PLATFORM NEDERLAND

BELTUG Be Connected

VOICE Bundesverband der IT-Anwender e.V.

Cigref SUCCEED WITH DIGITAL

SWIPO. A new Code of Conduct for data import and data export for SaaS Suppliers

Observations and Recommendations

November 2020

Contents

This paper and its recommendations are the result of the constructive collaboration between four European business user associations. These four joined forces and bundled their observations and advice for their respective members:

- Beltug, the largest Belgian association of CIOs and digital technology leaders – website
- Cigref, a network of major French companies and public administrations set up in order to develop its members' ability to acquire and master digital technology – website
- CIO Platform Nederland, the association for the CIO/CDO, their peers and IT professionals of large users of digital technology in the Netherlands – website
- VOICE e.V., the largest representation of digital decision makers on the user side in Germany – website

SWIPO. A new Code of Conduct for data import and data export for SaaS Suppliers

1 Executive Summary

Negotiating a SaaS outsourcing contract is a very important and difficult process. It requires days and weeks of work from the business, IT and lawyers, to study and negotiate in every detail the dozens of pages of the SaaS contract.

So, it would be interesting and useful for the Cloud Service Supplier to propose a contract that takes already into account some identified requirements of all Cloud Service Customers.

On 28 November 2018, the EU published Regulation 2018/1807 on the free transfer of non-personal data in the EU.

The EU started, together with users and Cloud Service Providers, 'SWIPO' – '**Swi**tching from Provider and **Po**rting non personal data' – working groups intended to produce a Code of Conduct (CoC) that the Cloud Service Providers should respect in their Cloud Service Agreements.

The first version of the SWIPO Code of Conduct related to SaaS services was published on 8 July 2020.

The good news is that many important points are described in detail, and that Cloud Service Suppliers who want to publicise that they comply with this SaaS CoC will have to adapt their contracts accordingly. This should save time during negotiations.

The bad news is that some important points for the users have not been included in the Code of Conduct.

Our advice – see Chapter 3 for more details

Take the potential problems associated with getting your data back very seriously.

- Talk to your internal stakeholders: business, IT, data security, DPO and compliance officers and:
  - make an inventory of your needs, risks and demands
  - think long term (> 10 years from now) – what can happen to your organisation
  - document the input
- Use the SaaS CoC (for those parts that are well-covered) to your advantage: ask if your vendor adheres to it or has the intention to do so. And if not, why?
- Consider building a data export schedule that matches your needs
- Start contract negotiation at the earliest moment: prepare contract wording that you send together with your request for tender

The full set of documents (IaaS CoC, SaaS CoC, Governance and other materials) is available for download from the SWIPO website.

- Include clauses that protect you against unilateral changes in conditions and charges (URLs, renewal at the end of term, etc.).
- In the event that Cloud Service Providers do not comply with their commitments in the Transparency Statements, do not hesitate to submit a complaint with the SWIPO legal entity.

To assist you in the above, we have developed a Data Portability Questionnaire with questions on porting to be answered by your internal staff during preparation and by the supplier during the tender. You can find it in Chapter 3.

This document introduces the essentials of the new SWIPO Code of Conduct for SaaS.

We take a general business (CIO) point of view to identifying its shortcomings and to providing advice on what to do. We also include some helpful tools for building your tenders.

Share this document with all those involved in the selection of a SaaS application: business project leads, technical staff, buyers, contract drafters and legal counsellors.

2 The Regulation, SWIPO and the current SaaS Code of Conduct

2.1 The Regulation

On 28 November 2018, the EU published Regulation 2018/1807 on the free transfer of non-personal data in the EU.

The goal of this Regulation is:

- to lift unwanted data localisation restrictions put in place by EU member states, and
- to counter legal, contractual and technical issues hindering or preventing users of data processing services from porting their data from one service provider to another or back to their own information technology (IT) systems, not least upon the termination of their contract with a service provider.

The full text of 'Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union' can be found via EUR-Lex.

Article 6 of the Regulation and its considerations (5)-(8), (16)-(17), (29)-(31) and (33)-(34) are of particular interest for SWIPO.

The second goal is achieved through the joint development of self-regulatory codes of conduct by users and Cloud Service Providers. The practical implementation was due by 29 May 2020.

