Fraunhofer ISST

Fraunhofer Institute for Software and Systems Engineering ISST

Levels of Assurance for Data Trustworthiness

A novel framework to promote trust in inter-organisational data sharing

IN COOPERATION WITH

FUJITSU

Executive Summary

The ongoing digital transformation has highlighted the critical importance of data trustworthiness, now recognised as an essential driver for innovation and growth. Untrustworthy data presents significant safety, security, and profitability risks, particularly in critical decision-making processes. To address the data usage risks faced by data consumers, Fraunhofer ISST and Fujitsu Research present a new framework for assuring data trustworthiness called Levels of Assurance for Data Trustworthiness (Data LoA).

Data LoA leverages the concept of Levels of Assurance from identity verification to promote trust and transparency in inter-organisational data sharing. The Data LoA framework involves three key actors: Data Providers, who assert a certain level of trustworthiness for their data; Assurance Providers, who independently audit and certify the trustworthiness claims made by the Data Providers; and Data Consumers, who evaluate these assertions to determine whether to use a provided data asset.

Rather than introducing a new standard, Data LoA seeks to unify new and existing data assurance approaches to create an interoperable system that can be applied across diverse industries and data types. Through its principled approach, we hope that Data LoA will facilitate a wider implementation of reliable, trusted data sharing and support initiatives such as emissions tracking and trustworthy AI development.

Authors

Fraunhofer ISST
Boris Otto
Florian Zimmer

Fujitsu Research
Takahide Matsutsuka
Mayuko Kaneko
Janosch Haber

Contact

Florian Zimmer
florian.zimmer@isst.fraunhofer.de

Fraunhofer Institute for Software and Systems Engineering ISST
Speicherstraße 6
44147 Dortmund, Germany
www.isst.fraunhofer.de

Fujitsu Research
fj-dslab-dataloa2025@dl.jp.fujitsu.com
4-1-1 Kamikodanaka, Nakahara-ku,
Kawasaki, Kanagawa 211-8588, Japan
www.fujitsu.com/global/about/research

Table of Contents

The Rising Demand for Data Trustworthiness

With the proliferation of online transactions and cloud services, digital trust is paramount. But trust goes beyond systems, organisations and individual users: data trust is now coming into focus. Information-driven technologies have been adopted across virtually all aspects of business, and due to the accelerating digital transformation, data is now the increasingly valuable commodity in which this information is stored.[i]

In 2020, the European Commission acknowledged data as an essential driver for innovation and growth in businesses and societies.[ii] This is partially grounded in the advent of large-scale Artificial Intelligence (AI), which has produced an unprecedented demand for high-quality model training data. Advances in machine learning and automated decision-making also mean that data holds value not only for the data producer and data owner but increasingly so for a diverse array of third-party data consumers.

Inter-organisational data sharing is set to contribute immense value to data-hungry AI applications. However, relying on shared data also exposes organisations to critical risks: unreliable data can lead to incorrect model predictions with significant impacts on profit, safety, and security.[1] This means that shared data often cannot – or should not – be used in critical operations, and potentially valuable data assets are left untapped.

This whitepaper introduces **Levels of Assurance for Data Trustworthiness** (hereinafter called Data LoA), a new overarching concept for assuring and assessing data trustworthiness. Data LoA unifies and standardises new and existing data trust[2] mechanisms to provide an easy-to-use tool for data providers to certify the trustworthiness of their data, and an intuitive grading system for data users to assess the trustworthiness of shared data assets.

We believe that a standardised, widely accepted framework for data trustworthiness is a crucial milestone for the future of frictionless commercial data sharing. Data LoA may also provide mechanisms for trustworthy data auditing, which is necessary for implementing and enforcing new EU regulations regarding Environmental, Social, and Governance (ESG) reporting.[iii]

> Untrustworthy data can lead to decision errors with significant impacts on safety, security and profit

1 In the context of inter-organisational data sharing, shared data refers to data made available by a data owner – not to be confused with shared access data.

