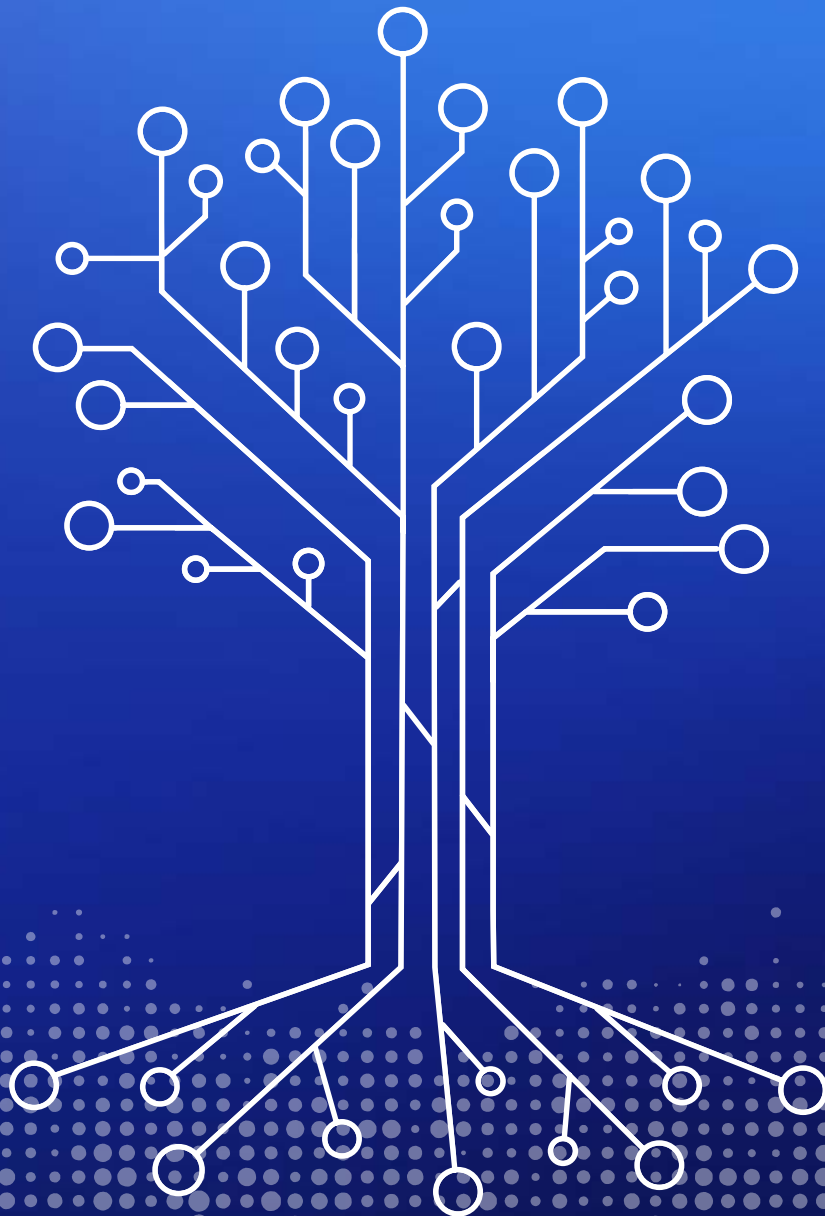


GAIA-X

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

This brochure is published as part of the public relations work of the Federal Ministry for Economic Affairs and Energy. It is distributed free of charge and is not intended for sale. The distribution of this brochure at campaign events or at information stands run by political parties is prohibited, and political party-related information or advertising shall not be inserted in, printed on, or affixed to this publication.

Content

Preamble	4
Objective of the document	5
Policies and rules	6
Architecture of standards	7
Process	7
Appendix	8
GAIA-X Policy Rules for Infrastructure	8
GAIA-X Policy Rules for Data & Software	18
GAIA-X Architecture of Standards („AoS“)	30

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 infrastructure 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 protection¹, reversibility² and security³, 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

