



EUROPEAN ALLIANCE
FOR INDUSTRIAL DATA,
EDGE AND CLOUD

INPUTS TO THE EUROPEAN DATA INNOVATION BOARD

COMMON TRUST PRINCIPLES FOR INTERCONNECTIONS IN AND BETWEEN CLOUD-EDGE ECOSYSTEMS, INCLUDING DATA SPACES



MAIN CONTRIBUTORS

Giulia Biagioni (TNO), Robin Camarasa (TNO), Björn Fanta (Fabasoft), Sara Madariaga (formerly Arsys), Arthur van der Wees (Arthur Strategies & Systems), Maria Barros Weiss (formerly IONOS)

EDITOR

Dimosthenis Kyriazis (University of Piraeus)

ABOUT THE ALLIANCE & THE WORKING GROUP

The **European Alliance for Industrial Data, Edge and Cloud** [1] brings together businesses, Member States' representatives, and relevant experts to jointly define strategic investment roadmaps to enable the next generation of highly secure, distributed, interoperable, and resource-efficient computing technologies. The work is facilitated by the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CNECT).

The **Cloud - Edge Working Group** (WG) brings together the main European Industry players in cloud computing that compiled the European Industrial Technology Roadmap for the Next-generation Cloud-Edge in 2023 [2]. Following the release of the aforementioned roadmap, specific WG members have collaborated on developing the current inputs with a focus on trust principles in computing environments (cloud to edge) and data spaces. The members of the WG that have co-authored this report are the following:

Arsys	IONOS
Arthur Strategies & Systems	TNO
Fabasoft	

The WG is chaired by Ignacio M. Llorente (OpenNebula Systems), co-chaired by Bjorn Hakansson (TNO) and Maria Barros Weiss (formerly IONOS), and facilitated by Ana Juan Ferrer (European Commission). The group that developed the current inputs is co-chaired by Björn Fanta (Fabasoft) and Arthur van der Wees (Arthur Strategies & Systems).

EXECUTIVE SUMMARY



In an increasingly interconnected digital world, the need for secure, trustworthy, and efficient data sharing is more critical than ever. Establishing trust among diverse stakeholders is not only a key enabler but also a primary success factor for sustainable digital ecosystems. Every ecosystem - whether industrial, governmental, or cross-sectoral - comprises multiple actors with distinct roles, responsibilities, and trust expectations.

This document explores the current landscape of data ecosystems, focusing on how trust can be built, managed, and extended. It begins with a classification of data types and their varying sensitivity and governance requirements. A central concept introduced is trust forwarding, which enables the extension of trust relationships across entities and platforms, forming the backbone of reliable data exchange.

Despite various ongoing initiatives and frameworks, a significant gap remains between the theory of trust principles and their practical implementation. This gap is compounded by the complexities of stakeholder alignment, governance models, and the varying definitions of trust values across domains.

We propose a set of future-oriented requirements and possible solutions aimed at bridging these challenges. Our recommendations include technical,

organizational, and policy actions that can foster trust in distributed environments. By aligning these recommendations with initiatives like Gaia-X, we demonstrate how the proposed approach can contribute to a federated and sovereign data infrastructure.

Finally, we highlight the added value of enabling new business models for data sharing within trustable environments —opening doors for innovation, competitive advantage, and sustainable growth.

TABLE OF CONTENTS

About the Alliance & the Working Group	3
Executive Summary	4
Introduction	6
The Need	7
Trust principles as enabler and main success factors.....	7
Every ecosystem consists of multiple stakeholders	9
The Landscape	10
Classification of data.....	10
Trust forwarding - an explanation.....	12
The Gap	14
Initiatives, stakeholders, and trust values	14
Challenges and complexities	17
The Proposal	18
Future requirements and possible solutions	18
Recommended actions	19
How the idea maps to an initiative like Gaia-X.....	21
Recommendations.....	22
Added Value: New Business Models for Data Sharing in Trustable Environments	26
References	28

INTRODUCTION

The current Inputs to the European Data Innovation Board, titled “Common trust principles for interconnections in and between cloud-edge ecosystems, including data spaces”, (hereafter referred to as “Inputs”) explores the evolving landscape of trustworthy digital ecosystems and their role in facilitating secure, transparent, and interoperable data sharing within and across sectors.

As digitalisation accelerates, various initiatives have emerged to promote data exchange and cloud-based ecosystems in Europe, yet trust - or more concretely, the lack of trust - remains a significant barrier to seamless collaboration, orchestration, and contextual integration.

This document identifies critical gaps in addressing the multiple trust components and related dimensions necessary for establishing robust data-sharing environments, particularly the need for standardised frameworks that integrate technical, organisational, operational, ethical, and regulatory considerations.

Key components of trust in data exchange, such as identity, accessibility, data control, digital sovereignty, security, privacy, integrity transparency, interoperability and others are outlined with an emphasis on their role in fostering ethical and reliable data sharing. The document identifies ongoing initiatives in the EU, noting the importance of interoperability across different digital ecosystems and related legal frameworks. Through these initiatives, trust-forwarding principles are derived, showcasing how trust components can be mapped to specific use cases.

Recommended actions in research and innovation highlight the need for clarity in terminology and the development of governance structures that support multi-actor, multi-system, cross-border, cross-sectorial and otherwise interconnected collaborations. Successful models for data sharing are emphasised, focusing on secure digital ecosystems and the application of “infonomics” [18] to quantify the value of data as a business asset. New value models and related business models, centred around secure data exchange, are presented as driving innovation, economic growth, collaboration across industries, increased competitiveness and prosperity for EU society, including the economy, at large.

Ultimately, the inputs provide a comprehensive view of the challenges and opportunities in building trustworthy data spaces, offering a foundation for creating new business models that enable efficient, ethical, and value-driven data sharing.

It is not solely a matter of technical implementation; rather, it involves achieving a balance between specific trust components and related context, ensuring they work in symbiosis of functional and non-functional capabilities.

THE NEED

Low levels of trust in data sharing has been identified as one of the main reasons behind limited data availability and use in Europe [3].

