International Standard FINAL DRAFT

ISO/IEC FDIS 5207

Information technology — Data usage — Terminology and use cases

ISO/IEC JTC **1**/SC **32**

Secretariat: **ANSI**

Voting begins on:
2024-01-23

Voting terminates on:
2024-03-19

Reference number
ISO/IEC FDIS 5207:2024(en)

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).

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 32, *Data management and interchange*.

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

The purpose of this document is to provide terminology and use cases in order to support organizations during the decision-making processes that occur throughout the use, sharing and exchange of data.

Given the breadth of data use, exchange and sharing activities, these use cases are presented with a description of the data usage activity including an overview of the data project, objectives, relevant entities involved, and the processes and interventions used in each case.

The use cases are structured to assist users in identifying the decision-making processes within data related activities, irrespective of the business or industry sector context. These use cases can provide users with guidance in considering where control measures can be applied to manage risks within the data process, the data lifecycle or the data environment.

This document can be used in the development of other International Standards and in support of communications among diverse stakeholders and other interested parties.

ISO/IEC 5207 was developed in collaboration with ISO/IEC 5212. Users of this document can refer to ISO/IEC 5212 for additional guidance for the decision-making process for the use, sharing and exchange of data.

Information technology — Data usage — Terminology and use cases

1 Scope

This document sets out terminology and use cases for data use, sharing and exchange. This document provides use cases detailing various types of data usage from both historical and hypothetical perspectives.

This document is applicable to all types of organizations.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological 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
information
<information processing> knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning

[SOURCE: ISO/IEC 2382:2015, 2121271, modified — Notes to entry deleted]

3.2
data
re-interpretable representation of *information* (3.1) in a formalized manner suitable for communication, interpretation, or processing

Note 1 to entry: Data can be used for communication, interpretation or processing by humans or automatic means.

Note 2 to entry: Communication, interpretation or processing can include the exchange or sharing of data by one or more entities.

[SOURCE: ISO/IEC 2382:2015, 2121272, modified — Note 1 to entry modified, Note 2 to entry replaced and Note 3 deleted]

3.3
metadata
data (3.2) that defines and describes other data

[SOURCE: ISO/IEC 11179-3:2023, 3.2.30]

3.4
data element
unit of *data* (3.2) that is considered in context to be indivisible

Note 1 to entry: The definition states that a data element is "indivisible" in some contexts. This means that it is possible that a data element considered indivisible in one context (e.g. telephone number) can be divisible in another context, (e.g. country code, area code, local number).

EXAMPLE The data element "age of a person" with values consisting of all combinations of 3 decimal digits.

[SOURCE: ISO/IEC 11179-31:2023, 3.23, modified — domain "<organization of data>" deleted]

3.5
data object
collection of *data* (3.2) that have a natural grouping and may be identified collectively

[SOURCE: ISO/TS 27790:2009, 3.20, modified — "as a complete entity" replaced by "collectively"]

3.6
data type
datatype
named set of distinct values, characterized by properties of those values, and by operations on those values

Note 1 to entry: Images, audio files and video files are considered complex data types.

[SOURCE: ISO/IEC 11404:2007, 3.12, modified — used "data type" instead of "datatype" as preferred term, used "named set" instead of "set" in definition and added Note 1 to entry]

3.7
data set
dataset
identifiable collection of *data* (3.2) available for access or download in one or more formats

Note 1 to entry: A data set can be a smaller grouping of data which, though limited by some constraint such as spatial extent or feature type, is located physically within a larger data set. Theoretically, a data set can be as small as a single feature or feature attribute contained within a larger data set.

Note 2 to entry: A data set can be presented in a tabular form and stored and distributed in tables in word processed documents, spread sheets or databases. It could also be presented in any one of a number of alternative formats, including AVRO, JSON, RDF and XML.

[SOURCE: ISO/IEC 11179-33:2023, 3.5]

3.8
data set collection
curated collection of one or more *data sets* (3.7)

[SOURCE: ISO/IEC 11179-33:2023, 3.6]

3.9
data set distribution
specific available form of a *data set* (3.7) or *data set collection* (3.8)

Note 1 to entry: Each data set might be available in different forms and each of these forms represents a different format of the data set or a different endpoint.