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	Yes	Mandatory	Third Party Certified	CISPE Data Protection Code of Conduct	
LOCATION	Transparency Non-EU Applicable Extraterritorial Regulations	Yes	Mandatory	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	Mandatory	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	Mandatory	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 configuration 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 (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 possibility for the data to be processed in different locations outside of the EEA and unless such data are only routed through such locations, the circumstances 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. e.g. risk appropriate transfer encryption, traceability of data processing, separate processing, restorability after incident,...	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-processors.	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	Portability of networks	Yes	Optional	Self Declaration or Third Party certified		
REVERSIBILITY Procedural Requirements	PR01 – Procedures for initiating switching and porting from the cloud service when it is a porting source	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Procedural Requirements	PR02 – Procedures for initiating switching and porting to the cloud service when it is a porting destination	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Procedural Requirements	PR03 – Available porting methods and formats, including available protections and known restrictions and technical limitations	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	



GAIA-X Policy Rules for Infrastructure (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
REVERSIBILITY Procedural Requirements	PR04 – Charges and terms associated with porting	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Procedural Requirements	PR05 – Procedures for activating a new cloud service when it is the porting destination	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Procedural Requirements	PR06 – The exit process for an existing cloud service, where it is the porting source, and where the CSC is aiming to terminate its use of the cloud service once porting is complete	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Procedural Requirements	PR07 – Available management capabilities for the porting and switching process (e.g. end-to-end management to prevent loss of service to the client)	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Portability Requiements	DP01 – The cloud service shall be capable of importing and exporting CSC Infrastructure Artefacts, in an easy and secure way, supporting the following scenarios: CSC to cloud service, cloud service to cloud service and cloud service to CSC. The Infra. CSP shall provide the support to enable the transfer of using structured, commonly used, machine-readable format.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Portability Requirements	DP06 – Where the CSC data involves Infrastructure Artefacts that rely on a feature or capability of the cloud service, the Infra. CSP shall provide an appropriate description of the environment for their execution and how the service dependencies can be satisfied.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Portability Requiements	DP08 – The Infra. CSP shall take reasonable steps to enable a CSC to maintain their service continuity while transferring data between providers, where technically feasible.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Scope and Compatibility Requirements	SCR01 – The Infra. CSP shall describe in the CSP transparency statement the capabilities necessary for effective cloud service switching, to minimize loss of functionality, particularly security functionality. It is acknowledged that the CSC and the Infra. CSP will define in the CSP transparency statement which derived data will be subject to the same porting requirements. Any porting capabilities relating to cloud service derived data should be clearly described in the CSP transparency statement, but there is no requirement for the Infra. CSP to support the porting of this data unless designated as in scope.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Scope and Compatibility Requirements	SCR02 – The CSP transparency statement shall specify the following: a) the scope of Infrastructure Artefacts available for transfer; b) any claim on Intellectual Property Rights the Infra. CSP has on CSC data and how these rights are executed after a switch.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Planning Requirements	PLR01 – the procedure to determine the testing of the mechanisms and schedule of a transfer, based on the CSC’s business needs, security risks, and technical and support capabilities expected of each of the Infra. CSP and the CSC. Testing should include both the testing of the mechanisms used for porting data to and from a cloud service and also of the APIs used to access and to manage the data when stored within the cloud service. Further guidelines on testing of the mechanisms including APIs may be adopted by the relevant governance body of the Code. Acceptance of the testing should be made with the CSC, in the frame of a transparent test process. CSC should be recommended by the Infra. CSP to have a test suite.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Planning Requirements	PLR02 – what constitutes appropriate duration for the transfer of the data using current best practices and available technology, including any solutions not using a network.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Planning Requirements	PLR03 – for the anticipated volume of Infrastructure Artefacts the appropriate mechanisms, availability peridos and price for the transfer	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	



