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

**11th June 2018**

**Draft Version 1.6**

**1st Draft of the SWIPO IAAS Core Drafting Group**

**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:**

Lorenzo Guintini, Aruba

Oliver Bell, AWS

Robert Jones, CERN

Norbert Derickx, CIO Platform

Patrick MAES, Credit Suisse

Mike Edwards, IBM

Najah Naffah, Prologue

Arena Fernandez, Santander

Antti Vilpponen, UpCloud

Table of Contents

1. Introduction3
2. Structure of the Code4
3. Purpose4
4. Scope5
5. Adherence7
6. Data Portability, Interoperability & IaaS cloud services switching Requirements7
7. Contractual Specifications9
8. Transparency10
9. Governance, Complaints and Enforcement10

 **10.** Review and changes to the Code13

**Annex A:** Template Declaration of Adherence15

**Annex B:** Glossary of Terms21

1. Introduction

1.1 Cloud computing provides transformational benefits to customers in terms of security, cost, flexibility, efficiency and scalability. The purpose of this Code of Conduct (Code) is to provide assurance to Cloud Service Customers (CSCs) that they can port their data and infrastructure artefacts to and from adhering IaaS cloud services and that they can switch between adhering IaaS cloud services.

Porting and switching can be between two different cloud services of Cloud Infrastructure Services Providers (CISPs), or between the CSC on-premises facilities and a cloud service, in either direction.

More generally, this Code will support the EU Free Flow of non-personal Data Regulation objectives. The EC has stated the purpose of the regulations is to “achieve a more competitive and integrated EU market for data storage and/or processing services and activities.”[[1]](#footnote-2) 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 CISPs who provide those cloud services.

The code supports an open and competitive cloud marketplace, which in turn will drive continued adoption and growth of cloud computing. In addition, this Code supports the EU Free Flow of Data Regulation objectives. To this end, the Code is based on the principle of transparency and will develop provision of specific capabilities.

1.2 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 seamless operations during the switching process. Adhering CISPs are required to provide openness and transparency. This is particularly important for less sophisticated or less capable customers, such as SMEs, but relevant to any organizations. The Code requires that a CISP which adheres to the Code for a given cloud service will provide appropriate capabilities and also adequate information, documentation, technical support and where appropriate, tools, for the CSC to perform porting and switching successfully. The porting of infrastructure artefacts like virtual machines and containers is covered however generic application portability is not addressed in this Code.

1.3 Data portability as addressed by this Code means the ability of a CSC to easily and safely transfer cloud service customer data, and any associated code or functionality, where needed, and to use that data, from one CISP cloud service to another, or between a CISP cloud service and CSC on premises facilities using in a structured, commonly used and machine-readable format.

1.4 In transferring data 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 CISP, the destination CISP and with any on-premises facilities involved to complete an efficient transfer of data. This Code recommends that a CSC is aware of the exit conditions for discontinuation of a cloud service before entering into a contract with a CISP’s and develops a cloud service migration plan in anticipation of such an operation and ensure that the source and destination cloud service(s) can meet the needs of the customer with regard to infrastructure portability and cloud service switching.

1.5 There is a wide spectrum of CISPs providing a variety of different cloud services. Data portability considerations do not necessarily apply to all cloud services in the same way.

Different cloud service capability types (e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)) can have quite different characteristics in terms of how they integrate cloud service customer data, and thus approach data portability quite differently in implementation. The Code is not intended to be a ‘one-size-fits-all’ Code of Conduct for how data portability is conducted for all cloud services or by all CISPs. It does not address the Platform as a Service (PaaS) or Software as a Service (SaaS) cloud services. CISPs adopting the Code are recommended and required to identify the cloud services which adhere to the Code requirements.

Note: This Code may be revised to meet the requirements of the final version of the EU 'Free Flow of non-personal Data Regulation'.

1. Structure of the Code

The Code is structured as follows:

Purpose: describes the ambitions of the Code with regard to data portability.

Scope: describes the field of application of the Code to which the Code applies.

Adherence: describes the conditions for CISPs declaring adherence to the Code.

Data Portability, Interoperability & IaaS cloud services switching Requirements: requirements for a CISP to be in compliance with the Code.

Contractual specification: describes the Service Agreement provisions appropriate to meet the requirements for data portability.

Transparency: describes how the adhering CISP demonstrates adequate compliance with the Code.

Governance: describes how the Code is managed, how complaints are to be addressed and how the Code will be enforced.

