# CISPE Cloud Switching Framework [V1.0]

## 1. Introduction

CISPE's Cloud Switching Framework is a practical service declaration framework that covers the entire switching process contemplated in the EU Data Act. The Framework provides comprehensive guidelines and technical requirements to help vendors and cloud customers to operationalize compliance with the upcoming obligations around data portability and switching. The CISPE Cloud Switching Framework covers:

- **Transparency**: Cloud providers must give customers clear, detailed information on the switching process, including procedures, data formats, costs, and technical limitations.
- **Contractual Obligations**: Contract between customers and cloud providers must allow the customer to switch or use multiple providers, and it must specify the provider's switching assistance obligations, data export requirements, and termination procedures.
- **Initiation of Switching**: Cloud providers must offer designated channels for customers to notify a switching request and to track progress of such requests.
- **Technical Requirements**: Cloud providers must make open interfaces, data export tools, and other technical capabilities available to facilitate switching while ensuring data security.
- **Termination**: Cloud providers must close the customer account once the customer confirms completion of the switch and requests closure, which will result in termination of the contract between the parties.

The responsibilities of the source Cloud Service Provider providing the data processing services and its Customer as set out in the Control Framework shall only apply to the services, contractual agreements or commercial practices provided by the Cloud Service Provider.

In drafting the Control Framework, inspiration was taken from concepts of ISO Standards and SWIPO Codes, including but not limited to:

- ISO/IEC 19941:2017.
- ISO/IEC 19086-1:2016.
- ISO/IEC TR 22678:2019.
- ISO/IEC 22123-1:2023.
- ISO/IEC 22624:2020.
- ISO/IEC 27017:2015.
- ISO/IEC 27018:2014.

## 2. Mapping EU Data Act – Control Framework

| **EU Data Act Proposal (Chapter VI Switching between data processing services) -** (Recitals: 78 - 106**)** | **Related Controls of Control Framework** |
|---|---|
| **Article 23**: Removing obstacles to effective switching between providers of data processing services. (Recitals 78, 79, 93) | Introduction |
| **Article 24**: Scope of the technical obligations. | Introduction<br>CR.01.8 |
| **Article 25**: Contractual terms concerning switching between providers of data processing services. (Recitals 93, 96) | TR.02.6<br>CR.01.1<br>CR.01.2<br>CR.01.3<br>CR.01.4<br>CR.01.5<br>CR.01.6 |
| **Article 29**: Gradual withdrawal of switching charges (Recitals 88-89) | TR.02.3<br>CR.01.8 |
| **Article 30**: Technical aspects of switching. (Recitals 86, 92, 95, 97) | TMR.02.1<br>TMR.02.2<br>TMR.02.3 |
| **Article 34:** Interoperability for the purposes of in-parallel use of data processing services (Recital 99) | TR.02.4<br>CR.01.8<br>TMR.02.3<br>TMR.02.4 |
| **Article 35:** Interoperability of data processing services (Recitals 100, 103-105) | TMR.02.3<br>TMR.02.4 |

**To self-certify your services under the Framework, please visit the following link: https://cispe.cloud/cloud-switching-framework**

## 3. Control Framework

| # | Section Title | Description | Control Requirements |
|---|---|---|---|
| **1** | **Transparency**<br><br>**Relevant Articles of the EU Data Act:** Articles 26, 27, 29(4)-(6), 31(1) | Data Portability provides numerous benefits to Customers. Therefore, one of the purposes of the Control Framework is to help ensure that the relationship between the Cloud Service Provider and the Customer is maintained in a transparent manner during the entire switching process. Due to the potential complexity of Data Portability, in order to be in conformity with the Control Framework, the Cloud Service Provider must provide the Customer with clear, transparent, and detailed information that can be understood by an average user. To reach this objective, the Transparency requirement applies in relation to all Sections of the Control Framework, namely Contractual relationship between the Cloud Service Provider and the Customer (Section 2), Initiation of the Switching Process (Request of the Customer) (Section 3), Technical Requirements for the Switching Process (Section 4), and Termination of the Switching Process (Section 5). | **TR.01: The Cloud Service Provider shall give transparent information on the switching process to the Customer.**<br><br>1. Before entering into an agreement for provision of data processing services (the "Contractual Agreement"), the Cloud Service Provider shall provide the Customer with information in sufficient detail to enable the customer to understand its process for facilitating customer switches and in-parallel use of multiple cloud service providers, which shall be understandable by an average user (e.g., through a pre contractual Cloud Service Provider transparency statement or an informative/explanatory Annex attached to the Contractual Agreement). The information is not required to be specific to the Customer and shall cover the Cloud Service Provider's switching process generally. Whatever option is selected by the Cloud Service Provider, the information is not required to be publicly available, and it can be subject to a non-disclosure agreement with the Customer. Therefore, the Cloud Service Provider shall:<br><br>a. Provide explanatory information to the Customer in relation to the Clauses related to the switching process or in-parallel use of services covered by the Contractual Agreement between the Parties involved, as referred to in Section 2; and<br><br>b. Provide a statement of adherence to the transparency requirement of this Control Framework. |