GAIA-X Policy Rules for Infrastructure (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
REVERSIBILITY Planning Requirements	PLR04 – allocation of responsibility and methods for providing security for the data to ensure, for example, access control, authentication of users, confidentiality and integrity through the process	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Planning Requirements	PLR05 – the period during which the CSC data will remain available for transfer once the termination of the source service is required by the CSC, and the nature of clear and timely warnings issued before CSC data is deleted.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Cloud Service Agreement Requirements	FR1 – The CSA shall be documented (including in electronic form) and legally binding between the Infra. CSP and the CSC	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Cloud Service Agreement Requirements	FR2 – The CSA may take any form, including but not limited to: a) a single contract; b) a set of documents such as a basic services contract with relevant annexes (data processing agreements, SLAs, service terms, security policies, etc.); or, c) standard online terms and conditions.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Transparency Requirements	TR01 – The terms and conditions necessary to meet this Code (including those referenced in clauses 5 of this Code) shall be described to potential CSC in clear terms and with an appropriate level of detail in a pre-contractual CSP transparency statement between the CSC and the Infra. CSP. Please note that ensuring pre-contractual information is available to potential CSCs does not require public disclosure and may be done in strict confidence (e.g. via NDA).	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Transparency Requirements	TR02 – The description provided for in TR01 shall provide an appropriate level of details including: a) all aspects of compliance with this Code; b) all documentation, available support and tools to transfer the CSC data from one Infra. CSP to another; c) a description of the overall data porting process and supported capabilities including any data back-up and recovery processes adopted for the purpose of protecting the data while undertaking the porting of the data, security measures, record management and, if agreed upon, the deletion of the CSC's data after the data porting is successfully completed (if the CSC intends to terminate the cloud service contract). If the deletion capability is provided to the CSC by the Infra. CSP, the CSC can do the deletion on its own. The deletion shall be completed by the source Infra. CSP, in the case where such capability is not provided to the CSC; d) the status and procedures for handling the CSC data on the Infra. CSP's infrastructure after termination including CSC instructions on any data retention, preservation or restoration obligations stipulated by applicable law or regulation; e) a clear description of any and all third-parties that have access to the data through the process; f) a clear description of the policies and process for accessing data in the event of Infra. CSP's bankruptcy or acquisition by another entity. These policies and process shall include CSC information without undue delay once a bankruptcy procedure has been started with the competent public authorities; and, g) if a third-party service provider is needed to convert, translate or transfer CSC's Infra-structure Artefacts, it should be explicitly mentioned in the CSP transparency statement.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	



GAIA-X Policy Rules for Infrastructure (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
REVERSIBILITY Transparency Requirements	TR03 – Before the CSC accepts the CSA, the Infra. CSP shall provide to the CSC a CSP transparency statement describing the mechanism(s) related to the porting of CSC data: a) from a CSC’s on-premise facilities to a Infra. CSP’s cloud service b) from another cloud service to the Infra. CSP 's cloud serviceAnd: c) to the CSC’s on-premise facilities from the Infra. CSP 's cloud service d) to another cloud service from the Infra. CSP 's cloud service The description shall provide an appropriate level of details including: e) procedures, terms and conditions, policies and costs, associated with such a data porting; f) appropriate information about the relevant technical, physical and organisational measures to undertake such data porting; g) if applicable, an explanation of the data model, data schema and data semantics and any policy facet considerations adopted by the Infra. CSP as these apply to the CSC data, and how these aspects are handled when considering data portability. h) All related costs areas that would be charged by the Infra. CSP.The Infra. CSP shall ensure that information related to data portability is made available to the CSC, including online and/or incorporated by reference into other contractual documents, and that the information is kept up to date."	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Transparency Requirements	TR04 – The Infra. CSP shall inform the CSC in a timely manner of any changes to the mechanisms and conditions, including identified costs, that would materially alter the portability of the CSC data. The CSC should be given the right to terminate the agreement in advance.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Transparency Requirements	TR05 – The Infra. CSP shall inform the CSC without undue delay if there are permanent changes in its Declaration of Adherence.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Portability Recommandation	DP02 – When exporting CSC Infrastructure Artefacts from a CSC to a cloud service, or between cloud services, the Infra. CSP should provide support to facilitate the interoperability between the CSC's capabilities including the user function, administrator function and business function related to the cloud service.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Portability Recommandation	DP03 – The Infra. CSP should provide Application Programing Interfaces related to the cloud service and , if provided, they shall be fully documented. These APIs should enable the transfer of Infrastructure Artefacts between participating parties. If there are any associated code libraries or dependencies they should be documented and made available.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Portability Recommandation	DP04 – The cloud service is not required under this Code to transform the CSC Infrastructure Artefacts where the destination environment requires the Infrastructure Artefacts to be in different formats than that offered by the source environment. Parties may agree otherwise in the CSA.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Portability Recommandation	DP05 – Transfer of CSC Infrastructure Artefacts to and from the cloud service should use open standards and open protocols for Infrastructure Artefacts movement.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	
REVERSIBILITY Portability Recommandation	DP07 – The Infra. CSP should provide a self-service interface that enables the CSC to carry out periodic retrieval of the CSC's data. This functionality can be subject to contract and may include additional costs.	Yes	Mandatory	Self Declaration or Third Party certified	SWIPO IAAS Code 2.9; Transparency Startement 0.7	