1. Purpose

3.1 The purpose of this Code is to provide a set of operational guidelines for CISPs, the adherence to which provides CSCs confidence that the CISP will facilitate a customer’s request to transfer their infrastructure artefacts, including associated data, from one cloud service to another, or between a cloud service and on premises facilities in an open, transparent, predictable and meaningful manner.

The Code is a voluntary instrument, allowing a CISP 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 against the controls in the Code.

CISPs should provide transparency in advance to a prospective CSC entering an agreement, by providing clear and adequately detailed information with regard to cost, process, tools and support available to enable a CSCs to conduct a data porting operation efficiently and effectively, without loss or degradation of control over the data, from the source cloud service to a destination cloud service, or between a cloud service and on premises facilities. Thus, the relevant cloud service must be capable of being both a source and a destination for data porting operations.

A CISP may demonstrate compliance with aspects of the Code through the adoption of standards or compliance with certifications related to application and data portability, such as ISO/IEC 19941:2017(E). Adoption of such standards or certifications further ensure an open competitive market in cloud computing, assuring CSCs they are not locked-in to a particular CISP and can readily transfer artefacts between providers or to on premises facilities. The Executive Board can evaluate new standards as they emerge, and provide guidelines relatively.

3.2 In the context of cloud computing both the CSC and the CISP have certain responsibilities. A Cloud Service Agreement should define the respective responsibilities of the CISP and the CSC for the duration of the term of the Cloud Service Agreement. This Code defines the responsibilities of the CISP with respect to data porting.

3.3 The Code does not replace a Cloud Service Agreement between the CISP and the CSC. The CISP and the CSC are free to define how the cloud service is delivered in a written agreement (the Cloud Service Agreement). CISPs should assess whether the Cloud Service Agreement 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 could be included in a cloud service agreement that fulfill the objectives of this Code.

3.4 The Code is not legal advice. Adherence to the Code does not guarantee a CISP's or a CSCs compliance with applicable law. CISPs 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]](#footnote-3).

3.5 This code is intended to satisfy the requirement for a self-regulatory Code pursuant to Article 6 of the European Commission’s proposed ‘Free Flow of non-personal Data Regulation’ and may be revised to meet the requirements of the final regulation.

3.6 CSCs may verify that a given cloud service adheres to the Code through a Public Register website listing all the cloud infrastructure services for each organization that have declared their adherence to this Code.

3.7 In the context of data portability and cloud service switching, the Code relates to *cloud service customer data*. Cloud service customer data is the class of data objects under the control 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 through the published interface of the cloud service (As defined in ISO/IEC 17788, 3.2.12)

Such artefacts includes: business data (structured and unstructured and in various type formats), configurations, logs, virtual machines, containers, source code and executables, security relevant data such as identity information, credentials, key material, relevant metadata information. This information may be in the form of documents, databases, images, audio and video clips, software programs, etc.

1. Scope

4.1. Nature of infrastructure cloud services

4.1.1. The Code consists of a set of requirements for CISPs with regard to data portability and cloud service switching. These requirements are referred to collectively in the Code as the Code requirements. This Code applies only to a CISP’s infrastructure capabilities cloud services. A CISP may declare its adherence to the Code requirements for any infrastructure capabilities cloud service if the service complies with the Code requirements.

4.1.2 It is not mandatory for the CISP to choose to declare the adherence of all of its infrastructure capabilities cloud services to the Code. If desired, a CISP can choose to only declare specific cloud services as adhering to the Code. CISPstaking 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 CISP in general.

4.1.3 Roles and responsibilities of multiple CISPs providing related services: Where a CISP is an inter-cloud provider[[3]](#footnote-4), using cloud services of peer CISPs in order to offer their own cloud service, the CSC has a Cloud Service Agreement (CSA) only with the primary CISP. It is the primary CISPs responsibility to have agreements in place with the peer CISPs that ensure that the primary CISP can honor the commitments it makes to the CSC in the CSA. Even if there are transparency requirements for the primary CISP to reveal its use of third party cloud services, the provision of data portability and cloud service switching capabilities are entirely the responsibility of the primary CISP.

If the CSC separately contracts for multiple cloud services with multiple CISPs and performs their own integration of those cloud services, the situation is completely different. Each CISP is only responsible for their own cloud services under these circumstances.

4.1.4 An adhering CISP is required by this Code to transfer the CSC artefacts to and from their cloud services in a structured, commonly used and machine readable format, including supporting the direct transfer to or from another cloud service and transfer to or from the CSCs on premises facilities.