| | | | |
|---|---|---|---|
| | | | 2. The Cloud Service Provider shall also provide the Customer with clear information on the elements listed below before entering into a Contractual Agreement. The information is not required to be publicly available, and it can be subject to a non-disclosure agreement with the Customer.<br><br>a. The standard service fees of the Cloud Service Provider;<br>b. In case the Cloud Service Provider and the Customer enter into a Contractual Agreement for a fixed duration, information regarding early termination penalties that might be imposed on the Customer, which may be equal to the amount of fees that the Customer would have been obliged to pay to the Cloud Service Provider for the entire term of the Contractual Agreement, if it had not been terminated prematurely by the Customer;<br>c. Information on the reduced switching charges (if applicable), including data egress charges that might be imposed on Customers.<br><br>3. The Cloud Service Provider shall make available to the Customer information on factors that might affect the duration and the level of complexity of their switch. This shall also include, where relevant (e.g., where the Cloud Service Provider offers custom-built features to the Customer), information addressing services that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, digital assets, or service architecture and information explaining how the cost and complexity of switching process could be impacted based on Customers' IT implementation decisions. |

| | | | |
|---|---|---|---|
| | **Relevant Articles of the EU Data Act:** Recital 82, Articles 25(2)(a)-(c) 26, 27, 28(1), 29, 34(2) | | **TR.02: The Cloud Service Provider shall provide transparent and detailed information to the Customer with respect to the elements related to the switching process.**<br><br>In relation to the information referred to in Section TR.01, the Cloud Service Provider shall, at least, provide transparent information to the Customer with respect to the following elements:<br><br>1. Descriptive information on the basics of the rights and obligations of the Cloud Service Provider and the Customer with respect to the switching process (e.g., the extent/degree of control that the Customer and the Cloud Service Provider shall have over the switching process);<br><br>2. Procedures and policies related to the switching process. This shall cover the procedural steps to be taken, and the roles and responsibilities of the parties involved during the process, including the roles and responsibilities of each party to ensure the security of the process;<br><br>3. the data structures, data formats, relevant standards and open interoperability specifications in which the exportable data will be available, including specifications related to any third-party technologies supported by the Cloud Service Provider, to the extent legally allowed;<br><br>4. A statement that the Cloud Service Provider will not charge (or will only charge up to its cost where permissible under the Data Act) for the following elements directly linked to the switching process or the in-parallel use of multiple Cloud Service Providers: (a) data transfer; (b) access to APIs to facilitate the transfer; (c) data formatting into an exportable format (i.e., a format where the data can be extracted out of the source Cloud Service Provider's environment), if necessary. The statement shall also include clear |

| | | | |
|---|---|---|---|
| | | | information on any conditions or other customer requirements implemented by the Cloud Service Provider to accurately identify whether the Customer's request duly qualifies as switching or in-parallel use of multiple Cloud Service Providers under the EU Data Act. The statement may also state any differences between the elements provided free of charge or at cost and paid for elements the Cloud Service Provider makes available;<br><br>5. Technical, physical, and organizational measures deployed by the Cloud Service Provider in relation to the switching process. This shall include information on how data integrity, continuity, and security can be preserved during the porting process, such as (i) a description of how the services and tools made available by the Cloud Service Provider can be used by the Customer during the overall switching process, (ii) a description of the supported capabilities, including any data back-up and recovery processes that the Customer could adopt to protect the sets of data during the porting process, (iii) a description of the security measures, and record management tools available to the Customers' use, (iv) the process for deletion of Customer data after the termination of the porting, and (v) technical limitations of the Cloud Service Provider's products and services that are known to the Cloud Service Provider and mitigation measures that may be adopted in case where such technical limitations occur).<br><br>6. The jurisdiction to which the IT infrastructure deployed for data processing of their individual services is subject. |
| **2** | **Contractual relationship between the Cloud Service Provider and the Customer** | In relation to Section 1, another purpose of the Control Framework is to increase clarity and transparency with respect to the aspects, procedures, rights, and obligations related to the switching process. To reach this end, the Contractual Agreement between the Cloud | **CR.01: Information regarding the Data Portability procedure must be covered by contractual clauses.**<br><br>The Cloud Service Provider must ensure that the information regarding Data Portability is covered by contractual clauses. This may be done in different forms, depending on the structure of the Contractual |

