Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services

22nd November 2019

Draft Version 2.9

SWIPO IAAS Drafting Group Contributors

Co-chairs

Alban Schmutz	Vice-President Strategic Development & Public Affairs, OVH
	Chairman of CISPE (Cloud Infrastructure Services Providers in Europe)
Freddy van den Wyngaert	General Secretary, EUROCIO

Members of the Core Drafting Group

Lorenzo Guintini,	Aruba	*Mike Edwards,*	IBM
James Mulhern,	AWS	*Najah Naffah,*	Prologue
Robert Jones,	CERN	*Arena Fernandez,*	Santander
Norbert Derickx,	CIO Platform	*Antti Vilpponen,*	UpCloud
Patrick Maes,	Credit Suisse		

Other Contributors include

Chiara Tomasi (Google), *Dimitra Stefanatou* (Arthur's Legal), *Enol Fernandez* (EGI), *Francisco Mingorance* (CISPE), *Johan Christenson* (City Network), *John Violos* (NTUA), *Jörg Hesse* (1&1 Internet), *Jules-Henri Gavetti* (Ikoula), *Julie Ngai* (Alibaba), *Julien Levrard* (OVH), *Marco Barbalinardo* (Almaviva), *Mariano Cunietti* (Enter), *Martin Chapman* (Oracle), *Michael Girg* (Deustche Börse), *Nicky Steward* (UKCloud), *Olivier Tirat* (BYO Networks), *Patrick Le Roux* (GoWizYou), *Sacha Lassiri* (Matilan), *Sébastien Lesimple* (Outscale), *Sébastien Moriceau* (Linkbynet).

(This list is subject to people consent)

Table of Content

The reader is made aware that all acronyms and definitions are available in the Annex B "Glossary of Terms and Acronyms".

© Copyright 2019, SWIPO IAAS working group members and contributors. All rights reserved.

1. Introduction

1.1 Overview

Cloud computing provides transformational benefits including security, cost, flexibility, efficiency and scalability. However, Cloud Service Customers (CSC) may have concerns relating to lock in and the ability to port their data.

The purpose of this Code of Conduct (Code) is to increase CSC's confidence regarding porting and switching between IaaS (Infrastructure as a Service) cloud services or between on-premise facilities and IaaS cloud services, at a low cost and with minimal disruption.

This Code supports the European Union (EU) Free Flow of non-personal Data Regulation objectives and the European Commission (EC) has stated purpose of the regulations to "achieve a more competitive and integrated EU market for data storage and/or processing services and activities."[1]

To achieve this, the EC has proposed regulations that the Commission hopes will reduce the number and range of data localization restrictions, facilitate cross-border availability of data for regulatory control purposes; improve the conditions under which users can switch data storage and/or processing service providers or port their data back to their own IT systems; and, enhance trust in and the security of cross-border data storage and/or processing. This Code is intended to promote these same objectives.

The code is based on the twin principles of providing the necessary technical capabilities to support the CSC activities in relation to the relevant IaaS cloud services and providing transparency about the capabilities of the IaaS cloud services and the behavior of the Infrastructure Cloud Service Providers (**"*Infra. CSPs*"**) who provide those cloud services.

The code intends to support an open and competitive cloud marketplace, which in turn should drive continued adoption and growth of cloud computing, including multi-cloud and hybrid cloud solutions to widen possibilities in the market.

Vendor lock-in is not an acceptable business practice. The Code will be regularly updated in order to keep pace with technological developments, according to governance rules.

1.2 Objectives

The target audience of the Code is any party who has an interest in provision of IaaS cloud services: e.g. *Infra. CSPs*, CSCs, third-party system integrators.

The intent of the Code is to support CSCs data portability and switching between IaaS cloud services, in order to support CSC choice and to enable operations during the switching process.

