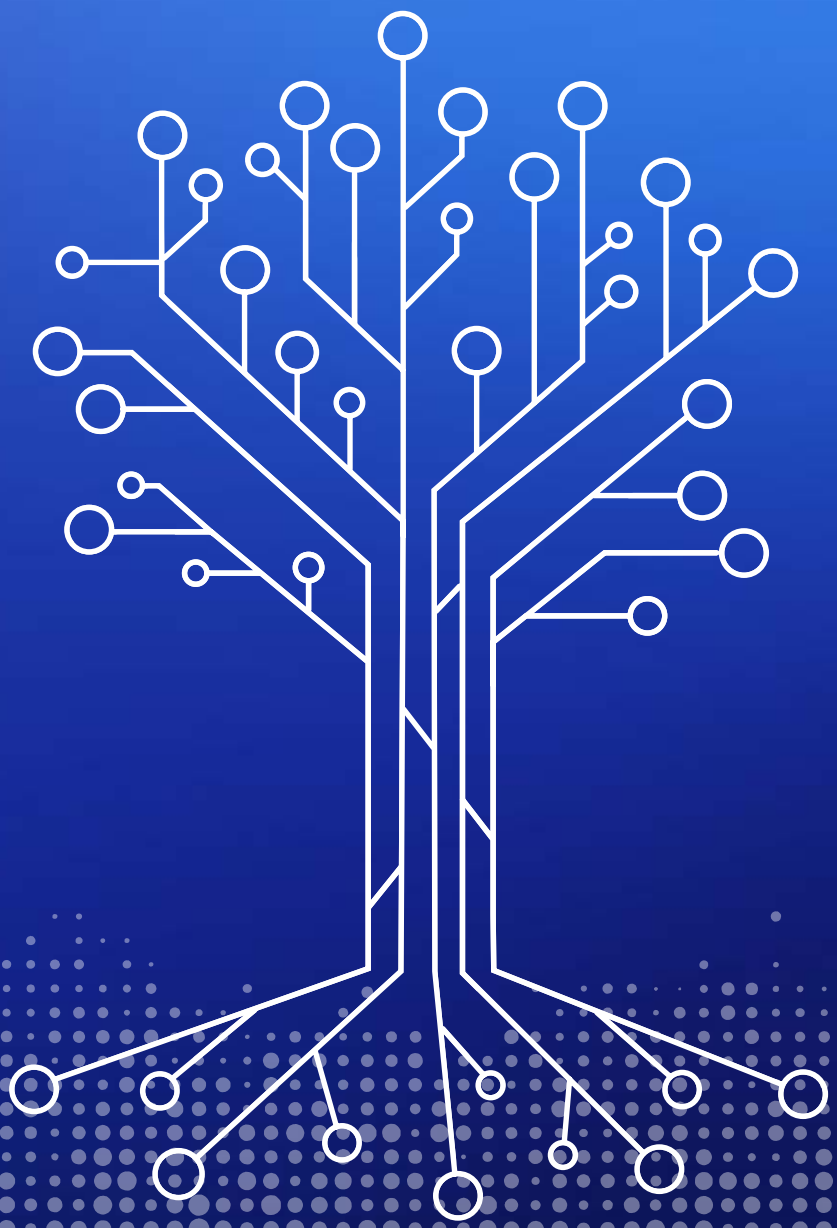
GAIA-X

GAIA-X: Policy Rules and Architecture of Standards



Imprint

Publisher
Federal Ministry for Economic Affairs and Energy
Public Relations Division
11019 Berlin
www.bmwi.de

Status
Mai 2020

Design
PRpetuum GmbH, 80801 Munich

This publication as well as further publications can be obtained from:
Federal Ministry for Economic Affairs and Energy (BMWi)
Public Relations
E-mail: publikationen@bundesregierung.de
www.bmwi.de

Central procurement service:
Tel.: +49 30 182722721
Fax: +49 30 18102722721

Content

Preamble

In the GAIA-X project, several European countries have joined forces to create a federated data infrastructure for Europe, its states, companies and citizens; a data infastructure that answers the needs of European industry in terms of digital sovereignty while promoting innovation and competitiveness for European stakeholders.

GAIA-X will enable mechanisms for the transparent, self-determined sharing and processing of data across different parties and will ensure that data-driven value creation remains with the individual participants. It will do this by defining the applicable policy rules and standards for federated ecosystems.

As already stated in the Franco-German position paper published on 18 February 2020, the values underpinning GAIA-X consist of:

1. European data protection
2. Openness, reversibility, and transparency
3. Authenticity and trust
4. Digital sovereignty and self-determination
5. Free market access and European value creation
6. Modularity and interoperability
7. Federation of infrastructure

This document can be seen as the starting point for a European process in which the European rules, regulations, laws and policies relevant to GAIA-X are identified and compiled.

The PRAAS document is also a basis for the active integration of GAIA-X into the processes connected with the EU Data Strategy. In particular, these steps support the proper implementation of existing regulations on data protection[1], reversibility[2] and security[3], and also include the intended regulations on a European Data Space and the fostering of data sharing. In that sense, GAIA-X can be seen as the nucleus of the European Federated Data Infrastructure.

