INTERNATIONAL STANDARD

ISO/IEC 23751

First edition
2022-02

Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework

Reference number
ISO/IEC 23751:2022(E)

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

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

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 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.

Introduction

For decades, organizations regarded data and its processing as an expense, necessary to business operations but not an opportunity. What has changed recently is the realization of the value of data and the added value that can potentially be generated by combining datasets. Artificial Intelligence (AI), Big Data, analytics, and cloud computing are making this value proposition much more obvious and the emergence of Internet of Things (IoT) is further driving the economic opportunities around data. Data is the raw material for AI, a key component of the fourth industrial revolution.

Sharing datasets to create combined datasets can have several technical, business, and regulatory challenges. One challenge is the lack of a common language to describe data sharing concepts across the entire data lifecycle and the lack of guidance for developing data sharing agreements (DSAs). This document offers standardized terminology for data sharing along with common building blocks that can be used in the development of DSAs. The aim of the project is to reduce the time and cost required to initiate data sharing projects.

Figure 1 illustrates the structure of this document, representing the Data Sharing Framework as defining both Data Qualitative Objectives (DQOs) and Data Level Objectives (DLOs) over six distinct aspects of data sharing. Each aspect is described in a separate section.

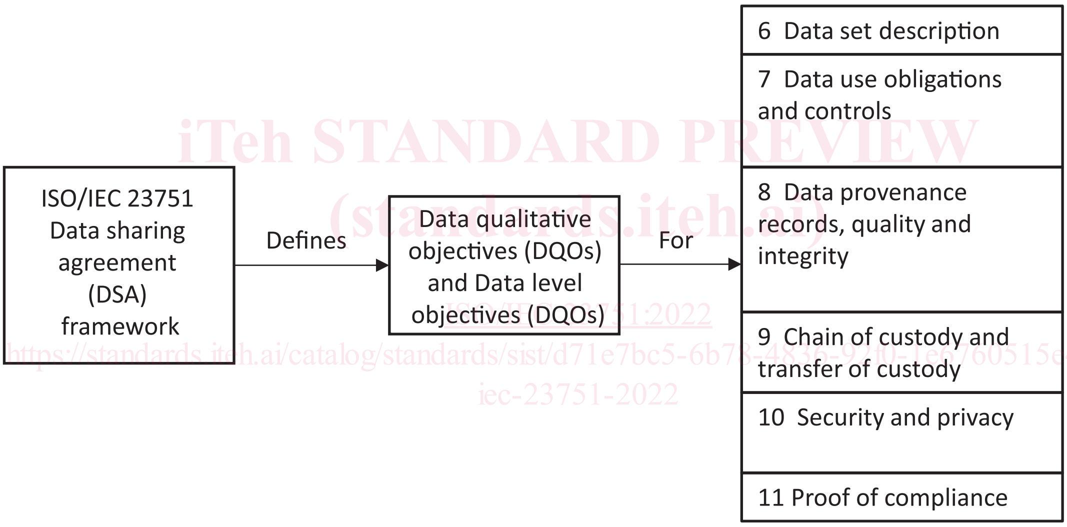

ISO/IEC 23751 Data sharing agreement (DSA) framework
Defines
Data qualitative objectives (DQOs) and Data level objectives (DQOs)
For
6 Data set description
7 Data use obligations and controls
8 Data provenance records, quality and integrity
9 Chain of custody and transfer of custody
10 Security and privacy
11 Proof of compliance

Figure 1 — Structure of this document

Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework

1 Scope

This document establishes a set of building blocks, i.e. concepts, terms, and definitions, including Data Level Objectives (DLOs) and Data Qualitative Objectives (DQOs), that can be used to create Data Sharing Agreements (DSAs). This document is applicable to DSAs where the data is intended to be processed using one or more cloud services or other distributed platforms.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
party
natural person or legal person, whether or not incorporated, or a group of either

[SOURCE: ISO/IEC 27729:2012,3.1]

3.2
data originator
party (3.1) that created the data and that can have rights

Note 1 to entry: A data originator can be an individual person.