The success of any data sharing, in and between cloud-edge ecosystems, as part of common European data spaces, requires building and sustaining the appropriate level of contextual trust between data-sharing stakeholders. Trust-based sharing between the data-sharing stakeholders includes demonstrating consistency and other elements of trustworthiness along the way.

Trust and trustworthiness are enablers in building, achieving, and sustaining collaborative digital, data and related ecosystems. All these contribute towards addressing societal challenges, by and for any and all relevant stakeholders, whether on the demand or supply side, public or private, large or small. They can also future-proof digital sovereignty of people, planet, society, and economy, peace, prosperity and partnerships.

Trust principles as enabler and main success factors

To enable the establishment, interconnection and future-proofing of trustworthy data exchanges in and between different cloud-edge ecosystems (including the common European data spaces that are currently under development in various stages [4]) several **primary trust principles** have been identified, such as those highlighted below:

Persona-centricity, digital sovereignty, data control, findability, accessibility, provenance, interoperability, usability, re-usability, freedom of choice, updateability, safety, security, privacy, data protection, data management, transparency, trustworthiness, dynamic assurance, resilience, governance, sustainability and accountability.

Trust principles such as the ones listed above have been set forth in several documents, such as the following:

- Declaration on Digital Rights and Principles of December 2022 [5]
- EU Fit for the Digital Age mission that the Commission has developed [6]
- Path to the Digital Decade 2030 [7], and related Digital Decade policy programme 2030, including main notable strategies such as the:
 - EU Data Strategy [3]
 - Cybersecurity Strategy [8]
 - Strategic Compass for Security and Defence [9]

- Declaration on EU Cloud Federation to build the next-generation cloud including edge in Europe [10]. On this, the EU Alliance for Industrial Data, Cloud and Edge was conceived and launched.

These primary trust principles obviously are and remain well in line with the Commission's 2024-2029 Missions and sub-missions [11], [12], and will further augment and support those.

Principles need context

The trust principles, which can be seen as the primary trust principles, need to be correlated with the relevant context, in order to enable interconnection and balance with other trust principles. Most of these trust principles have now been or are in the process of being transposed and mentioned in relevant European data-centric, digital market-centric, risk-based, and all-hazard based regulation and other policy instruments. Now, these have to be detailed into a deployable common approach. Even for such a common approach, principles need context. This will enable a foundation for establishing trust and for facilitating interconnection and future-proofing of trustworthy data exchanges in and between different cloud-edge ecosystems, including in and between data spaces.

Cloud-edge ecosystems, including in and between data spaces

While not every data space may be a cloud-edge ecosystem, each data space is an ecosystem and an infrastructure. Most importantly, the notion of data space is a concept. There is no one-size-fits-all structure of data spaces; each space is organised by different stakeholders taking into account the characteristics of those stakeholders and the specific purpose of the data space in a particular sector.

The current state of play regarding data spaces can be found in the 2nd Commission Staff Working document on common European data spaces dated 24 January 2024 [4], JRC's report "European data spaces 2023" [13], and JRC's report "Mapping the landscape of data intermediaries 2023" [14]. More recent definitions may have emerged from industry initiatives such as the IDSA by the time of this publication. However, this document does not seek to replicate or reorganize these, but builds on the aforementioned sources (i.e. [4], [13] and [14]).

Where the aim is to provide for a non-exhaustive overview of existing trust frameworks and possible applications, as already mentioned the currently existing and upcoming relevant European regulations and other policy instruments are the basis to start from in order to plot existing frameworks as well as the state of the art, identify the various gaps, and recommend how to address those gaps. All this, in order to understand how to structure and harmonise the identified

common approaches into selected cloud-edge ecosystems originating from the EU Alliance members.

Every ecosystem consists of multiple stakeholders

Investing in deployable and deployed trust principles from one end of a market does not equal trust. All sides of the market and each of the stakeholders in an ecosystem will need to invest. One of the main principle-based objectives is that if providers, manufacturers, vendors, partners and other supply side actors display consistency in the appropriate level of trust in their designs, deployments and the like, those deserve equally trustworthy procurers, customers, partners and other demand side actors in their (pre-)procurements, implementations and engagements, to collaborate, co-create and work with to build long-lasting relationships. Trust equals consistency over time. Data sharing is not a one-way street.

Obviously, specific implementations may vary based on the nature of the cloud-edge ecosystem, its participants, and the regulatory landscape in which it operates. It is therefore of paramount importance to carefully align with frameworks and specifications already published by the industry and research-oriented initiatives, for general frameworks as well as for specific vertical sectors.

The work of this Inputs to the European Data Innovation Board will address the topic of trust principles in four categories, which are derived from a relevant paper [15]:

- Strategic/ Structural - what do trust principles mean to make the EU fit for the digital age?
 - e.g. Digital Decade 2030, Data Act
- Managerial/ Behavioural - what are existing or possible future organisational schemes?
 - e.g. data sharing, data governance
 - Paradigms of company and community behaviour
- Financial/ Economical - what is the feasibility and (financial) sustainability?
 - i.e. financial sustainability of specific ecosystems, not the financial health of a company
- Technological - what does technology offer to bring the principles forward?
 - e.g. OSS, SIMPL, IPCEI, EU CSAs.

This report delivers added value in the scope of regulation and technological solutions that have to be aligned between EU public bodies and the private sector to make trust in data sharing between cloud-edge ecosystems possible.

THE LANDSCAPE

The current landscape of data management and technology solutions comprises ongoing research and emerging commercial advancements within the past two to three years. Given the thematic focus of this inputs, we will highlight recent innovations and practical applications specifically relevant to this domain. These selected solutions represent state-of-the-art progress and underscore pivotal trends shaping the future of data and security, especially in industrial contexts.