Adhering *Infra. CSPs* are required to commit to the underlying principles and to meet the requirements set down by the present code. This is particularly important for less sophisticated or less capable CSCs, such as Small and Medium Enterprises (SMEs), but relevant to any organization. The Code requires that a *Infra. CSP* which adheres to the Code for a given cloud service, provides appropriate capabilities and also adequate information, documentation, technical support and where appropriate, tools, for the CSC to perform

[1] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-framework-free-flow-non-personal-data

porting and switching successfully. The porting of Infrastructure Artefacts like virtual machines, containers and topologies is in scope.

1.3 Concepts

Data portability as addressed by this Code means the ability of a CSC to transfer **Infrastructure Artefacts**, including CSC data, infrastructure related software components and metadata (e.g. virtual machines, containers, topology data), and designated cloud service derived data, from one *Infra. CSP* cloud service to another, or between a *Infra. CSP* cloud service and CSC on premises facilities using structured, commonly used and machine-readable formats. Data portability should be enabled at a low cost and with minimal disruption.

Although it is difficult to give an estimated cost for an IaaS switching operation without knowing a certain number of parameters, it is required that *Infra. CSPs* provide clear information about the costing parameters for operations directly associated with porting and switching from/to their own services. This should increase the level of trust between the *Infra. CSP* and the CSC, needed in such a critical operation.

To assist the reader in their understanding of this code it is important to set out some of the key concepts and terms used throughout the code. Formal definitions of these concepts are provided in the glossary.

Infrastructure Artefacts
Cloud Service Customers (CSC) consume the compute, networking and or storage Cloud services provided by IaaS Cloud service providers (CSPs) by generating, configuring or otherwise supplying virtualized instances of their infrastructure.
The virtual machines, and or containers that make up those virtualized instances as well as the installed data and applications and their corresponding configuration constitute the customer's data that that make up discrete Infrastructure artefacts.

Cloud Switching
When a CSC supplies such infrastructure artefacts and consumes a CSP IaaS service they need to be assured that, should they choose to, they are able to retrieve their infrastructure artefacts and switch to using another cloud provider or using on premise systems. The event of switching from one to another is known as clouds switching.

Porting
In order for a CSC to switch cloud providers or back to on premise they must first be able to transfer their infrastructure artefacts by porting them between the source and destination environments.

Portability
For porting to be successful the infrastructure artefact must be able to operate in its new destination.

Interoperable

In order for the ported infrastructure artefacts to be able to function with and exchange any necessary data with its new environment and any other components it interacts with it must be interoperable.

Conversion/translation/transformation/reconfiguration
In order for infrastructure artefacts to be successfully ported and interoperable in a different environment it may be necessary to undertake a conversion, translation, transformation or reconfiguration.

Derived Data
In the course of a CSC consuming IaaS clouds services the underlying cloud service may generate and or derive data such event or active logs as a result of the CSC's use of the cloud service.

1.4 General Roles and Responsibilities

In transferring Infrastructure Artefacts from one cloud service to another, or between a cloud service and on premises facilities, it is incumbent on the CSC to work with the source *Infra. CSP*, the destination *Infra. CSP* and with any on-premises facilities involved to complete an efficient transfer of Infrastructure Artefacts.

This Code does not impose any obligation on the CSC, but recommends that a CSC i) is aware of the exit conditions for the discontinuation of a cloud service before entering into a contract with a *Infra. CSP*, ii) develops a cloud service migration plan in anticipation of such an operation and iii) ensures that the source and destination cloud service(s) can meet their needs with regard to infrastructure portability and cloud service switching. This could be achieved in a contractual arrangement between the *Infra. CSP* and/or a third party systems integrator and the CSC.

1.5 Cloud Service Models

There is a wide spectrum of *CSPs* providing a variety of different cloud services, and data portability approaches may differ between cloud services.