Such codes should define best practices and information requirements for facilitating the switching of Cloud Service Providers and the porting of data. They ensure that Cloud Service Providers supply professional users with sufficiently detailed, clear and transparent information before a contract for data storage and processing is concluded.

Despite the title of the Regulation and the definition of data in its Article 3 (1), the Regulation and the codes of conduct that implement it also apply to personal data, as personal and non-personal data in general cannot (and should not) be processed separately.

It is important to note that the Regulation does not affect the legal framework on the protection of natural persons with regard to the processing of personal data (including the GDPR).

2.2 SWIPO working groups

The groups that created the codes of conduct for IaaS and SaaS providers and their supportive documents named themselves 'SWIPO', which stands for **SWitching from provider and POrting non-personal data**.

SaaS CoC: Code of Conduct on switching and portability of data related to Software as a Service (SaaS), version 2020, 8 July 2020

IaaS CoC: Code of Conduct for data portability and cloud service switching for Infrastructure as a Service (IaaS) cloud services, version :2020 - v.3.0, 27 May2020

Although mentioned in the considerations of the Regulation, there is no code of conduct yet for PaaS.

Separate parties worked on IaaS and SaaS. As a result, the two codes of conduct differ in structure, style, wording and layout. From a user perspective, the IaaS CoC is the more complete and more instructive for its users.

The supportive documents 'SWIPO Common Scope and Approach' and 'Common Terminology' provide a set of definitions and some guiding principles.

The full set of documents (IaaS CoC, SaaS CoC, Governance and other materials) is available for download from the SWIPO website.

SWIPO principles

1. **Switching between service providers and data porting must be possible, effective, not cost consuming and easy.**
2. The ability to port data without hindrance is a key factor in facilitating user choice and effective competition on markets for data processing services. [Consideration 29]
3. In order to take full advantage of the competitive environment, professional users should be able to **make informed choices** and to **easily compare the individual components of various data processing services offered** in the internal market, including in respect of the contractual terms and conditions of porting data upon the termination of a contract. [Consideration 30]
4. **Trust enhancement in the security of cross-border data processing** is a key factor to improve the legal certainty for companies as regards compliance with the applicable security requirements when organisations outsource their data processing activities to service providers, including to those in other Member States. [Consideration 33]

5. **All security requirements related to data processing** that are applied in a justified and proportionate manner on the basis of Union or national law in compliance with Union law in the Member State of residence or establishment of the natural or legal persons whose data are concerned will **continue to apply** to processing of that data in another Member State**.** [Consideration 34]

(Source: SWIPO Common Scope and Approach Version 0.10, 10 June 2019, our bold and references to the corresponding considerations of the Regulation. The above principles do not appear anymore in the 2020 version of the document. This is very unfortunate as they should also be inspirational for the future evolution of the Code of Conduct).

2.3 The SWIPO legal entity

To implement the codes of conduct, a separate legal entity, called SWIPO AISBL, was created in May 2020, with members from the user and service provider communities.

The document 'SWIPO Common Governance for SWIPO Codes of Conduct under the Article 6 of the Free Flow of non-personal Data Regulation' defines its workings.

The Governance structure indicates an Executive Board, a General Assembly, Sector Groups, a Complaints Board and a Secretariat.

There are procedures concerning Voting, Membership, Review of Code (with 60-day public review phase), Adherence (membership not required, 36 months duration), a Public Register and Appeals.

The legal entity will regulate the declarations of adherence (which will be valid for a 36-month term), handle complaints on non-compliance, and steer the further evolution of the codes of conduct.

2.4 The SaaS Code of Conduct (CoC)

The SaaS CoC introduces a Data Portability Transparency Statement. This statement is provided by a potential Cloud Service Provider (CSP) to assist a potential Cloud Service Customer (CSC) in making informed choices and more easily compare components related to data porting as part of a market offering.

Annexe 1 of the SaaS CoC defines the template for the Transparency Statement.

The need for a written and legally binding Cloud Service Agreement (CSA) between the CSP and the CSC remains.