Classification of data

Data classification is a structured approach to categorising data based on factors like sensitivity, importance, and regulatory requirements. It enables organisations to effectively manage and safeguard data, aligning access controls, retention policies, and security measures to different data types. In this inputs, we will briefly outline key aspects:

- **Data:** The current most comprehensive definition of data is set forth in Article 2(i) of the Data Act, being: *“Data’ means any digital representation of acts, facts or information and any compilation of such acts, facts or information”*. This includes non-personal and personal data, metadata, derived data and the like.
- **Data Identification:** All data available to, for, in, from, and by industrial, sectorial, and related environments is crucial. Sources include, but are not limited to, sensors, machinery, production systems, supply chains, and administrative frameworks.
- **Categorisation:** Data should be categorised according to sensitivity, criticality, confidentiality, regulatory demands, and business impact, forming a basis for defining trust levels.
- **Classification Levels:**
 - Public: Openly shareable without restrictions.
 - Internal: Intended for internal use; may contain sensitive information.
 - Confidential: Requires strict access control due to high sensitivity.
 - Restricted: Enforced with stringent controls; compromise could lead to severe consequences.
- **Data Classification Process:** Organisations should adopt systematic processes, employing either manual methods or automated tools like data loss prevention (DLP) systems and machine learning algorithms to ensure precise classification.

Data domains

Industrial environments generate a wide array of data, encompassing various aspects of *operations, production, maintenance, quality control, and supply chain management*. This data is crucial for

optimising processes, improving efficiency, ensuring compliance, and driving innovation within organisations. *Process data* includes metrics generated from production activities, such as sensor readings, machine performance metrics, temperature, pressure, and flow rates. These variables are essential for monitoring and controlling manufacturing operations. *Quality control data* relates to product quality and inspection results, capturing measurements, defect detection, testing outcomes, and adherence to quality standards and specifications. *Maintenance data* provides valuable insights into equipment and machinery upkeep. It includes maintenance logs, schedules, work orders, records of equipment downtime, and failure reports, as well as predictive maintenance data derived from condition monitoring systems. *Supply chain data* encompasses procurement, logistics, and the management of raw materials, components, and finished goods throughout the supply chain. This includes inventory levels, supplier information, shipping schedules, and order status, all of which are vital for effective supply chain management. *Energy management data* focuses on energy consumption, efficiency, and optimisation within facilities. This data may involve tracking electricity, gas, and water usage, analysing energy tariffs, integrating renewable energy sources, and measuring sustainability metrics. *Environmental monitoring data* relates to the tracking and compliance of environmental conditions, such as air quality, emissions, wastewater discharge, hazardous waste management, and environmental impact assessments, ensuring adherence to regulations and sustainability goals. *Asset management data* involves the identification, tracking, and lifecycle management of physical assets. It includes information on asset inventory, asset condition, maintenance history, depreciation, and performance analysis. *Production planning and scheduling data* pertains to the management of production schedules, capacity planning, resource allocation, job orders, and production forecasts. This data is used to optimise production processes, meet demand efficiently, and maximise resource utilisation. *Labour and human resources data* covers workforce management aspects, such as employee scheduling, training records, productivity metrics, health and safety incidents, and compliance with labour regulations. *Financial data* pertains to financial transactions, budgeting, cost analysis, revenue generation, profitability, capital expenditures, and financial performance metrics. *Regulatory compliance data* is essential for meeting industry regulations, safety standards, environmental regulations, quality certifications, and other legal requirements. Finally, *remote monitoring and control data* is collected from systems like SCADA (Supervisory Control and Data Acquisition) systems, IoT devices, and centralised control systems, facilitating the oversight and control of industrial processes and equipment from remote locations.

Data quality

Maintaining high data quality is crucial for effective decision-making, process improvement, and operational efficiency. Poor data quality can lead to errors, inefficiencies, and safety risks. Addressing data quality aspects ensures that organisations have control over the *reliability* and

relevance of their data assets, enabling them to make informed decisions and enhance processes to achieve operational excellence.

Accuracy is essential for data to reflect true values or conditions, which is particularly important for precise measurements, process monitoring, and making sound decisions. For example, accurate sensor readings are vital for controlling manufacturing processes and ensuring product quality. Precision, or the level of detail in the data, is important for meaningful analysis. It allows for the detection of small variations, identification of trends, and accurate diagnosis of issues in applications - physical and digital. *Completeness* of data is necessary to provide a comprehensive understanding of processes, facilitate anomaly detection, and ensure compliance with regulations. Incomplete data can create gaps in analysis and hinder effective decision-making. Consistency involves maintaining uniformity of data across various sources, systems, and time periods. This is crucial for reliable comparisons, trend analysis, and effective integration of data from multiple sources. Inconsistent data can lead to errors and confusion. *Timeliness* refers to the relevance and currency of data for decision-making and analysis. Having timely data allows organisations to respond quickly to changing conditions, optimise processes in real-time, and avoid delays or disruptions. Relevance ensures that data is meaningful and aligned with operational objectives, performance metrics, and key performance indicators (KPIs). Irrelevant data can obscure important insights and lead to wasted resources. *Validity* is achieved when data adheres to predefined rules, standards, or criteria, which ensures its accuracy and reliability. Valid data is essential for compliance with regulations, adherence to quality standards, and maintaining industry best practices. Integrity involves protecting data from unauthorised access, tampering, or corruption. Maintaining data *integrity* is critical to safeguard sensitive information, defend against cyber threats, and ensure the reliability of data for decision-making and analysis.

Trust forwarding - an explanation

Trust forwarding is about ensuring that data stays secure, reliable, and authentic as it travels through networks. It means maintaining trust throughout the data's journey, from when it leaves a device to when it reaches its final destination. This process involves several protective steps to make sure data is not tampered with and remains secure.

First, trust is established between devices or entities in the network. This involves using methods like authentication (proving the identity of devices) and encryption (scrambling data so only the intended recipient can understand it). When data is sent, trust information, such as authentication tokens or digital signatures, is attached to it. This added information helps verify that the data is genuine and has not been altered. As the data moves through different checkpoints in the network, each device it encounters checks this trust information to confirm the data's integrity. This continuous verification process ensures that data remains reliable and secure from start to finish.

Key principles of trust forwarding include ensuring end-to-end security, so data is protected throughout its journey. Mutual authentication is also crucial, meaning that both parties - such as devices or systems - verify each other's identities to prevent unauthorised access. Data integrity checks are performed at every step to ensure no one has tampered with the information. Access controls are in place, which means only authorised users can view or modify the data, based on roles and permissions.