For a given cloud service, technologies or protocols may present incompatibilities that must be overcome to enable data portability (e.g., implementations of IP addresses, network protocols, APIs, data containers, types of storage and computing capacity technologies (e.g., different types of hard drives, CPUs or communication protocols)). This depends on the nature of the CSCs on premises facilities or of the other cloud service involved in the data porting operation.

In some of these cases, portability can only be achieved with documentation, technical support and tools to transfer the artefacts from one service to another.

In some contexts, it may be expedient to engage a third-party service provider to convert, translate or transfer customer’s artefacts.

4.2 Personal data vs non-personal data

This Code applies to the transfer of CSC artefacts including data, which could include both personal data and non-personal data. ‘Non-personal data’ has not yet been defined in EU legislation, but in certain cases has been discussed as ‘data other than personal data’.[[4]](#footnote-5)

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.

1. Adherence

5.1 A CISP that declares adherence with the Code will comply with all the Code Requirements described in Section 6 (Data Portability and Interoperability & IaaS cloud services switching Requirements), Section 7 (Contractual specifications), and 8 (Transparency) for any cloud service covered by its Declaration of Adherence.

5.2 The Declaration of Adherence confirms that the cloud service complies with the Code Requirements. The Declaration of Adherence and a detailed description of compliance measures shall be conveyed to the CSC. Reporting pursuant to ISAE3402 within Type I or Type II Statements or SSAE 16 may be used, provided such information is sufficient in detail and clarity to meaningfully comply with this Code.

5.3 The Declaration of Adherence remains valid for three (3) years for a specific version of the Code.

* + 1. Once the Declaration of Adherence is incorporated into the Portability Public Register:

the CISP is entitled to use the Declaration of Adherence for the cloud services covered by the Declaration of Adherence so long as it remains valid; and

if any change to the cloud service results in a material change to the CISP's Declaration of Adherence, then the CISP must promptly re-asses and update the Declaration.

This Public register is managed by the secretariat designated by the Executive Board.

* + 1. It is the CSCs responsibility to consider and decide whether the cloud services offered by a CISP adhering to this Code are appropriate for the processing of its data.

5.5 Cloud service certification

A CISP may demonstrate compliance with aspects of the Code through the adoption of standards or compliance with certifications related to interoperability and data portability.

1. Data Portability and Interoperability & IaaS cloud services switching Requirements

This section defines the requirements CSPs need to meet to be compliant with this code. Each sub-section identifies a class of requirements that are then further enumerated.

6.1 Procedural requirements

Purpose:

In order for a CSC to retrieve their data from a cloud service, to upload data to a new service, or to request a CISP to move their artefacts to another CISP, a number of processes and procedures need to be followed. As CISPs might have different process and policies in place, each CISP will need to inform them of their rules. The set of requirements below identifies the areas of detail that need to be provided to the CSC.

Requirements:

The procedures for data exchange shall clearly specify the requirements for:

PR-01 - Initiating switching and porting from the cloud service when it is a porting source

PR-02 - Initiating switching and porting to the cloud service when it is a porting destination

PR03 - How porting is done between the cloud service and another cloud service, where the cloud service is either the source or the destination

PR04 - Advising and agreeing charges and terms associated with porting

PR05 - 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 the CSC is aiming to terminate its use of the cloud service when the port is complete

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

6.2 Data Portability

Purpose:

Then following requirements identify what technical measures are needed to support the process of porting infrastructure artefacts.

Requirements:

DP01 - The source cloud service shall take all reasonable steps to enable a CSC to easily and securely transfer the cloud service customer data to another cloud service or to on premises facilities.

DP02 - The source cloud service shall provide to the CSC the capability and the technical support to transfer the cloud service customer data in a structured, commonly used and machine-readable format.

DP03 - Where the cloud service is the destination of porting and switching (i.e. cloud service customer data is ported to the cloud service), the cloud service shall provide support for interoperability between the CSC's user function, administrator function and business function and the cloud service.

[Note: 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.]

DP04 - Where the cloud service is the destination of porting and switching, the cloud service shall provide support for customer application programmatic access to the ported cloud service customer data.

[Note: It is expected that programmatic access to the cloud service customer data is provided through an API of some form. This API should follow a standard, but if it proprietary, the API should be fully documented and any associated required code libraries should be available to the CSC for use by customer applications.]

