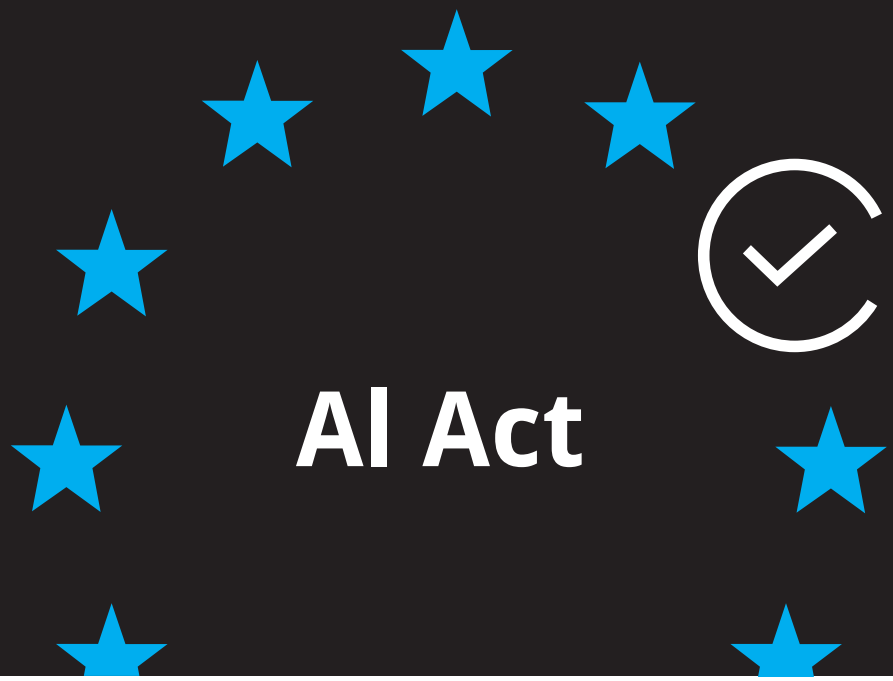
INTERNATIONAL DATA SPACES ASSOCIATION

Position Paper | March 2024

Data Spaces for the AI Act –

Analysis of the Standardization Request Regarding the European AI Act in the Context of Data Spaces



- ● Position Paper of members of the IDS Association and of the IDS-Industrial Community
- ○ Position Paper of bodies of the IDS Association
- ○ Position Paper of the IDS Association
- ○ White Paper of the IDS Association

Publisher

International Data Spaces Association
Emil-Figge-Str. 80
44227 Dortmund
Germany

Authors

Dr. Frank Wisselink, T-Systems
Sebastian Steinbuss, IDSA
Peter Koen, Microsoft

Cite as

Wisselink F., Steinbuss S., Koen P.: Data Spaces for the AI Act – Analysis of the Standardization Request Regarding the European AI Act in the Context of Data Spaces, International Data Spaces Association, March 2024
https://doi.org/10.5281/zenodo.10839129

Contributing organizations

INTERNATIONAL DATA SPACES ASSOCIATION

T Systems

Microsoft

Table of content

Summary

Currently the European Union (EU) is deciding on new regulation concerning artificial intelligence, also called the EU AI ACT. (1) It is a binding legislative act, which must be applied in its entirety across the EU. (2). Standards will provide the base for the implementation of the AI ACT. CEN/CENELEC has received a request from the EU to draw up and adopt European standards or European standardization deliverables in support of the AI Regulation. (3)

This so called "Standardization Request " (4) contains a for Data Spaces relevant requirement being "standardization deliverable(s) on governance and quality of datasets used to build AI systems". In this part the following needs to be standardized:

- specifications for adequate data governance and data management procedures to be implemented by providers of AI systems (with specific focus on data generation and collection, data preparation operations, design choices, procedures for detecting and addressing biases or any other relevant shortcomings in data).
- specifications on quality aspects of datasets used to train, validate, and test AI systems (including representativeness, relevance, completeness, and correctness).

