INTERNATIONAL STANDARD

ISO/IEC 22624

First edition
2020-02

Information technology — Cloud computing — Taxonomy based data handling for cloud services

Reference number
ISO/IEC 22624:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

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
Fax: +41 22 749 09 47
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 Symbols and abbreviated terms ... **2**
5 Overview: The need for a structured expression of data policies and practices based on a common data taxonomy ... **3**
6 Framework for the structured expression of data related policies and practices ... **4**
6.1 General ... 4
6.2 Framework elements ... 4
6.2.1 General ... 4
6.2.2 Data categories ... 5
6.2.3 Data identification qualifiers ... 6
6.2.4 Data usage scopes ... 7
6.2.5 Actions ... 8
6.2.6 Data classification ... 9
6.2.7 Further elements specific to the application domain ... 10
7 Using the framework ... **10**
7.1 Modes of framework usage ... 10
7.2 Framework element usage ... 11
7.2.1 Data categories ... 11
7.2.2 Data identification qualifiers ... 11
7.2.3 Scopes and actions ... 11
7.3 Policy expressions ... 11
7.4 Example ... 11
8 Expression of data related policies in relation to specific areas of concern ... **12**
8.1 General ... 12
8.2 Data geolocation ... 12
8.3 Cross border flow of data ... 13
8.3.1 Data jurisdictions considerations ... 13
8.3.2 Cross border data transfer ... 15
8.4 Data portability and data access ... 17
8.4.1 General ... 17
8.4.2 Data required for data portability or data access ... 17
8.4.3 Formats and portability ... 18
8.5 Data use ... 19
8.6 Data management ... 19
8.6.1 Data security ... 19
8.6.2 Data quality ... 21
8.7 Data governance ... 22
9 Application of the framework to codes of conduct ... **26**
Annex A (informative) **Example for use of this document** ... **30**
Bibliography ... **37**

© ISO/IEC 2020 – 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).

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 http://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.

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.

© ISO/IEC 2020 – All rights reserved

Introduction

Many of the policies and practices in place for handling data in the cloud computing ecosystem need to be described based on the category of the data they address. For instance, personally identifiable information (PII) impose specific data management requirements not only in terms of security but also with regard to mechanisms that allow cloud service users to whom such data relate to exercise control on the usage and transfer of such data. Organisational data such as cloud service usage information and telemetry data from cloud services, which can be used for operational purposes such as improvement of service quality, may have to fulfil specific quality requirements to be useful for a given application.

Customer content data can be related to intellectual property rights and possibly needs appropriate protection by the cloud service provider (CSP). Certain data can be transferred from one jurisdiction to another. Depending on their data category, different instruments (multi-national laws, corporate binding rules, bilateral agreements) are applicable to enable such transfers.

When such policies and practices are to be described, it is helpful to do so in a structured and consistent way so that they can be better expressed, evaluated, analysed, and compared by the stakeholders in the cloud computing ecosystem. ISO/IEC 19944 provides a comprehensive taxonomy defining a fine-grained system of data categories that can be applied to various domains of policies for the handling of data in a cloud computing ecosystem such as cross border data transfer, data geolocation, data usage, data access and data portability, data management including data quality management and data security, or data governance, and provides guidelines on how to describe data handling policies and practices within codes of conduct (CoC).

This document describes such a structured and common approach to express any desired data handling policies and practices. It is important to emphasize that the policies and practices themselves are out of the scope of this document. This document describes a common structure and approach to express any desired data handling policies and practices. It is important to emphasize that the policies and practices are out of the scope of this document. A set of examples from data handling domains are provided in the document as guidance to understand how to use ISO/IEC 19944 regarding application of policies and analysis of policy requirements to such domains.

© ISO/IEC 2020 – All rights reserved

Information technology — Cloud computing — Taxonomy based data handling for cloud services

1 Scope

This document:

— describes a framework for the structured expression of data-related policies and practices in the cloud computing environment, based on the data taxonomy in ISO/IEC 19944;

— provides guidelines on application of the taxonomy for handling of data based on data subcategory and classification;

— covers expression of data-related policies and practices including, but not limited to data geolocation, cross border flow of data, data access and data portability, data use, data management, and data governance;

— describes how the framework can be used in codes of conduct for practices regarding data at rest and in transit, including cross border data transfer, as well as remote access to data;

— provides use cases for data handling challenges, i.e. control, access and location of data according to ISO/IEC 19944 data categories.

This document is applicable primarily to cloud service providers, cloud service customers (CSCs) and cloud service users, but also to any person or organization involved in legal, policy, technical or other implications of taxonomy-based data management in 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, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 19944, *Information technology — Cloud computing — Cloud services and devices: Data flow, data categories and data use*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17788, ISO/IEC 19944 and the following apply:

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

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

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

3.1
codes of conduct
CoC
agreed set of behaviours between organisations to enhance customer and/or partner outcomes and experiences

© ISO/IEC 2020 – All rights reserved

3.2
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO 24534-5:2011, 3.11]

3.3
integrity
property of being designed such that any modification of the electronically stored information, without proper authorization, is not possible

3.4
availability
property of being accessible and useable upon demand by an authorized entity

[SOURCE: ISO 22600-1:2014, 3.7]

3.5
data access
process by which a system can read published data on another system

Note 1 to entry: This data access happens over a network connection and the data typically does not persist after the connection is terminated.

3.6
data transfer
copying or moving data from one system to another

3.7
data geolocation
geographic location of a data object at rest

4 Symbols and abbreviated terms

APEC	Asia-Pacific Economic Cooperation
BCR	Binding Corporate Rules
CBPR	Cross-border Privacy Rules
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CoC	Codes of Conduct
CSC	Cloud Service Customer
CSN	Cloud Service partner
CSP	Cloud Service Provider
DRM	Digital Rights Management
EU	European Union
EUII	End User Identifiable Information
GDPR	General Data Protection Regulation
GPS	Global Positioning System

© ISO/IEC 2020 – All rights reserved