INTERNATIONAL STANDARD

ISO/IEC 19944-1

First edition
2020-10

Cloud computing and distributed platforms — Data flow, data categories and data use —

Part 1: Fundamentals

Informatique en nuage et plates-formes distribuées — Flux de données, catégories de données et utilisation des données — Partie 1: Principes de base

Reference number
ISO/IEC 19944-1:2020(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).

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.c).

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.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information Technology*, Subcommittee SC 38, *Cloud Computing and Distributed Platforms*.

This first edition of ISO/IEC 19944-1, along with ISO/IEC 19944-2[1)] cancels and replaces ISO/IEC 19944:2017, which has been technically revised.

The main changes compared to the previous edition are as follows:

— provides additional material which principally deals with organizational data and the need to treat some organizational data in particular ways in order to ensure confidentiality, integrity and so on,

— the new concept of data facets is introduced and data facets are used to extend the expressiveness of data use statements, including adding the concept of which individuals or organizations have control over data,

— the new data use categories are introduced, including some that address the newer uses of data associated with artificial intelligence systems.

A list of all parts in the ISO/IEC 19944 series can be found on the ISO website.

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.

1) Under preparation. Stage at the time of publication: ISO/IEC PWI 19944-2:2020.

Introduction

This document provides a description of the ecosystem of devices and cloud services and the related flows of data between cloud services, cloud service customers, cloud service users and their devices. These are necessary to provide guidance about how data are used on the devices in the context of the cloud computing ecosystem and the associated location and identity issues that emerge from such use.

This document proposes a scheme for the structure of data use statements that can be used by cloud service providers to help cloud service customers understand and protect the privacy and confidentiality of their data and their users' data through increased transparency of policies and practices.

This document may be used in several ways including, but not limited to:

a) by cloud service providers and application developers to guide them in describing what they intend to do with data in their designs, so as to simplify privacy and data use reviews and to communicate this information to non-technical departments such as internal compliance, marketing and legal teams;

b) by organisations drawing up data use statements as part of drafting cloud service agreements and application contracts, privacy statements, etc., which could apply to documents internal to an organisation, in addition to public or legal documents;

c) by government regulators and agencies to advise on suitable ways of describing data flow and use;

d) by those preparing information on data flow and data use for communication to the press and the public.

This document cannot be used for compliance directly. Instead, it provides a set of concepts and definitions, including a data taxonomy and data use statement structure, that can be used for transparency about how data are used in an ecosystem of devices and cloud services.

This document also aims to improve the understanding of the data flows that take place in an ecosystem consisting of devices accessing cloud services. It does this through an extended cloud computing reference architecture (CCRA) (based on the architecture described in ISO/IEC 17789) that describes the impact of devices on cloud service ecosystems and the impact of cloud services on devices. It also describes the data flows that take place within the extended reference architecture.

To maintain a relationship of trust between the stakeholders of the ecosystem of devices and cloud services and also to meet the demands of laws and regulations, it is necessary for the device platform providers and the cloud service providers to be transparent about how they make use of the various data types that flow within the ecosystem.

There is a particular need to provide simple and clear statements to end users about what is done with data that relates to them. The data may be personally identifiable information (PII) and may be sensitive, in other words, this can be a privacy issue. Cloud service customers are likely to be concerned about how their data are used, even when the customer is an organization rather than an individual. The cloud service customer may be a data controller, holding personal data about their employees or their customers; in such a role, the cloud service customer has obligations relating to the processing of that data.

To assist cloud service providers and device platform providers in being transparent about their use of data, this document defines a simple language for making statements about data use, which can be used to create clear notification to end users and other interested parties.

This version of ISO/IEC 19944 contains additional material which principally deals with organizational data and the need to treat some organizational data in particular ways in order to ensure confidentiality, integrity and so on.

To assist with this, the new concept of data facets is introduced and data facets are used to extend the expressiveness of data use statements, including adding the concept of which individuals or organizations have control over data.

New data use categories are introduced, including some that address the newer uses of data associated with artificial intelligence systems.

Cloud computing and distributed platforms — Data flow, data categories and data use —

Part 1: Fundamentals

1 Scope

This document

— extends the existing cloud computing vocabulary and reference architecture in ISO/IEC 17788 and ISO/IEC 17789 to describe an ecosystem involving devices using cloud services,

— describes the various types of data flowing within the devices and cloud computing ecosystem,

— describes the impact of connected devices on the data that flow within the cloud computing ecosystem,

— describes flows of data between cloud services, cloud service customers and cloud service users,

— provides foundational concepts, including a data taxonomy, and

— identifies the categories of data that flow across the cloud service customer devices and cloud services.

This document is applicable primarily to cloud service providers, cloud service customers and cloud service users, but also to any person or organisation involved in legal, policy, technical or other implications of data flows between devices and cloud services.