Note 2 to entry: Examples of distributions include a downloadable CSV file, an API or an RSS feed. This represents a general availability of a data set.

[SOURCE: ISO/IEC 11179-33:2023, 3.7]

3.10
data representation
format, *data type* (3.6), character set and other characteristics used to represent *data* (3.2)

Note 1 to entry: *Data types* apply to individual *data elements* (3.4). Formats can apply to sets of data elements, such as records, tables or messages.

3.11
data transformation
conversion from one form of *data representation* (3.10) to another

Note 1 to entry: Transformation of a single *data element* (3.4) can involve a change of character set, *data type* (3.6) or both.

Note 2 to entry: Transformation of a *data set* (3.7) can involve a change of format, such as from XML to JSON, or from a table to a data matrix.

Note 3 to entry: Data transformation does not change the *data* (3.2) value, just the way it is represented. For example, when the letter 'A' is transformed from ASCII to EBCDIC, it is still the letter 'A', just represented in a different character encoding.

Note 4 to entry: Data transformation does not change the semantics of the data.

Note 5 to entry: Where the *metadata* (3.3) for the data includes data provenance, then the metadata should be updated to reflect the data transformation.

3.12
data translation
conversion of a *data* (3.2) value from one code set to another

EXAMPLE 1 Conversion of codes representing human sexes from 'M' or 'F' to '0' or '1', or vice versa.

EXAMPLE 2 Conversion of country codes from 2-alpha code to 3-alpha code or 3-numeric code.

Note 1 to entry: Translation is typically used to convert data from different sources into a standard set of values.

3.13
data product
collection of one or more *data objects* (3.5) that are packaged for or by a specific application

Note 1 to entry: A data product may still provide access to the underlying *data* (3.2) or alternatively be engineered to prevent access to the underlying *data* from which the data product was created.

Note 2 to entry: A data product that has been specifically created to prevent access to the underlying *data* should be noted as such and recorded in the *data set* (3.7) records.

[SOURCE: ISO 21961:2003, 1.5.2, modified — "data items" changed to "data objects". Notes 1 and 2 to entry added]

3.14
data project
programme of work that involves the use, sharing or exchange of *data* (3.2)

3.15
data process
steps involved in the creation, analysis, or alteration of a specific set of *data* (3.2)

3.16
data processing
systematic performance of operations upon *data* (3.2)

[SOURCE: ISO/IEC 23751:2022, 3.8]

3.17
data processing system
computer system
computing system
one or more computers, peripheral equipment, software, human operations, physical processes and *information* (3.1) transfer means that perform *data processing* (3.16)

[SOURCE: ISO/IEC 2382:2015, 2121290, modified — added "human operations and physical processes and *information* transfer means" and notes 1 and 2 to entry deleted.]

3.18
data environment
set of conditions under which *data processing* (3.16) or the *data process* (3.15) occurs

Note 1 to entry: The data environment can include the physical, operational, behavioural and organizational factors which may affect data process outcomes.

3.19
lifecycle
stages involved in the management of an asset

Note 1 to entry: The target of lifecycle in this document is *data* (3.2).

[SOURCE: ISO 55000:2014, 3.2.3, modified — 'life cycle' changed to 'lifecycle', and Note 1 to entry replaced]

3.20
data lifecycle
stages in the management of *data* (3.2)

Note 1 to entry: The target of *lifecycle* (3.19) in this document is data.

[SOURCE: ISO/IEC 20547-3:2020, 3.16, modified — "a" deleted from definition, Note 1 to entry reworded]

3.21
party
natural person or legal person, whether or not incorporated, or a group of either

[SOURCE: ISO 27729:2012, 3.1]

3.22
organization
unique framework of authority within which a person or persons act, or are designated to act towards some purpose

Note 1 to entry: The kinds of organizations covered by this part of ISO/IEC 6523 include the following examples:

a) an organization incorporated under law;

b) an unincorporated organization or activity providing goods and/or services including:

   1) partnerships;

   2) social or other non-profit organizations or similar bodies in which ownership or control is vested in a group of individuals;

   3) sole proprietorships;

   4) governmental bodies.

c) groupings of the above types of organizations where there is a need to identify these in information interchange.