1 EU General Data Protection Regulation (GDPR)

2 EU Free Flow of non-personal Data Regulation (FFoD), Art. 6 “Data Porting”

3 EU Cybersecurity Act

Objective of the document

The objectives outlined in this document describe a first methodology to collect relevant standards, policies and open APIs as crucial enablers for data sharing, interconnectivity and interoperability.

An important aim is to ensure a highest level of data protection, security, transparency, and portability/ reversibility.

In a federated infrastructure, the adherence of all components to common “ground rules” is of paramount importance. Those rules form the foundation of compliance to the GAIA-X framework and are also the basis for the certification and on-boarding process of GAIA-X.

This document focuses on providing a common understanding of how mutually agreed policies and rules underpin the guiding principles of GAIA-X.

Furthermore, it outlines the goal of GAIA-X to be based on standardised components and reversibility principles which guarantee openness, transparency, and integration of all relevant stakeholder communities.

In the appendix, there are two tables:

- GAIA-X Policy Rules for Infrastructure
- GAIA-X Policy Rules for Data & Software

and a description of a process to compile relevant standards:

- Architecture of Standards (AoS).

Policies and rules

Policies and rules form the basis of compliance to the GAIA-X framework. The participants using that framework accept data and infrastructure policy rules in a cross-company, sector, and cross-sector innovation ecosystem. This acceptance is achieved by mutual agreements on a set of policy rules, which are based on the European regulatory frameworks, and may include further requirements. The adherence to these policies and rules form a central element of the certification and on-boarding process of services to GAIA-X: all services declared within the GAIA-X ecosystem will have to respect the relevant policy rules. Moreover, companies not respecting such rules will not be allowed to be part of any of the GAIA-X governance mechanisms.

Examples are rules and policies:

- Concerning the processing of personal identifiable information according to the EU GDPR by fulfilling the relevant acknowledged criteria.

- On the compliance of all GAIA-X services to cybersecurity requirements (EU Cybersecurity Act), ensuring that all GAIA-X services provide an adequate level of security throughout the GAIA-X Ecosystem with regard to categories such as information security policies; personnel and training; asset management; identity and access management; cryptography and key management; physical infrastructure security; operational security and communications security.

- On portability and reversibility of data as outlined in the free flow of non-personal data regulation of the EU. Portability and reversibility are indispensable preconditions for avoiding lock-in effects and to give the user a free choice of compatible technical infrastructures.

- On transparency for contractual terms and conditions. For companies to become a GAIA-X provider, they will have to comply with the policies of that framework for collaborative development and sharing of data, giving the owner of the data the ability to exclusively decide on the usage of the data that is provided.

The first draft on existing policies and rules has been initially provided by a Franco-German working group. Due to the specifics of the respective service models, separate documents for IaaS and Data & Software were compiled. These GAIA-X Policy Rules for Infrastructure and for Data & Software summarise the current set of policies and can be found in Annex I to this document. The sets of rules will be regularly updated (up to twice a year) and the final versions are subject to the GAIA-X governance process.

Architecture of standards

Applicable standards are the key to set up a functioning sovereign infrastructure across Europe, enabling interoperability between different nodes, user-friendly service opportunities, exchangeability among different service providers in a sovereign data market, and the collaboration and data exchange between edge instances and cloud instances.

Various accepted standards and reference architectures for these areas do already exist or are currently under development. The Architecture of Standards (AoS) document describes a governed process that analyses and integrates already existing standards for data and sovereignty as well as infrastructure components (Annex II of this document). This AoS includes the process of mapping of applicable standards to the objectives of creating the GAIA-X Ecosystem. The AoS combines regulatory, industry-specific and technical standards to support the Federation Services implemented in the future GAIA-X Ecosystem.

Process

In the dynamic environment of platforms and services for innovative applications, the set of policy rules and applicable standards is steadily evolving. Therefore, the Franco-German working group drafted the first version to monitor relevant policy rules and standards and is continuously updating them. This work will be enhanced through further discussions with the EC and with other partners in Europe soon. Besides, France and Germany will intensify the interaction with user communities throughout Europe to define relevant use case scenarios. These use case scenarios are essential tools for analysing business requirements based on customer journeys and include additional necessary policy rules and standards applications.

Appendix

GAIA-X Policy Rules for Infrastructure (V1.1)