| | | | |
|---|---|---|---|
| | **Relevant Articles of the EU Data Act:** Recital 82, Articles 23(c), 24, 25, 30(6) | Service Provider and the Customer must be written, and detailed information regarding each party's respective roles within the entire switching process should be covered under contractual clauses. Additionally, the Contractual Agreement between the parties involved must cover all the possible switching scenarios, as follows (1) the Customer switching between Providers for a Cloud Service, (2) the Customer using Cloud Services from multiple Providers, (3) the Customer linking one Cloud Service to another Cloud Service, (4) the Customer linking in-house capabilities with Cloud Services, and (5) the migration of the Customer capabilities into Cloud Services. In terms of formality, to allow flexibility in the contractual stipulation, although the Contractual Agreement must be written, it can take place in different forms, the latter being a single contractual form, a set of documents related to the services with relevant annexes attached, or standard online terms and conditions. Regardless of the contractual form, the Cloud Service Provider must make the Contractual Agreement available to the Customer in a way allowing the Customer to store and reproduce it. | Agreements of the Cloud Service Provider (e.g., in standard online terms and conditions, directly in the main body of the Contractual Agreement, in a document included in the set of documents related to the services with relevant annexes attached, in publicly available materials that are referred in the Contractual Agreement). The contractual clauses dedicated to the porting process must include, at least, the following elements:<br><br>1. Clauses containing the rights and obligations of the Customer and the Cloud Service Provider of a data processing service in relation to switching between providers of such services or, where applicable, to an on-premises infrastructure. This shall include the rights of the Customer to port its exportable data or other digital assets to another Cloud Service Provider or to an on-premises infrastructure, including after having benefited from a free-tier offering. The clauses shall make it clear that the Cloud Service Provider shall not be required to develop new technologies or services to facilitate the switch, and shall not be required to disclose or port any digital assets protected by intellectual property rights or constituting a trade secret or confidential information, or take any action that would compromise the Customer or Cloud Service Provider's security and integrity of service.<br><br>2. Clauses allowing the Customer, upon request, to switch to a data processing service offered by another Cloud Service Provider or to port all exportable data, applications, and digital assets to an on-premises ICT infrastructure, without undue delay and in any event no longer than the 30-day mandatory maximum transition period or other transition period that may be agreed between the parties, provided that the Customer takes all actions needed on its side to conduct the switching process. This shall include:<br><br>a. an obligation of the Cloud Service Provider to support the Customer's exit strategy relevant to the contracted |

| | | | |
|---|---|---|---|
| | | | services, this support may be given through provision of all relevant information that informs the customer how they may exit the Cloud Provider's Services;<br>b. a clause specifying that the contract shall be deemed terminated and the Customer shall be notified of the termination, in one of the following cases, provided that the Customer takes the steps further described under Section TDP (Termination of the Switching Process):<br>i. where applicable (i.e., the Customer executed a complete switch and consequently retains no workloads with any of the services of the source Cloud Service Provider), upon the successful completion of the switching process to another Cloud Service Provider or an on-premises system;<br>ii. at the end of the maximum notice period agreed between the parties in accordance with Section CR01.3, in the case that the Customer does not wish to switch but to delete all its digital assets upon service termination;<br><br>3. A maximum notice period of 2 months for initiating the switching process, contingent upon the performance by the Customer of its obligations under Section IDP.01, as well as its obligations under the Contractual Agreement.<br><br>4. Clauses containing the process for adjusting the transition period.<br><br>5. Clauses containing a clear list of the obligations of the Cloud Service Provider in relation to the transition process which must be fulfilled to enable the Customer to complete the transition within the timeframes stated under Section CR.01.2, which shall at least contain the following:<br><br>a. The Cloud Service Provider, where it is technically feasible, will reasonably assist and facilitate the |

