Code of Conduct

Switching and Portability of data

related to Software as a Service (SaaS)

DRAFT V 1.5

Disclaimer

 While all precautions have been considered and taken into account when writing this document, the authors of this document accept no liability whatsoever for any inconvenience caused, nor the consequences of it.

Table of contents

1. Introduction

This is a voluntary code for Software as a Service offerings provided by Cloud Service Providers (CSP).

Adherence to the code is intended to support portability and switching, promoting transparency and therefore the ease, efficiency and security of data portability.

This code of conduct is the result of the efforts from Cloud Service Providers (CSP) and Cloud Service Customers (CSC) to support safe portability and/or migration of data in the effective switching between cloud services providers and between cloud service providers and cloud service customers' own IT services. This has been done with Commission support to address the obligations in Article 6 of the Free Flow on Non Personal Data Regulation (EU) 2018/1807.

Recognising that in business, it can be very difficult to separate personal and non-personal data it should be emphasised that this code is without prejudice to the application of the GDPR.

The intent is to ensure sufficient transparency such that a CSC can assess the level of effort required to achieve portability. The commitment to the code by the CSP is to ensure that porting is possible and that the level of required transparency has been achieved.

Compliance with the code, and applicability of the complaints procedure, is in effect throughout the contracting period and any relevant post contractual period declared in the transparency statement.

Only the data designated as in scope, in the format declared, is covered by the code and therefore subject to the commitments in the code. Should either data or customisations occur that are not part of this declaration, alternative arrangements should apply.

2. Structure of the code

The structure of the code is built up as follows.

2.1 Introduction

2.2 Interaction with other documents

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

2.2.1 Governance

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

2.2.2 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.

2.2.3 Common Terminology

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

2.3 Saas Code of Conduct CSP requirements

The CSP requirements are structured as

- Overall Requirements
- Data Export
- Data Import
- Additional or combined issues

2.4 Annex 1: Data Portability Transparency Statement (normative)

Terminology:

- "shall" indicates a **requirement**
- "should" indicates a **recommendation**
- "may" is used to indicate that something is permitted
- "can" is used to indicate that something is possible, for example, that an organization or individual is able to do something

3 SaaS Code of Conduct CSP requirements

3.1 Overall Requirements and recommendations

3.1.1
Adherence to this code of conduct will comprise of a public statement of adherence to the code, as per the SWIPO Governance, specifying the service declared as in scope by the CSP, adherence to the governance requirements of code members (as per 2.2.1) combined with a pre-contractual CSP transparency statement that explicitly addresses the CSP requirements set out in this code in sufficient detail to enable data porting.
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).

3.1.2
The CSP Transparency statement shall be formatted and documented as set out in Annex 1.

3.1.3
The CSP should provide a clear description to the CSC of the policies addressing access and porting of data in the event of CSP's bankruptcy, impact of ransom-trojan issues or acquisition by another entity.

3.1.4
The CSP shall make the availability of any data import/export functionality or services clear as part of the transparency statement including both during the contractual period and post contract.

3.1.5
The Code does not replace the written and legally binding CSA between the CSP and the CSC. A reference should be incorporated into the CSA covering the adherence of the service to this code and may include any relevant respective responsibilities. 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. The requirements described in this Code apply at all times, unless the CSC requests and agrees to any deviations.

3.1.6
The CSP shall provide support to allow CSCs to overcome interoperability and data porting issues either as described in this section (3.1.6) or by providing a justification and description of its alternative approach (e.g. through technical documentation and suitable standards).

The CSP can meet this requirement by maintaining and making available to CSCs an overview of reported incompatibilities and solutions, where incorporation is duly authorised by the reporting CSC, occurring with CSC developed or sourced systems.

3.2 Data Export

3.2.1
The source CSP shall have and specify an explicit and structured process for data export. The source CSP should include data management considerations (e.g. snapshots and incremental

approaches, records management policies and procedures, bandwidth assessment) and any relevant timescales, notice requirements, customer contact procedures (contact points, escalation etc) and impact on service continuity. This should include relevant SLO and SQO from the SLA. The process and documentation shall cover technical, contractual and licensing matters such that they are sufficient to enable porting and switching.