TOPIC	POLICY RULE	Included in the description of the service (Machine Readable)	Mandatory or Optional	Validation Mechanism : Self declaration or Third Party certified (may be through a Code of Conduct)	Tool	Comment
	RULES TO BE APPLIED TO THE PROVIDER					
POLICY	Public declaration of Adherence to the principles set out in Art. 6 of the Free Flow of Data Regulation of the European Union	Yes	Mandatory	Self Declaration	URL	
	The cloud provider shall regularly review the implementation of all GAIA-X Policy Rules examined in this catalogue in an internal audit procedure. For this purpose, the cloud provider defines control procedures and responsibilities.	No	Mandatory	Self Declaration or Third Party certified		
	At least one service declared, once GAIA-X in production phase.	No	Mandatory	Self Declaration or Third Party certified		
POLICY	Portability of licences: floating licences available in the same conditions than pay as you go model.	No	Mandatory	Self Declaration		
	RULES TO BE APPLIED TO THE SERVICE (INFRASTRUCTURE)					
LOCATION	Ability to choose data stored and processed within EU/EEA	Yes	Mandotory	Third Party Certified	CISPE Data Protection Code of Conduct	
LOCATION	Transparency Non-EU Applicable Extraterritorial Regulations	Yes	Mandotory	Self Declaration		Detailed list to be machine readable: Cloud Act, Patriot Act, China...
CONTRACT	No access to customer data by Cloud Infrastructure Provider, unless specifically authorized by the customer	Yes	Mandotory	Third Party Certified	CISPE Data Protection Code of Conduct	
SECURITY	European Cloud Security Certification - High or equivalent	Yes	Optional	Third Party Certified	ENISA Guidance (SecNumCloud ? C5 ?)	A list of equivalent Information security certifications/ attestations will be compiled and will follow the guidance of the ENISA
SECURITY	European Cloud Security Certification - Substantial or equivalent	Yes	Optional	Third Party Certified	ENISA Guidance (SecNumCloud ? C5 ?)	
SECURITY	European Cloud Security Certification - Basic or equivalent	Yes	Mandotory	Self declaration* (to be checked by independant Monitoring Body)	ENISA Guidance	
CONTRACT	The infrastructure cloud provider ensures, with appropriate technical or organisational precautions, that the cloud service is only provided after the conclusion of a legally binding contract with the cloud user.	No	Mandatory	Self Declaration or Third Party certified		
CONTRACT	The contract between the infrastructure cloud service provider and the cloud user clearly defines the respective role and shared responsibilities of the cloud provider and the cloud user with respect to security and data protection compliance as well as the technical config-uration of the environment.	No	Mandatory	Self Declaration or Third Party certified		
CONTRACT	The contract between infrastructure cloud provider and data controller falls under the jurisdiction of an EU member state	Yes	Mandatory	Self Declaration or Third Party certified		
CONTRACT	The legally binding contract provides that all data will only be processed upon documented instruction by the cloud user	No	Mandatory	Self Declaration or Third Party certified		
DATA PROTECTION	Where the cloud user uses cloud services to process personal data, the infrastructure cloud provider is a processor that shall comply with all obligations applicable to processors under GDPR.	No	Mandatory for services processing PII	–	CISPE Data Protection Code of Conduct	
DATA PROTECTION	The cloud provider shall not process cloud user personal data for data mining, profiling or marketing pruposes nor for accessing such cloud user personal data unless if it is necessary to provide the cloud sevices.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures that the processing of the cloud user's personal data is only carried out on the cloud user's instructions in accordance with the processing agreement.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider shall provide the cloud user with privacy, security, design and management information, in order to enable the cloud user to perform security and data protection impact assessments.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		

GAIA-X Policy Rules for Infrastructure (V1.1) (Continued)

TOPIC	POLICY RULE	Included in the description of the service (Machine Readable)	Mandatory or Optional	Validation Mechanism : Self declaration or Third Party certified (may be through a Code of Conduct)	Tool	Comment
DATA PROTECTION	For cloud services offering the possibilily for the data to be processed in different locations outside of the EEA and unless such data are only routed through such locations, the circum-stances of the transfer and appropriate safeguard shall be set out in the agreement entered into between the cloud user and the infrastructure cloud provider.	Yes	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures, with appropriate measures, that the cloud user has the opportunity to carry out the rectification and completion of personal data itself, or have it carried out by the infrastructure cloud provider.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures that the cloud user has the opportunity to carry out the erasure of personal data itself, or have it carried out by the cloud provider.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures that the cloud user has the opportunity to restrict the processing of personal data itself, or have the restriction carried out by the cloud provider.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	Where the infrastructure cloud provider is obligated to designate a data protection officer (DPO), it shall appoint one on the basis of professional qualities and expert knowledge of data protection law and practices, as well as on the basis of the ability to fulfil the tasks referred to in Article 39 GDPR	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider shall require an independent and external third party to regularly control the compliance of the cloud provider with these data protection requirements.	Yes	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures by the application of appropriate technical or organisational measures the confidentiality, veracity and availability of the data of the controller. Risk appropriate transfer encryptiono. Traceability of data processingo. Separate processingo. Restorabilty after incidentso ...	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
DATA PROTECTION	The infrastructure cloud provider ensures that a cloud service is only provided with the inclusion of sub-processors processing cloud user's data, if and to the extent that the cloud user has agreed to this sub-processing beforehand in the contract.	Yes	Mandatory for services processing PII	Self Declaration or Third Party certified		
SUB-PROCESSOR	The infrastructure cloud provider ensures that its sub-processors only act on the basis of a legally binding sub-processing agreement that is in accordance with the contract entered into between the cloud provider and cloud user.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
SUB-PROCESSOR	The infrastructure cloud provider informs the cloud user about the identity of all sub-processors processing the cloud user's data it involves at all levels as well as of any intended change of such sub-proccessors.	No	Mandatory for services processing PII	Self Declaration or Third Party certified		
REPORTING	The infrastructure cloud provider must notify the cloud user immediately in the event in which, during the period of validity of the contract the location of data processing changes from the one specified in the agreement for reasons in the area of responsibility of the cloud provider	No	Optional	Self Declaration or Third Party certified		
REPORTING	The infrastructure cloud provider ensures, with appropriate measures, that it notifies personal data breaches and their extent to the cloud user without undue delay.	No	Mandatory	Self Declaration or Third Party certified		
REPORTING	The infrastructure cloud provider shall maintain a record of processing activities composed of the information it has visibility on.	No	Mandatory	Self Declaration or Third Party certified		
REVERSIBILITY	Adherence to the principles of porting of data as described in Art. 6 of the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IaaS Code of Conduct; https://swipo.eu	

