ISO/IEC 19944-1:2020 (E)

Cloud computing and distributed platforms — Data flow, data categories and data use — Part 1: Fundamentals

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

3.1 Terms related to data categories
3.2 Terms related to cloud services and devices ecosystem
3.3 Terms related to privacy
3.4 Terms related to organizational data
3.5 Terms related to artificial intelligence
3.6 General terms

4 Abbreviated terms

5 Structure of this document

5.1 Document organization
5.2 Overview and reference architecture
5.3 Data taxonomies, data categories and data use statement structure

6 Overview of devices and cloud services ecosystems

6.1 Background and context — Impact of devices and personalized cloud services
6.2 Ecosystem of devices and cloud services
6.3 Devices and multiple user sub-roles
6.3.1 General
6.3.2 Bring your own device

7 Extending the CCRA to the devices and cloud services ecosystem

7.1 Overview
7.2 Personal and organizational environments
7.3 Device impact on the CCRA: User view
7.3.1 Cloud service provider
7.3.1.1 Sub-roles
7.3.1.1.1 General
7.3.1.1.2 CSP:device platform provider
7.3.1.2 Cloud computing activities
7.3.2 Cloud service customer
7.3.2.1 Sub-roles
7.3.2.1.1 General
7.3.2.1.2 CSC:cloud service user
7.3.2.2 Cloud computing activities
7.4 Device impact on the CCRA: functional view
7.4.1 General
7.4.2 Functional components in the functional view
7.4.2.1 Device
7.4.2.2 Device platform
7.4.2.3 Application
7.4.2.4 Application cloud service
7.4.2.5 Device platform cloud service
7.4.2.6 Application client component

7.4.2.7 Application marketplace
7.4.3 Functional view: data flows

8 Data taxonomy

8.1 Overview
8.2 Data categories
8.2.1 General
8.2.2 Customer content data
8.2.2.1 General
8.2.2.2 Credentials
8.2.2.3 Customer contact lists
8.2.2.4 Personal health data and medical records
8.2.2.5 Personal genetic data
8.2.2.6 Personal biometric data
8.2.2.7 Personal data of children
8.2.2.8 Political opinions
8.2.2.9 Financial details
8.2.2.10 Sensor measurement data
8.2.3 Derived data
8.2.3.1 General
8.2.3.2 End user identifiable information (EUII)
8.2.3.2.1 General
8.2.3.2.2 Telemetry data
8.2.3.2.3 Connectivity data
8.2.3.2.4 Observed usage of the service capability
8.2.3.2.5 Demographic information
8.2.3.2.6 Profiling data
8.2.3.2.7 Content consumption data
8.2.3.2.8 Client-side browsing history
8.2.3.2.9 Search commands and queries
8.2.3.2.10 User location
8.2.3.2.11 Social data
8.2.3.2.12 Biometric and health data
8.2.3.2.13 End-user contact data
8.2.3.2.14 User's environmental sensor data
8.2.3.3 Organization identifiable information (OII)
8.2.4 Cloud service provider data
8.2.4.1 General
8.2.4.2 Access and authentication data
8.2.4.3 Operations data
8.2.5 Account data
8.2.5.1 General
8.2.5.2 Account or administration contact information
8.2.5.3 Payment instrument data
8.3 Data identification qualifiers
8.3.1 General
8.3.2 Identified data
8.3.3 Pseudonymized data
8.3.4 Unlinked pseudonymized data
8.3.5 Anonymized data
8.3.6 Aggregated data
8.4 Orthogonal facets of data
8.4.1 General
8.4.2 Perspective used in the definition of data facets
8.4.3 Common orthogonal data facets
8.4.3.1 Introduction
8.4.3.2 Data facets based on control
8.4.3.2.1 Legal control of data compared to operational control
8.4.3.2.2 Operational control data facet
8.4.3.2.3 Legal control data facet
8.4.3.2.3.1 General
8.4.3.2.3.2 Legal entity data facet
8.4.3.2.3.3 Legal means data facet
8.4.3.3 Classification level data facet