How it works

- The CSP announces publicly that it adheres to the SaaS CoC
- The CSP redacts a (confidential) pre-contractual Data Portability Transparency Statement in the format described in Annex 1 of the Code
- This Transparency Statement is used by the potential CSC to assist in its selection of a solution
- The CSC has to check that the binding CSA refers to the code and the Transparency Statement, and includes 'any relevant respective responsibilities'

2.4.1 The key requirement

The critical contribution of the SaaS CoC is that it assures that an adhering CSP will have a functioning process for data export and import. Below is the key requirement for data export (our bold). There is a similar requirement for data import (Chapter 3.3.1).

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, and bandwidth assessment) and any relevant timescales, notice requirements, customer contact procedures (contact points, escalation, etc) and impact on service continuity. This should include the availability of the data export process both during and after the contractual period. This should also include relevant SLO (Cloud Service Level Objectives) and SQO (Cloud Service Qualitative Objective) from the SLA (Service Level Agreement). **The process and documentation shall cover technical, contractual and licensing matters such that they are sufficient to enable porting and switching.**

The full body of requirements comes in four sections: overall requirements and recommendations, data export, data import, and additional or combined issues. In the Transparency Statement, the CSP provides content and references for each requirement, if relevant for its service offering.

The SaaS CoC precisely defines the use of modal verbs in its requirements.

'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 organisation or individual is able to do something

2.4.2 Features covered in the Transparency Statement for Data Export and Import

- **An explicit and structured process for data export/import**
- CSP-imposed obligations on customers before exporting/importing can begin
- Known post-contractual licence fees or other liabilities (for export only)
- Tools and services incurring additional fees
- Any CSP-provided tools or services, and the fees associated with them
- The need for human interaction with the CSP
- Which data (including derived data) can be exported/imported
- Security audit-related data, available for export/import
- Recommended data standards, formats and/or file types
- Format and structure of the exported data /imported data + validators (import only)
- Cryptographic processes and services
- Security controls during data export
- Retention period and deletion processes (for data export only)
- Cost structure for data export/import
- Processes to maintain data integrity, service continuity and prevention of data loss specific to data exporting/importing
- Available mechanisms, protocols and interfaces
- Any known dependencies between the data to be exported and other data connected to another cloud service (for data export only)
- The use of subcontractors

3 Point of view of current CoC weaknesses from Beltug, Cigref, VOICE e.V. and CIO Platform Nederland

The above list of features shows that the current version of the SaaS CoC handles the technical aspects of porting rather adequately.

A supplier adhering to the SaaS CoC asserts the existence of a working process that is sufficient for porting (import/export data) and switching.

However, the adherence of a supplier to the SaaS CoC does not guarantee that the customer will be able to perform the porting process if and when needed for its business: e.g. to establish interoperability, to ensure business continuity, or to harden itself against organisational change.

Below, we will only handle the case of data export from the vendor to the customer, as the risk for a CSC of not getting its data back is the major one to be considered. Indeed, in the event that a data import is not successful, we expect the new vendor to be very co-operative in assisting its new customer to succeed.

3.1 The SaaS CoC does not assure data export for inter-operability, nor porting at all times

Today, most companies still have much of their IT on-premise. If they want to connect their data to a new IT solution or package, they can develop and easily implement an extract of all or part of the data in the timeframe corresponding to their needs.

This could be data export through incremental, asynchronous exchanges; daily backup; or based on another periodicity. For all these, we will refer to it as the 'periodic export'.

With the 'move IT to the cloud' market trend, once a company has migrated its data to a CSP, easy access to this data is not always possible.

This is why a specific contract clause, the 'periodic export clause', is required to allow a company to connect its data to a new IT solution or package outside the CSP's environment.

Example: A company has chosen a package available in cloud services to handle a large part of its operational business. At the same time, this company would like to innovate in marketing by linking with data sources that are not available in the environment of the chosen CSP, and by initiating actions to its customers based on these links. In the very fast digital landscape, it is critical that these actions can be triggered as soon as possible, daily or in real-time.

Data export should be easy, and be possible at any time at the discretion of the CSC for business continuity reasons as well: to enable the periodic testing of the export or to enable safeguarding of data in another place. Businesses also need this to respond to their GDPR obligations within the prescribed deadlines.

The CSP should allow the CSC to perform, at a reasonable price, the data export process for all or part of the CSC's data in the timeframe corresponding to the CSC's business needs. A 'reasonable price' means that the CSP should cover its costs (disk I/O, bandwidth, automated export process, etc.) and the CSC should not be locked-in by an unpredictable or unaffordable price.