2 With data trust we mean confidence in data quality, integrity and its applicability for intended use

Defining Data Trustworthiness

Data trustworthiness is usually described as the possibility to ascertain the correctness of data provided by a data source.[iv] Yet, a high degree of context and domain dependency so far have prevented the formulation of a generally accepted notion of data trustworthiness. Circumnavigating a holistic definition, literature oftentimes mentions and focuses on specific dimensions of data trustworthiness; most commonly data quality, availability, security, and compatibility.[v]

Data trustworthiness is especially closely linked with data quality, and the two terms are often used interchangeably. As data quality is a key factor for data trustworthiness and data trustworthiness assures data quality, assuring data trustworthiness also always addresses the issue of data quality assurance.

Assuring data trustworthiness means that at every step of the **Data Lifecycle,** appropriate measures have to be taken to ensure that the data's trustworthiness remains intact. Figure 1 visualises the data lifecycle for shared data, and presents examples of the data risks and data trust issues introduced at its different stages.

> Assuring data trustworthiness covers every step of the data lifecycle

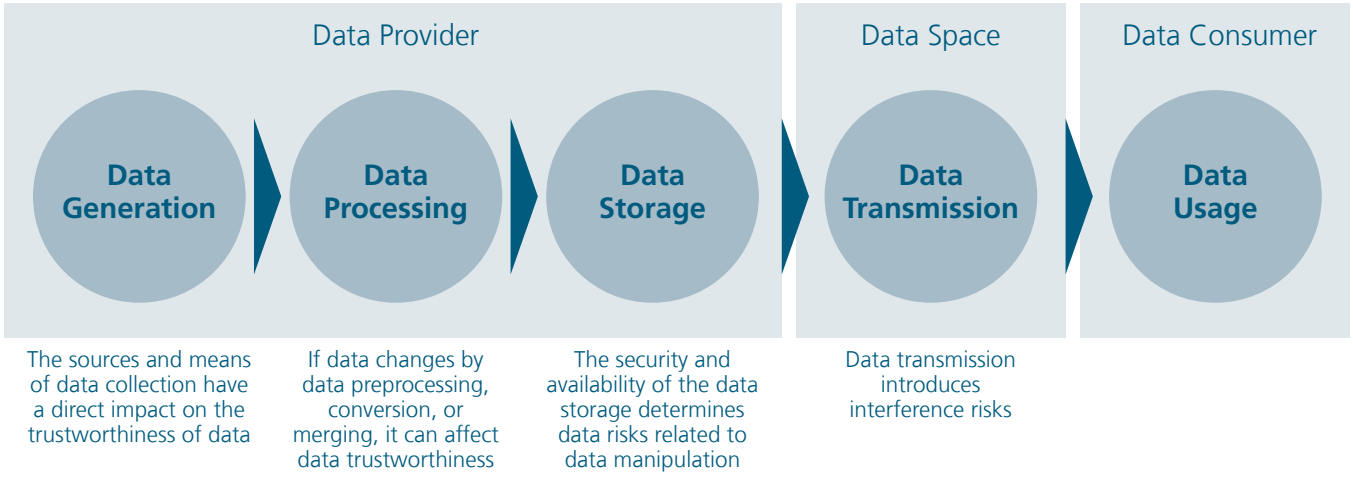

Figure 1: *The different stages of the data lifecycle for shared data. Each stage introduces specific data risks and requires certain trust measures to be implemented to create and uphold data trustworthiness.*

Data Consumer Risks in Data Sharing

A lack of trust and transparency between data-sharing participants is usually mentioned as one of the most fundamental barriers to more widespread adoption of inter-organisational data sharing.[vi] On the side of data providers, this boils down to challenges to **Data Sovereignty,** i.e. the concern to lose control over sensitive data.

In order to address these concerns, the concept of **Data Spaces** has emerged to provide an interoperable framework for data sharing under clearly defined – and automatically enforced – access and usage restrictions. However, Data Spaces rarely address the risks faced by data consumers and their need for trust in data providers and the data they provide.

In contrast to this, in the ISO/IEC 15408-1 standard for information security, data consumers are identified as risk owners – as they carry the potential risks associated with utilising (un-) intentionally modified, incomplete, low-quality, or otherwise compromised data for operational tasks such as data-driven decision-making processes.

Currently, data consumers often have no choice but to trust Data Providers and their data, as the trustworthiness of data assets cannot be readily assessed or verified.

