FINAL DRAFT
International Standard

ISO/IEC
FDIS
20151-1

Cloud computing and distributed platforms — Dataspaces —

Part 1: Concepts and characteristics

ISO/IEC JTC **1**/SC **38**

Secretariat: **ANSI**

Voting begins on:
2026-08-25

Voting terminates on:
2026-10-20

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC FDIS 20151-1:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **3**
5 Trusted data sharing using dataspaces ... **3**
5.1 General ... 3
5.2 Features and examples ... 4
5.2.1 Features ... 4
5.2.2 Examples ... 4
5.3 Operation ... 5
5.3.1 General ... 5
5.3.2 Interaction phases ... 6
5.4 Organizational autonomy ... 7
5.5 Data governance ... 7
5.6 Organizational interoperability ... 8
6 Dataspace concepts and related characteristics ... **9**
6.1 General ... 9
6.2 Maintain control ... 9
6.2.1 Concept ... 9
6.2.2 Characteristics of maintaining control ... 9
6.3 Establish trust ... 12
6.3.1 Concept ... 12
6.3.2 Characteristics of establishing trust ... 12
6.4 Discover data ... 14
6.4.1 Concept ... 14
6.4.2 Characteristics of discovering data ... 14
6.5 Negotiate data sharing contracts ... 15
6.5.1 Concept ... 15
6.5.2 Characteristics of negotiating data sharing contracts ... 15
6.6 Orchestrate data sharing and data use ... 16
6.6.1 Concept ... 16
6.6.2 Characteristics of orchestrating data sharing and data use ... 16
6.7 Observe actions ... 16
6.7.1 Concept ... 16
6.7.2 Characteristics of observing actions ... 17
6.8 Provide interoperability ... 17
6.8.1 Concept ... 17
6.8.2 Characteristics of providing interoperability ... 17
6.9 Optional services ... 18
7 Dataspace functional components ... **19**
7.1 General ... 19
7.2 Multi-level policies ... 19
7.3 Semantic models ... 20
7.4 Communication protocols ... 20
7.5 Processes and rules ... 21
Bibliography ... **23**

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Cloud computing and distributed platforms*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

Introduction

The use of data is now part of every aspect of the organization and the ecosystems in which it operates – such as supply chains, marketplaces and regulatory jurisdictions. As such, the value derived from the use of data is an important part of most economies.

When an organization itself generates data, it can govern, manage and extract the appropriate value from that data. However, much of the data used by an organization comes from others – along with possible restrictions on its use. Similarly, some of the data the organization generates can, with agreement, be used by others. To facilitate this use of data across multiple organizations – and to respect the rights and obligations associated with data while doing so – a method of trusted data sharing is needed.

Dataspaces provide a scalable and more automated approach to organizational agreements, and supporting software services that together enable trusted data sharing.

By providing clarity on the description of the data that is available to be shared as well as the agreed uses for the shared data, both the data provider and data recipient can make clear choices about data and improve its operational management as well as its overall governance and value.

This document provides an overview and concepts of dataspaces and their essential and optional characteristics. It builds on other cloud computing and distributed platforms documents such as ISO/IEC 22123-1 [1], ISO/IEC 23751 [2] and ISO/IEC 5140 [3] which describe cloud computing, data sharing agreements and multi-cloud concepts.

© ISO/IEC 2026 – All rights reserved

Cloud computing and distributed platforms — Dataspaces —

Part 1: Concepts and characteristics

1 Scope

This document specifies the foundational concepts for dataspaces and their essential characteristics. This document is applicable to all organizations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 22123-1, *Information technology — Cloud computing — Part 1: Vocabulary*

3 Terms and definitions

For the purposes of this document, the following terms and definitions given in ISO/IEC 22123-1, and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
dataspace
data space
environment (3.14) enabling trusted *data sharing* (3.6) between participating parties, based on an agreed *governance framework* (3.13), along with an agreed set of policies, semantic models, standardized protocols, processes, and facilitating services

3.2
dataspace participant
participant
party that is acting in a *dataspace participant role* (3.3)

Note 1 to entry: By being accepted to be a participant in the dataspace, the party agrees to the governance arrangements and therefore the policies of the dataspace.

3.3
dataspace participant role
participant role
set of activities within a *dataspace* (3.1) for the purpose of *data sharing* (3.6) or related activities

Note 1 to entry: Related activities can include auditing or observing roles that do not include data sharing or governance activities.