Different cloud service capability types, e.g., IaaS, Platform as a Service (PaaS), Software as a Service (SaaS), can have quite different characteristics in terms of how they integrate CSC data, and thus approach data portability quite differently. The Code is not intended to be a 'one-size-fits-all' response to how data portability is conducted for all cloud services or by all *Infra. CSPs*. It does not address the Platform as a Service (PaaS) or Software as a Service (SaaS) cloud services. *Infra. CSPs* adopting the Code identify their cloud services which are compliant.

1.6 Security

Security criteria for cloud services are out of the scope of this Code. Only security regarding

the switching of data itself is in the scope of this Code.

2. Structure of the Code

The Code is structured as follows:

- Purpose: describes the intent of the Code with regard to data portability and cloud service switching.
- Scope: describes the field of application to which the Code applies.
- Adherence: describes the conditions for *Infra. CSPs* declaring adherence to the Code.
- Portability, Interoperability & IaaS cloud services switching Requirements: requirements for a cloud service to comply with the Code.
- Contractual specification: describes the Cloud Service Agreement (CSA) provisions appropriate to meet the requirements for data portability and cloud service switching.
- Transparency: describes how the adhering *Infra. CSP* demonstrates compliance with the Code.
- Governance: describes how the Code is managed, how complaints are to be addressed and how the Code will be enforced.

3. Purpose

3.1 Intent of the Code

The purpose of this Code is to provide a set of high level requirements for *Infra. CSPs*, the adherence to which improves a CSCs' confidence that a *Infra. CSP* will facilitate a CSCs request to transfer their Infrastructure Artefacts from one cloud service to one other or more, or between a cloud service and on premises facilities in an open, transparent and meaningful manner.

- The Code is a voluntary instrument, allowing an *Infra. CSP* to evaluate and demonstrate its adherence to the Code requirements for one or more of its cloud services. This may be either by third-party certification or by self-assessment. An *Infra. CSP* must fully comply for each declared service.
- *Infra. CSPs* should be transparent in advance to a prospective CSC entering into an agreement, by providing clear and adequately detailed information with regard to technical information, cost, process, tools and support available to enable a CSC to

conduct a data porting operation efficiently and effectively, without loss, degradation or control of the data.

- The relevant cloud service must be capable of being both a source and a destination for data porting operations.
- An *Infra. CSP* may choose to demonstrate compliance with aspects of the Code through the adoption of standards or compliance with certifications related to application and data portability.

3.2 CSC and *Infra. CSP* Relationship

In the context of cloud computing both the CSC and the *Infra. CSP* have certain responsibilities. A CSA should define the respective responsibilities of the *Infra. CSP* and the CSC for the duration of the term of the CSA. This Code only covers the data porting and cloud service switching aspects of the CSA and only covers obligations on *Infra. CSPs*.

3.3 Legal Status

The Code does not replace a CSA between the *Infra. CSP* and the CSC. The *Infra. CSP* and the CSC are free to define how the cloud service is delivered in a written agreement, (the CSA). *Infra. CSPs* should assess whether the CSA that they offer new CSCs in connection with the cloud services meets the Code requirements before declaring their adherence. This code does provide guidance on elements that may be included in a CSA that fulfill the objectives of this Code. Prior to entering into a CSA, an *Infra. CSP* is required under this code to supply a pre-contractual CSP transparency statement for the adhering services that a CSC is interesting in using.

The Code does not constitute legal advice. *Infra. CSPs* have to comply with applicable laws and regulations, however adherence to this Code does not guarantee such compliance. *Infra. CSPs* and CSCs are encouraged to obtain appropriate advice on the requirements of applicable law including data protection laws such as the General Data Protection Regulation (GDPR)[2].

3.4 Infrastructure Artefacts

In the context of data portability and cloud service switching, this Code relates to Infrastructure Artefacts, which includes CSC data and designated cloud service derived data.

