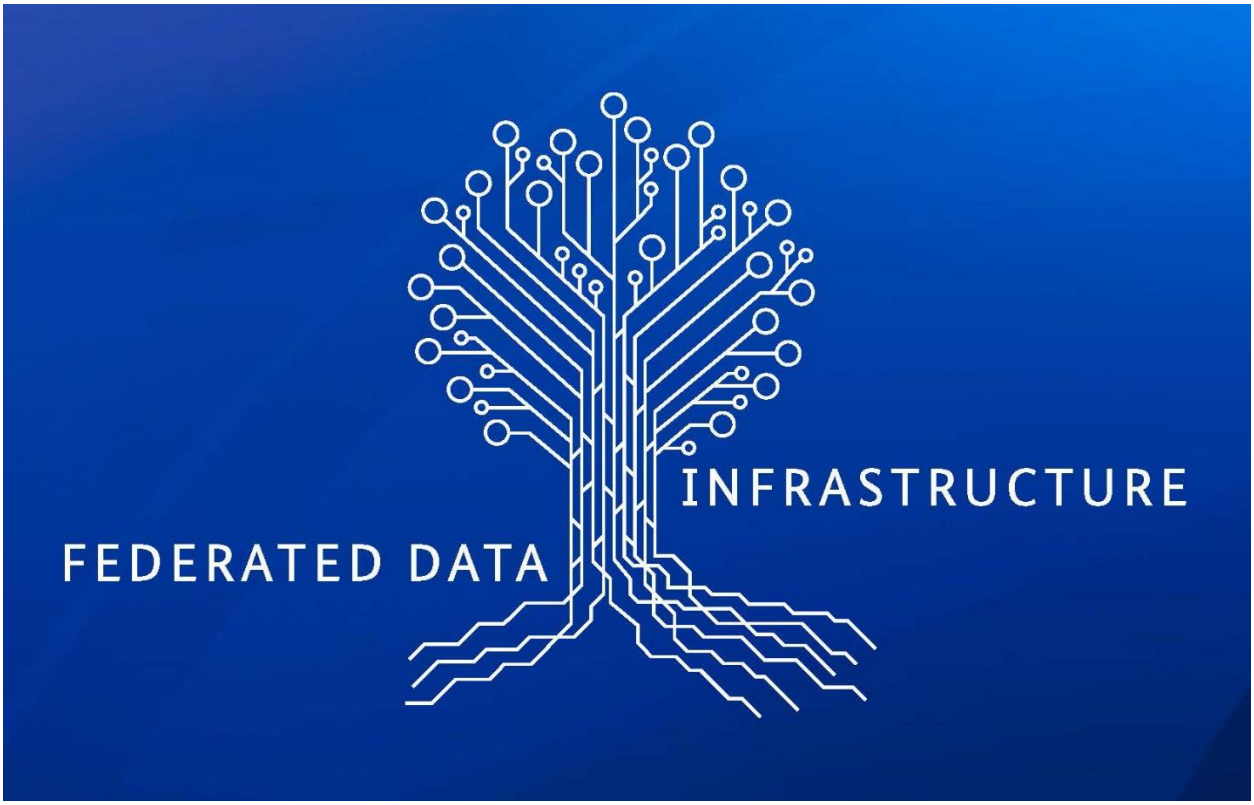
18 February 2020

Franco-German Position on GAIA-X



Franco-German Position on GAIA-X

We, representatives of industries, cloud services providers (CSP) and cloud services customers (CSC), from France and Germany and their respective governments, support GAIA-X in its objective to facilitate the creation of European data and AI driven ecosystems, to guarantee data sovereignty, and to ensure that value creation remains with the individual participants.

We agree that these ecosystems – in line with the European Data Space promoted by the European Commission – will focus initially on a number of sectors, including Mobility, Finance, Health, Living, Environment-Climate-Agriculture, Public Services, Industry 4.0 and others. All implementations will be built upon cloud and edge computing and will facilitate easy data-sharing and enable analytics and AI.

In addition, GAIA-X shall enable new business models within its community for data sharing and should create enabling services to provide equal and non-discriminatory access to such an ecosystem. Such models and services must be developed in accordance with European ethical consideration for AI, as well as implement the highest level of data protection, security, transparency and portability / reversibility. We shall also investigate the need of an overall far-reaching target architecture and complementary approaches for the vision of the federated data infrastructure, beyond existing cyber security and data protection approaches listed. In order to gain sustainable digital sovereignty, it is important to strengthen Europe's competitiveness in the global digital market.

We agree on the objectives of GAIA-X and on the current focus of the use cases as a nucleus for a future industrial and services ecosystem, for enabling a cloud service and data economy to create a new layer of data based smart services, and the mass adoption of AI services. Other European Member States will be invited to join our effort, paving the way to establish best practices worldwide.

The Project GAIA-X Concept Paper[1] gives examples in several domains, showing the benefits of GAIA-X for both users and providers.

The experience gained during the last several years on these topics of digital sovereignty has shown that users are willing to share what they consider as good practices in their domain, asking providers to translate these good practices into legal provisions which are being integrated in their contract framework, and which, together with a basic set of digital-infrastructure services around identity and trust, shall provide an important basis for a federated data infrastructure as the cradle of a vibrant European ecosystem.

A new layer of technologies shall be developed, enabling full data-control, traceability, auditability, reversibility and data interoperability, which would foster contractual interoperability for a federated data infrastructure, which automates and links a federated mesh of service providers as well as opened and automated links between them, opening the path to aggregated services or service chaining. "Data

[1] Project GAIA-X – A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem / Le projet GAIA-X – Une infrastructure de données en forme de réseau, berceau d'un Ecosystème Européen Vital

sovereignty by design" will be a guiding principle for the development of software for platforms and services.