[Explanation: This is the overriding requirement that enforces a compliant CSP to have a process that actually enables porting and switching. The requirement is for an explicit and working complete process that includes all elements of the following sections 3.2.2 to 3.2.17 as far as they are relevant for the respective service and for sufficient documentation and any necessary explanation. Therefore, there shall be no barrier or omission that affects portability. The binding specification obligations of the general process of this provision and all provisions hereafter of this section of the code are key transparency statements that must contain all relevant information CSCs need to allow them to evaluate the compatibility with their portability requirements and identify any other key issues which may require engagement with the CSP or lead to an alternate CSP selection. As such, CSPs should include reasonable explanations to avoid unnecessary engagements and complaints. Any lack of obviously required explanatory material to enable the purpose described above would by definition not be sufficient to be compliant with this Code. Obviously required explanatory material in this context includes brief but precise information that allow the respective group of CSCs to evaluate the compatibility of the general process for their specific switching and porting purposes. This means that general information is made available to enable the respective group of CSCs to understand why elements as defined in the sections 3.2.2 to 3.2.17 are in place or not relevant/applicable for the respective environment and designed in a way to not stand against the purpose of actually enabling porting and switching.]

3.2.2
The source CSP shall specify any CSP imposed or enforced obligations on CSCs before exporting data can commence. (i.e. any action required of the CSC to implement the source CSP's processes for data portability as specified in 3.2.1, shall be part of the CSP transparency statement).

3.2.3
The source CSP shall specify 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.

3.2.4
The source CSP shall specify any tools and services incurring additional fees for data export that are required by the source CSP processes for data portability as specified in 3.2.1.

3.2.5
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.

3.2.6

The source CSP shall specify whether or not the source CSP's processes for data portability as specified in 3.2.1. allow a CSC to be completely autonomous in exporting data i.e. when the CSC does not need human interaction with the CSP.

3.2.7
The source CSP shall specify which data, including derived data (e.g. computed field values, graphics, visualizations) can be exported from the service prior to the effective export date.

3.2.8
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).

3.2.9
The source CSP shall specify which data standards, formats 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.

3.2.10
The source CSP shall provide documentation on the format and structure of the exported data 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). As per 3.2.1 above this must be sufficient to enable porting and switching

3.2.11
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. The process shall allow the CSC to decrypt the exported Data.

3.2.12
The source CSP shall specify any security controls (e.g. access controls) available during data export.

3.2.13
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.

3.2.14
The source CSP shall specify the costs structure for data export and related procedures.

3.2.15
The source CSP shall specify any processes that it supports to maintain data integrity, service continuity and prevention of data loss specific to data exporting (e.g. pre and post transfer data back-up and verification, freeze periods and secure transmission and roll back functionality).

3.2.16

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…)

3.2.17
The Source CSP shall specify any dependencies between the data available for export and other data connected to another cloud service that are created unilaterally by the source CSP and that are not under control of the CSC.

3.2.18
The source CSP shall specify any processes, as part of the precontractual transparency document, to disclose use of subcontractors during data portability activity.

3.3 Data Import

3.3.1
The destination CSP shall have and specify an explicit and structured process for data import. The destination CSP should include data management considerations (e.g. snapshots and incremental approaches, records management policies and procedures, bandwidth assessment) and any relevant timescales, notice requirements and customer contact procedures (contact points, escalation etc) and impact on service continuity. The process and documentation shall cover technical, contractual and licensing matters such that they are sufficient to enable porting and switching.

[Explanation: This is the overriding requirement that enforces a compliant CSP to have a process that actually enables porting and switching. The requirement is for an explicit and working complete process that includes all elements of the following sections 3.2.2 to 3.2.17 as far as they are relevant for the respective service and for sufficient documentation and any necessary explanation. Therefore, there shall be no barrier or omission that affects portability. The binding specification obligations of the general process of this provision and all provisions hereafter of this section of the code are key transparency statements that must contain all relevant information CSCs need to allow them to evaluate the compatibility with their portability requirements and identify any other key issues which may require engagement with the CSP or lead to an alternate CSP selection. As such, CSPs should include reasonable explanations to avoid unnecessary engagements and complaints. Any lack of obviously required explanatory material to enable the purpose described above would by definition not be sufficient to be compliant with this Code. Obviously required explanatory material in this context includes brief but precise information that allow the respective group of CSCs to evaluate the compatibility of the general process for their specific switching and porting purposes. This means that general information is made available to enable the respective group of CSCs to understand why elements as defined in the sections 3.2.2 to 3.2.17 are in place or not relevant/applicable for the respective environment and designed in a way to not stand against the purpose of actually enabling porting and switching.]