[SOURCE: ISO/IEC 6523-1:2023, 3.1]

3.23
entity
party (3.21) or *data processing system* (3.17) with distinct and independent existence from a *data* (3.2) perspective

3.24
data originator
party (3.21) that created the *data* (3.2) and that can have rights

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

Note 2 to entry: Rights can include the right to publicity, right to display name, right to identity, right to prohibit *data use* (3.30) in a way that offends honourable mention.

[SOURCE: ISO/IEC 23751:2022, 3.2, modified – Note 2 to entry deleted, and Note 3 to entry renumbered as Note 2.]

3.25
data holder
party (3.21) that has legal control over *data* (3.2) to authorize *data processing* (3.16) of the data by other parties

Note 1 to entry: A *data originator* (3.24) can be a data holder.

[SOURCE: ISO/IEC 23751:2022, 3.4, modified — "control to authorize data processing of data" changed to "control over data to authorize data processing of data".]

3.26
data user
party (3.21) that is authorized to perform processing of *data* (3.2) under the legal control of a *data holder* (3.25)

[SOURCE: ISO/IEC 23751:2022, 3.5]

3.27
ratio scale
continuous scale with equal sized scale values and an absolute or natural zero point

[SOURCE: ISO/IEC 23751:2022, 3.11]

3.28
data level objective
DLO
commitment that a *data holder* (3.25) or a *data user* (3.26) makes for a specific, quantitative characteristic of a *data set* (3.7), where the value follows the interval scale or *ratio scale* (3.27)

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

[SOURCE: ISO/IEC 23751:2022, 3.12]

3.29
data qualitative objective
DQO
commitment that a *data holder* (3.25) or a *data user* (3.26) makes for a specific, qualitative characteristic of a *dataset* (3.7), 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.

[SOURCE: ISO/IEC 23751:2022, 3.13]

3.30
data use
handling or dealing with *data* (3.2) for a specific purpose

Note 1 to entry: This includes reproducing the data but does not include disclosing the data.

[SOURCE: ISO/TS 14265:2011, 2.11, modified — 'information' has been changed to 'data' in both the definition and Note 1 to entry.]

3.31
data exchange
concerning the representation, transmission, reception, storage, and retrieval of *data* (3.2)

[SOURCE: ISO/IEC 20944-1:2013, 3.21.13.1, modified — Note 1 to entry deleted]

3.32
data sharing
access to or processing of the same *data* (3.2) by more than one authorized *entity* (3.23)

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

Note 2 to entry: In this document, data sharing refers to allowing access to, or the execution of operations over, the original *data set* (3.7).

Note 3 to entry: The way in which data are shared fundamentally influences the available controls and the statements needed in a *data sharing agreement* (3.35).

[SOURCE: ISO/IEC 23751:2022, 3.7, modified — 'use of' changed to 'access to' in Note 1 to entry, Note 2 to entry replaced]

3.33
data usage
any activity involving *data* (3.2)

Note 1 to entry: Data usage includes *data use* (3.30), *data sharing* (3.32) and *data exchange* (3.31).

3.34
data usage framework
framework that sets out the characteristics which should be assessed by the *entity* (3.23) in possession of the *data* (3.2) and captured within the *metadata* (3.3) description

3.35
data sharing agreement
DSA
documented agreement that defines, guides and protects *data sharing* (3.32)

Note 1 to entry: A data sharing agreement generally includes a description of *data* (3.2), data sharing scenarios, roles and participants, platforms, processes, requirements and controls, rights, obligations and responsibilities etc.

3.36
data recipient
entity (3.23) that receives *data* (3.2) via *data sharing* (3.32) or *data exchange* (3.31)

3.37
data accountability
accountability for *data* (3.2) and its usage

Note 1 to entry: *Data usage* (3.33) includes *data use* (3.30), *data sharing* (3.32) and *data exchange* (3.31).