Note 2 to entry: The data originator can be distinct from the natural or legal person(s) mentioned in, described by, or implicitly or explicitly associated with the data. For example, PII can be collected by a data originator that identifies other individuals. Those data subjects (PII Principals) can also have rights, in relation to the data set.

Note 3 to entry: Rights can include the right to publicity, right to display name, right to identity, right to prohibit data use in a way that offends honourable mention.

3.3
data broker
party (3.1) that collects data from one or more sources and sells the data to one or more *data users* (3.5)

Note 1 to entry: In the context of data broker, sell means to provide data in exchange for money or other item of value.

3.4
data holder
party (3.1) that has legal control to authorize *data processing* (3.8) of the data by other parties

Note 1 to entry: A *data originator* (3.2) can be a data holder.

3.5
data user
party (3.1) that is authorized to perform processing of data under the legal control of a *data holder* (3.4)

3.6
chain of custody
demonstrable possession, movement, handling, and location of material from one point in time until another

[SOURCE: ISO/IEC 27050-1:2016, 3.1]

3.7
data sharing
access to or processing of 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.

3.8
data processing
systematic performance of operations upon data

[SOURCE: ISO 2382:2015, 2121276, modified — Notes 1, 2, 3 and 4 to entry were deleted.]

3.9
cloud service agreement
documented agreement between the cloud service provider and cloud service customer that governs the covered service(s)

Note 1 to entry: A cloud service agreement can consist of one or more parts recorded in one or more documents.

[SOURCE: ISO/IEC 19086-1:2016, 3.3]

3.10
data store
persistent repository for digital information

Note 1 to entry: A data store can be accessed by a single entity or shared by multiple entities via a network or other connection.

[SOURCE: ISO/IEC 20924:2018, 3.1.13]

3.11
ratio scale
continuous scale with equal sized scale values and an absolute or natural zero point

[SOURCE: ISO 3534-2:2006, 1.1.9, modified — The EXAMPLE and Note 1 to entry were deleted.]

3.12
data level objective
DLO
commitment a *data holder* (3.4) or a *data user* (3.5) makes for a specific, quantitative characteristic of a dataset, where the value follows the interval scale or *ratio scale* (3.11)

Note 1 to entry: A data level objective commitment can be expressed as a range.

3.13
data qualitative objective
DQO
commitment a *data holder* (3.4) or a *data user* (3.5) makes for a specific, qualitative characteristic of a dataset, where the value follows the nominal scale or ordinal scale

Note 1 to entry: A data qualitative objective can be expressed as an enumerated list.

Note 2 to entry: Qualitative characteristics typically require human interpretation.

Note 3 to entry: The ordinal scale allows for existence/non-existence.

3.14
public domain data
class of data objects over which nobody holds or can hold copyright or other intellectual property

Note 1 to entry: Data can be in the public domain in some jurisdictions, while not in others.

Note 2 to entry: The concept of public domain and the difference between this and "publicly available" is subtle and varies between jurisdictions. Readers should make themselves aware of the specific legal situation as it can apply to them.

[SOURCE: ISO/IEC 19944-1:2020, 3.4.4]

4 Symbols and abbreviated terms

AI	Artificial Intelligence
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DLO	Data Level Objective
DSA	Data Sharing Agreement
DQO	Data Qualitative Objective

5 Overview of DSAs

5.1 General

An emerging use of cloud services and other distributed platforms is the processing of data that the CSC has acquired from a data holder. Additionally, there are cases where the CSC processes data acquired from multiple data holders (multi-sourced data) and there are cases where two or more CSCs share data among themselves including data acquired from other data holders.

Advances in cloud data storage have made it possible to create security boundaries around datasets that are then part of a larger logical dataset. Some data repositories provide customized access privileges to data users, with data provenance and chain of custody information attached to each record. These can provide an alternative approach in data sharing scenarios where the data come from multiple, independent data stores

5.2 Data sharing scenarios

A Data Sharing Agreement (DSA) can define how one or more organizations providing data to one or more third parties, several organizations pooling information and making it available to each other or to third parties. This document helps to identify and address important issues when developing DSAs between two or more entities or individuals concerning the sharing of data or information of any kind between these entities or individuals.