| | | | |
|---|---|---|---|
| | | | Customer (and third parties authorized by the Customer) in porting his data. This reasonable assistance may be given through provision of all relevant information that informs the customer how they may port their data from the Cloud Provider's Services;<br>b. The Cloud Service Provider will support the Customer to maintain its business continuity through continued provision of the respective functions or services under the Contractual Agreement, without prejudice to the Cloud Service Provider's rights of suspension or termination for cause under the Contractual Agreement; and<br>c. The Cloud Service Provider will, where technically feasible, allow the Customer to use exportable data formats (i.e., a format where the data can be extracted out of the source Cloud Service Provider's environment) when using its Cloud Services, that would allow the Customer to export such data in a structured, commonly used, and machine-readable manner.<br><br>6. Clauses committing the Cloud Service Provider to provide an exhaustive list of all categories of data and digital assets which are exportable during the switching process. This shall include an exhaustive specification of categories of data specific to the internal functioning of provider's service that will be exempted from the exportable data, where a risk of breach of trade secrets of the provider exists, or any data that will be exempted due restrictions based on intellectual property laws (e.g., where the data constitutes proprietary information on the services of the Cloud Service Provider, including usage information created by the Cloud Service Provider) or where the transfer would compromise the Cloud Service Provider's security and integrity of service. |

| | | | |
|---|---|---|---|
| | | | 7. Clauses containing a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transition period referred to in Section CR.01.2, without prejudice to the Cloud Service Provider's rights of suspension or termination for cause under the Contractual Agreement. This shall include a clause guaranteeing full erasure of all exportable data and, digital assets generated directly by the Customer and/or relating to the Customer directly (other than any elements that may be retained by the Cloud Service Provider, in accordance with the last sentence of this paragraph), after the expiration of the retrieval period, provided that the switching process has been completed successfully, including customer notification of completion and account closure in line with Section TDP.[01]. In case the Cloud Service Provider retains any part of the exportable data or digital assets for financial or legal reasons, for security reasons or otherwise to maintain the integrity of its services, this shall also include clauses containing information on such data or digital assets.<br><br>8. Clauses explaining the data egress charges and any other switching charges that may be imposed by the Cloud Service Provider to the Customer.<br><br>9. Clauses outlining that the obligations related to the switching process set out in the contractual agreement shall only apply to the services, contractual agreements or commercial practices provided by the source provider of data processing services. |
| **3** | **Initiation of the Switching Process (Request of the Customer)**<br>**Relevant Articles of the EU Data Act:** Recital 85, | Section 3 focuses on the initiation of the switching process, and it contains the respective obligations of the Customers and of the Cloud Service Provider in this stage. | **IDP.01: Obligations of the Customer with respect to the initiation of the switching process.**<br><br>1. The Customer shall be responsible for providing the Cloud Service Provider with a notification that it intends to switch away from the Cloud Service Provider's services or that he will use |

| | | | |
|---|---|---|---|
| | Article 25(2)(d)-(f), 25(3), 27 | | multiple Cloud Service Providers in-parallel with the notified Cloud Service Provider's services, and/or that he intends to delete its digital assets and exportable data, meeting the following requirements:<br><br>a. The notification shall be done by using the channels designated by the Cloud Service Provider;<br>b. The notification shall include a clear selection by the Customer on whether the Customer intends to (i) switch away from the Cloud Service Provider's services to another Cloud Service Provider or to an on-premise system or that (ii) he will use multiple Cloud Service Providers in-parallel with the notified Cloud Service Provider's services and/or (iii) that he intends to delete all its digital assets and exportable data upon expiration of the notification period.<br>c. The notification shall include a clear scope of the data that will be transferred by the Customer as part of the switching process or the transfers that will form part of the Customer's in-parallel use of multiple Cloud Service Providers, including which data shall be ported, specifications (e.g. the data format that the Customer intends to use among the data formats supported by the Cloud Service Provider), destination (e.g. the details of the new or parallel Cloud Service Provider), and any other information requested by the Cloud Service Provider in order to help it adhere to its regulatory obligations and to allow verifying whether the Customer's requests duly qualifies as switching or in-parallel use of multiple Cloud Service Providers under the EU Data Act;<br>d. In case the Customer executed a complete switch, and thus retains no workloads with any of the services of the source Cloud Service Provider, the notification may be given alongside the notice to terminate the Contractual Agreement upon the successful completion of the switching process (which shall be confirmed by the Customer in accordance with Section TDP.01).<br>The notification shall include the Customer's intended period of |