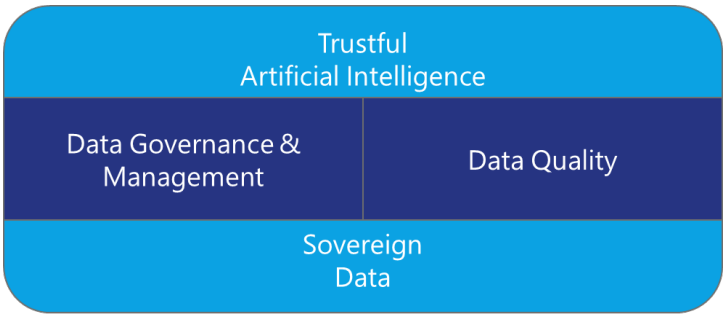


Figure 1 Relationship of Trustful Artificial Intelligence and Sovereign Data

While AI heavily depends on data and as described above on data governance, data management and quality of data, the concept of data spaces addresses this need and can be considered a foundational aspect to AI solutions, to fulfil several requirements of the upcoming AI act. Data Spaces provide a governance scheme for data ecosystems including various sets of policies for participants, as well as the provisioning, access, and usage of data in a data space. The technical components of a data space, i.e., data space connectors as participant agents that act on behalf of an organization and data ecosystem services, implement those aspects including the management and validation of participant's claims. The management of Trust between participants is a core function of data spaces and is specified in an extensible manner. AI related data management processes can be realized and validated, including proofs or claims. Trusted data sharing contracts in a data space enable the management of such proofs, which also include provenance tracking, and traceability of data assets, also providing observability of data transactions, if required.

Data spaces are already part of the international European standardization process and are being considered a reference and foundation for standardization activities of the AI act.

Furthermore, as AI models and the interaction between users and the models are also data, they may be considered as data assets of a data space which can be shared through data

spaces. With this regard such models may be managed with access and usage control mechanisms, as well as quality metrics like the source data as described in this document.

This paper describes how the requirements of the standardization request can be realized with the support of data space concepts, potential gaps, and further work.

1 Introduction

1.1 Scope

As depicted in Figure 2 this paper discusses the foundation of sovereign data management in data spaces and their usage to fulfil the requirements of the EU Standardization Request of the AI Act. The core consists of Data Governance & Management and Data Quality concepts of Data Spaces to enable the use of Trustful AI in Europe with Sovereign Data Concepts.