The Regulation does not prohibit the codes of conduct from addressing this topic.

Article 6.1 states: "The Commission shall encourage (…) the development of self-regulatory codes of conduct (…) in order to contribute to a competitive data economy, based on the principles of transparency and interoperability (…)" (our underlining).

The SaaS CoC is not very explicit on this, and focuses mainly on end-of-term data export. It does not prohibit more frequent porting during the term of the CSA.

You will need to question the feasibility of continuous porting in the tender, and to agree on practical and financial conditions in the CSA.

3.2 The SaaS CoC does not assure data export in case of organisational change

SaaS agreements, by their nature and strong lock-in, tend to be of long duration (> 10 years). In this period, very likely, both CSP and CSC will undergo organisational changes.

The SaaS CoC does not offer protection in the case of

- unwillingness by the CSP to agree on how to deal with its own default (e.g. bankruptcy) or re-organisation (merger, acquisition or divestment)
- unwillingness by the CSP to agree on how to deal with the data in the event of a default (e.g. bankruptcy) or re-organisation (merger, acquisition, divestment) by the CSC, so that the successor in law would not be able to port the data
- unwillingness by the CSP to agree on how to act in a situation of escrow or one in which a third-party guarantor could take over services for the benefit of the CSC's clients.

It is imperative that for porting there always is a sender and a receiver: the original CSP/CSC or their successors in law.

Exit provisions (including data porting) should survive the normal and abnormal evolution of both the CSC and CSP organisations: malicious attacks, restructuring, merger & acquisition, disinvestment, and even bankruptcy. Also, porting has to be possible at the termination of the agreement between CSC and CSP for whatever cause.

There should always be a sender and a receiver, whether the original CSP/CSC or its successor(s) in law.

Adherence to the SaaS CoC should imply that the CSP is willing to address those issues in the CSA according to the needs of a CSC, which is not the case.

From this perspective, the SaaS CoC is not comprehensive, and thus not in line with consideration 31 of the Regulation.

To avoid the need of data porting altogether, the assignment of a CSA by the CSC to a third party of its choice should be made easy. For the same reason, the CSA should not restrict the CSC to use the application to provide services to third parties (amongst others: members of the group of companies to which the CSC belongs and to future joint ventures in which the CSC would participate).

We strongly recommend that the CSC identify its needs, check the proposed CSA in detail (including exit, termination and assignment clauses) and complete it with provisions that offer peace of mind.

3.3 The SaaS CoC does not mitigate certain operational risks relevant to all CSCs

Some of the operational risks that are not mitigated in the SaaS CoC include:

- unwillingness by the CSP to allow porting for test purposes at the moment the CSC would like to perform it
- unwillingness by the CSP to enter into a project-based agreement with a third party chosen by the CSC when it does not have the porting skills itself
- unwillingness by the CSP to port the data in case the CSC is in breach for some aspects of the contract (e.g. late payment)
- loss of data: deletion of data by the CSP without explicit acknowledgement of the successful porting by the CSC
- scope creep: the SaaS CoC applies to data in scope as defined in the Transparency Statement that is valid when the contract is signed. The normal evolution of a SaaS application will lead to more or to obsolete data elements. Undocumented scope creep could result in those data elements not being eligible for porting.

Although consideration 30 of the Regulation allows the Codes of Conduct to contain model contractual clauses, the current versions of the SWIPO Codes do not provide any.

A CSC has to enter into time-consuming negotiations with all of its potential suppliers to resolve risks not covered by the Codes of Conduct. And there is no guarantee that the same phrasing will be possible in its contracts with all of its suppliers.

It is also a burden for the CSPs to enter into customised agreements– unless they intend to impose their Cloud Services Agreement (CSA) 'as is'.

In a real digital world, SaaS solutions are networked, with the suppliers of SaaS services themselves being customers of such services. And often, a total solution will involve a chain of suppliers. In the case of porting, data needs to move along this chain. If each customer/supplier interface has its own set of porting rules, this may become very cumbersome or even impossible.

A minimum set of standard contractual clauses on porting, applicable to all CSAs, would be beneficial to all CSCs and CSPs.

We strongly recommend that the CSC identify its needs and complete the CSA with provisions that offer peace of mind.