DP05 - The destination cloud service shall take all reasonable steps to enable a CSC to easily and securely transfer the cloud service customer data from another cloud service or from on premises facilities.

DP06 - The destination cloud service shall provide to the CSC the capability and the technical support to accept the cloud service customer data in a structured, commonly used and machine-readable format.

DP07 - The cloud service is not required under this Code to transform the cloud service customer data where the destination environment requires the data to be in a different format than that offered by the source environment.

DP08 - Transfer of the cloud service customer data to and from the cloud service where possible and appropriate should be made using open standards and open protocols for data movement.

DP09 - The cloud service should implement APIs that are either non-proprietary open standards or, if proprietary, make available with requisite technical information and support and at no cost such APIs, to execute the transfer of the cloud service customer data.

6.3 Scope and Compatibility Requirements

Purpose:

The following requirements help to identify the scope of responsibilities of a CISP.

Requirements:

The CISP and customer shall agree in the Cloud Service Agreement the extent of the data transfer and systems interoperability, necessary for effective cloud service switching, to guarantee no loss of minimum functionality, particularly security functionality. This shall include clear agreements on:

1. the scope of data transfer and storage, including, for example, security records and incident history
2. the compatibility requirements necessary to support non-functional data, such as security events and incident records

6.4 Planning

The CISP and CSC shall agree in the cloud Service Agreement as to performance, testing and the pricing mechanism to meet portability requirements for transferring data from the CISP, including:

1. the procedure to determine the testing of the APIs and schedule of a transfer, based on the customer’s business needs, security risks, and technical and support capabilities expected of each of the CISP and the customer. This may potentially include requirements for Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs) or other cloud service level objectives (see ISO/IEC 19086). Further guidelines on testing of the APIs could be adopted by the Executive Board of the Code at least after 6 months after its approval by the governance, based on uses cases and return of experiment of the market;
2. what constitutes appropriate duration for the transfer of the data using current best practices and available technology including agreement on the minimum network bandwidth and transfer rate requirements, including transfer solutions not using a network;
3. reference to the anticipated volume of data to be transferred and appropriate criteria for the duration for a transfer based on the volume and other relevant characteristics of the process (such as bandwidth, etc.), including an approach which provides for a maximum period acceptable to make the data available to the customer
4. 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
5. the period during which the cloud service customer data will remain available for transfer once the termination of the source service is demanded by the CSC, and the nature of clear and timely warnings issued before cloud service customer data is deleted.
6. Contractual specifications

7.1 The Cloud Services Agreement between the CISP 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 CISP and the CSC.

However, as highlighted in section 4 above, the CISP 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 CISP shall resolve any conflict between the Code and the CSA before declaring adherence to this Code.

7.2 Form of Cloud Service Agreement

The CSA shall be in writing (including in electronic form) and legally binding between the CISP and the CSC.

The CSA may take any form, including:

a single contract;

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

standard online terms and conditions.

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

1. Transparency

8.1.1 The terms and conditions necessary to meet this Code (including those referenced in clause 6 of this Code) shall be described to the CSC in clear terms and with an appropriate level of detail in the Cloud Service Agreement between the customer and the CISP.

8.1.2 Prior to concluding a CSA, the CISP shall disclose to the CSC in clear terms with an appropriate level of detail, the costs, procedures, terms and conditions and policies for data portability to and from the covered cloud services both from and to another cloud service or from and to on premises facilities, including capabilities necessary to support interoperability, including:

1. all aspects of compliance with this Code;
2. a description of the overall data porting process including the data back-up and recovery processes adopted for the purpose of protecting the data while undertaking the porting of the data by the CISP, including security measures, record management and, if agreed upon, the deletion of the customer’s data by the source CISP after the exchange is successfully completed (if the CSC intends to terminate the cloud service contract);
3. the disposition of the CSC data on the CISP’s infrastructure after exit with termination (e.g., the period of preservation as back up with restore capability, preservation as archival if stipulated by local laws or regulations for the requisite amount of time, or deletion of the CSC data) if the CSC intends to terminate the cloud service contract;
4. a clear description of the data deletion process;
5. a clear description of any and all third-parties that have access to the data through the process; and
6. guarantees and a description of the policies and process for accessing data in the event of CISP’s bankruptcy or acquisition by another entity.