GAIA-X Policy Rules for Data & Software

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		
POLICY	Support portability and switching, promoting transparency and therefore the ease, efficiency and security of data portability at a low cost and with minimal disruption	No	Mandatory	Self Declaration	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
POLICY	Prohibit the use of URLs to refer to documents that can be unilaterally changed by the CSP	No	Mandatory	Self Declaration	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
RULES TO BE APPLIED TO THE SERVICE (DATA & SAAS)						
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 Cybersecurity Act. Transition 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	
SCOPE	Include all CSC data (all data and data types defined and declared in scope in the Cloud Service Agreement (CSA) including Cloud Service Customer Data and Cloud Service Derived Data including metadata, management data, user & identity (access control etc) data and subject data (i.e. personal data on natural subjects), and any other elements (e.g. plugins, macros, code customised by or for the CSC) agreed upon between the CSC and the CSP)		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
SCOPE	Include for the avoidance of doubt all CSC data (personal data and non-personal data)		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
OVERALL REQUIREMENTS	Specify support to allow CSCs to overcome interoperability and data porting issues by providing a justification and description of its alternative approach (e.g. through technical documentation and suitable standards). The CSP can meet this requirement by maintaining and making available to CSCs an overview of reported incompatibilities and solutions, where incorporation is duly authorised by the reporting CSC, occurring with CSC developed or sourced systems		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	



GAIA-X Policy Rules for Data & Software (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
OVERALL REQUIREMENTS	Specify at request of the CSC, the contract with the CSC for the provision of support services in a project-mode with respect to data export/import to be performed. Such will be possible preceding to the conclusion of a CSA with the CSP.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
REVERSIBILITY	Specify in advance the right level of transparency to justify a fair price based on real operational costs, if there are any fees or charges related to data export/import during the contractual period and any agreed post contractual one. This can be done by detailing a cost structure plus a reasonable margin and/or by including some benchmarks on demonstrated market prices. The CSP preferably should provide the CSC with fixed lump sum or flat rates at the lowest cost possible.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
REVERSIBILITY	Specify an explicit and structured process for data export. Include data management considerations (e.g. snapshots and incremental approaches records management policies and bandwidth assessment) and any relevant timescales, notice requirements, customer contact procedures (contact points, escalation etc) and impact on service continuity. This should include relevant SLO and SQO from the SLA. The process and documentation shall cover technical, contractual and licensing matters such that they are sufficient to enable porting and switching.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any CSP imposed or enforced obligations on customers before exporting data can commence.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any known post contractual license fees or other liabilities, for example patent and licensing fees covering use of derived data or data formats or claims and cases that are ongoing.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any tools and services incurring additional fees for data export that are required by the source CSP processes for data portability as specified in 3.2.1.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any CSP provided tools or services (including for example addressing integration or interoperability support) that are available to assist the export process and any fees associated with those tools. You may specify any 3rd party tools or services.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify whether or not the source CSP's processes for data portability as specified in 3.2.1. allow a CSC to be completely autonomous in exporting data i.e. when the CSC does not need human interaction with the CSP.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify which data, including derived data (e.g. computed field values, graphics, visualizations) can be exported from the service prior to the effective export date.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify what, if any, security audit related data (e.g. access logs) is available for export (e.g. logs of user interactions with the cloud service that could be needed for security analysis and for supervisory request).		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify which data standards, formats and/or file types are recommended, used or available for data importing (e.g. binary, MIME, CSV, SQL, JSON, XML, Avro) for each and every data set available for import including any unstructured data.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Ensure that data standards are preferably based on current open standards. For textual data, as a minimum a flat file CSV format will be possible. Binary is only used if no other open formats exist for the type of data.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
REVERSIBILITY	Provide documentation on the format and structure of the exported data including where it can be sourced and under what terms if from a 3rd party source (including open or industry standard formats or exchanges (e.g. Open Financial Exchange format). As per A1.2.1 above this must be sufficient to enable porting and switching		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify what cryptographic processes and services are provided, if any, during data export (including unencrypted options) and how encryption keys are managed. The process shall allow the CSC to decrypt the exported Data.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any security controls (eg access controls) available during data export.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	



