Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services - CSP Transparency Statement

15th November 2019

1. Introduction

This companion document to the Code of Conduct for Data Portability and Cloud Service Switching for IaaS Cloud services v2.9[1] sets out a template for comparable pre-contractual transparency statements by *Infra.* CSPs to support potential customers in assessing data portability and switching. When making a declaration of adherence, an *Infra.* CSP shall complete this template and make it available to potential customers.

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

The information collected in this template will be exclusively based on a CSP's declarations. Where possible, the CSP should reference or aggregate existing material. Compliance with the code requires this template to be followed and that the content supplied enables customers to make informed choices.

The scope of this document does not include interoperability and integration issues i.e. use of common APIs, protocols or file formats to enable components from various vendors to interoperate, due to variability and complexity of IaaS models.

The CSP should declare the infrastructure artefacts in scope either in the relevant questions below or as an attached document. Optionally, the CSP may elect to include additional features or structures that are not *per se* IaaS artefacts to allow for more complex cases, such as multi-cloud, and recognizing there is no definitive demarcation with other cloud service models. Porting in this document refers to Infrastructure Artefacts that include CSC data, infrastructure related software components and metadata (e.g. virtual machines, containers, topology data), and designated cloud service derived data.

If a CSP references other material in completing this template, the CSP must specify how these external materials are maintained and include them in the change notification processes (as per TR04 and TR05 of the code).

[1] https://drive.google.com/file/d/10cUSPD1OmC3MxmndyHPAN-hcBCfSdmZZ/view

This transparency statement refers many times to the Cloud Service Agreement (CSA). Note that the CSA can take any form and is legally binding.

2. Transparency Statement Template

The transparency statement template is divided into two sections: a section covering requirements that must be included, and a section covering recommendations that only need to be included if supported by the CSP.

2.1 Requirements

The following requirements must be completed by the *Infra.* CSP.

2.1.1 Procedural Requirements

From Section 5.1 of the IaaS Code.

PR01 - Procedures for initiating switching and porting from the cloud service when it is a porting source

> [CSP to specify the mechanisms by which a CSC requests to retrieve its infrastructure artefacts from the CSP. Highlight if there are different procedures for copying artefacts either on premises or to another provider (e.g. backup), moving data (copy then delete) to either on-premises or to another provider without contract termination, or moving data to either on-premises or to another provider with contract termination.]
> *[Example checklist (informative):*
> - *Have references to the procedures for initiating porting been documented?*
> - *Do they apply to the in-scope service(s)?*
> - *Do they explain how to initiate porting at contract termination?*
> - *Do they explain how to initiate porting out of the service, where the contract continues?]*

PR02 - Procedures for initiating switching and porting to the cloud service when it is a porting destination

> [CSP to specify the pre-requisites and mechanisms by which a CSC can request infrastructure artefacts to be received by the CSP for use in a cloud service.]
> *[Example Checklist (informative):*
> - *Have references to the procedures for initiating porting into the service been provided?*
> - *Do they apply to the in-scope service(s)?*
> - *Do they explain how to initiate porting for the initial use of the service?*
> - *Do they explain how to initiate porting into a service already in use?]*

PR03 - Available porting methods and formats, including available protections and known restrictions and technical limitations

[CSP to specify the methods available (e.g. bulk uploads/ftp, via an API, physical shipment), and indicate if there are different options for import versus export.
CSP to specify what formats are supported for import, and what formats are supported for export.
CSP to specify what encryption methods are supported and/or other means to protect in transit data flows.
CSP to specify other restrictions and technical limitations such as file sizes, bandwidth, time of day etc, if any]
[Example Checklist (informative):

- *Have references to the various methods been provided? Are there different options for import vs export?*
- *Have references to the various formats been provided? Are there different options for import vs export?*
- *Have protection mechanisms and options been provided?*
- *Have restrictions and technical limitations been documented and provided?]*

PR04 - Charges and terms associated with porting

[CSP to provide references to any anticipated charges relating to porting of infrastructure artefacts data either in or out of the service.
CSP to provide references to legal terms and conditions that explicitly apply to porting. Highlight if there are differences in explicit terms and costs for porting data while still in contract versus at contract termination.]
[Example Checklist (informative):

- *Are details of known charges set out either in absolute terms or any pro-rata charges?*
- *Is the scope of any charges clear?*
- *Have the terms and conditions been supplied?*
- *Are the costs and terms clearly laid out?*
- *Do they address the full extent of any terms associated with porting?]*

PR05 - Procedures for activating a new cloud service when it is the porting destination

[CSP to provide references to the steps necessary to activate the cloud service, and the procedures to initialise with a CSC's infrastructure artefacts.]
[Example Checklist (informative):

- *Have references to service activation procedures been provided?*
- *Do they apply to the in-scope service(s)?*

- *Do the materials set out the steps necessary for service activation?*
- *Do the materials set out the steps for initialising a service with existing infrastructure artefacts?]*

PR06 - The exit process for an existing cloud service, where it is the porting source, and where the CSC is aiming to terminate its use of the cloud service once porting is complete

[CSP to provide references to the exit process where a customer is terminating their use of the cloud service.]
[Example Checklist (informative):
- *Have references to service exit and termination procedures been provided?*
- *Do they apply to the in-scope service(s)?*
- *Do the materials set out the steps necessary for service termination and exit?]*

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

[CSP to provide details of any available management capabilities that can be used to facilitate porting and switching (if applicable)]
[Example Checklist (informative):
- *What management capability to facilitate porting and switching are offered?*
- *Are these capabilities laid out for the customer?]*

2.1.2 Portability Requirements

From Section 5.2 of the IaaS Code.