8.2 Before the CSC accepts the CSA, the CISP shall provide to the CSC a description of the mechanism(s) related to the porting of cloud service customer data:

* from CSC on premises facilities to the selected cloud service
* from another cloud service to the selected cloud service
* from the selected cloud service to CSC on premises facilities
* from the selected cloud service to another cloud service

The description shall provide an appropriate level of details including:

procedures, terms and conditions, policies and costs, associated with such a transfer;

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

if applicable, an explanation of the data model, data schema and data semantics and any policy facet considerations adopted by the CISP as these apply to the cloud service customer data, and how these aspects are handled when considering data portability, both for:[[5]](#footnote-6)

functional data used during the operation of the service

non-functional data used to support or protect the service, particularly security-related

1. the location or locations where the cloud service customer data is stored. For security reasons, only a general location (such as a city or city region area) needs to be provided; If the CISP decides to relocate data, the CISP shall provide to the CSC adequate notice and opportunity to object to the relocation of the cloud service customer data.
2. All related costs that would be charged by the CISP.

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

8.3 The CISP shall inform the CSC in a timely manner of any changes to the mechanisms and conditions, including costs, that would materially alter the portability of the cloud service customer data.

8.4 The CISP shall inform the CSC within 48 hours if there are any changes in its Declaration of Adherence.

1. Governance, Complaints and Enforcement

9.1 Governance

9.1.1 The governance of the Code itself, will be constituted of an Executive Board with operational decision making power that will serve as the body to facilitate implementation, monitoring and enforcement, and a Secretariat for administrative support. The Executive Board should include a balanced representation of CSCs and CISPs.

9.1.2 The Executive Board, directly or through any task forces it chooses to create, may perform the following functions:

define and propose the content of the Code Declaration of Adherence and any guidelines for self-assessment;

identify appropriate existing standards and certification schemes that can be used to confirm compliance with all or parts of the Code.

define and adopt more detailed guidelines for the application and interpretation of the Code for specific use cases, data types, service provisioning models, sectors or industries;

define and adopt guidelines for the publication of complaints for non-compliance on the Public Register;

adopt Compliance Marks that may be used by adhering CISPs;

establish a Public Register of CISP’s which have issued a Declaration of Adherence with the Code Requirements and to publish non-compliance complaints against CISPs. This Public Register will be run by the secretariat; and

work on particular issues and new developments impacting the Code.

9.1.3 Any proposals for a decision by the Executive Board must be adopted through approval by a majority of two third of votes of the Executive Board members.

9.1.4 The Executive Board will invite interested third parties to submit an application to join the Executive Board with a view of strengthening the balanced representation of stakeholders interested in participating to the Code from both the private and public sectors. No organization or company may be represented by more than one person in the Executive Board.

9.1.5 The Code of Conduct Executive Board shall elect, by simple majority vote, a Chairman and a Vice-Chairman from amongst its members for a period of two years, with the possibility of renewing their mandate for any number of successive additional two year terms. The Code of Conduct Executive Board shall meet at least twice a year or as necessary either physically or remotely via electronic meetings or conference calls.

9.1.6 The Code of Conduct Executive Board shall likewise develop appropriate policies to assure that interests are disclosed and conflicts are avoided. Mechanisms will include separation of duties, recusal or other policies undertaken by the Code of Conduct Competent Executive Board. The Code of Conduct Executive Board will also create a mechanism to hear complaints of potential conflicts as well as appropriate appellate procedures related to decisions that impact organizations.

**9.2 Complaints**

9.2.1 Complaints Committee

The Governance of this Code will require the appointment of a Complaints Committee.

The Complaints Committee will be responsible for: (a) considering complaints about the compliance of services covered by a CISP's Declaration of Adherence with the Code Requirements, and (b) taking enforcement action against a non-compliant CISP and, where necessary, recommending such enforcement action to the Executive Board.

The Complaints Committee will be composed of 5 members, appointed by the Executive Board for a 2-year period. It shall at least include a balanced representation of (s) and CSC(s) and at least 1 independent member. In case of conflict of interest of one of the members of the Compliant Committee, the Executive Board may replace for the duration of the procedure the conflicted member in the Complaints Committee.

9.2.2 Complaints Process

The Complaints Committee will propose rules and an objective process to make, decide, appeal and communicate the outcomes of complaints about the compliance of services covered by a CISP's Declaration of Adherence with the Code Requirements (Complaints Process).

Once designated and confirmed, the Complaints Committee will publish, implement and administer and keep under review the Complaints Process. The Complaints Committee will publish and maintain up to date information on the Complaints Process on a Portability Public Register website.

