SWIPO AISBL Code of Conduct, V.1.2 for public consultation

Code artefact - software code created or provided by the CSC. In this context "software code" includes but is not limited to scripts, containers, complete programs, partial programs, code and function libraries, microservices, AI structures, virtual machine images, and other forms of compileable or executable software.

[Editors's note : New Definition – move to common terminology on final agreement]

Switching and Portability of data for Cloud Services

1. Introduction (tbd)

2. Structure of Code

The structure of the code is built up as follows.

Introduction

Structure of the Code (this section)

Interaction with other documents

This Code is part of the overall SWIPO activity. As such the Code operates under the following higher-level documents:

Governance

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

Declaration of Adherence

Declarations of Adherence shall use the SWIPO Declaration of Adherence Form

Complaints & Appeals

Complaints and Appeals under this Code will be managed according to the SWIPO Complaints and Appeals Procedure and related forms

Common Terminology

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

Code of Conduct CSP requirements

The CSP requirements are structured as

Adherence to the Code

General Requirements

(All subsequent requirements will correspond to clauses in the transparency statement)

Data Export Requirements

Data Import Requirements

Additional or Combined Requirements

Annex 1: Transparency Statement (Normative)

3. Adherence to the Code

3.1 For a service to adhere to the code the CSP shall unambiguously and explicitly specify the service and commit to the undertakings in the current SWIPO Declaration of Adherence form and all requirements documented in this code (this document). The Transparency statement as defined in Annex 1 of this document shall be the 'relevant transparency statememt' referred to in Section 2 of the Declaration of Adherence form. The Transparency statement may refer to external references and sources.

Moreover, being the provider lock-in a not acceptable business practice, any technological development should declare if it will introduce new technology development that might induce vendor-lock for services adhering the code. In addition no single product extention can be done solely for the purpose of locking in customers.

4. General Requirements

4.1 The CSP shall ensure the adherent service offers technical, contractual and licensing arrangements such that they are sufficient to enable porting and switching including the scenarios of porting and switching between the adherent CSP service to and from a CSC or to and from a CSC contracted third party CSP. These arrangements shall be documented in the transparency statement in sufficient detail for prospective CSCs to perform due diligence.

All cloud service customer data will be included. It must be transparently declared which cloud service derived data and account data are included. Cloud service provider data will not be included.The detail of the documented arrangements must enable the prospective CSCs to port data and switch service whatever will be the type of the provided cloud services, specifying all data generated or co-generated, including the relevant data formats and data structures, in a structured, commonly used and machine-readable format and , if needed for the execution of porting and switching , public interfaces (publicly available and free of charge) and existing European standards. If existing, open standards are preferred.

Moreover CSP will inform prospective CSCs about the data storage and backup location.

Note 1 Ensuring pre-contractual information in the transparency statement is available to potential CSCs does not require public disclosure and may be done in strict confidence (e.g. via NDA)

Note 2 The Transparency Statement forms part of the market offering and, unless deviations are mutually agreed, becomes contractually binding and a reference may be incorporated into the proposed CSA.

Note 3 Any material change affecting compliance would be covered under 4.1.2(4) of the common governance and 3(c) of the declaration of adherence form and constitute a material change to the contract or service triggering the normal rights to terminate.

Note 4 The arrangements documented in the transparency statement will permit to prospective CSCs to

(a) terminate , after a maximum notice period of 30 calendar days, the contractual agreement of the service;

(b) conclude new contractual agreements with a different provider of data processing services covering the same service type;

(c) porting its data, applications and other digital assets to another provider of data processing services;

(d) maintaining functional equivalence of the service in the IT-environment of the different provider or providers of data processing services covering the same service type

These arrangements will be related to the services, contractual agreements or commercial practices provided by the original provider.

Note 5 In case the Transparency Statement will be incorporated into a proposed CSA, the contract shall include at least the following:

(a) clauses allowing the customer, upon request, to switch to a data processing service offered by another provider of data processing service or to port all data, applications and digital assets generated directly or indirectly by the customer to an on-premise system, in particular the establishment of a mandatory maximum transition period of 30 calendar days, during which the data processing service provider shall:

(1) assist and, where technically feasible, complete the switching process;

(2) ensure full continuity in the provision of the respective functions or services.

(b) an exhaustive specification of all data and application categories exportable during the switching process, including, at minimum, all data imported by the customer at the inception of the service agreement and all data and metadata created by the customer and by the use of the service during the period the service was provided, including, but not limited to, configuration parameters, security settings, access rights and access logs to the service;

(c) a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transition period that was agreed between the customer and the service provider, in accordance with paragraph 1, point (a) and paragraph2.

2. Where the mandatory transition period as defined in previous paragraph is technically unfeasible, the provider of data processing services shall notify the customer within 7 working days after the switching request has been made, duly motivating the technical unfeasibility with a detailed report and indicating an alternative transition period, which may not exceed 6 months. Full service continuity shall be ensured throughout the alternative transition period

4.2 The CSP shall ensure at all times that its contractual rights and obligations described in the CSA do not diminish the requirements of this Code.