Secure communication protocols like TLS or SSL are used to encrypt data during transit, providing extra protection. Establishing a chain of trust involves using security anchors and certificates that guarantee the data's authenticity and integrity at every point in the network. Additionally, keeping systems securely configured and up to date is important to prevent vulnerabilities, and regular security audits help ensure everything remains protected. Monitoring and logging activities in the network allow organisations to detect any suspicious behaviour quickly and respond to potential threats.

By following these steps, organisations can build a strong system that protects sensitive data and maintains the trustworthiness of their operations. This approach helps prevent cyberattacks and ensures that critical data is always secure and reliable.

THE GAP

Across Europe, numerous initiatives aim to strengthen the connections between cloud-based ecosystems, promote fair data exchange, and accelerate digitalisation across industries. Despite these efforts, one significant barrier remains: a pervasive lack of trust and ongoing concerns about the potential unauthorised use of personal data, which hinders seamless data sharing.

At present, there is a notable emphasis on the technological components of trust and trust-forwarding in the digitalisation space. This focus is understandable, as creating de facto standards to address trust issues inherently requires technical implementation and ensuring feasibility. However, a crucial gap emerges: addressing trust solely from a technological standpoint fails to account for the holistic nature of trust requirements. As emphasised in the “The Need” section, all four trust categories must be integrated and treated as interconnected elements.

In the subsequent sections, an outline of existing data-space initiatives is provided, followed by an analysis of how core trust values and components can be leveraged and identified for efficient trust-forwarding within data spaces.

Initiatives, stakeholders, and trust values

Key initiatives, including Gaia-X, IDSA, iSHARE, FIWARE, BDVA, CSAs, Catena-X, MDS, Ind4.0, and C-Private, address parts of the challenge. Moreover, the idea of trust connectors exists to establish a European interoperable architecture for institutional and member states data exchange (i.e. gov2gov data exchange) [16]. However, the absence of a standardised trust framework still impedes secure data exchange across ecosystems. Establishing a comprehensive and agreed-upon standard for verifying and exchanging data is essential. Although advancements have been made in achieving technical and semantic interoperability, significant obstacles persist, particularly in the realms of organisational and regulatory interoperability. These challenges revolve around ensuring effective communication and collaboration while complying with regulations and legal standards, necessitating consensus on norms, regulations, and compliance mechanisms.

Different industries have different needs when it comes to data exchange, thus it is challenging to create a universal model that fits all sectors. Flexibility is key to adapting the recommendations cited in this document to meet the specific needs of each data space. To realise successful and trusted data spaces, it is important that all participants understand how the data spaces work and how the principles of trust are maintained. The success of these data spaces depends on having the right incentives in place. All parties must see the value of participating and sharing data in a trusted environment rather than sticking to the current systems.

To overcome these challenges, it is essential that the requirements for participating in these trusted data spaces and their governance structures meet the expectations and needs of everyone involved. These involved parties – stakeholders – are amongst the following:

Data Providers (i.e. producers), Data Consumers (i.e. users), Data Curators and Intermediaries, Governance Bodies and Regulatory Authorities, Cloud Service Providers, Trust Service Providers, Third-Party Auditors and Certifiers, End-Users and Citizens, Technology Providers (i.e. software, API, and protocol developers), Ethical and Privacy Advocacy Groups, Academic and Research Institutions.

Therefore, these stakeholders for trust-forwarding in data spaces are individuals, organisations, or entities involved in, or impacted by, the processes of data sharing, governance, security, and compliance within these spaces. These stakeholders play various roles in ensuring the transparency, integrity, and ethical use of data, particularly when it comes to maintaining trust and ensuring adherence to regulatory and security standards.

To map and address the needs of these stakeholders in the given initiatives and in data spaces in general, this report will base trust principles on the key values presented in the first section “The Need”, serving as a foundation for secure, ethical, and transparent data exchange. By focusing on trust aspects like data security, privacy, integrity, governance, transparency, accountability, and ethical considerations, organisations can establish a reliable framework for data sharing that aligns with all stakeholders’ needs (as depicted in the following figure).

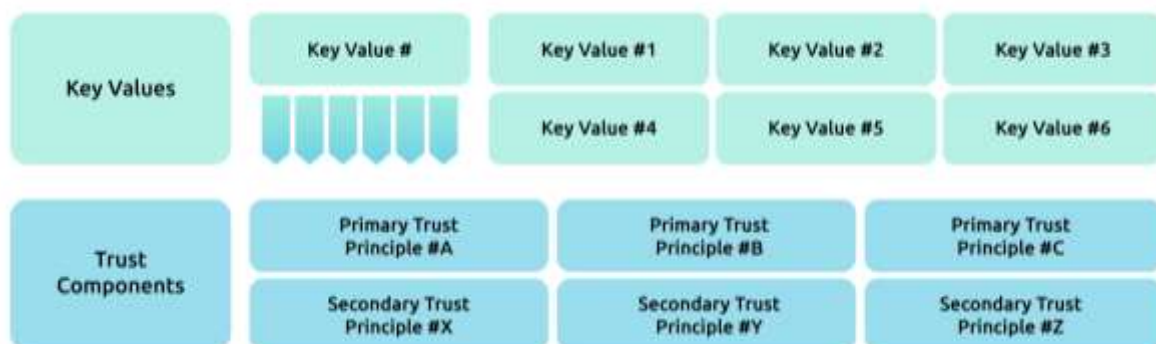


Figure 1: Key Values & Trust Components, by Arthur Strategies & Systems

Examples of derived trust components include:

- Confidentiality: Protect data from unauthorised access or disclosure during transmission and storage through robust encryption, access controls, and secure communication channels.
- Integrity: Ensure data remains accurate and unchanged, using mechanisms like digital signatures and validation checks to prevent tampering or corruption.
- Authentication: Verify identities in data exchanges, using strong methods like multi-factor authentication to prevent unauthorised access.

- Authorisation: Restrict data access based on roles and privileges, applying role-based or attribute-based controls to safeguard data.
- Non-repudiation: Provide undeniable proof of data exchange actions, employing digital signatures and audit trails to create a verifiable record.