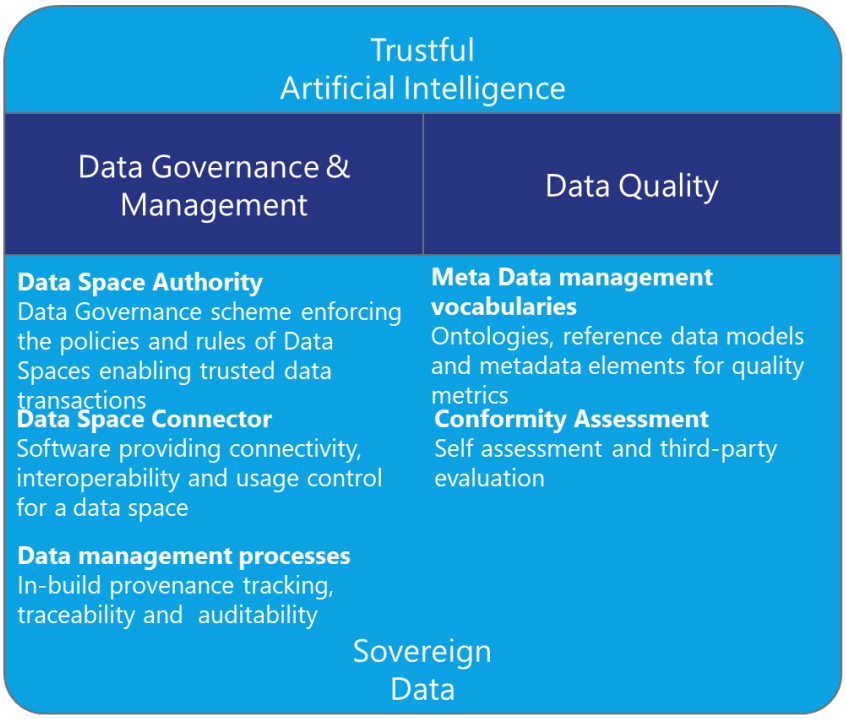


Figure 2 Data quality related requirements of the AI Act

1.2 Purpose of this document

The purpose of this paper is to highlight the importance of data space technology in the fulfilment of the requirements of the EU and the Standardization Request for the AI Act. In this document you will see an outline of the Standardization Request of the AI Act and the core concepts of data spaces. Data Spaces can support the fulfilment of the AI Act requirements in the field of Data Quality and Data Governance & Management. This document shall function as a foundation for discussion and serve the process of standardization activities.

2 Data governance and data quality metrics requirements from the AI act

The EU Artificial Intelligence ACT (1) is currently in its final state of drafting and political negotiation. The European AI Act is a comprehensive regulatory framework aiming to govern the development and deployment of artificial intelligence within the European Union, emphasizing high-risk applications, transparency, and human-centric values. The act regulates the use of Artificial Intelligence systems. Noncompliance can lead to penalties in the order of magnitude of several percent of yearly revenue per case. Companies will have to implement this binding legal regulation (2) if they offer AI products as defined in the AI Act and provide services on the EU market. In December 2023 the political agreement on the AI Act has been achieved by the co-legislators (5). Companies are expected to implement the necessary measures to comply with the act within 2 years. Standardization will be an important instrument for the implementation of the AI Act. CEN/CENELEC has been requested by the European Commission to draft these standards. The standardization request (3) contains regular engineering topics like risk management or logging and AI specific topics, such as the "governance" and quality of datasets used to build safe and trustworthy AI systems." Standards addressing this request are under development, considering the data life cycle and data quality models, measures, and objectives. The functionality of data spaces and the concept of sovereignty are an ideal solution to support AI Systems to fulfill parts of the data management requirements as envisioned by the EU. The core concepts of data spaces are a very compelling solution to the standardization requests.

3 Data spaces core concepts

The main concern in the concept of data spaces is data ownership/sovereignty. A data subject needs to stay in control of the usage of the data provided. This requirement leads to the need for a governed ecosystem based on interoperable data services and the clear and interoperable definition of data access and usage rules to implement trusted data sharing.

Based on this, the concepts of Data Spaces offer a foundation which is well suited for the requirements of AI systems as described above. A participant in a given Data Space connects via its participant agent, the Data Space Connector (see (6) and (7)), this agent can fulfil specific tasks regarding the quality of data, as well as governance. Measures for data quality and data quality management can be evaluated and certified via a self-assessment (declaration) or via third party evaluation. The results of this evaluation are provided as digital claims enabling trusted data sharing in the process of providing data for AI. By making use of the observability mechanisms of data spaces, sharing can be tracked, enabling observability of data usage or providing traceability for data provenance.

In general, a Data Space defines a clear governance structure for its participants, defined by the Data Space Governance Authority and provided as technical policies and business rules to which the participants need to adhere to. These policies and rules can easily be extended with data quality and quality management measures. To do so, the Data Space Governance Authority will add rules for data governance, based on existing and agreed standards and the requirements of the specific data space domain.

3.1 Foundational Roles in a Data Space and shared responsibility

The concept of data spaces as governed ecosystems of data providers and data consumers where data can be exchanged and shared in peer to peer relationships among many parties relies on a fundamental role model, which distinguishes at least three perspectives (see (8))

- The Data Space Governance Authority is a governing and management body defining the rules of the data space. Although it is defined as a body, it is not necessarily a legal organization or a centralized system. Depending on the requirements, policies and rules, the Data Space Governance Authority can also be implemented as a set of agreements between participants, leading to a decentralized system, or it can be implemented as a federation of authorities represented by multiple organizations.
- Data space participants are legal entities, which provide and consume data and services to the ecosystem under the agreed policies and rules of the data space. They implement the policies and rules via a management system or via technical means.
- Data space ecosystem services are optional concepts in a data space, which provide value adding services to the ecosystem. A clearing and logging service to provide observability and auditability is one example of such ecosystem services.
- Conformity assessment bodies or evaluators provide means for self-assessment (declaration) or third-party assessments, which validate the implementation of required processes (a management system) or systems and issue digital claims.