| | | | |
|---|---|---|---|
| | | | execution of the switching process as well as the confirmation that all actions that need to be conducted by the Customer will be taken for the execution of the switching process during the periods designated;<br>e. The notification shall be given maximum 2 months prior to the intended commencement date of the relevant transfers; and<br>f. The notification shall meet any other requirements that may optionally be provided by the Cloud Service Provider as part of the Contractual Agreement, or to seek to comply with its regulatory requirements or to prevent any fraudulent or abusive Customer conduct.<br><br>2. In the event of withdrawal of the switching request, the Customer shall notify the Cloud Service Provider as soon as reasonably practicable within no less than 14 days prior to the intended execution of the switching process, through the designated channel. In the event of requesting withdrawal beyond the period of 14 days prior to the execution, the Customer expresses the agreement to the terms for late withdrawal, documented and communicated by the Cloud Service Provider in line with Section IDP.02.3. |
| | **Relevant Articles of the EU Data Act:** Recital 85, Articles 25(2)(a), 25(4), (5), 27 | | **IDP.02: Obligations of the Cloud Service Provider with respect to facilitating the initiation of the switching process.**<br><br>1. The Cloud Service Provider shall be responsible for designating the channels for Customers to notify the request of initiation of the switching process. The designated channel shall meet the following requirements:<br><br>a. The channel shall explicitly request the relevant information about the switching process, including all information required in Section IDP.01.1; |

| | | | |
|---|---|---|---|
| | | | b. The channel shall, if relevant, provide explanations to terminology used and choices to be made, as needed, by means of pop-ups, just-in-time information, Frequently Asked Questions section, or other relevant means;<br>c. The channel shall include or make reference to any support mechanisms offered by the Cloud Service Provider in relation to the switching process, e.g., information guiding the Customer on the switching process and any other technical material made available to the Customers;<br>d. The channel shall be easily accessible and communicated to the Customers;<br>e. The channel shall verify the authenticity of the request, and include a possibility to withdraw the switching request;<br>f. The channel shall acknowledge the receipt of the notification on initiation of the switching process, including a copy of the information and specifications provided by the Customer;<br>g. The Cloud Service Provider shall be able to retain the receipt of every Customer notification in a secure repository for a specified time period in order to facilitate auditing and compliance processes; and<br>h. The channel shall be reviewed periodically as to the effectiveness and accessibility of the designated channel.<br><br>2. The Cloud Service Provider shall make available to the Customer tools or services that the Customer can use to have visibility over its use of the Cloud Services and determine the progress of its porting process. This can be done through a dedicated portal, dashboard, tickets, by mail, or any other suitable channels. In case the Customer fails to take the actions needed on its side to conduct the transition within the 30-day maximum transition period and provided that the Cloud Service Provider has fulfilled its obligations under Section CR.01.2, CR.01.5, CR01.6 and TMR.02.1-6, the Cloud Service Provider shall be entitled to apply an alternative transition period, which may not exceed 7 months. |