3.4 The SaaS CoC does not push adherents to moderate charges for data export, nor does it condemn the creation of vendor lock-in as a non-acceptable business practice

3.4.1 The SaaS CoC remains silent on cost moderation.

Although the Transparency Statement should provide a CSC with all elements needed to calculate porting fees, the notion of moderation of such charges, as expressed in the first SWIPO principle, is not replicated in the SaaS CoC. In the final version of the high-level document 'SWIPO Common Scope and Approach', these guiding SWIPO principles have even been removed. Why?

Are they no longer relevant for the future development of the SaaS CoC?

The position of the SWIPO SaaS working group co-chairs is that transparency and competition pressure will automatically lead to a low cost. We do not think this will work for SaaS, as the selection of a SaaS application is mainly made based on overall functionality, and not on the single aspect of porting. We would like to see the principle of cost moderation explicitly stated in the SaaS CoC as a reminder to the CSP, as is the case in the IaaS CoC.

Could we not consider the return of data at the end of an agreement and the ability to test to be integral parts of the service, covered by the regular usage fee?

There is indeed a danger of (additional) lock-in if porting charges are 'unreasonably' high.

Why not ask the adherents to provide a low-cost, automatic data export process that can be triggered at any time by the customer, and will port the data in the formats as used in the SaaS application (except for proprietary formats transformed in open-source ones)?

Why not ask the adherents not to charge for porting at the termination of a CSA and for intermediate testing? Could we not consider the return of data at the end of an agreement and the ability to test to be integral parts of the service, covered by the regular usage fee?

This would resolve the problem of needing to define what is to be considered a fair and reasonable charge for data export, without excluding the setting of fees in the event that more frequent exports or the performance of additional services impose extra costs on the CSP.

3.4.2 The SaaS CoC remains silent on vendor lock-in

The evolution from 'on-premise IT' to 'cloud services IT' has accelerated over the last years, and this trend will continue. When a company selects a Cloud Service Provider (CSP), there is competition on the market. Once a CSP chosen, and the migration complete, there is a de facto lock-in because of the time, costs and risks linked to migrating to another CSP.

Consideration 31 of the Regulation asks that the Codes of Conduct make clear that vendor lock-in is not an acceptable business practice. Contrary to the IaaS CoC, the SaaS CoC does not do so. Why not?

3.5 The SaaS CoC does not protect the CSC against adverse unilateral changes in contract terms

There is no guarantee that the porting process agreed upon at when the contract is signed will remain the same as initially defined.

Unilateral changes by the CSP could occur:

- via URLs in the CSP Transparency Statements (and thus by reference in the agreement)
- by the replacement of a Transparency Statement at the end of its 36 months validity
- at renewal of a SaaS agreement. Because of the lock-in, the negotiation leverage for the CSC has disappeared, enabling the CSP to impose new conditions

The SaaS CoC foresees that the customer may terminate the agreement if it cannot accept the unilateral changes. This remedy, of course, is of no practical use in a situation of vendor lock-in.

From a contracting point of view, there should be assurance that essential elements from the Transparency Statements – on which the CSC bases the decision to contract with the CSP – will not be changed by the CSP to the detriment of the CSC.

The risk of unilateral changes to contracts by including URLs is not limited to SaaS, but is a general risk in B2B agreements for use of software. EU legislation should define unlawful B2B clauses, as is the case in e.g. Article 15 of Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services.

The Belgian B2B-Act of 24 May 2019 blacklists certain unlawful B2B-clauses. Amongst others, is the following: "The contract clauses that serve to irrefutably establish the knowledge or acceptance of clauses by the other party, while the latter was not actually able to become acquainted with said clauses prior to the formation of the contract."

In our view, this prohibits the use of URLs.

We believe that an ex-ante EU regulation should protect customers against adverse unilateral changes to contracts.

We strongly recommend that the CSC add provisions to the CSA to protect against adverse unilateral changes.

3.6 Transparent Transparency Statements

We want to ensure that Transparency Statements issued by different CSPs can be easily analysed and compared. It would help if no URLs were used, if all cost elements were grouped, and if all statements would follow the same structure with all headings present.

The SaaS CoC remains silent on this practical aspect.

3.7 Lessons learned concerning the creation of self-regulatory codes of conduct

SWIPO was set up by the European Commission to have cloud service providers and users develop self-regulatory codes of conduct. The role of the Commission would be that of facilitator.