DSAs can be used in many different data sharing scenarios. Five representative scenarios are described below.

NOTE The arrows in the figures in this clause indicate data flow.

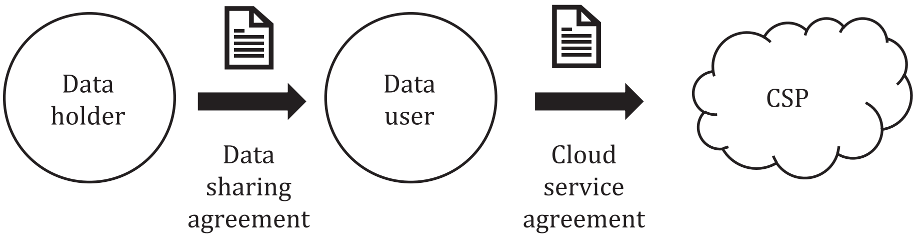


Figure 2 — Data sharing between two parties

Figure 2 shows a basic data sharing arrangement between a single data user and single data holder using a DSA. The CSP is not a party to the DSA but rather the data user is a CSC using cloud services provided by the CSP under a cloud service agreement.

EXAMPLE 1

The financial institution (Data Holder) clarifying to the financial institution bank teller (Data User) the DSA applied. The financial institution bank teller (Data User) can likewise want to understand the cloud service agreement with the CSP.

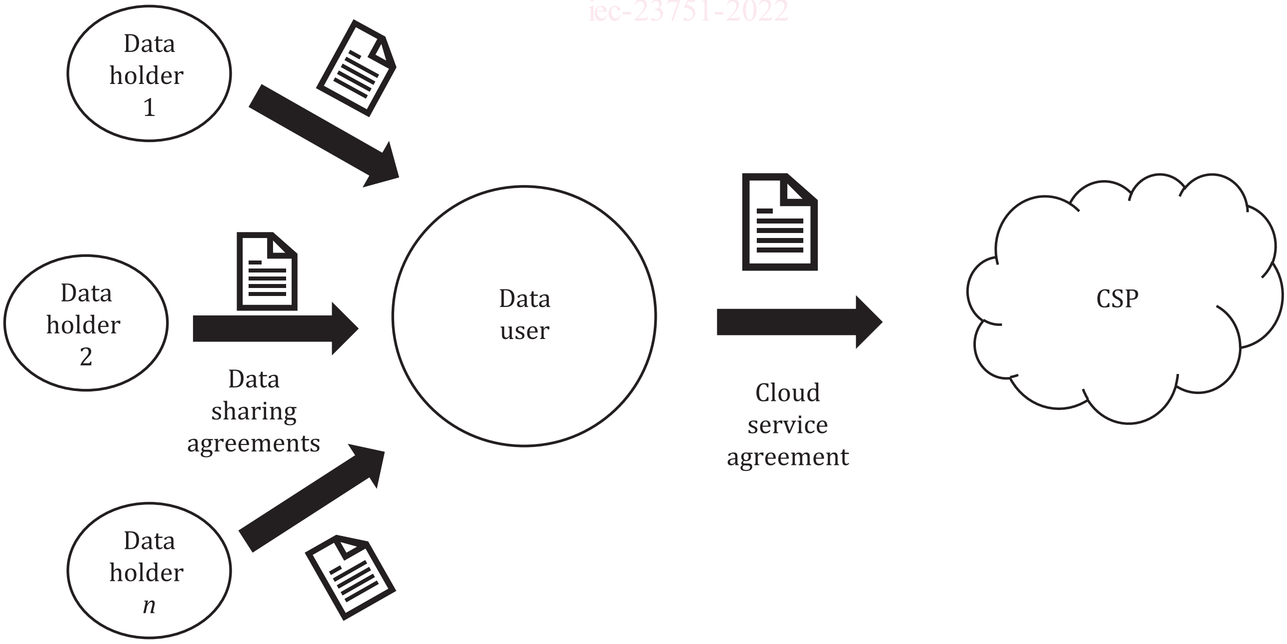


Figure 3 — Data sharing with one data user and multiple data holders

Figure 3 shows a data sharing arrangement between a single data user and multiple data holders. In this scenario the data user has a DSA with each data holder. As with the scenario in Figure 2, the CSC and CSP operate under a cloud service agreement and the CSP is not a party to the DSA.