Key Value #1 - A fair digital environment: Everyone should be able to effectively and freely choose which online services to use, based on objective, transparent, easily accessible, and reliable information.

(From the European Declaration on Digital Rights and Principles for the Digital Decade [17].)

- *Primary trust component #1.1: Data quality*
 - Secondary trust component #1.1.1: Accuracy
 - Secondary trust component #1.1.2: Integrity
 - Secondary trust component #1.1.3: Completeness
 - Secondary trust component #1.1.4: Validity
- *Primary trust component #1.2: Data privacy*
 - Secondary trust component #1.2.1: Data ownership and control
 - Secondary trust component #1.2.2: Confidentiality
 - Secondary trust component #1.2.3: Authorisation
- *Primary trust component #1.3: Transparency*
 - Secondary trust component #1.3.1: Identification of data exchange parties - Reputation
 - Secondary trust component #1.3.2: Standard data sharing contracts
 - Secondary trust component #1.3.3: Non-repudiation
 - Secondary trust component #1.3.4: Performance metrics
 - Secondary trust component #1.3.5: Audit and compliance checks
 - Secondary trust component #1.3.6: Procedures in case of breaches or misuse
- *Primary trust component #1.4: Data sharing infrastructure*
 - Secondary trust component #1.4.1: Sovereignty
 - Secondary trust component #1.4.2: Security
 - Secondary trust component #1.4.3: Interoperability
 - Secondary trust component #1.4.4: Sustainability

Key Value #2 - A protected, safe and secure digital environment: Everyone should have access to digital technologies, products, and services that are by design safe, secure, and privacy protective, resulting in a high level of confidentiality, integrity, availability, and authenticity of the information processed.

(From the European Declaration on Digital Rights and Principles for the Digital Decade [17].)

Challenges and complexities

Analysing the integration of these trust components in current initiatives reveals notable challenges. The landscape is complex, with diverse practices and expectations among different stakeholders. International literature and real-world applications often highlight varying interpretations rather than offering standardised frameworks.

One illustrative concept is that of data trusts. As a model for fostering trustworthy data environments, data trusts provide independent and fiduciary data management. They open avenues for negotiation that traditional data relationships typically lack. Implementing a data trust involves aligning on shared goals, setting up governance structures, distributing benefits equitably, and securing long-term funding. While the technological foundation for data trusts is achievable, the structures differ based on data type and context. The European Commission's mention of nine sector-specific data spaces in the Data Strategy as a corner stone of the Digital Decade 2030 strategy [3], and the mention of even more in its second staff working document on data spaces [4] (of January 2024) reflect this diversity.

Prominent initiatives like Gaia-X and IDSA emphasise values such as informational self-determination, participation, openness, and decentralisation. These principles, coupled with technical guidelines, help to prevent vendor lock-in and facilitate robust implementation. Yet, creating a truly trustworthy data space requires developing and validating a set of testable attributes. Operators and users must engage in detailed analysis and rigorous documentation to systematically establish trust. Ultimately, the real-world application and evaluation of these models will determine their effectiveness in creating dependable data-sharing environments.

THE PROPOSAL

This chapter builds on the earlier analysis and addresses the implementation of trust-forwarding principles within cloud ecosystems. Our aim is to offer concrete recommendations and outline future requirements for establishing secure and trusted data-sharing environments. By examining successful use cases and best practices from leading initiatives, we can derive key insights that inform the development of reliable and compliant cloud-based ecosystems. The following recommendations are designed to ensure that primary, secondary, and tertiary trust principles are upheld, creating a solid framework for ethical, secure, and efficient data exchange.

Future requirements and possible solutions

Trusted cloud ecosystems and data spaces possess key characteristics derived from known good practices. Access is restricted to individuals in designated roles who are authorised to view, edit, or retrieve data within the space, ensuring protection and security. Robust control and monitoring mechanisms prevent unauthorised changes to the data, maintaining its integrity in both form and content, so that the data remains recognisable and usable. Data within these spaces is maintained and accessible for specified periods of time, ensuring durability and persistence. An overseeing organisation monitors data deliveries, rejecting any unauthorised data and ensuring the security and reliability of the space. Only data in recognised, documented formats can be exchanged efficiently between data spaces, adhering to established standards and norms for interoperability. Mechanisms facilitate the search for specific subsets of data within datasets using search terms or queries, enhancing searchability. Additionally, metadata provides insights into datasets, their changes, roles involved, and underlying data structures. This metadata is crucial for introspection, reflection, and auditing purposes.

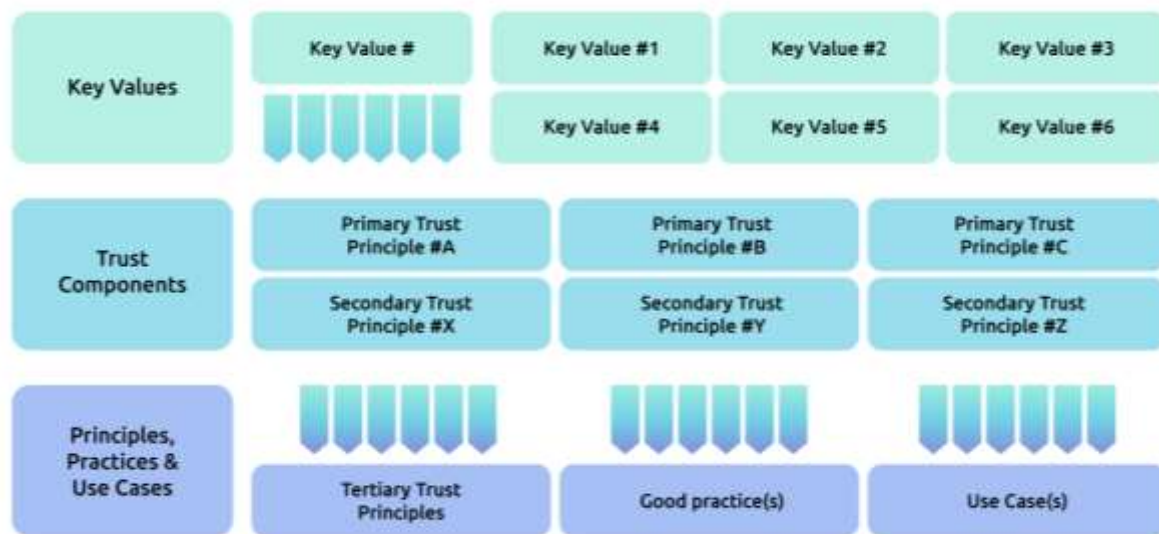


Figure 2: Key Values, Trust Components and Use Case Principles, by Arthur Strategies & Systems

Ensuring that data is protected, secure, durable, and verified is crucial for building trust among all stakeholders, especially citizens. Trust is established because protected data cannot be altered arbitrarily or without proper control. Secure data is safeguarded from unauthorised access or misuse, and durability means that data remains unchanged and accessible for the necessary duration. Reliable, audited data results from transparent processes that ensure its quality.

