Common Terminology

The purpose of this common terminology document is to contain a glossary of all the terms and acronyms that are used in all the Codes of Conduct.

Glossary of Acronyms

API – Application Programming Interface
CSP – Cloud Service Provider
CSA – Cloud Service Agreement
CSC – Cloud Service Customer
CSC Data – Cloud Service Customer Data
EC – European Commission
EU – European Union
GDPR – General Data Protection Regulation
IaaS – Infrastructure as a Service
PaaS – Platform as a Service
SaaS – Software as a Service
SLO – cloud service level objective
SQO – cloud service qualitative objective
SME – Small and Medium sized Enterprise

Special Terms relating to Compliance in the Codes

A set of words are used in the codes with special meanings that relate to compliance with the codes. These words are:

- **"shall"** indicates a requirement
- **"should"** indicates a recommendation
- **"may"** is used to indicate that something is permitted
- **"can"** is used to indicate that something is possible

Glossary of Terms

Application: software entity that provides a set of functions to a user

SOURCE: ISO/IEC 23004-1:2007(en), 4.2.2

Application Programming Interface: collection of invocation methods and associated parameters used by one piece of software to request actions from another piece of software

SOURCE: ISO/IEC TR 29108:2013, 3.1.12.2

Application Portability: ability to migrate an application from a source system to a target system.

SOURCE: ISO/IEC 19941:2017(en), 3.3.1

Certification: procedure by which a third party gives written assurance that a product or process conforms to specified requirements**.**

SOURCE: ISO 14024:2018(en), 3.12

Cloud capabilities type: capabilities of the Cloud Service provided by the CSP (one of: Software as a Service, Infrastructure as a Service, or Platform as a Service).

Cloud Computing: paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

SOURCE: ISO/IEC 17788:2014, 3.2.5

Cloud Data Portability: data portability from one cloud service to another cloud service, or between a CSC's system and a cloud service**.**

SOURCE: ISO/IEC 19941:2014, 3.2.2

Cloud Marketplace: the competitive, commercial marketplace for cloud services.

Cloud Service: One or more capabilities offered via cloud computing invoked using a defined interface**.**
SOURCE: ISO/IEC 17788:2014, 3.2.8

Cloud Service Agreement: documented agreement between the cloud service provider and cloud service customer that governs the covered service(s)**.**

SOURCE: ISO/IEC 19086-1:2016(en), 3.3

Cloud Service Category: group of cloud services that possess some common set of qualities.

SOURCE: ISO/IEC 17788:2014, 3.2.10

Cloud Service Customer: party which is in a business relationship for the purpose of using cloud services.

NOTE 1 – A business relationship does not necessarily imply financial agreements**.**
NOTE 2 – "Party" here can mean an individual ("natural person") or some form of organization ("legal person"), which can be public or private in nature.

SOURCE: ISO/IEC 17788:2014, 3.2.11

Cloud Service Customer Data: class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service, or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer via the published interface of the cloud.
service.

SOURCE: ISO/IEC 17788:2014, 3.2.12

Cloud Service Derived Data: class of data objects under CSP control that are derived as a result of interaction with the cloud service by the cloud service customer.

Note 1 to entry: Cloud service derived data includes log data containing records of who used the service, at

what times, which functions, types of data involved and so on. It can also include information about the numbers of authorized users and their identities. It can also include any configuration or customization data, where the cloud service has such configuration and customization capabilities.

SOURCE: ISO/IEC 17788:2014, 3.2.13

Cloud service level objective: commitment a cloud service provider makes for a specific, quantitative characteristic of a cloud service, where the value follows the interval scale or ratio scale

Note 1 to entry: An SLO commitment may be expressed as a range.

SOURCE: ISO/IEC 19086-1:2016, 3.5

Cloud service qualitative objective: commitment a cloud service provider makes for a specific, qualitative characteristic of a cloud service, where the value follows the nominal scale or ordinal scale

Note 1 to entry: A cloud service qualitative objective may 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 19086-1:2016, 3.6

Cloud Service Provider: party which makes cloud services available.

SOURCE: ISO/IEC 17788:2014, 3.2.15

CSP Transparency Statement: Document that records how the requirements of a SWIPO Code of Conduct for a particular set of service offerings are addressed by a CSP.

Note 1 to entry: A CSP Transparency Statement shall be available to a potential CSC prior to their entering into a contract with the CSP.
Note 2 to entry: A CSA should include references to CSP Transparency Statements that are applicable to the cloud services covered by the CSA.

Cloud Switching/Cloud Service Switching: process where a cloud service customer changes from using one cloud service to using a second functionally similar cloud service, where the second cloud service typically is offered by a different cloud service provider

Code means this Code of Conduct.

Competent Supervisory Authority: supervisory authority designated by the EU or by a Member State for the performance of tasks and the exercise of powers as defined in the Free Flow of non-personal data regulation.

Compliance: adherence by a CSP to the Code of Conduct with regard to a Declared Service.

Compliance Mark: Trade Mark published and owned by the code governing organization made available to an adhering CSP, for the purpose of enabling the CSP to publicly identify a Declared Service as in adherence with the Code. A CSP may display a Compliance Mark in association with any Declared Service in adherence with the Code.

Data: reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing

Note 1 to entry: Data can be processed by humans or by automatic means.