8.4.3.4 Categorization data facet
8.4.3.5 De-identification degree data facet
8.4.3.6 Custom data facets
8.4.3.7 Composite facets and associated attributes
8.4.3.7.1 General
8.4.3.7.2 Customer content data
8.4.3.7.3 Cloud service provider data
8.4.3.7.4 Derived data
8.4.3.7.5 Individual, organizational, and public domain data
8.4.3.7.5.1 Introduction
8.4.3.7.5.2 Rights and obligations
8.4.3.7.5.3 Building new composite facets from legal control data facet
8.4.3.7.5.4 Co-controlled data
8.4.3.7.5.5 Change of control over the data lifecycle
8.4.3.7.5.6 Legal control of organizational data
8.4.4 Use of data facets to describe data taxonomy

9 Data processing and use categories

9.1 Overview
9.2 Data processing categories
9.2.1 General
9.2.2 Data partitioning
9.2.2.1 General
9.2.2.2 Horizontal partitioning or sharding
9.2.2.3 Vertical partitioning
9.2.3 Data integration
9.2.4 Data fusion
9.2.5 Data improvement
9.2.6 Encryption
9.2.7 Replication
9.2.8 Data Deletion
9.2.8.1 General
9.2.8.2 Secure data deletion
9.2.9 Re-identification
9.3 Data use categories
9.3.1 General
9.3.2 Provide
9.3.2.1 General
9.3.2.2 Provide operational support for contracted service
9.3.2.3 Improvement of business support for contracted service
9.3.3 Improve
9.3.4 Personalize
9.3.5 Offer upgrades or upsell
9.3.6 Market/advertize/promote
9.3.6.1 General
9.3.6.2 Promote based on contextual information
9.3.6.3 Promote based on personalization
9.3.7 Share
9.3.7.1 General
9.3.7.2 Share when required to provide the service
9.3.8 Collect
9.3.9 Train (AI system)
9.4 Scopes: Boundaries of collection and use of data
9.4.1 Scope concepts
9.4.2 Scope types
9.4.2.1 General
9.4.2.2 Capability
9.4.2.3 Application or service
9.4.2.4 Services listed in the cloud service agreement
9.4.2.5 Cloud service provider's cloud services
9.4.2.6 Cloud service provider's products and services
9.4.2.7 Third-party product and services
9.4.2.8 Third-party and data processors
9.4.3 Scope characteristics

9.4.3.1 General
9.4.3.2 Guaranteed capabilities of a scope
9.4.3.3 Controlling entity of a scope
9.4.3.4 Scope location
9.4.4 Network connection between scopes
9.4.4.1 General
9.4.4.2 Guaranteed capabilities of a network connection
9.4.5 Control of source scope over result scope

10 Data use statements

10.1 Overview
10.2 Data use statement structure
10.2.1 Structure definition
10.2.2 Describing the scope of applications and cloud services that apply to use statements
10.2.2.1 Using single or dual scope definitions
10.2.3 Assumptions about when data are collected and used
10.2.4 Defining promotion targets
10.2.5 Data types
10.2.6 Data qualifiers for data types
10.2.7 Examples of statements about data flow in the devices and cloud services ecosystem
10.2.8 Exceptional use statements
10.2.8.1 General
10.2.8.2 Structure
10.2.8.3 Grantor
10.2.8.4 Grantee
10.2.8.5 Exceptional use
10.2.8.6 Grant trigger
10.2.8.7 Grant period
10.2.9 Data sharing
10.3 Use of orthogonal data facets in data use statement
10.3.1 General
10.3.2 Use of elements in the data facets as attributes
10.3.3 Hierarchy of elements/attributes of data based on facets
10.3.4 Use of attributes to describe PII
10.3.5 Use of attributes to tag IP data
10.3.6 Use of attributes to tag IP data from shared pools, while respecting partner IP

11 Data lineage and data provenance

11.1 General
11.2 Tracing data lineage

12 Use of taxonomy and data use statement in other computing environments

13 Use of data taxonomy and use statements in Artificial Intelligence scenarios

Annex A (informative) Diagrams of data categories and data identification qualifiers

A.1 Data categories
A.2 Data identification qualifiers

Page count: 65