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 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 17789:2014, *Information technology — Cloud computing — Reference architecture*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17788 and the following 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 http://www.electropedia.org/

3.1 Terms related to data categories

3.1.1
account data
class of data specific to each CSC that is required to administer the *cloud service*

Note 1 to entry: Account data is typically generated when a cloud service is purchased and is under the control of the CSP.

Note 2 to entry: Account data consists of data elements provided by the CSC, such as name, address, telephone, etc.

3.1.2
end user identifiable information
EUII
derived data associated with a user that is captured or generated from the use of the service by that user

3.2 Terms related to cloud services and devices ecosystem

3.2.1
device
physical entity that communicates directly or indirectly with one or more *cloud services*

3.2.2
application marketplace
set of *cloud services* providing a digital marketplace intended to offer applications and other digital content for a particular *device platform* (3.2.4) allowing users to browse and download applications and other content

Note 1 to entry: An application marketplace may be offered to the public, or to private groups such as a corporate environment.

Note 2 to entry: A *device* (3.2.1) can use more than one application marketplace.

3.2.3
application cloud service
cloud service that supports applications running on a given *device* (3.2.1), where the cloud service is provided by a party other than the *device platform provider* (3.2.5)

3.2.4
device platform
operating system and related feature set that provides the core capabilities for a *device* (3.2.1)

Note 1 to entry: An *application marketplace* (3.2.2) is specific to a device platform.

3.2.5
device platform provider
device platform cloud service provider
cloud service provider that provides *cloud services* necessary to support a *device platform* (3.2.4) including managing needed digital identities

Note 1 to entry: The cloud service provider that offers the *application marketplace* (3.2.2) is typically the same as the device platform provider, but it is not required to be.

3.2.6
device platform cloud service
cloud service offered by the *device platform provider* (3.2.5) to support the *device platform* (3.2.4)

Note 1 to entry: An *application marketplace* (3.2.2) can be an example of device platform cloud service.

3.3 Terms related to privacy

3.3.1
personally identifiable information
PII
personal data
any information 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 (3.3.3). 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 holding the data, or by any other party, to establish the link between the set of PII and the natural person.

Note 2 to entry: This definition is included to define the term PII as used in this document. A public cloud PII processor (3.3.2) is typically not in a position to know explicitly whether information it processes falls into any specified category unless this is made transparent by the cloud service customer.

[SOURCE: ISO/IEC 29100:2011/Amd1:2018, 2.9]

3.3.2
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information* (PII) (3.3.1) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others, e.g. *PII processors* (3.3.4) to process PII on its behalf while the responsibility for the processing remains with the PII controller.

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

3.3.3
PII principal

natural person to whom the *personally identifiable information* (PII) (3.3.1) relates

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

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

3.3.4
PII processor
privacy stakeholder that processes *personally identifiable information* (PII) (3.3.1) on behalf of and in accordance with the instructions of a *PII controller* (3.3.2)

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.4 Terms related to organizational data

3.4.1
individual data
class of data objects under the control, by legal or other reasons, of a natural person

Note 1 to entry: Individual data can be a mixed dataset (3.4.6).

Note 2 to entry: Customer content data is individual data when the CSC is a natural person.

3.4.2
organizational data
class of data objects under the control, by legal, contractual or other reasons, of an organization

Note 1 to entry: An organization can be a for-profit company, a non-profit organization, a public or government agency, a non-governmental organization or an international organization, and can be small, medium or large.

Note 2 to entry: Customer content organizational data when the CSC is an organization and thus not a natural person.

Note 3 to entry: Cloud service provider data (ISO/IEC 17788) is always organizational data by nature.

Note 4 to entry: Organizational data can be a *mixed dataset* (3.4.6).

3.4.3
organizational protected data
OPD
organizational data whose protection is required based on the policies established by governance of data process

Note 1 to entry: Organizations have policies that govern the data under their control. ISO/IEC 38505-1 identifies and examines higher level governance concerns regarding the use of data which is relevant from the perspective of governance of data.

Note 2 to entry: Organizational data can contain OPD and PII.

3.4.4
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 may apply to them.

3.4.5
non-personal data
class of data objects that does not contain *PII* (3.3.1)

Note 1 to entry: data objects that were originally PII and were later made anonymous are non-personal data.

3.4.6
mixed dataset
set of data objects that contain both *PII* (3.3.1) and *non-personal data* (3.4.5)

3.4.7
data principal
entity to which data relates

Note 1 to entry: The term “data principal” is broader than “PII principal” (or “data subject” as used elsewhere) and is able to denote any entity such as a person, an organization, a device, or a software application.

[SOURCE: ISO/IEC 20889:2018, 3.4]

3.5 Terms related to artificial intelligence

3.5.1
artificial intelligence
<system> capability of an engineered system to acquire, process and apply knowledge and skills

Note 1 to entry: knowledge are facts, information, and skills acquired through experience or education.