In theory, suppliers and users would be on a level playing field. In practice, suppliers are represented by some leading, world-class SaaS providers, and users by a variety of interested companies and a few branch organisations. It is clear that the user side shows a broader diversity in individual interests and does not have the same dedicated resources as the supplier side to bundle its actions.

This has resulted in a SaaS CoC with supplier bias.

The European Commission is, however, aware of this imbalance, and has planned to audit the efficiency of the Codes of Conduct and the underlying self-regulation approach.

Future efforts to create self-regulatory codes of conduct would profit from some closer monitoring and facilitation from the Commission:

- by providing the working parties with independent specialised legal counsel, e.g. on competition law and contract law
- by performing a neutral quality check to see if the result meets the goals of the Regulation
- by giving the Commission the ability to oblige the working groups to address certain aspects, e.g. concerning standard contractual clauses
- by giving the Commission the power to periodically review the adequacy of the codes of conduct, as is the case of Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services (Article 18, b)

We want the EU Commission to propose ex-ante regulations to take care of elements not 'spontaneously' covered in the Codes of Conduct: amongst others to enable porting at all times as well as porting from and to successors in law to the CSC/CSP. and to protect against adverse unilateral contract changes through the use of URLs.

4 Advice and conclusion

4.1 Advice to our members

Beltug, Cigref, VOICE e.V. and CIO Platform Nederland commented on the draft Codes of Conduct produced on 29 November 2019. We proposed some additional requirements to make the Codes more comprehensive, more balanced, and thereby better aligned with the goals of the Regulation. Please find some of our proposed provisions in Annexe 1.

Certain remarks were taken into account in the SWIPO SaaS CoC published on 20 July 2020, but many shortcomings remain.

Our advice:

Take the potential problems associated with getting your data back very seriously.

- Talk to your internal stakeholders: business, IT, data security, DPO and compliance officers, and
    - make an inventory of your needs, risks and demands
    - think long term (> 10 years from now): will you still be there?
    - document the input
- Use the SaaS CoC (for those parts that are well-covered) to your advantage: ask if your vendor adheres to it or has the intention to do so. And if not, why?
- Consider building a data export schedule that matches your needs
- Start contract negotiation at the earliest moment: prepare contract wording that you send together with your request for tender
- Include clauses that protect you against unilateral changes in conditions and charges (URLs, renewal at the end of term, etc.)
- If CSPs do not comply with their commitments in the Transparency Statements, do not hesitate to submit a complaint with the SWIPO legal entity

Please note that this is in addition to GDPR concerns.

To assist you in the above, we have developed a Data Portability Questionnaire with questions on porting to be answered by your internal staff during preparation, and by the supplier at tender time. You can find it here.

Please share this document and the questionnaire with your business stakeholders, technical staff, buyers, contract drafters and legal counsellors involved in the selection of a SaaS application.

5 Conclusion

From the above, it may be clear that the current SaaS CoC is not perfect. We expect the SWIPO legal entity to continue to work on trust-creating model contract wording for the benefit to all. Should SWIPO AISBL defaults on this, we call upon the EU Commission to create comprehensive standard contractual clauses to cover the risks mentioned above.

Nevertheless, Beltug, Cigref, VOICE e.V. and CIO Platform Nederland will actively promote the use of the SaaS CoC by informing our members and by gathering feedback that we will provide to the SWIPO legal entity.

We wish you a safe journey.

Annexe 1

Wording proposed by Beltug, Cigref, VOICE e.V. and CIO Platform Nederland to improve the SaaS CoC

The below clauses were proposed to enhance the SaaS CoC version 1.5. The language was not accepted. Therefore, we repeat it here for your benefit, and as a suggestion to improve the SaaS CoC 2020 version.

Disclaimer: The proposed clauses are suggestions only. In providing these clauses, Beltug, Cigref, VOICE e.V. and CIO Platform Nederland do not offer any legal advice or any warranty that these clauses are enforceable in any given context. The use of these clauses and their enforceability needs to be validated from a legal perspective on a case-by-case basis.

- [Definition of the scope of the Code of Conduct in the CSA]

  This Code applies to all data (all data and data types defined and declared in scope in the CSA 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), and any other elements (e.g. plugins, macros, code customised by or for the CSC) agreed upon between the CSC and the CSP.