> Data consumers who cannot validate the trustworthiness of shared data carry the risk of ill-informed decision-making

Levels of Assurance for Data Trustworthiness (Data LoA)

Fraunhofer ISST and Fujitsu Research are collaborating on an overarching solution that combines new and existing approaches to assure data trustworthiness in a standardised framework.

Our new framework for data trustworthiness aims to enable data consumers to intuitively assess the trustworthiness of the data provider's data assets. **Data LoA (Levels of Assurance for Data Trustworthiness)** reduces the risks associated with data from external sources and unlocks the operational value of third-party data assets.

We define Data LoA as the degree of confidence that a data asset's underlying information can be trusted to be true.

The foundation of our Data LoA framework is borrowed from a domain with very similar risk and transparency concerns: identity verification. Levels of Assurance (LoA) here refer to the degree of confidence that can be assigned to some kind of entity, process, or system acting or operating as claimed. LoAs are an assurance technique used to evaluate and grade complex scenarios in order to simplify and improve risk management and decision-making processes.

Examples of LoA approaches for identity validation include the ISO/IEC 29115 standard, the eIDAS regulation as proposed by the European Commission, or the NIST 800-63-A guidelines – but LoAs can be found in some other domains as well.

LoAs are risk-based, defining which dimensions of risk must be addressed and mitigated in order to assure the credibility of a claim. The different LoA levels define the processes, management activities, or technologies needed to establish a specific degree of confidence in the claimed identity. In other words, the higher the perceived risk, the greater the required confidence in the correctness of a claimed identity and, consequently, the higher the required LoA level associated with that identity claim. This relationship between risk, assurance and trustworthiness is visualised in Figure 2.

The LoA approach of assuring confidence on a few simple levels by stipulating the processes, practices, and technologies required to reach a certain certification level lends itself particularly well to the problem of assuring data trustworthiness in inter-organisational data sharing, enhancing its transparency in highly regulated data spaces and across borders.

Data LoA assesses and assures the processes, measures, and technologies involved in ensuring data trustworthiness. This covers a wide range of trust dimensions including data quality, integrity, security, and compatibility across all stages of the data lifecycle, and will take inspiration from data sharing experts such as the CEN working group on Trusted Data Transaction.[vii]

> Data LoA assures the level of confidence that a Data Consumer can put into the trustworthiness of their data

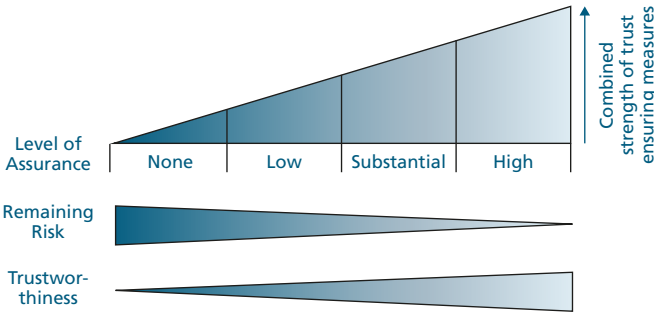

Figure 2: *The correlation between trust-ensuring measures and the risk-owner's trust in LoA-based applications. The different LoA levels specify which measures have been taken to ensure a given claim, e.g. on the claimant's identity. The higher the LoA level, the stronger the trust ensuring measures that are required to reach it – and hence, the higher the trustworthiness of the claim they relate to.*

Actors in the Data LoA Framework

We propose three main actors within the Data LoA framework: a Data Provider, a Data Consumer, and an Assurance Provider. As the diagram in Figure 3 shows, each of these actors has different responsibilities in their interaction with one another:

The **Data Provider** claims that a given data asset they provide offers a certain degree of trustworthiness. Specifically, by providing a certain Data LoA level, the Data Provider claims that appropriate measures were taken to establish a specific degree of confidence in the data's trustworthiness.

The **Data Consumer** intends to use a shared data asset, and thus carries the risk of leveraging untrustworthy data. In the LoA framework, the Data Consumer assesses provided data assurances in order to decide whether or not to use a certain data asset based on the remaining risks associated with its trustworthiness.