Having a source of high-quality, verified data that is readily available and easy to access is vital for making informed policy decisions in a democratic society. Such data, collected from reputable sources, stands apart from unverified or misleading information, like fake news. Beyond societal benefits, access to trustworthy data also drives economic growth by providing a solid basis for market decision-making. In the business world, data within organisations should be treated as a valuable asset. The field of "infonomics" [18], which merges "information" and "economics", focuses on assessing the economic value of these information assets.

Recommended actions

The research conducted for this report shows that the idea of trustworthy data spaces is still developing. One of the challenges is that there is a lack of consistency in the terms used and how roles and functions within data environments are defined. This inconsistency occurs since data spaces are designed for different purposes, which affects their structure. The latter makes it challenging to develop a clear technical model, as having precise definitions is crucial. Without these clear definitions, assumptions are made, which means the model can change depending on different interpretations.

Furthermore, the development of trustworthy data spaces is happening on an international, or at least European, level. The participants in these projects come from various countries and backgrounds, which adds another layer of complexity. As a result, it is important that the systems for managing data can work together across borders, not just in terms of technology but also the legal rules that govern them.

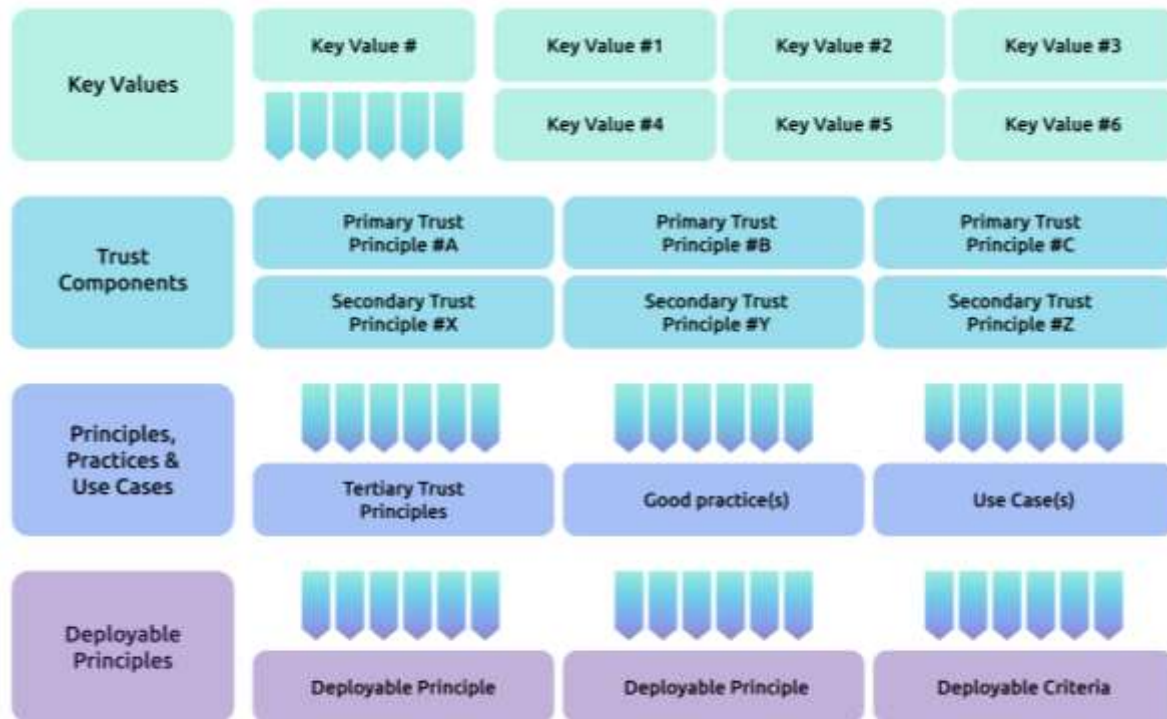


Figure 3: Collaborative Trust Framework - Structure & Flows, by Arthur Strategies & Systems

Different industries have different needs when it comes to data exchange, thus it is difficult to create a universal model that fits all sectors. Flexibility is key to adapting the ideas in this report to meet the specific needs of each data space.

To create successful and trusted data spaces, it is important that all participants understand how the data spaces work and how the principles of trust are maintained. The success of these data spaces depends on having the right incentives in place. All parties must see the value of participating and sharing data in a trusted environment rather than sticking to the current systems.

To overcome these challenges, it is essential that the requirements for participating in these trusted data spaces and their governance structures meet the expectations and needs of everyone involved. Gaia-X – for instance – addresses this as of late 2024 in their way forward [19].

How the idea maps to an initiative like Gaia-X

Gaia-X's values for fostering trust are centred around the primary and secondary trust components of *accountability, transparency, and reliability*, which have been discussed earlier in this report. These values are embedded in the Gaia-X trust framework, which is designed to ensure verifiable compliance and operational integrity across the ecosystem.

Within this trust framework, the approach is to leverage *verifiable credentials* and *linked data representations* to construct a *FAIR (Findable, Accessible, Interoperable, Reusable)* knowledge graph of verifiable claims as a tertiary trust principle use case. Verifiable credentials serve as structured data graphs that provide cryptographic proof of compliance with certifications, such as ISO standards issued by accredited bodies, and validate the occurrence of operations or interactions between entities, such as agreements or transactions. These credentials include essential details, such as the verifiable claim's subject, the entities involved, the issuer, and a digital signature that guarantees authenticity and integrity.