4.3 The CSP shall ensure any CSC is entitled to perform the data export process at termination of the CSA by one of the contracting parties for whatever cause subject only to any requirements imposed by law, regulation or judicial process.

4.4 The CSP should offer the option for conversion or translation of transferred data to another open standard format.

4.5 The CSP shall always meet the requirements of the GDPR where these might override the Article 6 objectives. However, reasonable steps shall be taken to meet the objectives without violating GDPR.

4.6 The CSP must establish in advance which rights (i.e. intellectual property licensing right) the CSC has to acquire in order to ensure the service and the portability of the data.

4.7 Any unilateral change made by CSP must not undermine the Article 6 Objectives; if this should happen, the CSP must provide for a reasonably long period before the changes become effective so as to enable the CSC to change to a new provider. **5 Data Export Requirements**

5.1 The CSP shall declare all data and data types in scope for data export including infrastructure artefacts, code artefacts, any derived data and meta data either in the transparency statement or as an attached document as preferred to allow for more complex services.

Note 1 This is subject to the requirements of 4.1.

5.2 The source CSP shall have and specify an explicit and structured process for data export. The specification shall include:

5.2.1 Data management considerations (e.g. snapshots and incremental approaches, records management policies and procedures, minimum network bandwidth required)

5.2.2 Relevant Timescales

5.2.3 Notice Requirements

5.2.4 Customer contact procedures (contact points, escalation etc)

5.2.5 Impact on service continuity

5.2.6 Availability of the export procedure during and post the contractual period

5.2.7 Any CSP or third party tools or services required for data export

5.2.8 Any CSP imposed or enforced obligations on CSCs before data exporting can commence

5.2.9 Explicit declaration on whether or not the source CSP's processes for data portability allow a CSC to be completely autonomous in exporting data

5.2.10 Any required activation or termination steps to initiate transfer and terminate service(s)

5.2.11 Any required dependencies such as code libraries which if required shall be documented and made available

5.3 The source CSP shall specify all relevant fees in sufficient detail to allow the CSC to calculate export costs including:

5.3.1 The fee structure as charged by the CSP for data export and related procedures under the proposed CSA.

5.3.2 The fee structure for any other CSP or third party tools (as per 5.2.7)

5.3.3 Any known post contractual license fees or other liabilities, for example patent and licensing fees covering use of derived data or data formats or claims and cases that are ongoing.

5.3.4 the total costs for switching that will never exceed the costs incurred by the provider of data processing services that are directly linked to the switching process concerned and will be reduced according the European law and regulation

5.4 The source CSP shall specify which data standards, formats , data types and/or file types are recommended, used or available for data exporting (e.g. binary, MIME, CSV, SQL, JSON, XML, Avro) for each and every data set available for export including any unstructured data.

5.5 The source CSP shall specify the available mechanisms, protocols and interfaces that can be used to perform data export (e.g. VPN LAN to LAN, Data Power, SFTP, HTTPS, API, physical media…)

5.6 The source CSP shall provide documentation on the format and structure of the exported data and any related APIs including where it can be sourced and under what terms if from a 3rd party source (including open or industry standard formats or exchanges e.g. Open Financial Exchange format).

5.7 The source CSP shall specify what cryptographic processes and services it provides, if any, during data export (including unencrypted options) and how encryption keys are managed explicitly ensuring the CSC can decrypt any encryped data.

5.8 The source CSP shall specify any security controls (e.g. access controls) available during data export.

5.9 The source CSP shall specify any access to, retention period and deletion processes (including notification of deletion) of data, including differing categories of data (including derived data and management data) after the expiration of contract.

5.10 The source CSP shall specify any processes or services that it provides or supports to maintain data integrity, service continuity and prevention of data loss specific to data exporting . Where they exist this shall include but is not limited to:

- **5.10.1** pre and post transfer data back-up and verification
- **5.10.2** freeze periods
- **5.10.3** secure transmission arrangements
- **5.10.4** Roll back functionality
- **5.10.5** Testing functionality

5.11 The Source CSP shall specify any dependencies between the data available for export and other data connected to any other cloud services that are created unilaterally by the source CSP and that are not under control of the CSC.

5.12 The source CSP shall specify any processes, as part of the precontractual transparency document, to disclose use of subcontractors during data portability activity or any third party access to the data through the exporting process.

5.13 The source CSP shall specify what, if any, security audit related data (e.g. access logs) is available for export (e.g. logs of user interactions with the cloud service that could be needed for security analysis and for supervisory request).

5.14 The source CSP shall specify any source CSP provided tools or services (including for example addressing integration or interoperability support) that are available to assist the export process and any fees associated with those tools. The source CSP may specify any 3rd party tools or services (NB optional as opposed to required tools).

5.15 Where higher order data types are supported, including infrastructure and code artefacts the execution environment and dependencies shall be specified.

5.16 The source CSP will declare a minimum period during which the customer's data will remain available for transfer from the CSC in the event of termination of the services provided by the CSP.