The **Assurance Provider** ideally should be an independent third party acting as a trustworthy auditor and assurer between the Data Provider and the Data Consumer. Although not strictly necessary, having independent audits and assurances greatly improves the amount of trust that a Data Consumer can put into the assured claims.

Levels of Assurance for Data Trustworthiness refer to the degree of confidence that a data asset's underlying information can be trusted to be true

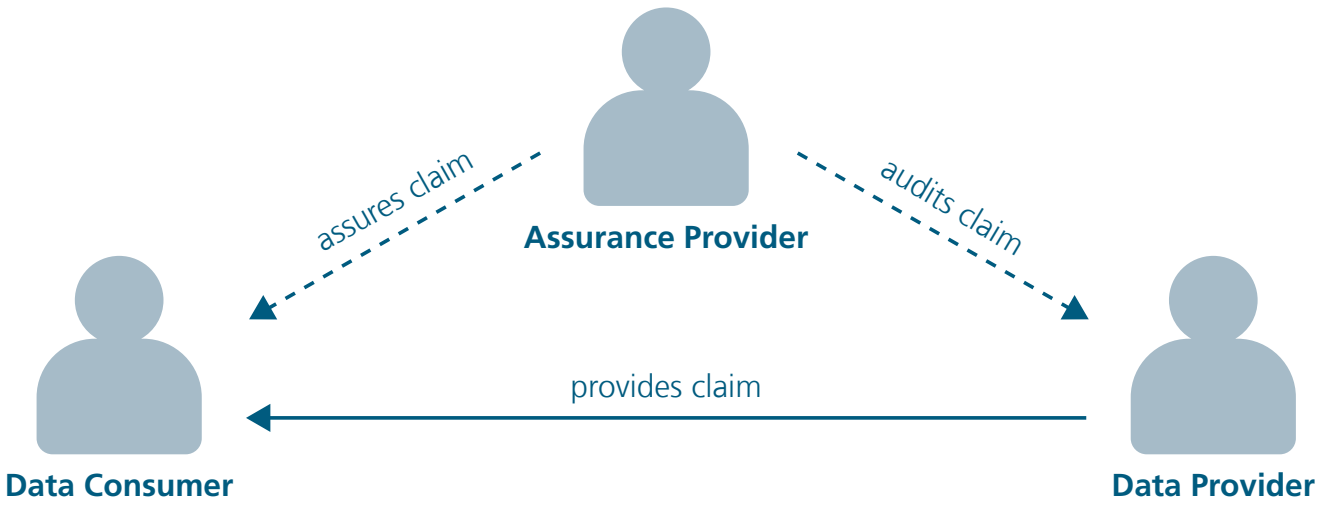

Figure 3: *Data LoA actors and their relationships. The* **Data Provider** *claims that a given data asset offers a certain degree of trustworthiness. The* **Assurance Provider** *is a trustworthy auditor who assures the Data Provider's claims. The* **Data Consumer** *assesses the data assurances to decide whether or not to use the shared data asset.*

Figure 4 shows the information flow in a Data LoA assurance process. In order to establish a Data LoA, the Data Provider needs to generate a data asset and an associated claim of trustworthiness. This claim is presented to the Assurance Provider, who conducts an audit of the given claim. To do so, the Data Provider needs to provide sufficient evidence to the Assurance Provider to substantiate their trustworthiness claim. It is then at the discretion of the Assurance Provider to certify the data asset's trustworthiness assurances at a specific level.

Assurance Providers can include reputable authorities, such as Trust Anchors and Trusted Data Sources, including governmental agencies. Given that data trustworthiness encompasses a range of factors, it might be necessary to have multiple Assurance Providers, each independently verifying specific attributes of trustworthiness. However, in certain data-sharing ecosystems, the presence of peer-controlled networks may hinder the establishment of concrete Assurance Providers at all, rendering reliance on a central authority impractical. In such cases, it may be essential to validate claims through a peer-reviewed approach.

By assessing the assured claim against the potential risks of using the data asset for a specific application, the Data Consumer can decide whether they trust the data sufficiently to use it. This means that the final risk and decision responsibility still lies with the Data Consumer, but they are now provided with much stronger, standardised evidence to inform their decision making.