| | | | |
|---|---|---|---|
| | | | In such case, the Cloud Service Provider must notify the extension of the transition period to the Customer in writing as soon as possible upon completion of the initially agreed transition period. In the event that the Customer still hasn't completed the actions needed on its side to conduct the transition within 7 months, the Customer and the Cloud Service Provider shall mutually decide on the continuity of Cloud Services.<br><br>3. The Cloud Service Provider shall document and communicate their arrangements regarding late withdrawal requests, which may optionally include requirement of a paid additional support package, additional fees, or refusal.<br><br>4. The Cloud Service Provider's obligations under this Section IDP.02 are contingent upon the performance by the Customer of its obligations under Section IDP.01, as well as its obligations under the Contractual Agreement. |
| **4** | **Technical Requirements for the Switching Process**<br><br>**Relevant Articles of the EU Data Act:** Recital 82, Recital 97, Articles 23(e), 25(4), 30, 35 | Section 4 addresses the technical measures deployed and implemented by the Cloud Service Provider to assist the Customer during the switching process. Additionally, Section 4 addresses the obligations, roles, and responsibilities of the Customer to allow the Cloud Service Provider to support the switching process in adherence to the requirements of the Control Framework. Section 4 also addresses the relation between the security and integrity of the data sets ported from one source to another, and it outlines the obligations of the Cloud Service Provider to help ensuring such security and integrity in all possible porting scenarios, including (1) the Customer | **TMR.01: Obligations of the Customer with respect to technical requirements for Data Portability.**<br><br>While performing the switching process, after initiating the process in line with Section 3, the following requirements shall be met by the Customer:<br><br>1. The Customer shall conduct the switching process through the use of APIs, effective tools to transfer data and digital assets and any other services made available by the Cloud Service Provider. The Customer shall inform the Cloud Service Provider in writing of any additional requirements and specifications that may have an impact on the obligations of the Cloud Service Provider relating to the process, which were not conveyed during the initiation of the process, as soon as they have become known to the Customer. |

| | | | |
|---|---|---|---|
| | | switching between Providers for a Cloud Service, (2) the Customer using Cloud Services from multiple Providers, (3) the Customer linking one Cloud Service to another Cloud Service, (4) the Customer linking in-house capabilities with Cloud Services, and (5) the migration of the Customer capabilities into Cloud Services. Finally, Section 4 addresses the quality of the technical measures deployed by the Cloud Service Provider during the switching process, as well as setting standards regarding the manners in which the Customer shall conduct the switching process, which shall be made possible by the Cloud Service Provider without causing hindrance to the quality of the Customer set of data during or after the porting. | 2. Provided that the Cloud Service Provider duly complies with its obligations listed under Section CR.01.2, CR.01.5, CR01.6 and TMR.02.1-6, the Customer shall<br>a. bear the responsibility for executing the porting for switch or commencement of in-parallel use of services in accordance with the relevant timelines, unless such timelines are affected from a technical unfeasibility, which shall be duly justified by the Cloud Service Provider and notified to the Customer within 14 working days together with an alternative period for completion of the switch, and,<br>b. be solely responsible for any changes to the timelines that are caused by any additional requirements or specifications not conveyed by the Customer during the initiation of the process;<br><br>3. The Customer shall bear the end responsibility for maintaining interoperability of data between the source and destination providers, subject to the requirements imposed on the Cloud Service Provider in line with Section TMR.02.<br><br>**TMR.02: Obligations of the Cloud Service Provider with respect to technical requirements for Data Portability.**<br><br>The Customer shall conduct the switching process through the use of APIs, effective tools to transfer data and digital assets and any other services made available by the Cloud Service Provider. While assisting the Customer in the switching process, the following requirements shall be met by the Cloud Service Provider:<br><br>1. Where the source Cloud Service Provider provides the Customer services concerning scalable and elastic computing resources limited to infrastructural elements (e.g. servers, networks and the virtual resources necessary for operating the infrastructure, but |

| | | | |
|---|---|---|---|
| | | | that do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements), the Cloud Service Provider shall take all reasonable measures in their power to facilitate functional equivalence in the use of the destination service. Customers acknowledge that functional equivalence is dependent on their individual use of the source Cloud Service Provider's services and their intended use of the destination Cloud Service Provider's services. The source Cloud Service Provider may facilitate this by providing capabilities, all adequate information relevant to its services and functionalities that can be used by the Customer, such as APIs, data formats and structures, publishing technical documentation to support the Customer during the process or, where appropriate, highlighting any tools that might be necessary. The information shall allow for Customers' assessment of work required to switch services or use services in-parallel with those from other Cloud Service Providers. The information may highlight certain elements that are unique to the Cloud Service Provider's service (such as identity and access management, definitions, security) and cannot be ported to the destination Cloud Service Provider's services. The information may optionally include references to other solutions providing interoperability while retaining functional equivalence in the use of the new service, product recommendations, and other additional guidance. The Cloud Service Provider is not required to develop new technologies (e.g., developing new interfaces) or services (e.g., migration services, consulting services on how to achieve functional equivalence with the new Cloud Service Provider) to facilitate the switching process or in parallel use of multiple Cloud Service Providers, and shall not be required to disclose any digital assets protected by intellectual property rights or constituting a trade secret or confidential information, or take any action that would |