GAIA-X Policy Rules for Data & Software (V1.1)

TOPIC	POLICY RULE	Included in the description of the service (Machine Readable)	Mandatory or Optional	Validation Mechanism : Self declaration or Third Party certified (may be through a Code of Conduct)	Tool	Comment
	RULES TO BE APPLIED TO THE PROVIDER					
POLICY	Public declaration of Adherence to the principles set out in Art. 6 of the Free Flow of Data Regulation of the European Union	Yes	Mandatory	Self Declaration	URL	
POLICY	The cloud provider shall regularly review the implementation of all GAIA-X Policy Rules examined in this catalogue in an internal audit procedure. For this purpose, the cloud provider defines control procedures and responsibilities.	No	Mandatory	Self Declaration or Third Party certified		
POLICY	At least one service declared, once GAIA-X in production phase.	No	Mandatory	Self Declaration or Third Party certified		
POLICY	Portability of licences: floating licences available in the same conditions than pay as you go model.	No	Mandatory	Self Declaration		
	RULES TO BE APPLIED TO THE SERVICE (INFRASTRUCTURE)					
LOCATION	Ability to choose data stored and processed within EU/EEA		Mandatory	Third Party Certified	CISPE Data Protection Code of Conduct	
LOCATION	Transparency Non-EU Applicable Extraterritorial Regulations		Mandatory	Self Declaration		Detailed list to be machine readable: Cloud Act, Patriot Act, China...
SECURITY	European Cloud Security Certification – High		Optional	Third Party Certified	ENISA Guidance (SecNumCloud ? C5 ?)	Decision to be made, once the ENISA output is clear based on the Cybsercurity Act. Tansition mechanism (SecNum Cloud and/or C5) to be agreed until ENISA scheme made public.
SECURITY	European Cloud Security Certification – Substantial		Optional	Third Party Certified	ENISA Guidance (SecNumCloud ? C5 ?)	
SECURITY	European Cloud Security Certification – Basic		Mandatory	Self declaration* (to be checked by independant Monitoring Body)	ENISA Guidance	
REVERSIBILITY	Adherence to the principles of porting of data as described in Art. 6 of the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IaaS Code of Conduct; https://swipo.eu	
GDPR CONTRACT	The infrastructure cloud provider ensures, with appropriate technical or organisational precautions, that the cloud service is only provided after the conclusion of a legally binding contract with the cloud user.		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR CONTRACT	The contract between the infrastructure cloud service provider and the cloud user clearly defines the respective role and shared responsibilities of the cloud provider and the cloud user with respect to security and data protection compliance as well as the technical configuration of the environment.		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR CONTRACT	The contract between infrastructure cloud provider and data controller falls under the jurisdiction of an EU member state		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR CONTRACT	The legally binding contract provides that all data will only be processed upon documented instruction by the cloud user		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider shall not process cloud user personal data for data mining, profiling or marketing purposes nor for accessing such cloud user personal data unless if it is necessary to provide the cloud sevices.		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The contract between CSP and data controller falls under the jurisdiction of an EU member state		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The subject-matter and the duration of the processing must be outlined as specifically as possible in the legally binding agreement on the order processing		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The legally binding data processing agreement provides that all data will only be processed upon documented instruction by the controller		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	

→

GAIA-X Policy Rules for Data & Software (V1.1) (Continued)

TOPIC	POLICY RULE	Included in the description of the service (Machine Readable)	Mandatory or Optional	Validation Mechanism : Self declaration or Third Party certified (may be through a Code of Conduct)	Tool	Comment
GDPR DATA PROTECTION	The cloud provider ensures by the application of appropriate technical or organisational measures the confidentiality, veracity and availability of the data of the controller		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that the processing of the cloud user's data is only carried out on the cloud user's instructions		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The obligations of the cloud provider to return data media, return data and erase data after the end of the data processing must be set out in a legally binding order processing agree-ment		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that a cloud service is only provided with the inclusion of sub-processors, if and to the extent that the cloud user has agreed to this sub-processing beforehand in writing or text form.		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that its sub-processors only act on the basis of a legally binding sub-processing agreement that is in accordance with the legally binding processing agreement between the cloud provider and cloud user		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider informs the cloud user about the identity of all sub-processors it involves at all levels		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The obligations of the cloud provider to return data media, return data and erase data after the end of the data processing must be set out in a legally binding order processing agreement		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider must notify the cloud user immediately in the event in which, during the period of validity of the agreement, the place of data processing changes from the one specified in the agreement for reasons in the area of responsibility of the cloud provider		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures, with appropriate measures, that it notifies personal data breaches and their extent to the cloud user without undue delay		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider shall maintain a up-to-date record of processing activities		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that the cloud user has the opportunity to provide data subjects with information about the data processing and give them a copy of the personal data, or arrange this via the cloud provider.		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures, with appropriate measures, that the cloud user has the opportunity to carry out the rectification and completion of personal data itself, or have it carried out by the cloud provider		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that the cloud user has the opportunity to carry out the erasure of personal data itself, or have it carried out by the cloud provider		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that the cloud user has the opportunity to restrict the processing of personal data itself, or have the restriction carried out by the cloud provider		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	Where the cloud provider is obligated to designate a data protection officer (DPO), it shall appoint one on the basis of professional qualities and expert knowledge of data protection law and practices, as well as on the basis of the ability to fulfil the tasks referred to in Article 39 GDPR		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider shall only process the cloud user's personal data where this is required to achieve the specified purposes of the processing		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider ensures that the cloud user has the opportunity to transmit the personal data provided by a data subject to this person or another controller in a structured, commonly used and machine-readable format, or have it transmitted by the cloud provider		Mandatory	Self Declaration or Third Party certified	IAAS GDPR Document	
GDPR DATA PROTECTION	The cloud provider assists the cloud user in the execution of its data protection impact assessment. If the cloud provider is aware of a high risk of processing due to a data protection impact assessment carried out beforehand by the cloud user, the cloud provider must take risk-appropriate precautions.		Mandatory	Self Declaration or Third Party certified	SAAS GDPR Document	
DATA SHARING	The components used for sharing data shall provide a sufficiently high degree of trust and security regarding the in-tegrity, confidentiality and availability of information exchanged.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	