Due to the collaborative aspects of data spaces, the system is based on shared responsibility principles. The responsibilities of each role need to be clearly defined and are subject of the data space policies and rules. Nevertheless, some of the responsibilities are inherent to the structure and characteristics of the data space concept itself:

- The Data Space Governance Authority is responsible to provide and enforce the policies and rules of the Data Space, including the onboarding of participants, including the issuing and a validation of the membership credentials and their revocation, especially in the case where a participant does not adhere to the given rules.
- A Participant needs to implement the given rules of a Data Space and specify policies for data and service usage as a provider. To be a trustworthy partner in such an ecosystem, the consuming participants provide claims about their internal system structures and management processes to provide evidence on the implementation of the required policies.
- All Data Space ecosystem services will implement at least the requirements of the participants.

The IDSA Rulebook (8) provides an overview of the different policies applicable in the context of Data Space (see Figure 3). Policies in Data Spaces are ideally suited to provide guidance for data usage in AI scenarios. Four distinct kinds of policies are distinguished:

- Membership policies simplify trust creation in the Data Space by providing base attributes required for participation.
- Access policies control the access to data and services.
- Contract policies control under which conditions data can be shared, including environments and system requirements.
- Usage policies control how data can be used once shared and thus describe rights and obligations for the data usage.

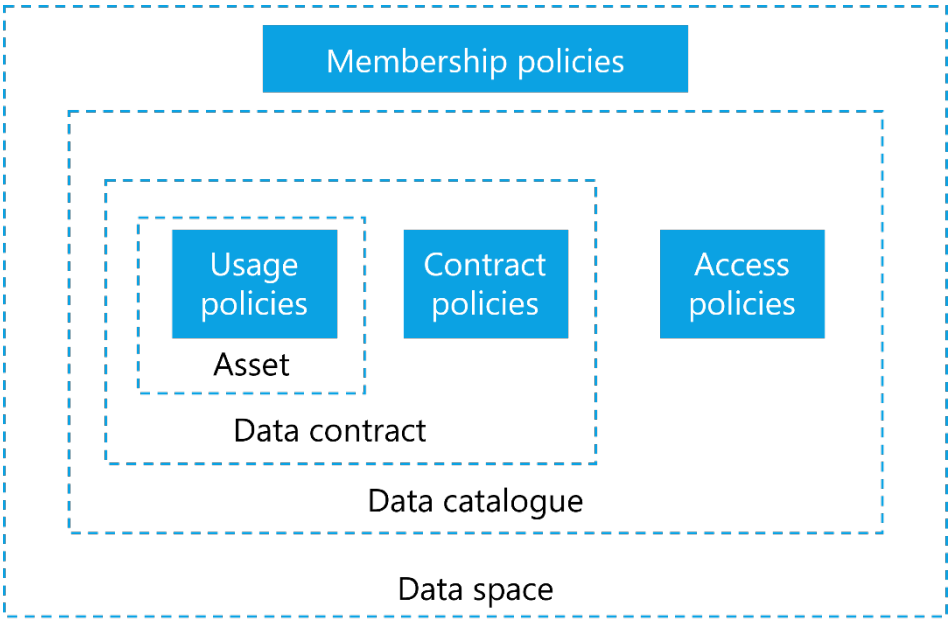


Figure 3 Different policies in data spaces, source: IDSA Rulebook (8)

Those measures enable reliable data usage in AI scenarios for all parties and support achieving the requirements from the AI Act.

3.2 Parameters

The concept of Data Spaces is meant to be a generic foundation for data-driven business-ecosystems. As such, it needs to be extensible with domain or application specific processes, tools, and rules. For use in the context of the requirements of the AI act, technical descriptions towards data quality aspects in AI Data Spaces need to be defined, as described in the subsequent chapter. Additionally, management processes for the evaluation of data quality need to be available and agreed in such data spaces and measures to assess the conformance of such processes to the requirements need to be established as part of an overarching Data Space certification framework (see (9)).