By doing this, Gaia-X achieves deployable principles and offers a technology stack and architecture example:

- The trust framework (designed by Gaia-X and mapped to the architecture of participating systems) ensures that stakeholders' claims and operations are verified before execution. This involves the automatic validation of credentials to confirm that all required information is complete. Technologies such as semantic-based constraint languages (e.g. SHACL) are proposed within the ecosystem to validate the completeness and correctness of credentials before granting permissions. For example, if a stakeholder claims compliance with a specific ISO certification to publish service information in a digital space (such as a marketplace), Gaia-X fosters the development of systems capable of verifying the existence and validity of the corresponding credential before permitting actions based on that claim, such as publishing a service offering.
- This verification mechanism promotes *accountability* by ensuring that all operations, interactions, and agreements are traceable and linked to the responsible parties. It enhances *transparency* by providing clear, verifiable evidence of compliance and actions within the ecosystem. Lastly, it ensures *reliability* by establishing trust through digitally signed and verified claims and operations.
- The *decentralised approach* of the digital clearing houses in Gaia-X further aims to reinforce trust. Any entity can establish a system to verify operations by creating mechanisms to validate credentials based on a unified and standardised way of describing information. As presented above, this standardisation is achieved through the *verifiable credential data model* and *semantic-based ontologies* provided by Gaia-X. These tools ensure consistency and interoperability across systems, enabling credentials and claims to be validated using a shared understanding of their structure and meaning.

This approach gives stakeholders the possibility to independently perform the verification process as well, transforming credential validation into a decentralised activity. By eliminating the reliance on a single central authority, it fosters a distributed mechanism where credentials and claims can be reliably verified across multiple independent entities, provided the data holders grant the necessary permissions or the individual accessing such data is authorised to do so.

Ultimately, in addition to fostering accountability, reliability, and transparency, Gaia-X has a plan for ensuring regulatory compliance. This is enabled in the technical design by translating regulations and policies into executable norms that can be applied to the collection of graph data about operations. To do this, norms are translated into a machine-understandable format using standardised languages such as ODRL.

Recommendations

This section addresses four key challenges. Each of them presents a key narrative and picks up the development of the recommendations by presenting detailed key information aligned with recommended actions, derived from the outlined methodology of this report. To support actionable outcomes, recommended measures are introduced as initial steps towards establishing deployable principles, providing a foundation for the formulation of a comprehensive EU strategy based on the provided recommendations.

The characteristics of robust and reliable cloud ecosystems, as described below, aim to enhance compliance with core values and trust principles (primary and secondary) while bolstering European competitiveness. The tertiary trust principles serve to illustrate the alignment of these values with practical use cases. While the foundational analysis for this discussion is provided in the earlier sections of this document, it is important to acknowledge that certain conceptual simplifications were applied to ensure clarity and focus.

The trust principles methodology, when put into action, leads to the identification of the following challenges.

Challenge #1 - Trust Principle: Transparency

Narrative

Transparency is one of the trust principles (as mentioned above), allowing for independent verification of claims and opening the door to new market players. It represents an enabler and success factor for federated multi-provider ecosystems and sovereignty. Transparency should be emphasised as a core principle of trust and certification. Transparency also plays a key role in zero-trust approaches and enables continuous verification and monitoring.

Recommended actions

- *Establish robust standards and frameworks*: Develop interoperable transparency standards aligned with trust forwarding principles, emphasising security and resilience, and create objective standards for measuring cybersecurity and resilience capabilities, combining existing certification schemes with new levelling and labelling frameworks managed by independent, accountable bodies.
- *Advance risk assessment methodologies*: Design and implement a granular risk assessment grid tailored to specific stakeholder needs, enabling informed evaluations of providers and solutions.
- *Strengthen Europe's global position*: Promote European transparency principles internationally to secure a competitive edge over less transparent markets and incorporate zero-trust methodologies to enhance secure, continuous data validation and access.
- *Enhance transparency in procurement and compliance*: Promote transparency-first procurement policies that accommodate diverse needs, integrate transparent compliance metrics into public tenders to foster fair competition and innovation, and develop shared transparency frameworks to enable independent verification of compliance and security claims.

Challenge #2 - Federated multi-provider ecosystems

Narrative

Centralised systems increase systemic vulnerabilities, are a source of conflicts of interest, and currently favour big (non-EU) market players. Encouraging the use of open-source solutions to build an interoperable base for the EU cloud ecosystem can reduce dependency on foreign technologies and enhance transparency.

Recommended actions

- Economic incentives
 - Fund research and development for *distributed and federated systems* to replace monolithic architectures.
 - Establish funding and policy support for *federated, multi-provider systems* to enhance resilience and innovation.
 - Create *incentives for SMEs and open-source initiatives* by reducing bureaucratic hurdles, such as excessive auditing requirements.
- Standardisation efforts
 - Establish standards and incentives for *multi-provider architectures that prevent single points of failure*.
- Transparent governance
 - Implement governance models aligned with *zero-trust principles*, emphasising transparency and accountability.

- Create *independent, multi-stakeholder trust councils* to oversee trust frameworks and foster fair competition.
- Include open-source solutions in procurement policies, emphasising their *transparency and collaborative approach*.

Challenge #3 - Sovereignty

Narrative

Non-EU proprietary technologies dominate the market, exposing users to vendor lock-in and undermining innovation and resilience in Europe. Additionally, reliance on non-European cloud solutions exposes European systems to extraterritorial laws, such as the Clarifying Lawful Overseas Use of Data (CLOUD) Act of March 2018 [20], which undermines data sovereignty and compromises security.