LoAs are usually provided on three or four distinct levels, ranging from no or low assurances to trustworthiness to very high assurances. In the case of Data LoA, the processes, measures, and technologies involved in assuring data trustworthiness will need to cover a wide range of trust dimensions such as quality, integrity, security, and compatibility across all stages of the data lifecycle, and each Data LoA level will have its own requirements as to which degree of assurance is obtained.

To assure a claim, Data Providers need to produce sufficient evidence that proves the degree of trustworthiness associated with their data assets

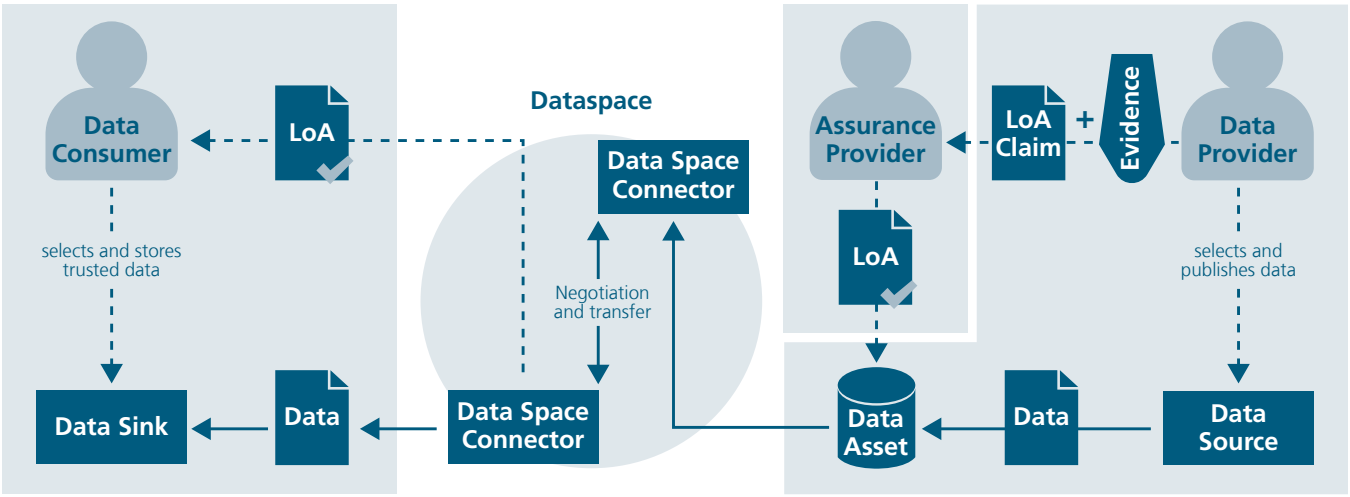

Figure 4: *Example Data LoA exchange in the context of inter-organisational data sharing in a Data Space. The Data Provider creates a Data LoA claim for a data asset generated from data stored in their data source. The Assurance Provider assesses the LoA claim against the evidence provided by the Data Provider, and assures the claimed LoA level. The data asset is then listed in the Data Space, where the data provider and data consumer negotiate a suitable data exchange through their Data Space Connectors. The Data Consumer finally verifies the Data LoA and transfers the data asset to their data sink if it meets their trustworthiness requirements.*

Value Drivers of Assuring Data Trustworthiness

The development of Data LoA is driven by use case scenarios in which having to rely on untrustworthy data can be costly, lead to non-compliance with laws and regulations, or simply is impossible due to the potential risks.

Concretely, we suggest that establishing confidence in data trustworthiness provides the most value if one or more of the following three conditions hold:

1. The Data Provider is not (explicitly) trusted.
While this may hold for any inter-organisational data sharing where trust on an organisational level has not been previously established, this value driver especially covers scenarios where Data Providers stand to benefit from providing incorrect or manipulated data – e.g. when self-reporting auditing data. In these scenarios, establishing trust through independently assuring applied trust measures can render provided data assets trustworthy even if the Data Providers themselves cannot be trusted.