EXAMPLE 2

An insurance broker (Data User) has a relationship with three insurance companies (Data Holders), with each having unique DSAs. The insurance broker has a single cloud service agreement with their respective CSP.

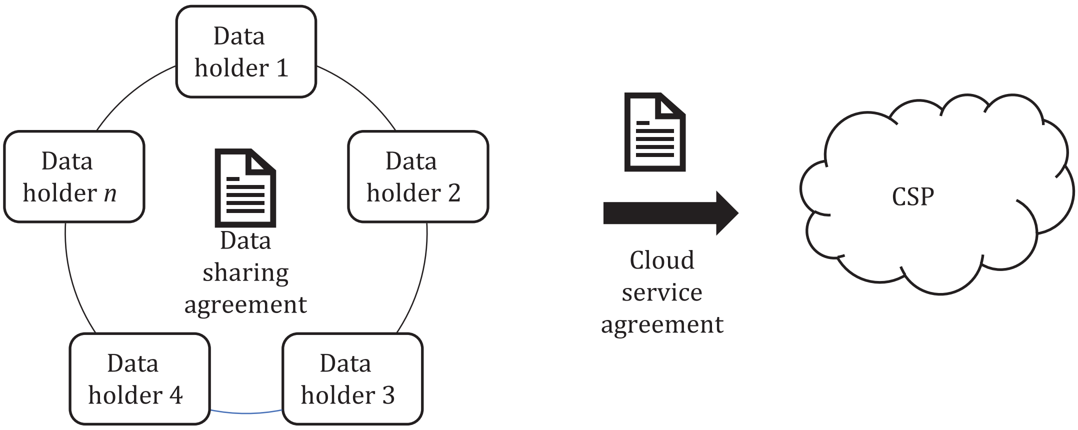


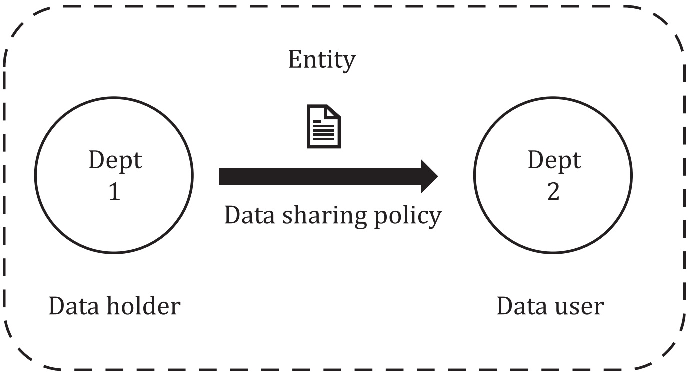
Figure 4 — Data sharing between multiple data holders

Figure 4 shows a scenario where two or more data holders share data under a common DSA and then as a group, they make use of cloud services from a CSP under a cloud service agreement.

EXAMPLE 3

A group of government agencies (Data Holders) have a mutually agreed upon DSA and have a common cloud service agreement with a CSP.

The data sharing scenarios in Figures 3 and 4 include the issues of multi-sourced data which are described in ISO/IEC TR 23186.



NOTE Entity does not include natural persons.

Figure 5 — Data sharing between departments within the same organization

Figure 5 shows data sharing between departments within the same entity where the sharing can be governed by one or more policies rather than by a contractual agreement. In some jurisdictions, it can be necessary to have a signed agreement between the data holder and the data user even if they are within the same entity. For the purposes of this document, data sharing policies can include the same elements of trust as DSAs.

EXAMPLE 4

A single financial institution offers banking and insurance from two distinct lines of business where they need clarity by means of either policies or agreements or both to govern the permitted data sharing from one line of business (Data Holder) to a Data User (such as Customer Relationship Management) in another line of business.