Such artefacts could include: business data (structured and unstructured and in various

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

formats), configuration data, logs, virtual machines, containers, source code and executables, security relevant data such as identity information and credentials, relevant metadata information. The CSP transparency statement defines the type of cloud service derived data that is within scope, which could be none. Infrastructure Artefacts may be in the electronic form of documents, databases, images, audio and video clips, software programs, etc.

4. Scope

4.1. Nature of Infrastructure Cloud Services

4.1.1 This code applies only to cloud services which belong to the IaaS cloud service category, as defined in the ISO/IEC 17788 standard. Such cloud services are termed "IaaS cloud services".

4.1.2 The Code consists of a set of requirements for *Infra. CSPs* with regard to data portability and cloud service switching. These requirements are referred to collectively in the Code as the Code requirements. An *Infra. CSP* may declare its adherence to the Code requirements for any IaaS cloud service it provides where that service complies with the Code requirements.

4.1.3 It is not mandatory for the *Infra. CSP* to choose to declare the adherence of all of its IaaS cloud services to the Code. If desired, an *Infra. CSP* can choose to only declare specific cloud services as adhering to the Code. *Infra. CSPs* taking this approach must ensure that CSCs are made unambiguously aware of which cloud services the Code applies to. Equally, it must be made clear to the potential CSC that the Code applies to the specified cloud services offered, and not to all the cloud services of the *Infra. CSP* in general.

4.1.4 Roles and responsibilities of multiple *Infra. CSPs* providing related services: Where an Infra. CSP is an inter-cloud provider[3], using cloud services of peer *Infra. CSPs* in order to offer their own cloud service, the CSC has a CSA only with the primary *Infra. CSP*. It is the primary Infra. CSPs responsibility to have agreements in place with the peer Infra. CSPs that are designed to ensure that the primary *Infra. CSP* can honor the commitments it makes to the CSC in the CSA. The provision of data portability and cloud service switching capabilities are entirely the responsibility of the primary *Infra. CSP*.

If the CSC separately contracts with multiple *Infra. CSPs* and performs their own integration of the contracted cloud services, each *Infra. CSP* is only responsible for their own cloud services under these circumstances.

[3] Inter-cloud provider is explained in more detail in ISO/IEC 17789.

4.1.5 An adhering *Infra. CSP* is required by this Code to make available for transfer the CSC's Infrastructure Artefacts to and from their cloud services in structured, commonly used and machine readable formats. This may include support for the direct transfer to or from another cloud service and transfer to or from the CSCs on premises facilities.

The variety of technologies, protocols and methods of implementation, such as IP addresses, network protocols, APIs, data containers, storage and computing capability technologies, may present data portability incompatibilities. This depends on the nature of the CSC's on premises facilities or of the other cloud service involved in the data porting operation.

Typically, portability can only be achieved with a combination of documentation, technical support and tools to transfer the Infrastructure Artefacts from one service to another.

Infra. CSPs are not responsible for conversion or translation of transferred data, unless they agree to this with the CSC or third party in a contract.

4.2 Personal data vs non-personal data

This Code applies to the transfer of CSC Infrastructure Artefacts including data, which could include both personal data and non-personal data.

Since the definition of personal data is intentionally broad, it is important to recognize the complexity that arises when large volumes of data are generated, for example, by machines and sensors, and can include both personal and non-personal data[4].

The Free flow of non-personal data regulation recognizes such mixed sets of data and states that where personal and non-personal data are inextricably linked the application of GDPR should not be prejudiced.

4.3 Policy aspects of portability

The transfer of Infrastructure Artefacts between a source and a target has to comply any applicable legal, regulatory, organizational and policy frameworks (see ISO/IEC 19941:2014, 5.2.2 and 5.2.3 for an explanation).

This includes regulations on data locality, rights to access, use and share data, and mutual responsibilities with respect to security and privacy between *Infra. CSPs* and CSCs. While technically it may be possible to transfer Infrastructure Artefacts between parties, local laws may prevent this from happening. For example, national security data might not be transferable outside an EU Member State.