3.3.2

The destination CSP shall specify any CSP-imposed or enforced obligations on customers before importing data. (i.e. any action required of the CSC to implement the destination CSP processes for data portability as specified in 3.3.1 shall be part of the CSP transparency statement).

3.3.3
The destination CSP shall specify any tools incurring additional fees for data import that are required by the destination CSP processes for data portability as specified in 3.2.1.

3.3.4
The destination CSP shall specify any CSP provided tools or services (including for example addressing integration or interoperability support) that are available to assist the import process and any fees that are associated with those tools or services. The CSP may specify any 3rd party tools or services.

3.3.5
The destination CSP shall specify whether or not the customer can be completely autonomous in importing data i.e. when the CSC does not need human interaction with the CSP.

3.3.6
The destination CSP shall specify which data, including any derived data from a source exporting service (e.g. computed field values, graphics, visualizations) can be imported into the service.

3.3.7
The destination CSP shall specify what, if any, security audit related data can be imported (e.g. logs of user interactions with the cloud service that could be needed for security analysis and for supervisory request).

3.3.8
The destination CSP shall specify which data standards, formats 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 import including any unstructured data.

3.3.9
The destination CSP shall specify the format/structure required of imported data and where definitions are available and under what terms (including open or industry standard formats or exchanges (e.g. Open Financial Exchange format). The CSP should specify any available validators and if so what type (e.g. structure, format, storage type, volume, links), from where and under what terms. As per 3.3.1 above this must be sufficient to enable porting and switching.

3.3.10
The destination CSP shall specify what encryption processes are used during data import (including unencrypted options) and how encryption keys are managed

3.3.11

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

3.3.12
The destination CSP shall specify the costs structure for data import and related procedures (eg volume restrictions).

3.3.13
The destination CSP shall specify any processes that it supports to maintain data integrity, service continuity and prevention of data loss specific to data importing (e.g. pre and post transfer data back-up and verification, freeze periods and secure transmission and roll back functionality).

3.3.14
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 …)

3.3.15
The destination CSP shall specify any processes, as part of the precontractual transparency document, to disclose use of subcontractors during data portability activity.

3.4 Additional or combined issues

3.4.1
The CSP may specify any additional known migration services existing (either CSP or 3rd party) and how are they available on the market.

3.4.2
The CSP shall specify the notification processes and timescales for any changes to the material included in its transparency declaration to be communicated to users.

Annex 1: Data Portability Transparency Statement (normative)

A1.1 Explanatory note

This Annex sets out a template for comparable pre-contractual transparency statements by SaaS CSPs to support potential users in assessing data import/export issues.

The documentation requirements match the code requirements and aim at documenting how data portability can be achieved in a SaaS cloud, whilst highlighting and identifying any barriers to switching (eg: IPR, proprietary formats etc).

The information that will be collected in this note will be exclusively based on CSPs declarations. **It is primarily meant to reference or aggregate existing material. Compliance with the code requires this format be followed and the content is sufficient to enable porting and switching.**

This document specifically excludes from scope interoperability and integration issues i.e. I/O, API and transactional data transfers due to variability and complexity of SaaS models.

The CSP should self-declare data and data types in scope either in the relevant questions below or as an attached document as preferred to allow for more complex services. Optionally this may include additional features or structures that are not per se SaaS data to allow for borderline cases (for example plugins or macros). Data as used in this document means all data and data types declared in scope including Cloud Service Customer Data and Cloud Service Derived Data including metadata, management data, user & identity (access control etc) data and subject data (i.e. personal data on natural subjects).

If CSP maintained external sources are used by reference, then the CSP must also specify how these external sources are maintained and include them in the change notification processes. (as per A1.4.2)

A1.2 Data Export

A1.2.1
Specify an explicit and structured process for data export. Include data management considerations (e.g. snapshots and incremental approaches records management policies and bandwidth assessment) and any relevant timescales, notice requirements, customer contact procedures (contact points, escalation etc) and impact on service continuity. This should include relevant SLO and SQO from the SLA. The process and documentation shall cover technical, contractual and licensing matters such that they are sufficient to enable porting and switching.

[CSP content and references]

A1.2.2
Specify any CSP imposed or enforced obligations on customers before exporting data can commence.

[CSP content and references]

A1.2.3
Specify 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.

[CSP content and references]

A1.2.4
Specify any tools and services incurring additional fees for data export that are required by the source CSP processes for data portability as specified in 3.2.1.

[CSP content and references]

A1.2.5
Specify any 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. You may specify any 3rd party tools or services.