GAIA-X Policy Rules for Data & Software (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
REVERSIBILITY	Specify any access to, retention period and deletion processes (including notification of deletion) of data, including differing categories of data (including derived data and management data) after the expiration of contract.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify the costs structure for data export and related procedures.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any processes that it supports to maintain data integrity, service continuity and prevention of data loss specific to data exporting (e.g. pre and post transfer data back-up and verification, freeze periods and secure transmission and roll back functionality).		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify the available mechanisms, protocols and interfaces that can be used to perform data export (e.g. VPN LAN to LAN, Data Power, SFTP, HTTPS, API, physical media ...)		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any known dependencies between the data to be exported and other data connected to another cloud service.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any processes, as part of the precontractual transparency document, to disclose use of subcontractors during data portability activity.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify a procedure to determine the testing of the mechanisms and schedule of a data transfer based on the CSC's business needs, security risks, and technical and support capabilities of both parties. Acceptance of the testing should be made with the CSC in the frame of a transparent test process		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
REVERSIBILITY	Allow the CSC to perform the data export process (for all or part of the data) at the CSC's discretion on the time basis corresponding to the CSC business needs, which could be data export at any moment, data export through incremental asynchronous exchanges, daily backup or with another periodicity. and not only a global export at the end of the contract.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
REVERSIBILITY	Allow the CSC to perform the data export process at termination of the CSA by one of the contracting parties for whatever cause		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
REVERSIBILITY	Specify an explicit and structured process for data import. Include data management considerations (eg snapshots and incremental approaches records management policies and bandwidth assessment) and any relevant timescales, notice requirements and customer contact procedures (contact points, escalation etc) and impact on service continuity. The process and documentation shall cover technical, contractual and licensing matters such that they are sufficient to enable porting and switching.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any CSP imposed or enforced obligations on customers before importing data.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any required tools incurring additional fees for data import.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any CSP provided tools or services (including for example addressing integration or interoperability support) that are available to assist the import process and any fees that are associated with those tools or services. You may specify any 3rd party tools or services.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify whether or not the customer can be completely autonomous in importing data i.e. when the CSC does not need human interaction with the CSP.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify which data, including any derived data from a source exporting service (e.g. computed field values, graphics, visualizations) can be imported into the service.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify what, if any, security audit related data can be imported (e.g. logs of user interactions with the cloud service that could be needed for security analysis and for supervisory request).		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify which data standards or formats are recommended, used or available for data importing (e.g. CSV, SQL, JSON, XML, Avro) for each and every data set available for import including any unstructured data.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Ensure that data standards are preferably based on current open standards. For textual data, as a minimum a flat file CSV format will be possible. Binary is only used if no other open formats exist for the type of data.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	



GAIA-X Policy Rules for Data & Software (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
REVERSIBILITY	Specify the format/structure required of imported data and where definitions are available and under what terms (including open or industry standard formats or exchanges (e.g. Open Financial Exchange format). Specify any available validators and if so what type (eg structure, format, storage type, volume, links), from where and under what terms. As per A1.3.1 above this must be sufficient to enable porting and switching.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify what encryption processes are used during data import (including unencrypted options) and how encryption keys are managed		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any security controls (eg access controls) used during data import.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify the costs structure for data import and related procedures (e.g. volume restrictions).		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any processes that it supports to maintain data integrity, service continuity and prevention of data loss specific to data importing (eg pre and post transfer data back-up and verification, freeze periods and secure transmission and roll back functionality).		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify the available mechanisms, protocols and interfaces that can be used to perform data import (e.g. VPN LAN to LAN, Data Power, SFTP, HTTPS, API, physical media ...)		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any processes, as part of the precontractual transparency document, to disclose use of subcontractors during data portability activity.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify any additional known migration services existing (either CSP or 3rd party) and how are they available on the market.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
REVERSIBILITY	Specify the notification processes and timescales for any changes to the material included or referenced in its transparency declaration to be communicated to users.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
SERVICE CONTINUITY	Continuity of service: Specify a clear description to the CSC of the policies addressing access and porting of data in the event of CSP's bankruptcy, impact of ransom-trojan issues or acquisition of the CSP by another entity. These policies and process shall include CSC information without undue delay once such event would occur		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS Code 1.5	
SERVICE CONTINUITY	Continuity of service: In case of acquisition of the CSP by another entity such entity will enter into all rights and obligations of the CSP and the continuation of the services will be guaranteed by this entity for a period of at least 18 months starting with the acquisition.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
SERVICE CONTINUITY	Continuity of service: Allow the CSA to contain provisions with regards to the porting of CSP data to the CSC or to a third party in case of CSC's bankruptcy, in which case such third party towards the CSP will enter into all CSC's right and obligations of the CSA.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
SERVICE CONTINUITY	Continuity of service: Allow the CSA to contain provisions with respect to its assignment in case of mergers, acquisitions and other changes of the CSC or disinvestments made by the CSC.		Optional	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
SERVICE CONTINUITY	Continuity of service: Provide a clear description to the CSC of the polices addressing contacting the CSC in a clear and timely manner and the retention of CSC data in case of CSC's non-payment or bankruptcy, which will at least be 12 months starting with the event of default		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
SERVICE CONTINUITY	Continuity of service: Only delete CSC's data from its systems after having received an explicit written approval thereto from the CSC. In case of CSC's bankruptcy this approval is to be given by the person in charge of the wind-up of the CSC.		Mandatory	Self Declaration or Third Party certified	SWIPO SAAS – Additional proposals from BELTUG & CIGREF	
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	