[SOURCE: ISO/IEC CD 22989[2)]]

2) Under preparation. Stage at the time of publication: ISO/IEC CD 22989:2020.

3.5.2
artificial intelligence
<engineering discipline>discipline which studies the engineering of systems with the capability to acquire, process and apply knowledge and skills

Note 1 to entry: knowledge are facts, information, and skills acquired through experience or education.

[SOURCE: ISO/IEC CD 22989]

3.5.3
artificial intelligence system
AI system
system using AI

[SOURCE: ISO/IEC CD 22989]

3.5.4
machine learning
ML
process using computational techniques to enable systems to learn from data or experience

[SOURCE: ISO/IEC CD 23053[3)]]

3.5.5
machine learning model
mathematical construct that generates an inference, or prediction, based on input data

Note 1 to entry: for supervised learning, a machine learning model results from the training or a machine learning algorithm

Note 2 to entry: for example, if a univariate linear function (y = w0 + w1(x)) has been trained using linear regression, the resulting model could be y = 3 + 7(x).

[SOURCE: ISO/IEC CD 23053]

3.5.6
model training
<machine learning> task of determining optimal model parameters from a given dataset

[SOURCE: ISO/IEC CD 23053]

3.5.7
trained model
result of model training

[SOURCE: ISO/IEC CD 23053]

3.5.8
training data
samples used to fit a machine learning model

[SOURCE: ISO/IEC CD 23053]

3) Under preparation. Stage at the time of publication: ISO/IEC CD 23053:2020.

3.6 General terms

3.6.1
lifecycle
evolution of a system, product, service, project or other human-made entity, from conception through retirement

[SOURCE: ISO/IEC 29110-4-3:2018, 3.15]

3.6.2
transparency
open, comprehensive and understandable presentation of information

[SOURCE: ISO 21931-2:2019, 3.33]

4 Abbreviated terms

AI	Artificial Intelligence
BYOD	Bring Your Own Device
CCRA	Cloud Computing Reference Architecture
CSA	Cloud Service Agreement
CSC	Cloud Service Customer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
CSU	Cloud Service User
EUII	End User Identifiable Information
GPS	Global Positioning System
IaaS	Infrastructure as a Service
IoT	Internet of Things
IP	Intellectual Property
IP	Internet Protocol
ML	Machine Learning
OPD	Organizational Protected Data
PII	Personally Identifiable Information
SLA	Service Level Agreement
USB	Universal Serial Bus

5 Structure of this document

5.1 Document organization

This document is organized to describe two topic areas.

— Overview and reference architecture (Clauses 6 and 7).

— Data taxonomies, data categories and data use statement structure (Clauses 8, 9 and 10).

5.2 Overview and reference architecture

Overview and reference architecture are covered as follows.

— Clause 6 provides the foundation of the document covering the "Overview of devices and cloud services ecosystems". The clause describes the ecosystem and stakeholders where devices and cloud services operate.

— Clause 7, "Extending the cloud computing reference architecture to the devices and cloud services ecosystem" covers an extension of the architecture specified in ISO/IEC 17789 to include devices and the flow of data between devices and cloud services.

5.3 Data taxonomies, data categories and data use statement structure

Data taxonomies, data categories and data use statement structure (applicable to data exchanges between devices and cloud services) are covered as follows.

— Clause 8, "Data taxonomies" describes categories of data that can be captured, processed, used and shared. This taxonomy extends the definitions in ISO/IEC 17788 of cloud service customer data, cloud service derived data, cloud service provider data and account data. The taxonomy described in this clause is used in creating data use statements covered in Clause 10.

— Clause 9, "Data processing and use categories" describes the various categories of data processing and operations. "Data use categories" and related "scopes" described in this clause are required for understanding of the data use statements structure covered in Clause 10.

— Clause 10, "Data use statements" describes the syntax and statement structure for expressing how data are used by CSPs and their partners.

6 Overview of devices and cloud services ecosystems

6.1 Background and context — Impact of devices and personalized cloud services

This document builds on the foundation provided by the CCRA, ISO/IEC 17789, to accommodate data and its flow within the ecosystem of devices and cloud services.

Many kinds of devices are used as clients for accessing cloud services. These devices rely on support from cloud services which have an association between the device and the cloud service. Unique identifiers are created and maintained to enable that association. The interaction between the device and the cloud service requires an understanding of the flow of data between devices, cloud services, cloud service customers and cloud service providers. This interaction also makes the discussion of data classification and access and use become more complex.

NOTE This document uses the term "device" in the context of a cloud service user as defined in ISO/IEC 17788:2014, 3.2.17, which includes natural person, or entity acting on their behalf. Examples of such entities include devices and applications. This document is written such that there is no conceptual difference between types of devices, provided the device is acting as a cloud service user using cloud services.