GAIA-X Policy Rules for Data & Software (V1.1) (Continued)

TOPIC	POLICY RULE	Included in the description of the service (Machine Readable)	Mandatory or Optional	Validation Mechanism : Self declaration or Third Party certified (may be through a Code of Conduct)	Tool	Comment
DATA SHARING	The components used for sharing data allow each other to check integrity of each other's software stack via remote attestation.	Yes	Mandatory		DIN SPEC 27070	
DATA SHARING	The components used for sharing data allow data providers to define usage policies that will be published together with the data offered.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	
DATA SHARING	Components used for data sharing shall provide a self-description (i.e. metadata) via a defined interface.	Yes	Mandatory	Self Declaration	DIN SPEC 27070	
	Components used for data sharing offering data send usage policy to be applied to components requesting data every time connection is established.	Yes	Mandatory		DIN SPEC 27070	
DATA SHARING	The components used for sharing data shall facilitate technical enforcement of data usage policy specified.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	
DATA SHARING	The administrators of the data provider side cannot change rules regarding data flow without data provider taking notice of the change and approving it.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	
DATA SHARING	The components used for sharing data verify authenticity and integrity of all system components prior to execution.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	
DATA SHARING	The components used for data sharing shall log each access control decision, every access to data, any changes made to its configuration and every case in which a service receives fewer resources than requested in the form of an integrity protected log entry in its domain.	Yes	Mandatory	Third Party certified	DIN SPEC 27070	
DATA SHARING	The data consumer and provider shall identify its organization via unified digital identities.	Yes	Mandatory	Third Party certified	eIDAS regulation Nr. 910/2014	
DATA SHARING	The data consumer and provider shall identify the components used for data sharing and processing via unified digital identities.	Yes	Mandatory	Third Party certified	eIDAS regulation Nr. 910/2014	

GAIA-X Architecture of Standards („AoS“)

Addressing key objectives of GAIA-X

The objectives described in the core positioning paper and further consultation with other interested parties outlined the implementation of services towards a *“highest level of data protection, security, transparency and portability/reversibility“* and encouraged to *“investigate the need of an overall far-reaching target architecture“*.

This document describes an initial methodology to reference technical standards (e.g. for IAM, Common Data Standards...) and to collect relevant standards, policies and open APIs as key enablers for Data Sharing, Portability and Interoperability.

AoS and Policies

These set of policies are being mapped to already existing set of policies in the context of the GAIA-X objectives which are being defined by existing governance bodies and applicable for the EU. For companies to become GAIA-X provider they will have to comply to the policies as set by the GAIA-X stakeholders. Figure 1 provides an illustrative example of such a retrieval. The mapping to existing policy and Code of Conduct (CoC) documents has been initially provided by a sub working group. The official requirement list is subject to a GAIA-X governance process as predefined in the Working Group “Certification and Accreditation”.

“Architecture of Standards” will extend the concept of policies with a set of regulatory and technical standards which shall ensure that a provider being compliant to the GAIA-X “Architecture of Standards”.

Figure 1: Relation Objectives, Policies and AoS to existing Initiatives and Stakeholder