A CISP, a customer or a competent supervisory authority can make a complaint to the Complaints Committee in accordance with the Complaints Process. The Complaints Committee shall review and decide on that complaint in accordance with the Complaints Process.

9.2.3 The costs for the complaint process shall be borne by the complaining party. In the event the Complaints Committee finds the CISP which is subject of the complaint has violated this Code, the costs shall be reimbursed by the CISP to the complaining party.

**9.3 Remedies against non-compliance**

If in its final decision the Complaints Committee finds that a CISP is non-compliant with the Code Requirements, then the Complaints Committee may:

* request the CISP to take specific remediating measures within a reasonable timeframe to comply the Code;
* in case of failure by the CISP to implement the requested remediating measures (at all or in time), recommend that the CISP's Declaration of Adherence be suspended or revoked in respect of the non-compliant service; and
* use publicity means (e.g. press releases) to make the market aware of repeated cases of infringements.

If a CISP's Declaration of Adherence is suspended or revoked:

* the Complaints Committee shall promptly remove the affected service(s) from the CISP's Declaration of Adherence on the Portability Public Register;
* the Complaints Committee shall specify a reasonable timeframe for when the CISP must stop using the Compliance Mark in respect of the relevant service; and
* the CISP shall stop using the Compliance Mark in respect of the relevant service within the timeframe specified by the Complaints Committee.

In the case of suspension, these measures shall apply until such suspension is lifted.

The enforcement measures above are:

* the sole and exclusive remedies for a CISP's non-compliance with the Code Requirements; and
* are without prejudice to the customer’s rights under applicable EU law or the Service Agreement.

The option for a customer to make a complaint does not give the customer any direct rights or remedies against the CISP or the Complaints Committee under or in connection with the Code.

The Complaints Committee does not accept any responsibility for a CISP's compliance with the Code. Nor will the Complaints Committee be liable to any party under any cause of action or theory of liability for any loss or damages arising from an act or omission of the Complaints Committee or a CISP in connection with the Code.

 **10 Review and changes to the Code**

**10.1 Review of the Code**

A review of the Code may be initiated by:

* The Executive Board of the organization(s) managing the Code; or
* The Executive Board of the organization(s) managing the Code upon request of CSCs or CISPS; or
* a competent supervisory authority acting in an official capacity; or
* 10% of the General Assembly of the governing organization(s)

**10.2 Changes to the Code**

In order to prepare the update of the Code, the Executive Board could appoint a task force to prepare a draft of an update Code. This task force should be representative of the CSCs and CISPs, and the variety of sizes and geographical origin of organizations. The composition of the task force should be balanced between CSCs and CISPs. The draft updated Code will be submitted to the Executive Board.

Changes to the Code must be adopted by the Executive Board before being submitted to the General Assembly. The update Code will be valid once approved by the General Assembly.

Before adoption, the Executive Board may decide to submit a change to the Code for consideration and comment to a competent supervisory authority.

A major update to the Code shall not be decided more than once a year.

As soon as practicable after a change to the Code has been adopted, the Secretariat shall publish an updated version of the Code on the Portability Public Register. The 2 previous version of the Code will remain available publicly: only the 3 last versions of the Code will be supported.

CISPs are required to renew or re-confirm their Declarations of Adherence within a year of the updated version of the Code being published on the Public Register.

The Public Register will state clearly against version of the Code a cloud service is adherent.

The CISP shall state clearly to its CSCs which version of the Code a cloud service is adherent.

In the meantime, and in order to avoid confusion, new CSC contracted under the Declared service as well as existing CSCs under contract has to be informed of the transition period by the CISP. The right to use any label will not be granted anymore after 12 months of the update of the Code if the CISPs didn’t re-confirm their Declarations of Adherence. A CISP who shows that its service adheres to the Code Requirements by presenting a Certificate together with its Declaration of Adherence may rely on an existing Certificate to show that the service adheres to the updated version of the Code without having to undergo a new or separate audit to obtain a new certificate or report.

**ANNEX A**

**Template Declaration of Adherence**

This is a Declaration of Adherence ("**Declaration**") with the ‘Code of Conduct for Data Portability and Service Provider Switching for Cloud Infrastructure as a Service Providers’ (the "**Code**"). Unless they are otherwise defined, capitalised terms used in this Declaration will have the meaning given to them in the Code.