It is the responsibility of all parties to ensure applicable laws and appropriate software licensing requirements, as relates to them, are followed before, during and after the transfer.

[4] According to the Free Flow of non-personal Data the EC will issue specific guidance (Art. 8.3).

This code does not cover policy related aspects of portability, though an *Infra. CSP* may provide guidance, especially with respect to licensing.

5. Portability, Interoperability & IaaS cloud services switching Requirements & Recommendations

This section defines requirements Infra. CSPs need to meet to be compliant with this code. Each sub-section identifies and defines a class of requirements.

5.1 Procedural Requirements

Purpose:

In order for a CSC to retrieve their data from a cloud service, to upload data to a new cloud service, or to get assistance from an *Infra. CSP* to port their Infrastructure Artefacts to a cloud service of another *Infra. CSP*, a number of processes and procedures shall be followed. The *Infra. CSP* shall inform the CSC up front of the processes and of the applicable policies.

Requirements:

The following identifies the areas of detail that shall be provided to the CSC:

PR01 - Procedures for initiating switching and porting from the cloud service when it is a porting source

PR02 - Procedures for initiating switching and porting to the cloud service when it is a porting destination

PR03 - Available porting methods and formats, including available protections and known restrictions and technical limitations

PR04 - Charges and terms associated with porting

PR05 - Procedures for activating a new cloud service when it is the porting destination

PR06 - The exit process for an existing cloud service, where it is the porting source, and where the CSC is aiming to terminate its use of the cloud service once porting is complete

PR07 - Available management capabilities for the porting and switching process (e.g. end-to-end management to prevent loss of service to the client)

5.2 Portability

Purpose:

The following requirements and recommendations identify the technical measures to support the process of porting Infrastructure Artefacts.

Requirements and recommendations:

DP01 - The cloud service shall be capable of importing and exporting CSC Infrastructure Artefacts, in an easy and secure way, supporting the following scenarios: CSC to cloud service, cloud service to cloud service and cloud service to CSC. The *Infra. CSP* shall provide the support to enable the transfer of Infrastructure Artefacts using structured, commonly used, machine-readable format.

DP02 – When exporting CSC Infrastructure Artefacts from a CSC to a cloud service, or between cloud services, the *Infra. CSP* should provide support to facilitate the interoperability between the CSC's capabilities including the user function, administrator function and business function[5] related to the cloud service.

DP03 – The *Infra. CSP* should provide Application Programing Interfaces related to the cloud service and, if provided, they shall be fully documented. These APIs should enable the transfer of Infrastructure Artefacts between participating parties. If there are any associated code libraries or dependencies they should be documented and made available.

DP04 - The cloud service is not required under this Code to transform the CSC Infrastructure Artefacts where the destination environment requires the Infrastructure Artefacts to be in different formats than that offered by the source environment. Parties may agree otherwise in the CSA.

DP05 – Transfer of CSC Infrastructure Artefacts to and from the cloud service should use open standards and open protocols for Infrastructure Artefacts movement.

DP06 – Where the CSC data involves Infrastructure Artefacts that rely on a feature or capability of the cloud service, the *Infra. CSP* shall provide an appropriate description of the environment for their execution and how the service dependencies can be satisfied.

DP07 – The *Infra. CSP* should provide a self-service interface that enables the CSC to carry out periodic retrieval of the CSC's data. This functionality can be subject to contract and may include additional costs.

DP08 - The *Infra. CSP* shall take reasonable steps to enable a CSC to maintain their service continuity while transferring data between providers, where technically feasible.

5.3 Scope and Compatibility Requirements

[5] CSC user function, administrator function and business function are described in ISO/IEC 17789 and support for interoperability of these with the cloud service is described in ISO/IEC 19941.

Purpose:

The following requirements help to identify the scope of responsibilities of an *Infra. CSP*.