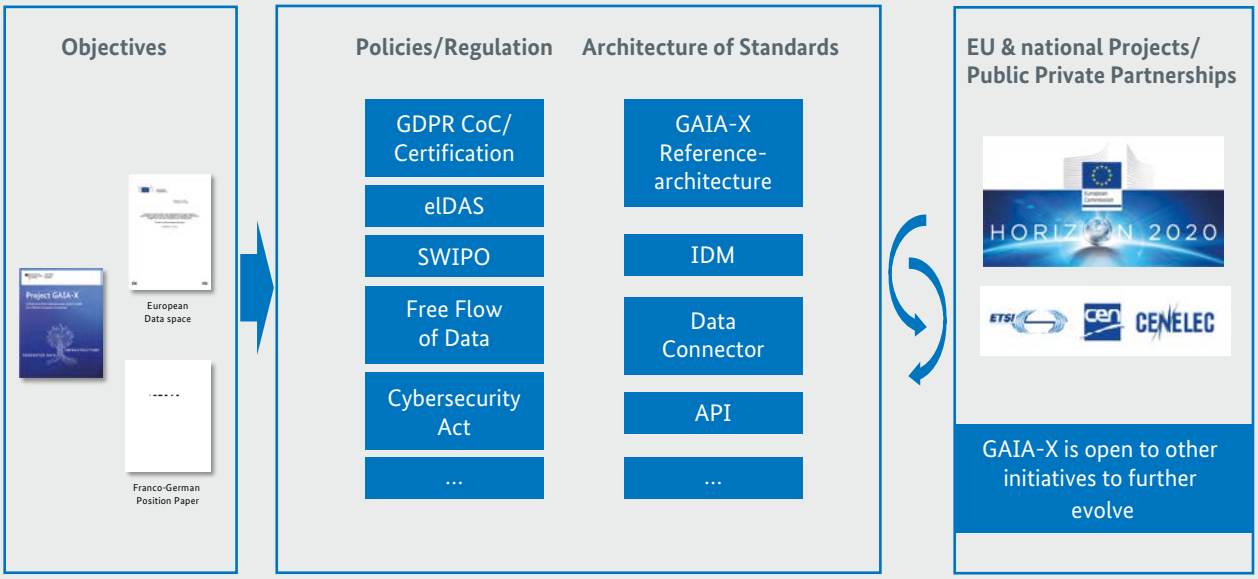
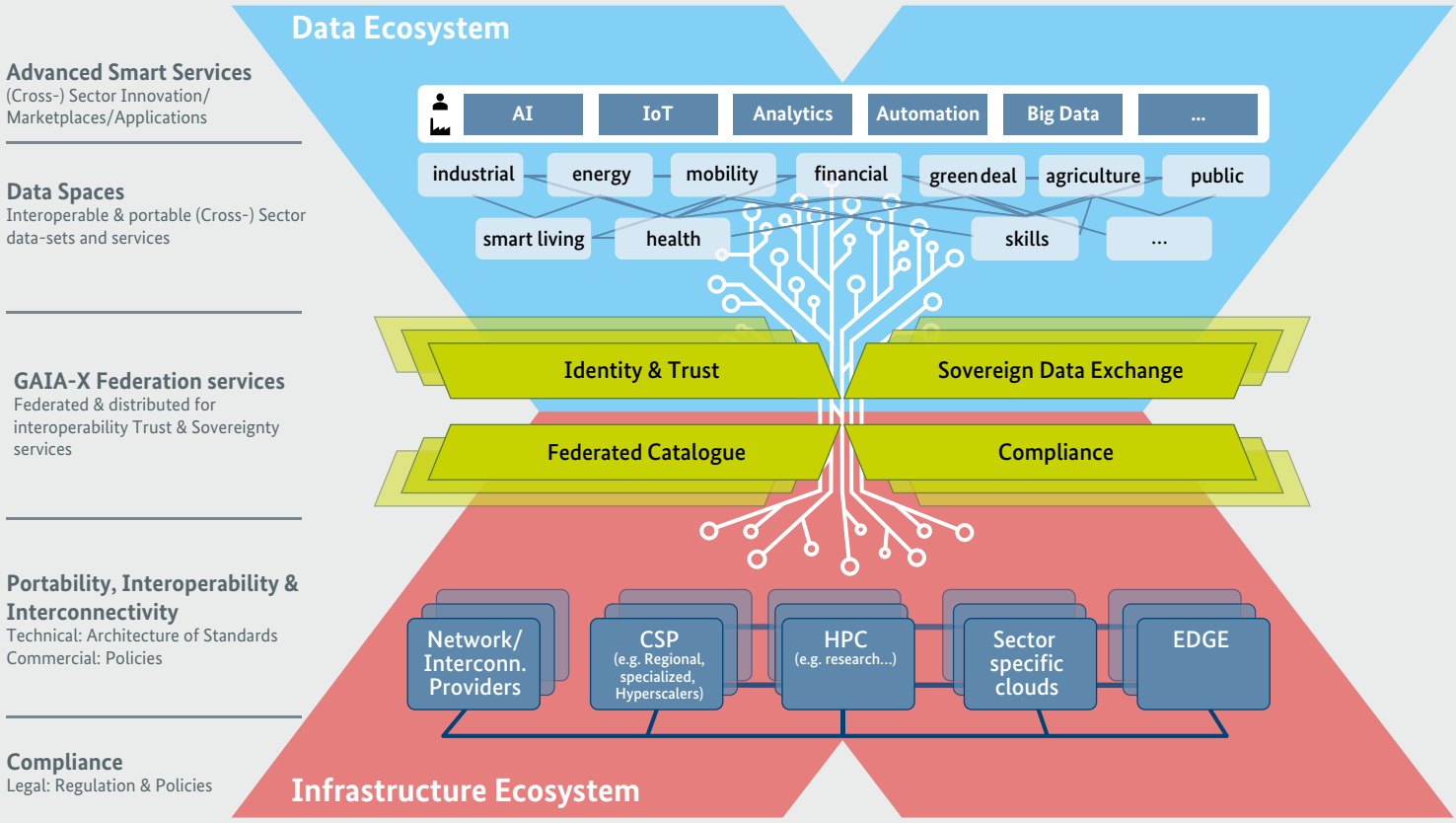


Figure 2: GAIA-X Overview



AoS and governing bodies

There are different roles in the overall GAIA-X setup and an Architecture of Standards needs to reflect those setups, in general:

- Regulatory standards: This relates specifically to legal and regulatory standards set in a jurisdictive
- Industry specific standards: Industry groups have been working on the definition of vertical ontologies and API's; depending on specific privacy rules or business criticality specific industry compliance rules may be defined
- Technical Standards: Interoperability across providers requires a level of standardization across different technical building blocks.