- [Normal and abnormal evolution of both CSP and CSC – partially covered for CSP defaults in the IaaS CoC v3.0 TR03 f)]

  The CSP shall provide a clear description to the CSC of the policies addressing access and porting of data in the event of CSP's bankruptcy, the impact of ransom-trojan issues or acquisition of the CSP by another entity. These policies and process shall include CSC notification without undue delay once such event would occur.
  In case of acquisition of the CSP by another entity, such entity will enter into all rights and obligations of the CSP and the continuation of the services will be guaranteed by this entity for a period of at least 18 months starting with the acquisition.
  The CSP shall allow the CSA to contain provisions with regards to the porting of CSP data to the CSC or to a third party in case of CSC's bankruptcy, in which case such third party towards the CSP will enter into all CSC's right and obligations of the CSA.
  The CSP shall allow the CSA to contain provisions with respect to its assignment in case of mergers, acquisitions and other changes of the CSC or disinvestments made by the CSC.

  The CSP shall provide a clear description to the CSC of the polices addressing contacting the CSC in a clear and timely manner and the retention of CSC data in case of CSC's non-payment or bankruptcy, which will at least be 12 months starting with the event of default.

- [Assistance in the form of third-party support]

  At the request of the CSC, the CSP shall contract with the CSC for the provision of support services in a project-mode with respect to data export/import to be performed. Such will be possible preceding to the conclusion of a CSA with the CSP.

- [Wording on testing inspired by the IaaS CoC v3.0, PLR01]

  The source CSP shall provide a procedure to determine the testing of the mechanisms and schedule of a data transfer based on the CSC's business needs, security risks, and technical and support capabilities of both parties. Acceptance of the testing should be made with the CSC in the frame of a transparent test process.

- [Alternate wording on testing]

  The source CSP shall enable the CSC with a procedure to test the export of data at no extra charge for the CSC. The CSC shall be able to perform such a test at minimum once a year, and after each upgrade of the CSP application used.

- [Porting at termination for any cause]

  The CSC shall be entitled to perform the data export process at the termination of the CSA by one of the contracting parties for whatever cause.

- [Export at any time]

  The source CSP shall allow the CSC to perform the data export process (for all or part of the data) at the CSC's discretion on the time basis corresponding to the CSC business needs, which could be data export at any moment, data export through incremental asynchronous exchanges, daily backup or with another periodicity, and not only a global export at the end of the contract.

- [The final decision to delete should not be at the discretion of the CSP]

  The CSP shall only delete CSC's data from its systems after having received an explicit written approval thereto from the CSC. In case of CSC's bankruptcy, this approval is to be given by the person in charge of the wind-up of the CSC.

- [Cost moderation]

  If there are any fees or charges related to data export/import during the contractual period and any agreed post-contractual one, the source CSP shall provide in advance the right level of transparency to justify a fair price based on real operational costs. This can be done by detailing a cost structure plus a reasonable margin and/or by including some benchmarks on demonstrated market prices.

  The CSP preferably should provide the CSC with a fixed lump sum or flat rates at the lowest cost possible.

- [To protect the customer from unilateral changes by a CSP]

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

  Future changes to the Code or to transparency statements from the CSP during the term of a CSA or its extensions, will not have any adverse effect to the CSC, in particular with respect to technical porting capabilities, the timings or the charges.

- [To facilitate the comparison of service offerings]

  The transparency statements of all CSPs will have the same structure, numbering and headings as described in Annex 1. If not applicable, the content of a section will mention 'Not relevant for the services offered'.

- [As the nature of the Transparency Statement is to be transparent]

  In the transparency statement, the use of URLs to refer to documents that can be unilaterally changed by the CSP and would diminish any capability or right of the CSC under the CSA is prohibited.

- [To facilitate contracting]

  The CSP shall make available the totality of materials included (or referred to) in its transparency statement in a single downloadable printable and dated file, that in printed form can be attached to the CSA, or in its electronic form can be safeguarded by the CSC and referred to in the CSA as being part of the agreement

- [Loss of the adherent status, as per IaaS CoC v3.0, TR06]

  The CSP shall inform the CSC without undue delay if there are permanent changes in its Declaration of Adherence to the Code.