Good practices on data localization enabling European data to be stored, secured, operated and processed exclusively in European jurisdictions upon choice of customers have been translated in a set of regulations, codes of conduct, policies, best practices and business model(s). Following these objectives, using the existing relevant tools[2], will be mandatory to comply to for services of entities participating in GAIA-X.

Among the good practices which have emerged since 2016 we can list as examples for the area of **infrastructure**:

- **Reversibility**: Changing the cloud provider with portability for data and services, in the frame of Art. 6 "Porting of Data" of the European Free Flow of Non-personal Data Regulation. First codes of conduct have been handed over to the European Commission.
- **European CSP Certification scheme:** The scheme was developed by a European Working Group, including German BSI (C5) and French ANSSI (SecNumCloud), and handed over to ENISA in June 2019.[3] Based on the European Cybersecurity Act or within the framework of the New Legislative Framework, certification schemes for an efficient on-boarding of cloud infrastructure services providers into GAIA-X should be developed. To this end, GAIA-X has to develop the appropriate self-description and discovery schemes.
- **Security of Data:** Security policy is associated to the data about its usage and shall be controlled irrespective of the providers. Beyond existing cybersecurity approaches the need and requirements for a trusted execution within the edge environment should be considered.
- **Identity and Access Management (IAM):** Resources and devices shall be identified in a way which is common regardless of the provider. All agents and devices, like all assets, are identified regardless which provider is involved in a GAIA-X service instantiation. This is covered by **interoperability, common trust requirements** (international technical standards and harmonized legal framework) and an approach covering the GAIA-X IAM requirements. Both GAIA-X core components and provider offer a sufficiently high degree of security regarding the integrity, confidentiality, traceability and availability of GAIA-X identities.
  The solution will be selected based on industry best practices and accepted international standards. It forms the GAIA-X baseline for the flexibility regarding different technical and national/legal requirements. On top, distributed access and (decentralized) identity management schemes, including verifiable credentials[4], should be considered enabling a robust ecosystem comprising hundreds of thousands of GAIA-X nodes.
- **Energy Efficiency:** Transparency of energy consumption and its comparability regarding equivalent workloads should be encouraged. Users should have better visibility of the energy

[2] For tools related to data protection, those following guidelines of the European Data Protection Board (EDPB) will strongly be considered

[3] https://cspcerteurope.blogspot.com/2019/06/final-public-private-recommendation-for.html

[4] https://www.w3.org/TR/did-core/

consumed by processing of their data, including in the context of the self-description. Criteria may be applied to all type of cloud facilities, including edge computing facilities.

- **Protection against non-European extra-territorial regulations: Protection against abuse of national regulations** that allow to access data stored in cloud infrastructures or services is an essential part of the European federated data infrastructure.

In addition, the **portability of applications** among cloud providers requires:

- **Avoiding "lock in"** by agreeing on open API describing the use of technical facilities provided by between SaaS offerings and third parties, including individual bricks internally (for example changing the data storage service or other individual services).
- **Common Data Standards** enabling data sharing through file exchange or functional API (as in PSD2 for Finance).
- **Common Definition of Data Security Policy** defining data security policy in logical and legal terms.
- **Encryption** to be used for stored data where relevant, with a portability of the keys used to encrypt and interoperability of key management systems.
- **Virtualisation of Distributed Data** across multiple service providers (e.g., data-cashing, data-prefetching) to enable distributed cooperating application and services.
- **Edge Computing** as a possible processing paradigm to create possibilities for real-time processing and distributed algorithms, cloud native apps vs. edge apps.
- **Data Portability and Interoperability**: Data interoperability has to go further than data portability, i.e., domain specific data semantic harmonization is the next degree of data interoperability and should include inter alia through (domain-specific) standardized management dishes for digital twins.
- **Service and Contractual Interoperability** to enable on demand CSP collaboration.

GAIA-X should nevertheless go further than incorporating already existing best practices, especially in the domain of service interoperability, data interoperability and data sovereignty. At the same time, the European R&D community will be encouraged to participate and add resources.

Maximum transparency will be one of the unique selling points of GAIA-X, creating benefits for users and suppliers. Transparency about applicable law to data should also be provided by services providers, whereas it concerns infrastructure as a service (IaaS) as well as for software as a service (SaaS).

We propose to leverage the user requirement efforts already undertaken to map these good practices to each vertical and see whether it needs to be completed and rank them by priority.

Translating good practices for infrastructure and for application portability into specific provisions for contracts will be an important task to be addressed as soon as possible. All relevant questions concerning security, data protection and operational aspects have to be addressed. Beyond legal wording, the automation of certifications through self-description or auto-discovery and the automation of auto-contracting (contract changing) should be considered.

Against the background of the joint press release of the French Ministry of Economy and Finance and the German Federal Ministry for Economic Affairs and Energy of 29 October 2019[5], we agree that both ministries will initiate in parallel the discussion about the organization and governance. At the same time, the representatives of French and German industries continue their collaboration on technology.

To keep the momentum which this project currently enjoys, we believe that the presentation to other EU Member States should take place as soon as possible using this Franco-German position paper as a basis. This does not preclude the Franco-German process to continue in parallel.

[5] https://www.bmwi.de/Redaktion/EN/Pressemitteilungen/2019/20191029-press-release-on-franco-german-common-work-on-a-secure-and-trustworthy-data-infrastructure.html /