In general, the mapping of technology and policy sections will lead to a summary of GAIA-X Core Building Blocks with reference to

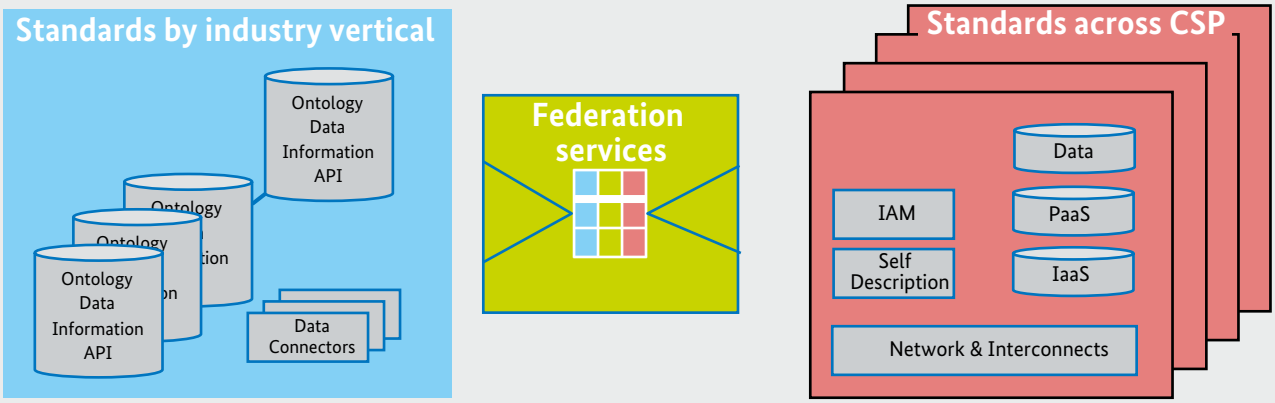
- Technical Standards
- Governance entities
- Regulatory working groups
- Public Private Partnerships

to assemble the landscape of standards for GAIA-X.

End to End compliance, interoperability and portability

Mapping the standards to the objectives and policies enables an ecosystem, which gives assurance to all participants. Smart services build on top support the creation of compliant innovation services, fulfilling the key objectives of GAIA-X.