[CSP content and references]

A1.2.6
Specify whether or not the source CSP's processes for data portability as specified in 3.2.1. allow a CSC to be completely autonomous in exporting data i.e. when the CSC does not need human interaction with the CSP.

[CSP content and references]

A1.2.7
Specify which data, including derived data (e.g. computed field values, graphics, visualizations) can be exported from the service prior to the effective export date.

[CSP content and references]

A1.2.8

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).

[CSP content and references]

A1.2.9
Specify which data standards, formats 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 import including any unstructured data.

[CSP content and references]

A1.2.10
Provide documentation on the format and structure of the exported data 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). As per A1.2.1 above this must be sufficient to enable porting and switching

[CSP content and references]

A1.2.11
Specify what cryptographic processes and services are provided, if any, during data export (including unencrypted options) and how encryption keys are managed. The process shall allow the CSC to decrypt the exported Data.

[CSP content and references]

A1.2.12
Specify any security controls (eg access controls) available during data export.

[CSP content and references]

A1.2.13
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.

[CSP content and references]

A1.2.14
Specify the costs structure for data export and related procedures.

[CSP content and references]

A1.2.15
Specify any processes that it supports to maintain data integrity, service continuity and prevention of data loss specific to data exporting (e.g. pre and post transfer data back-up and verification, freeze periods and secure transmission and roll back functionality).

[CSP content and references]

A1.2.16
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 …)

[CSP content and references]

A1.2.17
Specify any known dependencies between the data to be exported and other data connected to another cloud service.

[CSP content and references]

A1.2.18
Specify any processes, as part of the precontractual transparency document, to disclose use of subcontractors during data portability activity.

A1.3 Data Import

A1.3.1
Specify an explicit and structured process for data import. Include data management considerations (eg snapshots and incremental approaches records management policies and bandwidth assessment) and any relevant timescales, notice requirements and customer contact procedures (contact points, escalation etc) and impact on service continuity. The process and documentation shall cover technical, contractual and licensing matters such that they are sufficient to enable porting and switching.

[CSP content and references]

A1.3.2
Specify any CSP imposed or enforced obligations on customers before importing data.

[CSP content and references]

A1.3.3
Specify any required tools incurring additional fees for data import.

[CSP content and references]

A1.3.4
Specify any CSP provided tools or services (including for example addressing integration or interoperability support) that are available to assist the import process and any fees that are associated with those tools or services. You may specify any 3rd party tools or services.

[CSP content and references]

A1.3.5
Specify whether or not the customer can be completely autonomous in importing data i.e. when the CSC does not need human interaction with the CSP.

[CSP content and references]

A1.3.6
Specify which data, including any derived data from a source exporting service (e.g. computed field values, graphics, visualizations) can be imported into the service.

[CSP content and references]

A1.3.7
Specify what, if any, security audit related data can be imported (e.g. logs of user interactions with the cloud service that could be needed for security analysis and for supervisory request).

[CSP content and references]

A1.3.8
Specify which data standards or formats are recommended, used or available for data importing (e.g. CSV, SQL, JSON, XML, Avro) for each and every data set available for import including any unstructured data.

[CSP content and references]

A1.3.9
Specify the format/structure required of imported data and where definitions are available and under what terms (including open or industry standard formats or exchanges (e.g. Open Financial Exchange format). Specify any available validators and if so what type (eg structure, format, storage type, volume, links), from where and under what terms. As per A1.3.1 above this must be sufficient to enable porting and switching.

[CSP content and references]

A1.3.10
Specify what encryption processes are used during data import (including unencrypted options) and how encryption keys are managed

[CSP content and references]

A1.3.11
Specify any security controls (eg access controls) used during data import.

[CSP content and references]

A1.3.12
Specify the costs structure for data import and related procedures (eg volume restrictions).

[CSP content and references]

A1.3.13
Specify any processes that it supports to maintain data integrity, service continuity and prevention of data loss specific to data importing (eg pre and post transfer data back-up and verification, freeze periods and secure transmission and roll back functionality).

[CSP content and references]

A1.3.14
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 …)

A1.3.15
Specify any processes, as part of the precontractual transparency document, to disclose use of subcontractors during data portability activity.

A1.4 Additional or combined issues

A1.4.1

Specify any additional known migration services existing (either CSP or 3rd party) and how are they available on the market.

[CSP content and references]

A1.4.2

Specify the notification processes and timescales for any changes to the material included or referenced in its transparency declaration to be communicated to users.

[CSP content and references]