5.17 The source and destination CSPs shall work together to minimise disruption of service during migration, according to the specific needs of the customer.

6 Data Import Requirements

6.1 The CSP shall declare all data and data types in scope for data import including infrastructure artefacts, code artefacts, derived data or meta data either in the transparency statement or as an attached document as preferred to allow for more complex services.

Note 1 This is subject to the requirements of 4.1.

6.2 The destination CSP shall have and specify an explicit and structured process for data import. The specification shall include:

6.2.1 Data management considerations (e.g. snapshots and incremental approaches, records management policies and procedures, bandwidth limitations)

6.2.2 Relevant Timescales

6.2.3 Notice Requirements

6.2.4 Customer contact procedures (contact points, escalation etc)

6.2.5 Impact on service continuity

6.2.6 Availability of the import procedure during the contractual period

6.2.7 Any CSP or third party tools or services(including data validators) required for data import

6.2.8 Any CSP imposed or enforced obligations on CSCs before data importing can commence

6.2.9 Explicit declaration on whether or not the source CSP's processes for data portability allow a CSC to be completely autonomous in importing data

6.2.10 Any required activation steps to initiate transfer

6.2.11 Any required dependencies such as code libraries which if required shall be documented and made available

6.3 The destination CSP shall specify all relevant fees in sufficient detail to allow the CSC to calculate import costs including:

6.3.1 The fee structure as charged by the CSP for data import and related procedures under the proposed CSA.

6.3.2 The fee structure for any other CSP or third party tools (as per 6.2.7)

6.4 The destination CSP shall specify which data standards, formats , data types and/or file types are recommended, used or available for data importing (e.g. binary, MIME, CSV, SQL, JSON, XML, Avro) for each and every data set available for export including any unstructured data.

6.5 The destination CSP shall specify the available mechanisms, protocols and interfaces that can be used to perform data import (e.g. VPN LAN to LAN, Data Power, SFTP, HTTPS, API, physical media…)

6.6 The destination CSP shall provide documentation on the format and structure required of imported data and any related APIs including where it can be sourced and under what terms if from a 3rd party source (including open or industry standard formats or exchanges e.g. Open Financial Exchange format).

6.7 The destination CSP shall specify what cryptographic processes and services it provides, if any, during data import (including unencrypted options) and how encryption keys are managed explicitly ensuring the CSC can decrypt any encryped data.

6.8 The destination CSP shall specify any security controls (e.g. access controls) available during data import.

6.9 The destination CSP shall specify any access to, retention period and deletion processes (including notification of deletion) of data, including differing categories of data (including derived data and management data) that is only used during the import process (e.g data that is transformed or reformatted during the import process).

6.10 The destination CSP shall specify any processes or services that it provides or supports to maintain data integrity, service continuity and prevention of data loss specific to data importing . Where they exist this shall include but is not limited to:

6.10.1 pre and post transfer data back-up and verification

6.10.2 freeze periods

6.10.3 secure transmission arrangements

6.10.4 Roll back functionality

6.10.5 Testing functionality

6.11 The destination CSP shall specify any dependencies to any other cloud services that are created unilaterally by the destination CSP during the import process that are not under control of the CSC.

6.12 The destination CSP shall specify any processes, as part of the precontractual transparency document, to disclose use of subcontractors during data portability activity or any third party access to the data through the importing process.

6.13 The destination CSP shall specify what, if any, security audit related data (e.g. access logs) can be imported (e.g. logs of user interactions with the cloud service that could be needed for security analysis and for supervisory request).

6.14 The destination CSP shall specify any destination CSP provided tools or services (including for example data validators and addressing integration or interoperability support) that are available to assist the import process and any fees associated with those tools. The source CSP may specify any 3rd party tools or services (NB optional as opposed to required tools).

6.15 Where higher order data types are supported , including infrastructure and code artefacts the execution environment and dependencies shall be specified.

7 Additional or Combined Requirements

7.1 The CSP shall specify the notification processes and timescales for any changes to the material included in its transparency statement or relevant to the adherence or declaration of adherence to be communicated to CSCs.

7.2 The CSP shall also specify how any CSP maintained external sources or references are maintained and include them in the change notification processes

7.3 The CSP shall specify any support provided to assist CSCs in interoperability and data porting issues (for example through technical documentation, interoperability standards or reported issues and solutions when authorised by submitting CSCs).

7.4 The CSP shall specify any policies or solutions either included or offered addressing access and porting of data in the event of CSP's bankruptcy, impact of ransom-trojan issues or acquisition by another entity.

Note 1 : Acquisition that constituted a change in legal provider or otherwise affected compliance would be covered under 4.1.2(4) of the common governance and 3(c) of the declaration of adherence form. In normal circumstances contractual commitments including code adherence would transfer.

Note 2: Bankruptcy will be covered the relevant laws covering the CSP and stages and options before final bankruptcy may vary but, as with ransomware, this is an opportunity for the CSP to highlight any exceptional options, for example 3rd party escrow contracts or insurances.