SOURCE: ISO/IEC 2382:2015(en), 2121272

Data Portability: ability to easily transfer data from one system to another without being required to re-enter data

Note: It is the ease of moving the data that is the essence here. This might be achieved by the source system supplying the data in exactly the format that is accepted by the target system. But even if the formats do not match, the transformation between them may be simple and straightforward to achieve with commonly available tools. On the other hand, a process of printing out the data and rekeying it for the target system could not be described as "easy".

SOURCE: ISO/IEC 17788:2014, 3.2.21

Data Porting: the transfer of data from one IT environment to another.

Declaration of Adherence: declaration by the CSP to the governing body of the Code that the CSP adheres to the Code of Conduct with regard to the Declared Service.

Declared Service: cloud service which is identified by a CSP, for which the CSP declares it adheres to the Code of Conduct.

Designated Cloud Service Customer Data/Designated CSC data: cloud service customer data specifically identified in the CSA.

Designated Cloud Service Derived Data: Cloud Service Derived Data that a CSC may be entitled to access and port.

Note 1: typically a CSA will define the types of cloud service derived data that is within scope.

Destination CSP: CSP which provides the cloud service to which the CSC will port the CSC's data from a source environment.

EU Free Flow of Data Regulation: EU regulation relating to the free movement of non-personal data across borders which provides that every organization should be able to store and process data anywhere in the European Union.

See: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2018:303:0059:0068:EN:PDF

GDPR: General data protection regulation. EU wide regulation on the privacy of personal data.

See: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

Infrastructure Artefacts: Cloud Service Customer data, including infrastructure related software components and metadata (e.g. virtual machines, containers, topology data), and designated cloud service derived data.

Note: The CSC and CSP define in the CSA what cloud service derived data is included.

Infrastructure as a Service: cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type

Note: The cloud service customer does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer may also have limited ability to control certain networking components (e.g., host firewalls).

SOURCE: ISO/IEC 17788:2014, 3.2.24

Infrastructure capabilities cloud services: cloud services in which the cloud service customer can provision and use processing, storage and networking resources.

Interoperability: ability of two or more systems or components to exchange information and to use the information that has been exchanged.

SOURCE: ISO/IEC 17788:2014, 3.1.5

ISAE3402: International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization.

Issued by the International Auditing and Assurance Standards Board (IAASB), which is part of the International Federation of Accountants (IFAC). ISAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting.

See: http://isae3402.com/ISAE3402_overview.html

ISO/IEC 17788: ISO/IEC 17788 "*Cloud computing – Overview and Vocabulary*" is an international standard that provides common terminology and the definition of concepts applicable to cloud computing.

See: https://standards.iso.org/ittf/PubliclyAvailableStandards/c060544_ISO_IEC_17788_2014.zip

ISO/IEC 19086: ISO/IEC 19086 "*Cloud computing — Service level agreement (SLA) framework*" is an international standard that provides a set of common cloud SLA building blocks (concepts, terms, definitions, contexts) that can be used to create cloud Service Level Agreements (SLAs).

See: https://standards.iso.org/ittf/PubliclyAvailableStandards/c067545_ISO_IEC_19086-1_2016.zip

ISO/IEC 19941: ISO/IEC 19941 "*Cloud computing — Interoperability and portability*" is an international standard that specifies cloud computing interoperability and portability types, the relationship and interactions between these two cross-cutting aspects of cloud computing and common terminology and concepts used to discuss interoperability and portability, particularly relating to cloud services.

See: https://standards.iso.org/ittf/PubliclyAvailableStandards/c066639_ISO_IEC_19941_2017.zip

on premises: computing facilities where applications are run and data is stored that belong to and are operated by a CSC

Note: Sometimes the term "in-house" is used.

Platform as a Service: cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.

SOURCE: ISO/IEC 17788:2014, 3.2.30

Peer Cloud Service Provider: cloud service provider who provides one or more cloud services for use by one or more other cloud service providers as part of their cloud services.

SOURCE: ISO/IEC 17789:2014, 3.2.5

Port: transfer from one IT system to another.

Portability Public Register: publicly available list of specific cloud services having been declared under the Code and the CSPs declaring them.

Primary CSP: CSP with which the Cloud Service Customer (CSC) has a Cloud Service Agreement (CSA) where the CSP subcontracts part or all of the cloud services to a peer CSP.

Recovery Point Objective: point to which information used by an activity must be restored to enable the activity to operate on resumption.

SOURCE: ISO 22301:2012, 3.44

Recovery Time Objective: period of time following an incident within which product or service must be resumed, or activity must be resumed, or resources must be recovered.

SOURCE: ISO 22301:2012, 3.45

Software as a Service: cloud service category in which the cloud service customer is able to use the CSP's applications

Note: The capability provided to the cloud service customer is to use the cloud service provider's applications running on a cloud infrastructure. The applications are accessible from various client devices

through either a thin client interface, such as a web browser (e.g. web-based email), or an API. The cloud service customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings

Scope and Compatibility Principles: baseline commitments regarding (1) the extent to which the nature and volume of the information about the data to be ported, and (2) the service meets requirements to ensure adequate compatibility, between the respective cloud service environments of the source CSP and a prospective destination CSP.

Source CSP: CSP which provides the cloud service from which the CSC ports the CSC's data to a destination.

Standard: for the purposes of this document, a standard, a technical specification, or an ICT technical specification as defined in EU Regulation 1025:2012

SSAE 16: Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization.

An organization can communicate information about its controls is through an SSAE 16 Service Organization Control (SOC) report.
See: http://ssae16.com/SSAE16_reports.html