Recommended actions

- *Promote open-source adoption and SME participation*: Include open-source solutions in procurement policies to leverage their transparency and collaborative approach, and create incentives for SMEs and open-source initiatives by reducing bureaucratic barriers, such as excessive auditing requirements.
- *Enhance funding and support for resilient systems*: Establish funding programmes and policy support for federated, multi-provider systems to foster resilience and drive innovation in the European cloud ecosystem.
- *Strengthen supply chain integrity and sovereignty*: Implement audit mechanisms to ensure hardware and software in supply chains meet sovereignty requirements and mandate zero-trust compliance for systems handling sensitive data, integrating continuous validation and secure access protocols.
- *Prioritise European-led cloud sovereignty*: Support initiatives that focus on sovereign and secure cloud solutions, strengthening Europe's leadership in transparent and trustworthy digital infrastructure.

Challenge #4 - Skills

Narrative

Lack of knowledge of data sharing related technologies leads to distrust and inability to make informed decisions. Understanding the technologies behind data sharing is crucial for making informed decisions and fostering a positive attitude towards data ecosystems. The Digital Decade policy programme sets ambitious targets for 2030, aiming to have 20 million ICT specialists and ensuring that at least 80% of the population possesses basic digital skills. It also seeks to digitally transform businesses, with goals such as 75% of EU companies using cloud, AI, or big data, and over

90% of SMEs achieving a basic level of digital intensity. However, the first version of the Digital Decade report shows that, at the current pace, these targets are unlikely to be met.

Recommended actions

- Promote *existing trustworthy, efficient, sovereign, innovative, and advanced ICT services* through the use of digital infrastructures and services deployed in multi-country projects.
- Provide *exploitation strategies for advanced ICT solutions among businesses* (particularly SMEs).
- Develop and promote *dedicated skilling programmes*.

ADDED VALUE: NEW BUSINESS MODELS FOR DATA SHARING IN TRUSTABLE ENVIRONMENTS

The shift towards more transparent and secure data exchange is reshaping industries, offering new opportunities for business models centred around trust and data sharing. In today's interconnected world, data is one of the most valuable resources. However, without a secure, reliable framework for sharing and using data, its full potential cannot be realised. Trustworthy data spaces provide the foundation for innovative business models by ensuring data is protected, accurate, and accessible, while also addressing the legal and regulatory requirements that vary across sectors.

The value of data-sharing business models lies in the ability to unlock previously untapped data-driven opportunities. By creating secure, trusted environments for data exchange, companies can share insights, collaborate across industries, and access new markets. These models allow organisations to monetise their data in ways that were previously not possible, offering products and services that are based on shared, verified data, such as tailored solutions in healthcare, logistics, and finance.

A representative example of an emerging business model is the concept of data spaces or data trusts, where data is shared securely among different parties while maintaining control over sensitive information. In these models, participants can offer data access under strict conditions, ensuring compliance with privacy laws and enabling the responsible sharing of valuable datasets. This opens up opportunities for industries to develop new services and products based on the collective intelligence of multiple data providers.

Additionally, infonomics, the emerging field of valuing data as an asset, plays a key role in redefining business models. Companies can now assess the economic value of their data, leveraging it to create new revenue streams. Through the careful management and sharing of data, organisations can tap into new sources of income, expand their networks, and build new partnerships based on data-driven insights.

By fostering a data-sharing economy, businesses can engage in more strategic collaborations. These models enable new types of partnerships where data is shared between companies, governments, and even individuals, all while ensuring that privacy, security, and compliance are maintained. In these trusted ecosystems, data is not just a resource – it becomes a competitive advantage.

New business models in data sharing also present economic growth opportunities, particularly for sectors like healthcare, energy, and agriculture, where access to high-quality, real-time data can

lead to better decision-making, increased productivity, and more personalised services. For instance, healthcare providers can use shared data for better patient outcomes, while energy companies can optimise resource usage and sustainability through shared data on consumption patterns.

Ultimately, the value of these business models is not just in sharing data but in creating a culture of collaboration and mutual benefit. By removing barriers to secure data exchange and ensuring all parties involved benefit from shared data, organisations can unlock new sources of innovation, while improving trust and accountability across ecosystems.

REFERENCES

- [1] Cloud Alliance, <https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance>
- [2] European Industrial Technology Roadmap for the Next-generation Cloud-Edge, <https://ec.europa.eu/newsroom/dae/redirection/document/102590>
- [3] European strategy for data, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066>
- [4] 2nd Commission Staff working document on Common European Data Spaces, <https://digital-strategy.ec.europa.eu/en/library/second-staff-working-document-data-spaces>
- [5] European Declaration on Digital Rights & Principles, EU's "digital DNA", signed on 15 December 2022, and in force per January 2023, <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>
- [6] A Europe fit for the digital age, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en
- [7] The Path to the Digital Decade, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en#the-path-to-the-digital-decade
- [8] Cybersecurity Strategy for the Digital Decade, <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>
- [9] Strategic Compass for Security and Defence, <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>
- [10] Declaration on EU Cloud Federation: Towards a next generation cloud for Europe, <https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe>
- [11] Commissioners-designate (2024-2029), https://commission.europa.eu/about/commission-2024-2029/commissioners-designate-2024-2029_en
- [12] A new plan for Europe's sustainable prosperity and competitiveness, https://commission.europa.eu/priorities-2024-2029/competitiveness_en
- [13] European data spaces 2023, JRC, <https://op.europa.eu/en/publication-detail/-/publication/dcac6aee-0e7a-11ee-b12e-01aa75ed71a1/language-en>
- [14] Mapping the landscape of data intermediaries 2023, JRC, <https://op.europa.eu/en/publication-detail/-/publication/379cf850-4553-11ee-9854-01aa75ed71a1/language-en>
- [15] HICI: An Approach for Identifying Trust Elements The case of technological trust perspective in VBEs, <https://ieeexplore.ieee.org/iel5/4159773/4159774/04159872.pdf>
- [16] European Interoperability Reference Architecture v6.1.0, <https://interoperable-europe.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/release/610>
- [17] European Digital Rights and Principles, <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>
- [18] Douglas B. Laney, Infonomics: The Business Value of Information and How to Manage It
- [19] Gaia-X Architecture, https://docs.gaia-x.eu/technical-committee/architecture-document/latest/gx_conceptual_model/
- [20] Clarifying Lawful Overseas Use of Data (CLOUD) Act, <https://www.justice.gov/criminal/media/999391/dl?inline>