2. The data transmission process is not trusted.
In an ideal case, data assets are technologically secured in their generation, transmission and utilisation. Fully securing all steps of the data life cycle, however, is not always possible or advisable, and in practice, trust oftentimes has to stand in for security. This value driver is based on scenarios where the data transmission is prone to data loss or interference, or where data travels through channels that make it more likely that data might be (unknowingly) processed or manipulated between its generation and utilisation. In these scenarios, establishing a verifiable assurance of data trustworthiness can reduce the need for fully secured solutions – in intra- as well as inter-organisational data sharing applications – and lead to higher confidence in utilising shared data for data-driven decision-making.

3. Data integrity is a critical risk.
In some data-driven applications, the sheer risk of relying on untrustworthy data is unacceptable due to the magnitude of potential consequences. This includes high-security and high-stakes critical operations where data needs to be correct, secured, and trusted. These scenarios produce the third value driver for Data LoA, which can be applied alongside established security measures to further improve the confidence in the trustworthiness of obtained data assets and their appropriateness for crucial data-driven applications.

Independent assurances of data trustworthiness can instill confidence in data even when the Data Provider cannot be trusted

Use Case Scenarios

Third-party data providers can be different operational branches, service providers, supply chain members, business partners, industry collaborators – or have no pre-existing relationship at all. Data LoA provides a standardised platform for all of these possible constellations to assure and assess the trustworthiness of data assets exchanged – independent of the industry, domain and data type.

Use Case Scenario 1: Supply Chain Traceability

When an airplane manufacturer procures parts from a supplier, they require detailed information about e.g., the materials, manufacturing processes, and quality control. To collect, store and transmit this information, a digital ledger (e.g. a **Digital Product Passport**) is assigned to each product.

In this scenario, Data LoA can be used to ensure the trustworthiness of the information stored in the ledger. Through its standardised approach, even smaller suppliers have the ability to assure and certify data trustworthiness to an internationally accepted standard, and the airplane manufacturer can easily assess and compare assurances made by different providers. This greatly simplifies and improves data orchestration, and reduces integration and security challenges for complex data ecosystems.

To add Data LoA to a digital product ledger, parts suppliers simply select one of the pre-defined Data LoA levels according to the measures they have taken to ensure its trustworthiness. This standardised approach improves transparency, traceability and efficiency throughout the supply chain and reduces costly risks of manipulation and interference.

Scenario 1

Data LoA can be used to ensure the trustworthiness of the information stored in a digital product ledger, simplifying data orchestration and reducing integration and security challenges for complex data ecosystems

Use Case Scenario 2: High-risk Data Verification

When an electricity grid provider runs automated diagnostics on operational data from the nodes in their network, they need to guarantee that all information received from these sources is genuine, correct and complete. Because this data is highly sensitive and connected to high risks when manipulated, grid providers already employ multiple data security measures. Still, risks remain as long as the trustworthiness of the received data cannot be established beyond a doubt.

In this scenario, Data LoA can be used as an additional level of assurance, automatically validating that no data has been lost or corrupted since it has been generated by a certified source. By unifying trust assuring measures for different trust dimensions, Data LoA comprehensively assures data trustworthiness beyond the security of the data transmission. This allows the grid provider to further mitigate the risks of leveraging remotely generated data – which in this case could have a severe impact on safety and security.

Scenario 2

Data LoA can be applied alongside established security measures to further improve a Data Consumer's confidence in the trustworthiness of a data asset

Use Case Scenario 3: Self-reported Emissions Auditing

When emissions data is gathered through self-reporting, auditors need to be able to verify that auditees relay their emissions data truthfully. In this scenario, Data LoA can be used to assure data trustworthiness even when Data Providers cannot be trusted to report correct data. Any trustworthiness claims made by an auditee need to be proven to the Assurance Provider, who assure data trustworthiness relative to the trust ensuring measures taken by the Data Provider.

The unified grading structure of Data LoA allows auditors to specify which standardised LoA level is required for self-reported emissions data, and clearly communicates to auditees which measures need to be employed to achieve the required degree of trustworthiness.

Scenario 3

Data LoA can be used to assure data trustworthiness even when Data Providers cannot be trusted to report correct data

Use Case Scenario 4: Federated Machine Learning

When a machine supplier wants to provide predictive maintenance or **Collaborative Condition Monitoring (CCM)** for their devices, they need operational data from a diverse set of machine operators to develop and run dedicated prediction models.

