2.3.3 In case of a joint controllership, the provider shall publish a point of contact for data subjects.

3 Cybersecurity

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

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

3.1.2 Information security policies: provide a global information security policy, derived into policies and procedures regarding security requirements and to support business requirements

3.1.3 Risk management: ensure that risks related to information security are properly identified, assessed, and treated, and that the residual risk is acceptable to the provider

3.1.4 Human resources: ensure that employees understand their responsibilities; are aware of their responsibilities regarding information security, and the organisation's assets are protected in the event of changes in responsibilities or termination

3.1.5 Asset management: identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle

3.1.6 Physical security: prevent unauthorised physical access and protect against theft, damage, loss, and outage of operations

3.1.7 Operational security: ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging, and monitoring events, and dealing with vulnerabilities, malfunctions, and failures

3.1.8 Identity, authentication, and access control management: limit access to information and information processing facilities

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

3.1.10 Communication security: ensure the protection of information in networks and the corresponding information processing systems

3.1.11 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.

Remark: this objective should be understood in the context of cybersecurity. Further portability objectives are defined in section 4

3.1.12 Change and configuration management: ensure that changes and configuration actions to information systems guarantee the security of the delivered cloud service

3.1.13 Development of information systems: ensure information security in the development cycle of information systems

3.1.14 Procurement management: ensure the protection of information that suppliers of the Provider can access and monitor the agreed services and security requirements

3.1.15 Incident management: The provider shall ensure a consistent and comprehensive approach to the capture, assessment, communication, and escalation of security incidents

3.1.16 Business continuity: The provider shall plan, implement, maintain, and test procedures and measures for business continuity and emergency management

Note: this rule is consistent with rule 5.1.7, which is more advanced in the case of label level 3

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

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

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

3.1.20 Product safety and security: provide appropriate mechanisms for cloud customers to enable product safety and security.

4 Portability

The section refers to the application of Art. 6 (1) Free Flow of Data Regulation (FFoDR). It applies to any service offering, regardless of its provider, type, purpose, or processed category of data.

4.1 Switching and porting of data

4.1.1 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

4.1.2 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.

5 European Control

This section applies to any service offering, regardless of its provider, type, purpose, or processed category of data. However, requirements shall only apply subject to the indicated labels. This section

aims for addressing the customer's or domain specific needs, e.g., by limiting storage and/or processing to the area of EU/EEA.

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

5.1 Processing and storing of data in EU/EEA

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

5.1.2 For label level 3, the provider shall process and store all data exclusively in the EU/EEA

5.1.3 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

5.1.4 For label level 3, the provider's registered head office, headquarters and main establishment shall be established in a member state of the EU/EEA

5.1.5 For label level 3, shareholders in the provider, whose registered head office, headquarters, and main establishment are not established in a member state of the EU/EEA shall not, directly, or indirectly, individually, or jointly, hold control of the provider. Control is defined as the ability of a natural or legal person to exercise decisive influence directly or indirectly on the provider 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)

5.1.6 For label level 3, in the event of recourse by the provider, in the context of the services provided to the customer, to the services of a third-party company - including a subcontractor - whose registered head office, headquarters and main establishment is outside of the European Union or who is owned or controlled directly or indirectly by another third-party company registered outside the EU/EEA, the third-party company shall have no access over the customer data nor access and identity management for the services provided to the customer. The provider, including any of its sub-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

5.1.7 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

5.2 Access to data

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.

C. Data Sharing within data spaces

Next to the rules for cloud service providers in the previous section, we anticipate that additional rules will be defined for the participants in data spaces and data sharing ecosystems. This is currently work-in-progress. Relevant objectives and guidelines will be elaborated and provided in a future version of this policy rules document.