1. **Services covered by this Declaration**

This Declaration covers the cloud infrastructure service(s) below (the "**Services**"). If this Declaration is being made for more than one service, please include details for each service below.

|  |  |  |
| --- | --- | --- |
|  | **Service Name**(Will appear on the Portability Public Register) | **Further information**(Optional and will not appear on Portability Public Register) |
| Service 1 | [Insert] | [Insert] |
| Service 2 | [Insert] | [Insert] |
| Etc |  [Insert] |  [Insert] |

1. **CISP making the Declaration**

This Declaration should be made by an entity which is a seller of record of the Service(s) (the "**CISP**"). If this Declaration is being made by more than one CISP, please include details for each CISP below and in the declaration at Section 5. This information will appear on the Portability Public Register.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Legal name** | **Address** | **Contact Office or Person** |
| Seller of Record 1 | [Insert] | [Insert] | [Insert] |
| Seller of Record 2 | [Insert] | [Insert] | [Insert] |
| Etc |  [Insert] |  [Insert] |  [Insert] |

1. **Support for the Declaration provided by the CISP**

This Declaration is supported by:

* Certification by an independent third party auditor.
* A self-assessment by the CISP.

Your choice will determine which Compliance Mark the CISP is eligible to use for the Service(s).

1. **Declaration**

By signing below the CISP confirms that:

* 1. as of the date of this Declaration the Services adhere to the Code Requirements;
	2. the CISP will comply with the complaints and enforcement procedures in Section 9 (Governance, Complaints and Enforcement) of the Code; and
	3. if any change to the Service(s) or the Code means a material update to this Declaration is required, then (i) the CISP must promptly notify the Secretariat, and (ii) cooperate with the Secretariat to update those materials.

**[CISP NAME]**

By: Name: Title:

Date:

**ANNEX B**

**Glossary of Terms**

**Application** means a self-contained computer program that performs a particular function directly for the user (examples of applications include email programs, word processors, enterprise software, accounting software, and database management programs).

**Application Programming Interface (API)** means a set of functions and procedures that provide an interface to allow the creation of applications which access the features or data of an operating system, application, or other service.

**Application Portability** means the ability to port an application from one IT environment to another.

**Certification** means an official document attesting to a status or level of achievement with regard to compliance with a defined standard or qualification (e.g., meeting an ISO standard). Compliance with a standard is typically evaluated by a third-party, which provides certification as to compliance.

**Cloud Computing** means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST definition at <http://csrc.nist.gov/publications/PubsSPs.html#800-145>.

**Cloud Infrastructure Service Provider (CISP)** means a Cloud Service Provider that offers Infrastructure as a Service to its Cloud Service Customers.

**Cloud Marketplace** means the competitive, commercial marketplace for Cloud Services.

**Cloud Service** means Cloud Computing resources provided by a Cloud Service Provider over the Internet that may include selection, deployment and ongoing management of Cloud Computing resources by the Cloud Service Provider.

**Cloud Service Agreement** means the contract for services between the CISP and the Cloud Service Customer.

**Cloud Service Customer (CSC)** means the direct customer of a Cloud Service Provider.

**Cloud Service Provider (CSP)** means a Cloud Service Provider is a provider of cloud services to Cloud Service Customer.

**Cloud Switching/Cloud Service Switching** means the ability of a Cloud Service Customer to port their data from one Cloud Service Provider to another Cloud Service Provider or other IT environment.

**Compliance** means the adherence by a CISP to the Code of Conduct with regard to a Declared Service.

**Compliance Marks** means the Trade Mark published and owned by the CISPE made available to an adhering CISP, for the purpose of enabling the CISP to publicly identify a Declared Service as in adherence with this Code. A CISP may display a Compliance Mark in association with any Declared Service in adherence with this Code.

**Code** means this Code of Conduct.

**Data** means information in a form that is efficient for movement or processing in an IT environment (e.g., in computing, information is typically translated into binary digital form).

**Data Portability** means the ability to transfer data easily from one IT environment to another.

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

**Declaration of Adherence** means a declaration by the CISP to CISPE that the CISP adheres to this Code of Conduct with regard to the Declared Service.

**Declared Service** means a cloud infrastructure service which is identified by a CISP, for which the CISP declares it adheres to this Code of Conduct.

**Destination CISP** means the CISP which provides the Cloud Infrastructure Service to which the CSC will port the CSC’s data from a Source CISP.

**EU Free Flow of Data Regulation** means the EU regulations relating to the free movement of non-personal data across borders which provides that every organisation should be able to store and process data anywhere in the European Union. <https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data>

**Infrastructure artefacts** includes data, virtual machines or containers that may be an object of portability at a IaaS level.