| | | | |
|---|---|---|---|
| | | | compromise the Customer or Cloud Service Provider's security and integrity of service.<br><br>2. Where the Cloud Service Provider provides the services referred to in Section TMR.02.1, the Cloud Service Provider shall, where technically feasible (e.g., where the desired outcome is not impractical or significantly difficult to achieve due to technical challenges, limitations or security constraints), allow the Customer to unbundle these services from other data processing services provided by the Cloud Service Provider, so that the Customer can use them independently from other data processing services of the Cloud Service Provider, if he wishes so. The Cloud Service Provider shall not contravene this requirement where the Customer uses a number of these services to build an application which they later decide to move to another provider. The Cloud Service Provider may optionally still offer discounts based on a Customer's committed use of these services.<br><br>3. Where the Cloud Service Provider does not deal with services as referred to in Section TMR.02.1, the Cloud Service Provider shall make open interfaces available to an equal extent to all of its Customers and the concerned destination service providers free of charge in order to facilitate the switching process. These interfaces shall include information on the service concerned to enable the development of software to communicate with the services, for the purposes of data portability and interoperability. The Cloud Service Provider shall not be required to develop new open interfaces to facilitate the switching process and shall not be required to disclose any digital assets protected by intellectual property rights or constituting a trade secret or confidential information, or take any action that would compromise the |

| | | | |
|---|---|---|---|
| | | | Customer or Cloud Service Provider's security and integrity of service.<br><br>4. Where the Cloud Service Provider does not deal with services as referred to in Section TMR.02.1, the Cloud Service Provider shall ensure compatibility with common specifications based on open interoperability specifications or harmonised standards for interoperability at least twelve months after the references to these open interoperability specifications or harmonised standards were published in the central Union data processing service standards repository.<br><br>5. The Cloud Service Provider shall provide the Customer with the ability to export the data in a structured, commonly used, and machine-readable format (e.g., where applicable, in line with harmonized standards between Cloud Service Providers dealing with the same service types);<br><br>6. In order to allow the Customer to maintain confidentiality and integrity of the data ported, the Cloud Service Provider:<br><br>a. shall enable the Customer to initiate the process to port the data to the destination provider (or in-parallel service Provider) of choice;<br>b. shall provide the customer with the ability to port the data in line with information security requirements of the contract without any additional fees. Additional safeguards may optionally be provided by the Cloud Service Provider for a reasonable fee, such as encryption in transit to specification requested (e.g., TLS v1.3); and<br>c. may optionally make available tools enabling the Customer to verify the integrity of the data ported upon egress (e.g., hash verification, checksums). If technically feasible, the Cloud Service Provider shall enable the |

| | | | |
|---|---|---|---|
| | | | Customer to cooperate with the new provider of choice to verify integrity of data upon entry to the new cloud;<br><br>7. The Cloud Service Provider shall allow the Customer to collect and preserve logs of the activities performed in scope of the switching process under the respective instruction (e.g., Customer instructions and requests);<br><br>8. The Cloud Service Provider may optionally charge Customers for the use of additional services and tools (if available) to assist with, and provide security of, porting beyond the abovementioned requirements, such as testing the execution of the switch, data restructuring or advanced verification of which feature is interoperable with which third-party cloud service providers' services. The Customers shall bear the responsibility for correct use of said tools. |
| **5** | **Termination of the Switching Process**<br><br>**Relevant Articles of the EU Data Act:** Articles 23(a), 25(c), (g), | Section 5 addresses the termination of the switching process, including both scenarios (1) where the Customer executed a complete switch and retains no workloads with any of the services of the source Cloud Service Provider, and thus terminating the relationship between the Cloud Service Provider and the Customer, and/or (2) where the Customer switches away to another Cloud Service Provider only for some of the services whilst the Customer wishes to keep using other services of the original Cloud Service Provider, meaning that the relationship between the Cloud Service Provider and the Customer will still be ongoing after the porting with respect to the | **TDP.01: Obligations of the Customer with respect to the completion and termination of the switching process.**<br><br>1. The Customer shall be responsible for providing the Cloud Service Provider with a notification confirming the completion of the transition to the destination Cloud Service Provider, i.e., porting of all its exportable data, applications and digital assets .In case the Customer could not complete the transition to specification due to any omission by the Cloud Service Provider to comply with its regulatory obligations or obligations under this Control Framework, the Customer shall also be responsible for flagging such omissions, using the Cloud Service Provider's designated process.<br><br>2. In the absence of any omissions flagged by either party, upon provision of such notification by the Customer, the transition |