4 Data quality aspects in data spaces

Data Spaces are an important enabler to make AI safe and trustworthy. Data Quality needs to be provided by the usage of technical means and by establishing management processes, as described in the section above. Furthermore, data quality needs to be described and data

needs to be shared in data-driven value-chain to support AI services and models. To do so, data needs to be defined and made available with technical and semantic interoperability. The usage of linked data principles and semantic data descriptions as described for Data Spaces (6) is an important enabler for AI. Data Quality descriptions and metrics need to be described using Meta Data and reusable, standardized vocabularies. Data Spaces provide tools and measures to support such requirements, however the definition of vocabularies and meta data needs to be provided by the application domain, in this case the general domain of AI.

5 Data Spaces are predestined to enable safe and trustworthy AI

This paper presents the standardization requirements based on the AI Act with regards to data quality and how the concepts of Data Spaces can be used to achieve those. Data Spaces provide means to achieve trustworthy ecosystems, interoperability, and governance for data-driven business-ecosystems (10), such as AI. Such aspects are a strict requirement for the application of AI in industrial use cases. The usage and extension of the existing Data Space concepts, tools and processes provide an ideally suited foundation. Data Spaces are used in practical implementations and are subject to current international standardization.

6 Related standards and standardization activities

- ISO/IEC 8183 Data Quality for Analytics and Machine Learning: Data Life Cycle
  - Scope: ISO/IEC 8183 (11) provides an overarching data life cycle framework that is instantiable for any AI system that is applicable across different levels of the organization from idea conception to system decommissioning stages with common terminologies and processes.
- ISO/IEC 5259-x Data Quality for Analytics and Machine Learning
  - Scope: A holistic approach is needed to oversee the implementation and operation of data quality measures, data quality management requirements and guidelines, and data quality process for various types of analytics and machine learnings with adequate controls throughout the ISO/IEC 8183 AI Data Life Cycle Framework.
- ISO/IEC 5259-1 Overview, terminology, and examples
  - Scope: This document provides the means for understanding and associating the individual documents of the ISO/IEC "Artificial intelligence — Data quality for analytics and ML" series and is the foundation for conceptual understanding of data quality for analytics and machine learning. It also discusses associated technologies and examples (e.g., use cases and usage scenarios).
- ISO/IEC 5259-2 Data Quality Measures (WORKING DRAFT)
  - Scope: This document provides a data quality model, data quality measures and guidance on reporting data quality in the context of analytics and machine learning (ML). This document is built on ISO 8000 series, ISO/IEC 25012:2008 and ISO/IEC 25024. The aim of this document is to enable organizations to

achieve their data quality objectives and is applicable to all types of organizations.

- ISO/IEC 5259-3 DQ Management Requirements & Guidelines
  - Scope: This document specifies requirements and provides guidance for establishing, implementing, maintaining, and continually improving the quality of data used in the areas of analytics and machine learning. This document does not define a detailed process, methods, or metrics. Rather it defines the requirements and guidance for a quality management process along with a reference process and methods that can be tailored to meet the requirements in this document. The requirements and recommendations set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size, or nature.
- ISO/IEC 5259-4 Data Quality Process Framework
  - Scope: This document provides general common organizational approaches, regardless of type, size, or nature of the applying organization, to ensure data quality for training and evaluation in analytics and machine learning. It includes guidelines for (a) supervised machine learning regarding the labelling of data used for training machine learning systems, including common organizational approaches for training data labelling; (b) unsupervised machine learning; (c) semi-supervised machine learning; and (d) reinforcement machine learning. This document is applicable to training and evaluation data that comes from different sources, including data acquisition and data composition, data pre-processing, data labelling, evaluation, and data use. This document does not define specific services, platforms, or tools.
- ISO/IEC 5259-5 Data Quality Governance Framework
  - Scope: This document provides a data quality governance framework for analytics and machine learning to enable governing bodies of organizations to direct and oversee the implementation and operation of data quality measures, management, and related processes with adequate controls throughout the data life cycle. This document can be applied to any analytics and machine learning. This document does not define specific management requirements or process requirements specified in 5259-3 and 5259-4 respectively.
- ISO/IEC 5259-6 Data Quality Visualization
  - Scope: This document is an overview of data visualization within the context of Artificial Intelligence (AI) and Machine Learning (ML) applications. It is intended to provide examples of where data visualization may be employed by various stakeholders at different stages of the AI life cycle.
- ISO JTC1/SC38 AWI 20151 Information technology - Cloud computing and distributed platforms - Dataspace concepts and characteristics
  - Scope: Describe the concept and the characteristics of dataspaces created for the purpose of data sharing, including characteristics such as trust created through agreed policies, models, technologies and processes and identification and review of existing projects and standards that relate to or support dataspaces, including data sharing frameworks and applicable cloud deployment models.