**Infrastructure as a Service (IaaS)** means the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). NIST definition at <http://csrc.nist.gov/publications/PubsSPs.html#800-145>.

**Infrastructure capabilities cloud services** means Cloud services delivered as Infrastructure as a Service.

**Interoperability** means the ability of two or more systems or components to exchange information and to use the information that has been exchanged. See, Institute of Electrical and Electronics Engineers, *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries* (New York, NY: 1990). With respect to software, the term interoperability is used to describe the capability of different programs to exchange data via a common set of exchange formats, to read and write the same file formats, and to use the same protocols. <http://www.newworldencyclopedia.org/entry/Interoperability#cite_ref-2>

**ISAE3402** means the International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization, was 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 19086** means ISO/IEC 19086 seeks to establish a set of common cloud SLA building blocks (concepts, terms, definitions, contexts) that can be used to create cloud Service Level Agreements (SLAs). The document specifies (a) an overview of cloud SLAs, (b) identification of the relationship between the cloud service agreement and the cloud SLA, (c) concepts that can be used to build cloud SLAs, and (d) terms commonly used in cloud SLAs. See, <https://www.iso.org/standard/67545.html>

**ISO/IEC 19941** means ISO/IEC 19941 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://www.iso.org/standard/66639.html>

**Platform as a Service (PaaS)** means the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.[[6]](#footnote-7) The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. NIST definition at <http://csrc.nist.gov/publications/PubsSPs.html#800-145>.

**Peer CISPs** the secondary CISP, where a service offered by a primary CISP in a Cloud Service Agreement (CSA) to a Cloud Service Customer (CSC) is subcontracted by that primary CISP to be provided by a secondary CISP.

**Port** means to transfer from one IT environment to another.

**Primary CISP** means the CISP with which the Cloud Service Customer (CSC) has a Cloud Service Agreement (CSA) and this CISP subcontracts services offered to the CSC under the Cloud Service Agreement to a third-party CISP.

**Recovery Point Objective (RPO)** is age of files (based on the point in time the backup was made compared to the point in time of the failure of the computer, software, system or network) that must be recovered from backup storage for normal operations to resume if a computer, software, system, or network fails.

**Recovery Time Objective (RTO)** the acceptable period of time to recover from a computer, software, system or network failure for normal operations to resume. RTO is based on a Business Impact Analysis (BIA) to determine the tolerable duration of an interruption to normal business operations.

**Software as a Service (SaaS)** means the capability provided to the customer is to use the service provider’s applications running on a cloud infrastructure.[[7]](#footnote-8) 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 a program interface. The consumer 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. NIST definition at <http://csrc.nist.gov/publications/PubsSPs.html#800-145>.

**Scope and Compatibility Principles** means the 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 Source CISP’s and a prospective Destination CISP’s respective IT environments.

**Service Provisioning Model** means the model for Cloud Service provided by the CSP (e.g., Software as a Service, Infrastructure as a Service, or Platform as a Service).

**Source CISP** means the CISP which provides the Cloud Infrastructure Service from which the CSC will port the CSC’s data to a Destination CISP.

**SSAE 16** means the 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. A SOC 1 report focuses on controls at the service organization that would be useful to user entities and their auditors for the purpose of planning a financial statement audit of the user entity and evaluating internal control over financial reporting at the user entity.  The SOC 1 report contains the service organization's system description and an assertion from management.  In addition, the independent service auditor (i.e., CPA firm) opinion or service auditor report is included. <http://ssae16.com/SSAE16_reports.html>

1. <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-framework-free-flow-non-personal-data> [↑](#footnote-ref-2)
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 [↑](#footnote-ref-3)
3. Inter-cloud provider is explained in more detail in ISO/IEC 17789. [↑](#footnote-ref-4)
4. For instance while discussing the proposal for a Digital Content Directive. In this regard, the European Data Protection Supervisor (EDPS) provided a non-binding opinion on the notion of personal data: ‘In the light of the broad definition of personal data under the GDPR, it is likely that almost all data provided by the consumer to the provider of the digital content will be considered as personal data”. [↑](#footnote-ref-5)
5. See, Van Der Wees, Arthur and Hayward, Douglas, SMART 2016/0032 Switching of Cloud Services Providers presentation (2017, IDC), p.20. See also ISO/IEC 19941. [↑](#footnote-ref-6)
6. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. [↑](#footnote-ref-7)
7. A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer. [↑](#footnote-ref-8)