[SOURCE: ISO/IEC 38505-1:2017, 3.4, modified — "use" replaced by "usage" and Note 1 to entry replaced.]

3.38
competent person
person who has acquired, through training, qualification, experience or a combination of these, the knowledge and skill enabling that person to correctly perform the required tasks

[SOURCE: ISO 11525-1:2020, 3.4]

3.39
responsible data officer
officially nominated individual with *data accountability* (3.37)

Note 1 to entry: Responsibility should include enterprise-wide governance and utilization of *information* (3.1) as an asset, via *data processing* (3.16), analysis, *data* (3.2) mining, information trading and other means.

Note 2 to entry: The responsible data officer can be an individual which reports to a governing body which oversees data related activities, can be a delegated position for a specific task such as a major financial project or can be a responsibility under a permanent role within an *organization* (3.22) such as Chief Executive Officers (CEOs), Heads of Government Organizations, Chief Financial Officers (CFOs), Chief Operating Officers (COOs), Chief Information Officers (CIOs), or Chief Data Officers (CDOs), and similar roles.

Note 3 to entry: The delegated data authority should be recognized as a *competent person* (3.38).

3.40
chain of custody
demonstrable possession, movement, handling, and location of material from one point in time until another

[SOURCE: ISO/IEC 27050-1:2019, 3.1]

3.41
access level
level of authority required from a resource owner to access a protected resource

Note 1 to entry: In the context of this document, items to which an access level may be specified are limited to a *data set* (3.7), a *data set collection* (3.9) and a *data set distribution* (3.8).

Note 2 to entry: For the public, the level of authority might describe the degree of public availability of a *data set*.

EXAMPLE Public, restricted public and non-public.

[SOURCE: ISO/IEC 11179-33:2023, 3.3]

3.42
confidential information
information (3.1) that is not intended to be made available or disclosed to unauthorized individuals, *entities* (3.23) or *data processes* (3.15)

[SOURCE: ISO/IEC 27002:2022, 3.1.7, modified — “processes” replaced by “data processes”]

3.43
sensitive information
information (3.1) that needs to be protected from unavailability, unauthorized access, modification or public disclosure because of potential adverse effects on an individual, *organization* (3.22), national security or public safety.

[SOURCE: ISO/IEC 27002:2022, 3.1.33]

3.44
identifiable natural person
individual who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to their physical, physiological, mental, economic, cultural or social identity

[SOURCE: ISO 22857:2013, 3.7, modified — term changed from “identifiable person”, “one” changed to individual”, “his” changed to “their”.]

3.45
personal information
personal data
any *information* (3.1) on or about an identifiable individual that is recorded in any form, including electronically or on paper

EXAMPLE Information about a person's religion, age, financial transactions, medical history, address or blood type.

[SOURCE: ISO/IEC 15944-5:2008, 3.103, modified — added "personal data" as an admitted term. Changed Note 1 to entry to EXAMPLES.]

3.46
data subject
individual about whom *personal data* (3.45) are recorded

[SOURCE: ISO 5127:2017, 3.13.4.01, modified – Note 1 to entry deleted]

3.47
personally identifiable information
PII
any *information* (3.1) that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the *PII principal* (3.48). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the *privacy stakeholder* (3.49) holding the *data* (3.2), or by any other *party* (3.21), to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd1:2018, 2.9, modified — "NOTE" replaced by "Note 1 to entry"]

3.48
PII principal
natural person to whom the *personally identifiable information (PII)* (3.47) relates

Note 1 to entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym *data subject* (3.46) can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.49
privacy stakeholder
natural or legal person, public authority, agency or any other body that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to *personally identifiable information (PII)* (3.47) processing

[SOURCE: ISO/IEC 29100:2011, 2.22]

3.50
PII controller
privacy stakeholder (3.49) (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.47) other than natural persons who use *data* (3.2) for personal purposes

Note 1 to entry: A PII controller sometimes instructs others, e.g. *PII processors* (3.51) to process *PII* on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2011, 2.10]