© ISO/IEC 2026 – All rights reserved

3.4
dataspace governance authority role
DSGA role
set of activities provided by one or more parties that establishes, governs, manages and enforces the technical policies and business rules of a *dataspace* (3.1)

3.5
data policy
human and machine-readable set of rights and obligations regarding access and use of data

3.6
data sharing
<dataspace> access to the same data by more than one authorized entity

Note 1 to entry: Use of the data can be synchronous or asynchronous.

Note 2 to entry: Data can be shared, for example, (i) by allowing access to, or the execution of operations over, the original dataset, or (ii) by giving a copy of the data to the interested entity.

Note 3 to entry: The way in which data is shared fundamentally influences the available controls and the statements needed in a data sharing agreement.

[SOURCE: ISO/IEC 23751:2022 [4], 3.7, modified - removed 'or processing of']

3.7
data sharing contract
formal and legally binding agreement between *dataspace participants* (3.3) containing policies, terms and conditions for *data sharing* (3.6)

Note 1 to entry: Data sharing contracts usually contain information about access to data, including its metadata, and data use.

Note 2 to entry: A data sharing contract is usually much more specific than a data sharing agreement which is often broader and often at an organizational level.

3.8
data use
handling or dealing with data for a specific purpose

[SOURCE: ISO/IEC 5207:2024 [5], 3.30, modified – Note 1 to entry removed]

3.9
trust
assumption that a product, service or entity will behave as expected for a given circumstance

3.10
trust anchor
well-defined, shared authority that creates *assurances* (3.11)

Note 1 to entry: The authority is shared in the sense that its services are used by multiple parties.

Note 2 to entry: The trust anchor can be relied on without the use of other parties.

3.11
assurance
grounds for justified confidence that a claim has been or will be achieved

[SOURCE: ISO/IEC/IEEE 15026-1:2019 [6], 3.1.1]

3.12
governance
human-based system comprising directing, overseeing and accountability

[SOURCE: ISO/IEC 38500:2024 [7], 3.3]

© ISO/IEC 2026 – All rights reserved

3.13
governance framework
strategies, policies, decision-making structures and accountabilities through which the organization's *governance* (3.12) arrangements operate

[SOURCE: ISO/IEC TR 38502:2017 [8], 3.1]

3.14
environment
context determining the setting and circumstances of all influences upon a system

Note 1 to entry: The environment of an entity of interest includes external entities that can have various influences upon an entity, such as developmental, technological, business, operational, organizational, political, economic, legal, regulatory, ecological and social influences as well as external physical effects such as electromagnetic radiation, charged particles, gravitational effects, and electric and magnetic fields.

Note 2 to entry: A label attached as a qualifier to the term environment identifies a particular context within another context, such as development environment, test environment, and operational environment.

[SOURCE: ISO/IEC/IEEE 42010:2022 [9], 3.13]

4 Abbreviated terms

API	application programming interface
DSGA	dataspace governance authority
DTF	dataspace trust framework

5 Trusted data sharing using dataspaces

5.1 General

The rapidly increasing demand for data across various industries has created a pressing need for a solution that facilitates secure, scalable, and trusted data sharing.

Many organizations (including government departments, academic research groups and businesses) have high level data sharing agreements at the organization level. Such agreements often take a long time to create and are then not detailed enough to be usefully enforced or automated. Further they do not describe the details of particular sets of data to be shared - such as expected quality, time and conditions of use. A more detailed, more automated approach to negotiating, enacting and enforcing agreements at the organizational level down to the data level is often needed so organizations can confidently share data.

Traditional data sharing methods often involve centralized repositories (such as a data lake of shared data) or direct exchanges (e.g. File Transfer Protocol (FTP) or email). Applying these methods at scale among independent parties can cause difficulties in managing interoperability as well as raise data governance concerns such as fair value, data use and provenance of data.

Dataspaces offer a novel approach to these challenges by enabling a decentralized and interoperable ecosystem where organizations can collaborate and share data while maintaining an appropriate level of control. By establishing a trustworthy environment for data sharing, dataspaces help overcome the barriers that hinder data-driven innovation and collaboration across different sectors.

At the heart of dataspaces lies the principle of trusted data sharing, which is crucial for fostering collaboration among participants. Participants in a dataspace can share data knowing that their rights are protected, and that the data is used in accordance with mutually agreed-upon terms. This trustworthiness is further reinforced by the ability to enforce data use policies and manage access rights, ensuring that all participants adhere to the agreed set of policies, semantic models, protocols and processes. As a result, dataspaces not

© ISO/IEC 2026 – All rights reserved