- ISO JTC1/SC38 TS 10866 Digital Sovereignty and organizational autonomy
    - Scope: To cover Use Cases, which describe the need for organizational autonomy and digital sovereignty.
- CEN/CENLEC Trusted data transactions
    - Scope: Establish terminology, describe concepts and mechanisms in the field of data exchange to form a foundational understanding on which trusted data transactions can be based. To identify attribute-based criteria for the decision-making grid that baselines how to create trust in data transactions, while being independent of architectural choices or technical implementations. It can be used in all cases where stakeholders need to establish trust for the purpose of data exchange.
- IEEE P3800 Data Trading System
    - Scope: Create a family of standards to support and enable Data Trading.
- CEN/CENELC Focus Group on Data, Dataspace, Cloud and Edge
    - The CEN/CENELC Focus Group on Data, Dataspace, Cloud and Edge was established in March 2024 and has a foreseen lifetime for three years. The Focus Group has the goal to identify standardization needs in relation to Data, Dataspaces, Cloud & Edge and how to address them, the data economy along the value chain in various dataspaces, data governance, data interoperability and quality.

7 Outlook

The document provides a first assessment of the EUs AI Act requirements for standardization and how data space concepts can support this. Including a list of existing standards and ongoing standardization activities, it shall function as a foundation for discussion and to provide transparency to the experts in the field. Based on the feedback to this document and the preliminary results of ongoing work and discussions an updated version of the document will be provided in the future.

References

1. **Office, European Union Publications.** [Online] [Cited: 06 15, 2023.] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.
2. **General, European Union Directorate.** [Online] [Cited: 6 15, 2023.] https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en.
3. **European Union, European Commision.** [Online] [Cited: 06 15, 2023.] https://single-market-economy.ec.europa.eu/single-market/european-standards_en#:~:text=Standards%20ensure%20interoperability%20and%20safety,support%20EU%20legislation%20and%20policies..
4. **Commission, European Union European.** [Online] [Cited: 06 15, 2023.] https://ec.europa.eu/docsroom/documents/52376.
5. **Commission, European.** European approach on Artificial Intelligence. [Online] Decmber 2023. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.
6. **International Data Spaces Association, e.V.** *IDS Reference Architecture Model 4.* Dortmund : International Data Spaces Association, 2023. IDS-RAM 4.
7. **Steinbuss, Sebastian and Giussani, Giulia.** *Data Connector Report.* Dortmund : International Data Spaces Association, 2024. 11.
8. **International Data Spaces Association, e.V.** *IDS Rulebook.* Dortmund : International Data Spaces Association, 2023. 2.
9. —. *IDS Certification Scheme V2.* Dortmund : International Data Spaces Association, 2021.
10. **Nagel, Lars and Lycklama, Douwe.** *Design Principles for Data Spaces.* s.l. : OpenDEI, 2021.
11. **ISO/IEC JTC 1/SC 42 Artificial intelligence .** *ISO/IEC FDIS 8183 - Information technology — Artificial intelligence — Data life cycle framework.* s.l. : ISO. ISO/IEC FDIS 8183.