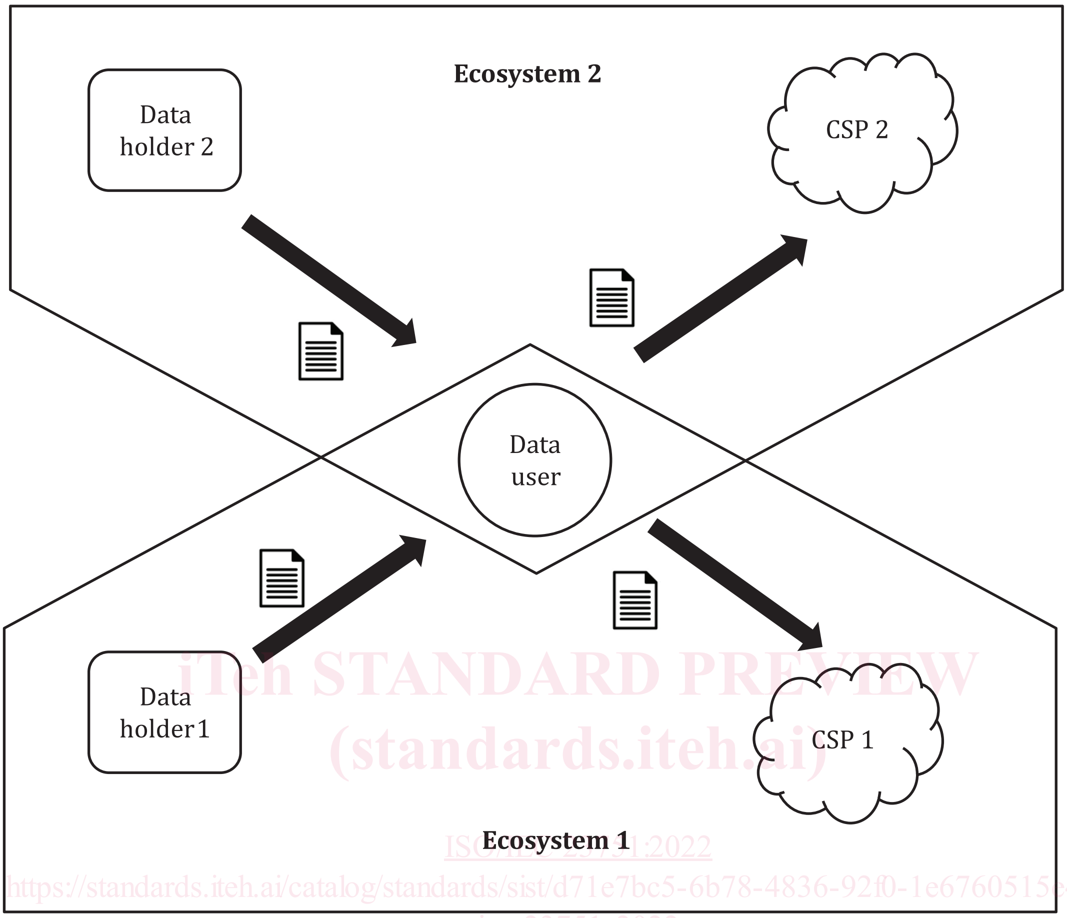


Figure 6 — Data sharing in a multiple ecosystem

As shown in Figure 6, data sharing can include more than one ecosystem. Ecosystems refer to networks of interconnected organisations which share infrastructures and services. Figure 6 displays two ecosystems. The first ecosystem includes one data holder, one data user and one cloud service provider (CSP). The second ecosystem includes the same data user working with another data holder and another CSP. The following observations can be made:

- Some business stakeholders (e.g. a data user) can have to manage DSAs from different ecosystems.
- DSAs used in a given ecosystem often include common elements, for instance.
- The introduction of policies established through a specific ecosystem governance scheme.
- The use of common cybersecurity and protection controls based on shared cybersecurity and privacy risk analysis.

EXAMPLE 5

A health application ecosystem and a financial application ecosystem have separate DSA with the same data user (a data analytics company).

A more comprehensive data sharing ecosystem can contain any combination of the scenarios described, e.g. modelling the data sharing implemented, rolled up for an overall government or corporate perspective.