Figure 3: Mapping of different standards

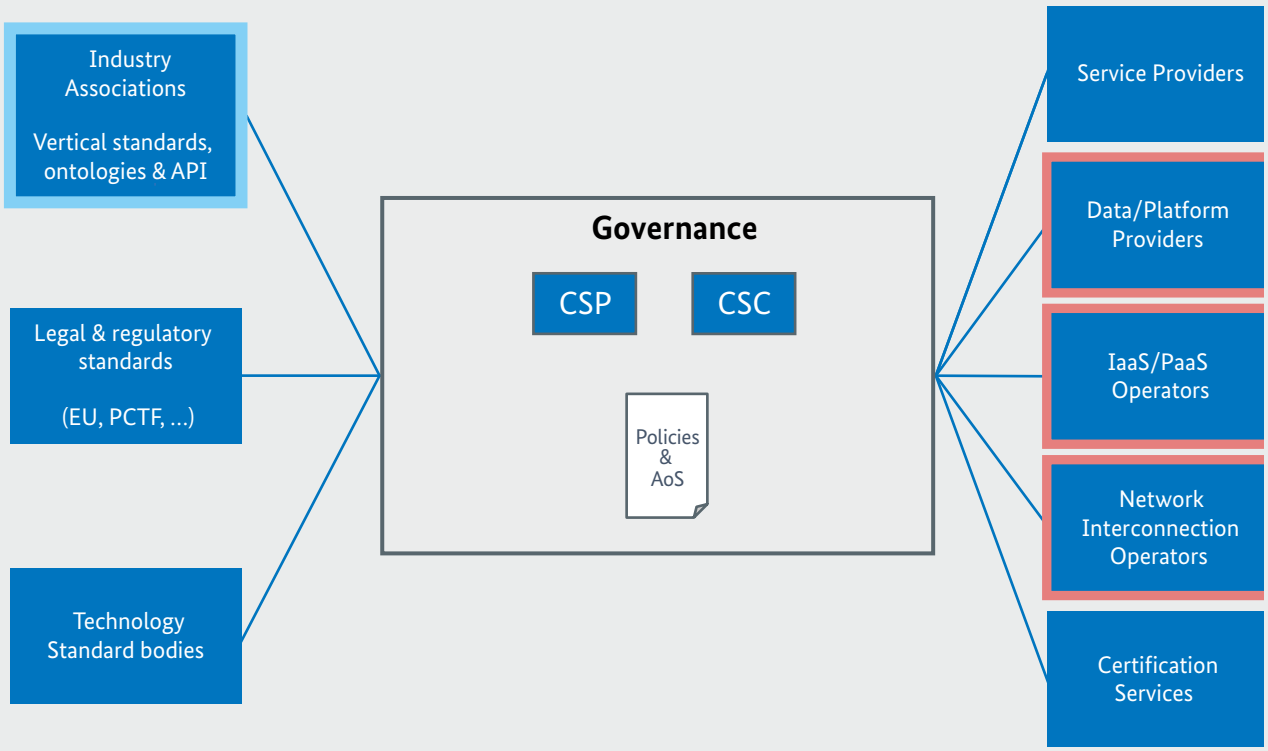


Definition of Ontologies, specific APIs (and their semantic), required technology standards and compliance defined by (existing) **Industry Associations**

Federated trust and sovereignty services across different consumers and providers (where needed)

Alignment of technical standards and set of technologies/products across Cloud Service providers provide
- Interoperability
- Portability

Figure 4: Impact of Policy rules and AoS on future governance structure



AoS Governance

As standards continuously evolve, GAIA-X should establish a governance that manages the evolution of the PRAAS (“Policy, Rules, Architecture Standards”) documents. The interfaces to the other standard bodies communicate both ways: feeding GAIA-X requirements into existing standards as well as providing input from innovation driven by the various external standard bodies. As the impact to the provider- and consumer data and -ecosystems needs to be assessed, cloud service providers and cloud services consumers need to be able to provide input into the decision process.

All these activities are subject of ongoing consultation with relevant bodies out of the EU, like ETSI, CEN and CENELEC as most relevant European Standard Organizations (ESO).

AoS Guiding Principles

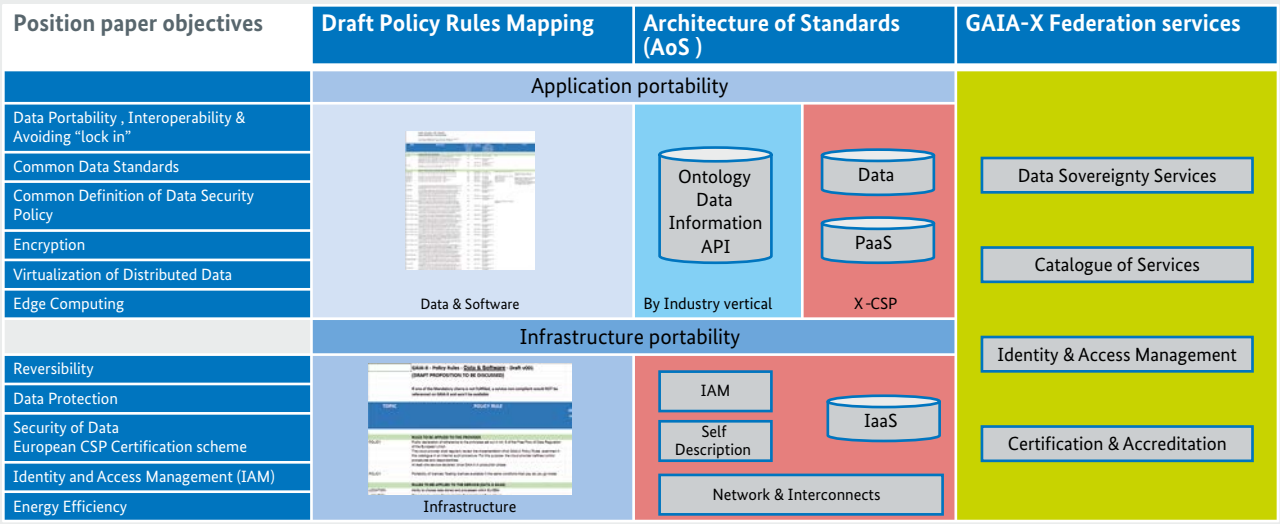
- The “Architecture of Standards” (AoS) defines the list of technical and regulatory standards which are relevant for GAIA-X objectives
- For a technical standard, to become part of the AoS, it must have a governing community which is open to all Cloud Service Providers and Customers or facing a regulatory authority.
- Does not enforce dependencies to provider specific services
- Standards are not exclusive (e.g. it shall remain possible to use and integrate with other PaaS, SaaS, Databases from the same provider) however usage of such services may impact the compliance level
- Cloud service providers or –customers are not obliged to implement the full set of services defined in the AoS, the selection may impact the compliance level
- The Architecture of Standards will be subject to a lifecycle and governance process, it is open to incorporate new emerging and developing standards

Current Status

The Architecture of Standards is – together with the policy rules and the GAIA-X federation services a core element to achieve compliance to the objectives.

There is already an initial process to collect policies and rules for the various layer as shown in Figure 5:

Figure 5: Mapping of Policy Rules and AoS to the original objectives set by the position paper



The document on Policy Rules and the Architecture of Standards (PRAAS) for the federated GAIA-X Data and Infrastructure Ecosystem is a first draft on existing policies and rules and has been initially provided by the members of a Franco-German working group.