In recent years, **Federated Learning** has emerged as a new machine learning paradigm allowing for privacy-preserving AI model development. In Federated Learning, individual data providers train relatively small model updates locally, and only send updated model parameters rather than the raw training data to be integrated in a central, joint model.

Utilising Federated Learning to develop a predictive model for the CCM use case, the machine supplier has no insights into what data has been used by machine operators to develop their local model updates. This means that they are at risk of basing their maintenance predictions on bad, fake, artificial or even maliciously modified data – which can have potentially significant consequences on machine safety.

In this scenario, Data LoA can be used to assure that relevant measures have been taken to ensure that all local training data is genuine and trustworthy. This reduces the risk of prediction mistakes due to bad data and improves the reliability, trustworthiness and impact of maintenance suggestions.

Scenario 4

Data LoA can be used to assure that AI model training data is genuine and trustworthy

Implementing the Data LoA Framework

Data LoA is being developed on a conceptual level to align with the complex design requirements stipulated by real-world data sharing use cases. The successful implementation of Data LoA hinges on a collaborative approach that brings together diverse stakeholders to define clear specifications and build a robust ecosystem. This section outlines key action plans to foster collaboration and ensure the framework's relevance and effectiveness.

To ensure the successful implementation of Data LoA, a collaborative approach centred around leveraging existing industry bodies is paramount. We propose utilising platforms and working groups already operated by these organisations, as these bodies possess established relationships with domain experts, potential users (Data Providers and Consumers), and Assurance Providers, offering an ideal foundation for fostering discussions, sharing best practices, and contributing to the continuous evolution of Data LoA. By tapping into the resources and expertise of existing industry bodies, we can accelerate the development of Data LoA and maximise its relevance and penetration within specific sectors.

Data trustworthiness definitions and requirements will vary across industries and data types. We therefore advocate for the collaborative development of LoA profiles tailored to specific use cases. These profiles will provide concrete guidance on the specific controls, processes, and evidence required to achieve each Level of Assurance within a given domain.

Through this setup, we hope that Data LoA will be a crucial milestone in the development of inter-organisational data sharing where a trust barrier between Data Providers and Data Consumers currently introduces friction in the data sharing process and prevents a more wide-spread adoption. We however also believe that it is an attractive new framework for e.g. the increasing efforts in reporting on Environmental, Social, and Governance (ESG) and for introducing new approaches to developing reliable and trustworthy AI applications.

To ensure the successful implementation of Data LoA, a collaborative approach centred around existing industry bodies is paramount

References

i Otto, B., ten Hompel, M., and Wrobel, S., editors (2022). *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage. Springer eBook Collection.* Springer International Publishing and Imprint Springer, Cham, 1st ed. 2022 edition.

ii European data strategy. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

iii Regulation (EU) 2024/3005 of the European Parliament and of the Council of 27 November 2024 on the transparency and integrity of Environmental, Social and Governance (ESG) rating activities, and amending Regulations (EU) 2019/2088 and (EU) 2023/2859. https://data.consilium.europa.eu/doc/document/PE-43-2024-INIT/en/pdf

iv Haron, N., Jaafar, J., Aziz, I. A., Hassan, M. H., and Shapiai, M. I. (2017). Data trustworthiness in internet of things: A taxonomy and future directions. In *2017 IEEE Conference on Big Data and Analytics (ICBDA),* pages 25–30.

v Xu, J. and MacAskill, K. (2023). A carbon data trustworthiness framework for the construction sector. In *Proceedings of the 2023 European Conference on Computing in Construction and the 40th International CIB W78 Conference,* Computing in Construction. European Council for Computing in Construction.

vi Jussen, I., Schweihoff, J., and Möller, F. (2023). Tensions in inter-organizational data sharing: Findings from literature and practice. In *2023 IEEE 25th Conference on Business Informatics (CBI),* pages 1–10. IEEE.

vii CEN/WS TDT (July 2024). Trusted data transaction: Part 1: Cwa 18125. https://www.trusted-data-transaction.org/en/

Image Credits

©Angs – AdobeStock, title, p.5
©Image generated with Adobe Firefly, p.4
©JR-50 – AdobeStock, p.6
©main_asn – AdobeStock, p.13