Requirements:

SCR01 - The *Infra. CSP* shall describe in the CSP transparency statement the capabilities necessary for effective cloud service switching, to minimize loss of functionality, particularly security functionality. It is acknowledged that the CSC and the *Infra. CSP* will define in the CSP transparency statement which derived data will be subject to the same porting requirements. Any porting capabilities relating to cloud service derived data should be clearly described in the CSP transparency statement, but there is no requirement for the Infra. CSP to support the porting of this data unless designated as in scope.

SCR02 - The CSP transparency statement shall specify the following:

a) the scope of Infrastructure Artefacts available for transfer;
b) any claim on Intellectual Property Rights the *Infra. CSP* has on CSC data and how these rights are executed after a switch.

5.4 Planning Requirements and Recommendations

The CSP transparency statement shall address performance, testing and the pricing mechanism necessary to meet portability requirements for transferring data from the *Infra. CSP*, including:

PLR01 - the procedure to determine the testing of the mechanisms and schedule of a transfer, based on the CSC's business needs, security risks, and technical and support capabilities expected of each of the *Infra. CSP* and the CSC. Testing should include both the testing of the mechanisms used for porting data to and from a cloud service and also of the APIs used to access and to manage the data when stored within the cloud service. Further guidelines on testing of the mechanisms including APIs may be adopted by the relevant governance body of the Code. Acceptance of the testing should be made with the CSC, in the frame of a transparent test process. CSC should be recommended by the *Infra. CSP* to have a test suite;

PLR02 - what constitutes appropriate duration for the transfer of the data using current best practices and available technology, including any solutions not using a network;

PLR03 - for the anticipated volume of Infrastructure Artefacts the appropriate mechanisms, availability periods and price for the transfer;

PLR04 - allocation of responsibility and methods for providing security for the data to ensure, for example, access control, authentication of users, confidentiality and integrity through the process; and,

PLR05 - the period during which the CSC data will remain available for transfer once the termination of the source service is required by the CSC, and the nature of clear and timely warnings issued before CSC data is deleted.

6. Contractual Specifications

6.1 Cloud Service Agreement

The Cloud Services Agreement between the *Infra. CSP* and the CSC shall determine the terms under which the data portability and switching of the cloud service is delivered.

The Code does not replace the CSA between the *Infra. CSP* and the CSC. A reference should be incorporated into the CSA covering the adherence of the service to this code.

The*Infra. CSP* shall ensure at all times that its contractual rights and obligations described in the CSA do not diminish the requirements of this Code. The requirements described in this Code apply at all times, and the *Infra. CSP* shall resolve any conflict between the Code and the CSA before declaring adherence to this Code.

6.2 Form of the Cloud Service Agreement

FR1 - The CSA shall be documented (including in electronic form) and legally binding between the *Infra. CSP* and the CSC.

FR2 - The CSA may take any form, including but not limited to:

a) a single contract;

b) a set of documents such as a basic services contract with relevant annexes (data processing agreements, SLAs, service terms, security policies, etc.); or,

c) standard online terms and conditions.

Note: The differing forms and content of a CSA is discussed in ISO/IEC 19086 Part 1.

7. Transparency Requirements

TR01 - The terms and conditions necessary to meet this Code (including those referenced in clauses 5 of this Code) shall be described to potential CSC in clear terms and with an appropriate level of detail in a pre contractual CSP transparency statement between the CSC and the *Infra. CSP*. Please note that ensuring pre-contractual information is available to potential CSCs does not require public disclosure and may be done in strict confidence (e.g. via NDA).