GAIA-X Policy Rules for Data & Software (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 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 services.		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	
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 agreement		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	



GAIA-X Policy Rules for Data & Software (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	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	
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	
DATA SHARING	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.

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”.

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

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

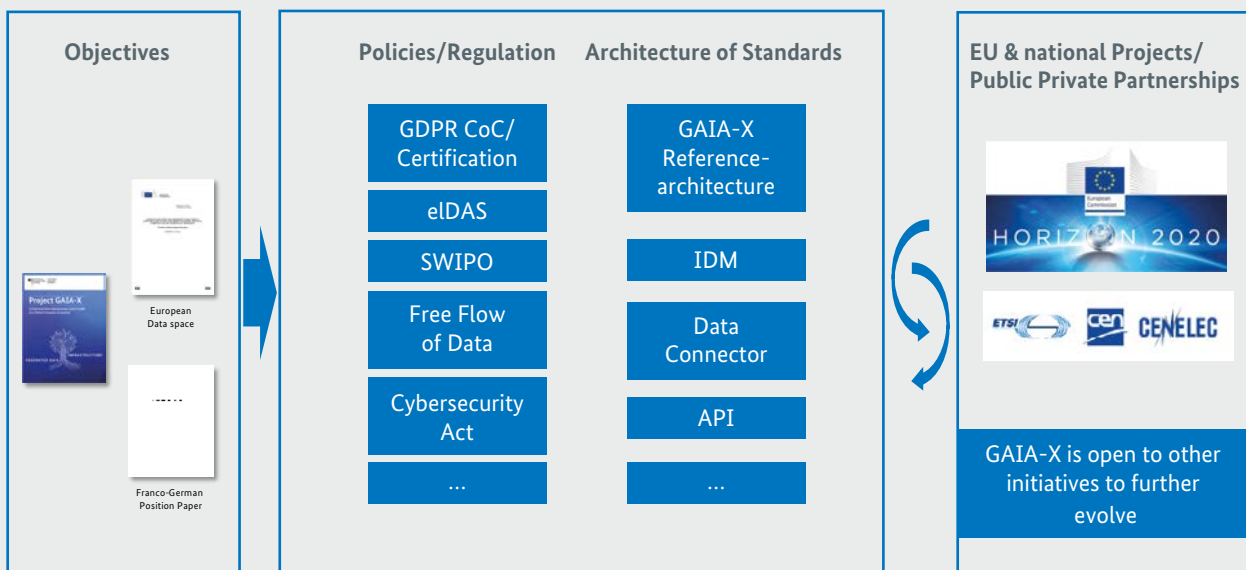
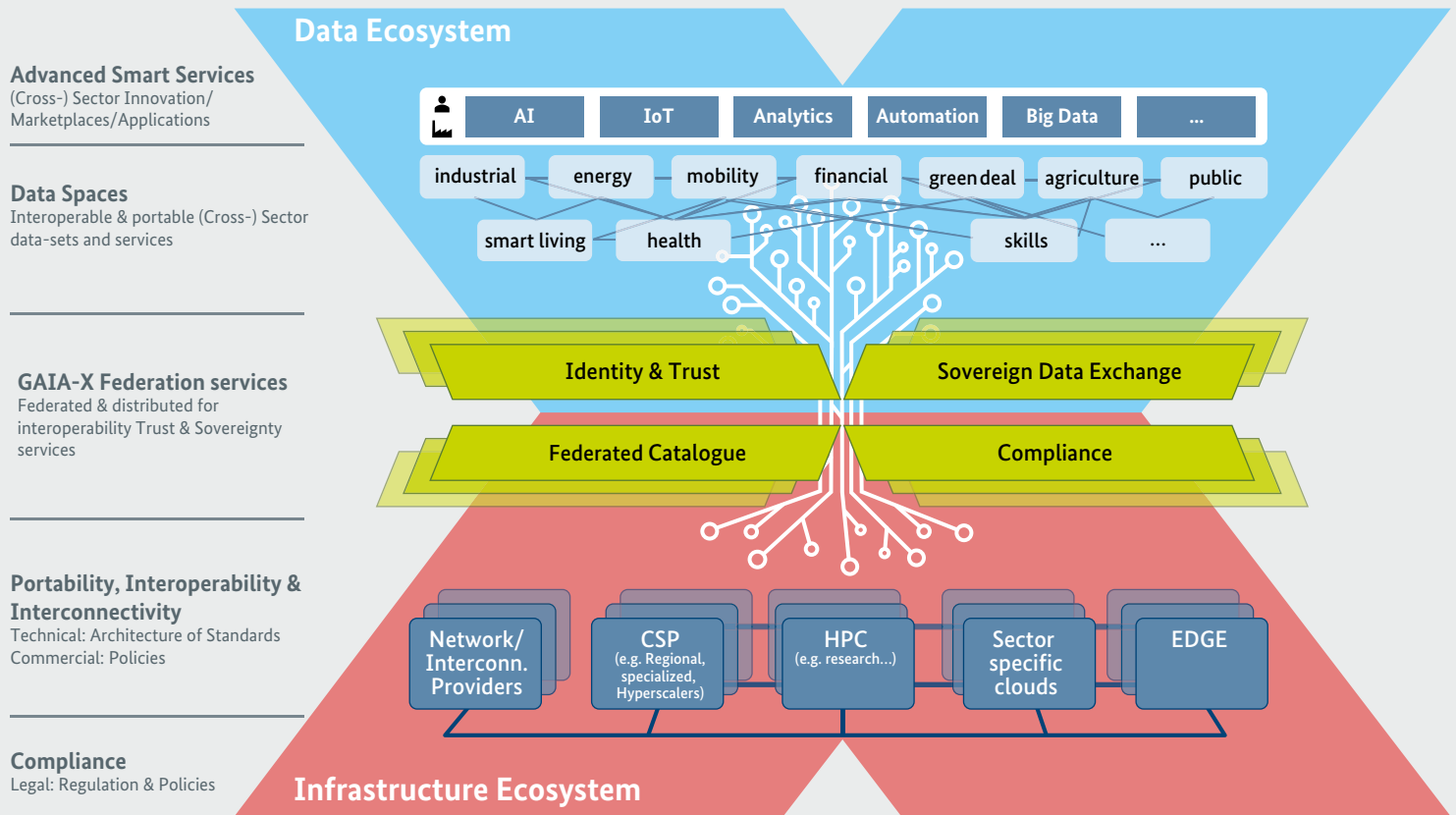