| | | | |
|---|---|---|---|
| | | services which have not been subject to a switching. | period shall be completed and the data retrieval period referred to in Section CR.01.7 shall start.<br><br>3. In case the Customer executed a complete switch, and thus retains no workloads with any of the services of the source Cloud Service Provider, upon completion of the data retrieval period, the Customer shall submit a request to close its account(s) with the source Cloud Service Provider, which may be done using the interface made available by the Cloud Service Provider. The Contractual Agreement shall be deemed terminated upon completion of the account closure process.<br><br>**TDP.02: Obligations of the Cloud Service Provider with respect to the completion and termination of the switching process.**<br><br>1. Upon receipt of the confirmation from the Customer of the completion of the transition to the destination Cloud Service Provider, i.e., porting of all its exportable data, applications and digital assets, the Cloud Service Provider may flag any omissions by the Customer, if and to the extent that it has visibility over the process.<br><br>2. In the absence of any omissions flagged by either party, and upon receipt of the Customer's notification confirming completion of the transition to the destination Cloud Service Provider, i.e., porting of all its exportable data, applications and digital assets, the transition period shall be completed and the data retrieval period referred to in Section CR.01.7 shall start.<br><br>Upon completion of the data retrieval period, and provided that the Customer has submitted a request to close its account with the source Cloud Service Provider, the Contractual Agreement shall be deemed terminated upon completion of the account closure process. |

## 4. Complaints and Enforcement

The Association of Cloud Infrastructure Service Providers of Europe (CISPE) is responsible for the governance of this Framework.

**4.1 Complaints committee:** The Executive Board of CISPE will appoint a Complaints Committee. The Complaints Committee will be responsible for: (a) considering complaints about the compliance of services covered by a Cloud Service Provider's Declaration of Adherence with the Framework, and (b) taking enforcement action against a non-compliant Cloud Service Provider and, where necessary, recommending such enforcement action to the Executive Board of CISPE.

**4.2 Complaints Process**

4.2.1 The Complaints Committee will propose to the Executive Board rules and a process to make, decide, appeal and communicate the outcomes of complaints about the compliance of services covered by a Cloud Service Provider's Declaration of Adherence with the Control Framework (Complaints Process).

4.2.2 Once approved by the Executive Board, the Complaints Committee will publish, implement and administer and keep under review the Complaints Process. The Secretariat will publish and maintain up to date information on the Complaints Process on the CISPE Public Register.

4.2.3 A CISPE member, 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.

**4.3 Enforcement**

4.3.1 If in its final decision the Complaints Committee finds that a Cloud Service Provider is non-compliant with the Control Framework, then the Complaints Committee may:

(a) request the Cloud Service Provider to take specific remediating measures within a reasonable timeframe to comply the Framework; and

(b) in extreme or repeated cases of non-compliance, or in case of failure by the Cloud Service Provider to implement the requested remediating measures (at all or in time), recommend to the Executive Board that the Cloud Service Provider's Declaration of Adherence be suspended or revoked in respect of the non-compliant service.

(c) If a Cloud Service Provider's Declaration of Adherence is suspended or revoked the Secretariat shall promptly remove the relevant Cloud Service Provider's Declaration of Adherence on the CISPE Public Register, the Cloud Service Provider shall stop using the Compliance Mark in respect of the relevant service within the timeframe specified by the Complaints Committee.

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

4.3.3 The enforcement measures above are the sole and exclusive remedies for a Cloud Service Provider's non-compliance with the Control Framework and are without prejudice to the Customer's rights under the EU Data Act, or the terms of the agreement between the Customer and the Cloud Service Provider.

4.3.4 The option for a customer to make a complaint does not give the customer any direct rights or remedies against the Cloud Service Provider or CISPE under or in connection with the Framework.

4.3.5 CISPE does not accept any responsibility for a Cloud Service Provider's compliance with the Framework. Nor will CISPE 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 CISPE or a Cloud Service Provider in connection with the Framework.