TR02 - The description provided for in TR01 shall provide an appropriate level of details including:

a) all aspects of compliance with this Code;

b) all documentation, available support and tools to transfer the CSC data from one *Infra. CSP* to another;

c) a description of the overall data porting process and supported capabilities including any data back-up and recovery processes adopted for the purpose of protecting the data while undertaking the porting of the data, security measures, record management and, if agreed upon, the deletion of the CSC's data after the data porting is successfully completed (if the CSC intends to terminate the cloud service contract). If the deletion capability is provided to the CSC by the *Infra. CSP*, the CSC can do the deletion on its own. The deletion shall be completed by the source *Infra. CSP*, in the case where such capability is not provided to the CSC;

d) the status and procedures for handling the CSC data on the *Infra. CSP's* infrastructure after termination including CSC instructions on any data retention, preservation or restoration obligations stipulated by applicable law or regulation;

e) a clear description of any and all third-parties that have access to the data through the process;

f) a clear description of the policies and process for accessing data in the event of *Infra. CSP*'s bankruptcy or acquisition by another entity. These policies and process shall include CSC information without undue delay once a bankruptcy procedure has been started with the competent public authorities; and,

g) if a third-party service provider is needed to convert, translate or transfer CSC's Infrastructure Artefacts, it should be explicitly mentioned in the CSP transparency statement.

h) TR03 - Before the CSC accepts the CSA, the Infra. CSP shall provide to the CSC a CSP transparency statement describing the mechanism(s) related to the porting of CSC data:

a) from a CSC's on-premise facilities to a *Infra. CSP*'s cloud service
b) from another cloud service to the *Infra. CSP* 's cloud service

And:

c) to the CSC's on-premise facilities from the *Infra. CSP* 's cloud service
d) to another cloud service from the *Infra. CSP* 's cloud service

The description shall provide an appropriate level of details including:

e) procedures, terms and conditions, policies and costs, associated with such a data porting;

f) appropriate information about the relevant technical, physical and organizational measures to undertake such data porting;

g) if applicable, an explanation of the data model, data schema and data semantics and any policy facet considerations adopted by the *Infra. CSP* as these apply to the CSC data, and how these aspects are handled when considering data portability.

h) All related costs areas that would be charged by the *Infra. CSP*.

The *Infra. CSP* shall ensure that information related to data portability is made available to the CSC, including online and/or incorporated by reference into other contractual documents, and that the information is kept up to date.

TR04 - The *Infra. CSP* shall inform the CSC in a timely manner of any changes to the mechanisms and conditions, including identified costs, that would materially alter the portability of the CSC data. The CSC should be given the right to terminate the agreement in advance.

TR05 - The *Infra. CSP* shall inform the CSC without undue delay if there are permanent changes in its Declaration of Adherence.

8. Governance, Complaints & Appeals, Adherence and Validity

8.1 Governance

This Code is governed under the SWIPO Common Governance and common policies, which are provided in separate documents.

8.2 Complaints & Appeals

Complaints and Appeals under this Code will be managed accordingly of the respective Annex 1 “Complaints” and Annex 2 “Appeals” of the SWIPO Common Governance document.

8.3 Common Terminology

Terminology, definitions and abbreviations are defined in the SWIPO Common Terminology Document

8.4 Compliance Obligations

An *Infra. CSP* that declares adherence with the Code shall comply with all the Code Requirements described in Section 5 (Portability, Interoperability & IaaS cloud services switching Requirements), Section 6 (Contractual Specifications), and 7g (Transparency Requirements) for any cloud service covered by its Declaration of Adherence.

8.5 Compliance Validity

Once the Declaration of Adherence is incorporated into the SWIPO Public Register:

The *Infra. CSP* is entitled to promote the adherence for the cloud services to the Code, once the Declaration of Adherence is listed in the SWIPO Public Register, so long as it remains valid;

8.6 Assessing Suitability

It is the CSCs responsibility to consider and decide whether the cloud services offered by an *Infra. CSP* adhering to this Code are appropriate for the processing of its data.

ANNEX B – GLOSSARY OF TERMS AND ACRONYMS

Glossary of Acronyms

Infra. CSP – Infrastructure Cloud Service Provider

EC – European Commission

EU – European Union

SME – Small and Medium Enterprise