Figure 2: GAIA-X Overview



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 jurisdiction
- **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

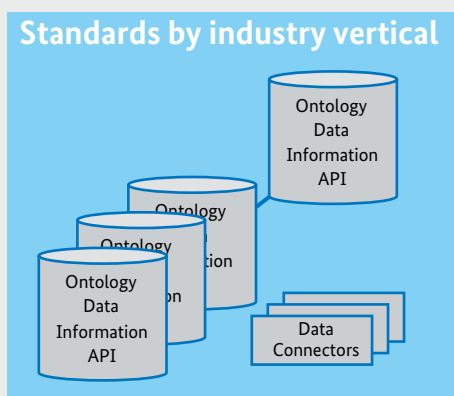
- Technical Standards
- Governance entities
- Regulatory working groups
- Public Private Partnerships

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.

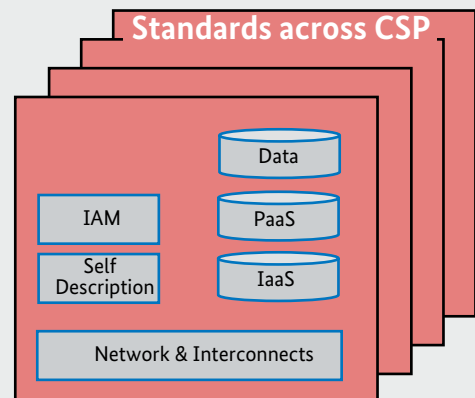
Figure 3: Mapping of different standards



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



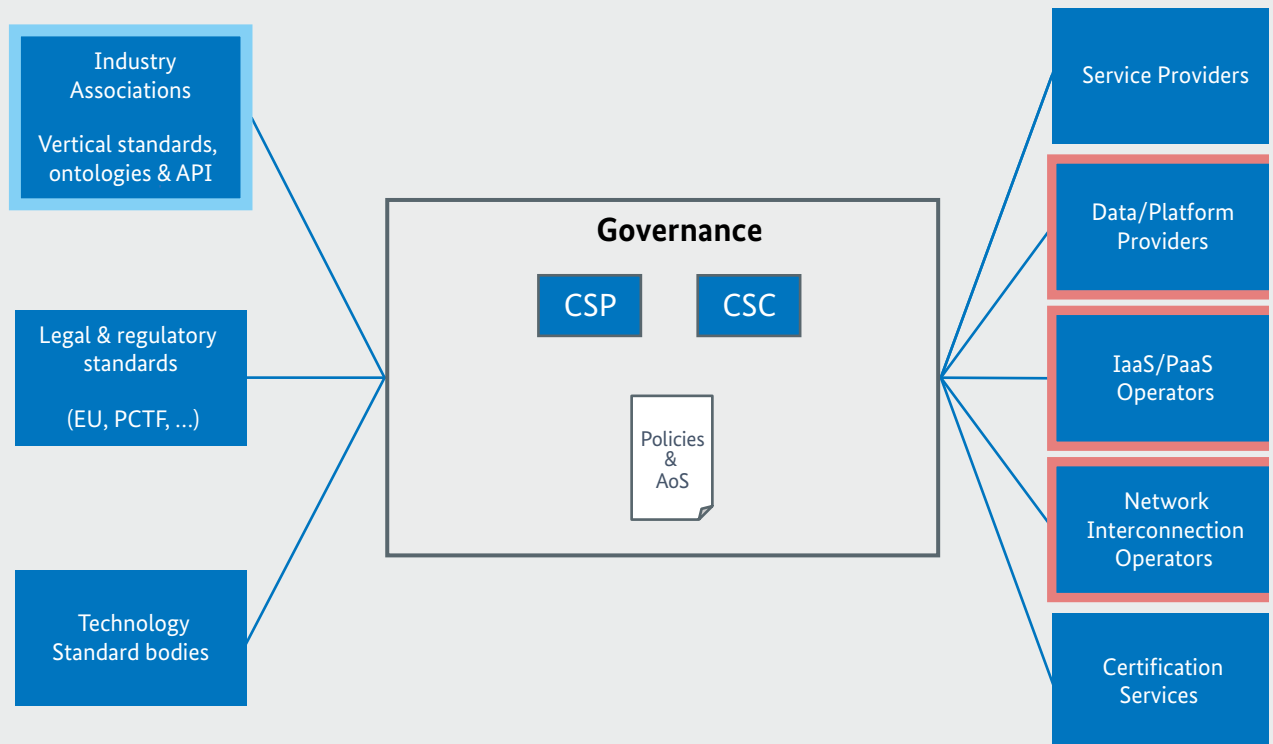
Federated trust and sovereignty services across different consumers and providers (where needed)



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

Position paper objectives	Draft Policy Rules Mapping	Architecture of Standards (AoS)	GAIA-X Federation services
	Application portability		
Data Portability , Interoperability & Avoiding “lock in”	 Data & Software	<div><div>Ontology Data Information API</div><div>By Industry vertical</div></div> <div><div>Data</div><div>PaaS</div><div>X-CSP</div></div>	<div>Data Sovereignty Services</div>
Common Data Standards			<div>Catalogue of Services</div>
Common Definition of Data Security Policy			
Encryption			
Virtualization of Distributed Data			
Edge Computing			
	Infrastructure portability		
Reversibility	 Infrastructure	<div><div>IAM</div><div>Self Description</div><div>Network & Interconnects</div></div> <div><div>IaaS</div></div>	<div>Identity & Access Management</div>
Data Protection			<div>Certification & Accreditation</div>
Security of Data			
European CSP Certification scheme			
Identity and Access Management (IAM)			
Energy Efficiency			

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.