DP01 - The cloud service shall be capable of importing and exporting CSC Infrastructure Artefacts, in an easy and secure way, supporting the following scenarios: CSC to cloud service, cloud service to cloud service and cloud service to CSC. The *Infra. CSP* shall provide the support to enable the transfer of Infrastructure Artefacts using structured, commonly used, machine-readable format.

[CSP to indicate the capabilities to both import and export the infrastructure artefacts applicable to the cloud service.
The capabilities must support the source or destination being the customer's on-premises facilities or may support to another cloud service.
The capabilities must be both secure and easy to use.

The import and export capabilities must use structured, commonly used, machine-readable formats.]

[Example Checklist (informative):

- *Have the capabilities to import/export infrastructure artefacts been provided?*
- *Is it clear what the applicable artefacts are?*
- *Does at least one of the relevant import/export capabilities support export/import from a Customer's on on-premise environment or is at least agnostic about the source/destination?*
- *Does at least one of the relevant import/export capabilities support either directly or indirectly import/export from another Cloud service or is at least agnostic about the source/destination?*
- *Is it clear what structured, commonly used, machine-readable formats are supported for import/export?*
- *Are there measures in place or available for a customer to utilize to import/export their infrastructure artefacts in a secure way?*
- *If there are differences in capabilities and supported formats between import and export, have these been made clear?]*

DP06 – Where the CSC data involves Infrastructure Artefacts that rely on a feature or capability of the cloud service, the *Infra. CSP* shall provide an appropriate description of the environment for their execution and how the service dependencies can be satisfied.

[CSP to provide references to information about features or capabilities of the cloud service that Infrastructure artefacts rely upon to function.]

[Example Checklist (informative):

- *Has material that details the features or capabilities of the cloud service that the infrastructure artefacts applicable to that service rely upon to function been provided?*
  Has the execution environment and service dependencies been described?]

DP08 - The *Infra. CSP* shall take reasonable steps to enable a CSC to maintain their service continuity while transferring data between providers, where technically feasible.

[CSP to specify how it supports a CSC to maintain service continuity and to document any limitations in such support.]

[Example Checklist (informative):

- *Is there a process for a CSC to indicate a successful transfer?*
- *Is there a process for a CSC to reverse a transfer especially just before contract termination?*
  Is it clearly documented when infrastructure artefacts will be deleted?]

2.1.3 Scope and Compatibility Requirements

From Section 5.3 of the IaaS Code.

SCR01 - The *Infra. CSP* shall describe in the CSP transparency statement the capabilities necessary for effective cloud service switching, to minimize loss of functionality, particularly security functionality. It is acknowledged that the CSC and the *Infra. CSP* will define in the CSP transparency statement which derived data will be subject to the same porting requirements. Any porting capabilities relating to cloud service derived data should be clearly described in the CSP transparency statement, but there is no requirement for the *Infra.* CSP to support the porting of this data unless designated as in scope.

[CSP to describe details of the capabilities necessary to switch out or switch into the service. CSP should supply details of which derived data is in scope and which is able to be ported, and any requirements such porting is subject to.
The details must outline how the customer can minimize loss of functionality including security functionality in switching.]
[Example Checklist (informative):

- *Have the capabilities necessary for switching in and out of the cloud service been described?*
- *Is there a clear definition of what derived data is in scope for porting i.e. a clear statement of the designated cloud service derived data?*
- *Have the requirements, limitations, and capabilities for porting designated cloud service derived data been provided?*
- *Has the provider outlined the steps necessary to minimize loss of functionality including security functionality when switching?]*

SCR02 - The CSP transparency statement shall specify the following:

a) the scope of Infrastructure Artefacts available for transfer;
b) any claim on Intellectual Property Rights the *Infra. CSP* has on CSC data and how these rights are executed after a switch.

[CSP to supply details of Infrastructure artefacts types that can be transferred.
CSP to detail any IPR it claims on customer data and how those rights are executed after a switch.]
[Example Checklist (informative):

- *Provide a list of the service's infrastructure artefacts that are within scope and that can be transferred.*
- *Have any claims by the CSP on the IPR of the customer's data been documented?*

- *Has it been asserted what the IPR rights are and how they are executed following a switch out of the service?]*

2.1.4 Planning Requirements

From Section 5.4 of the IaaS Code.

PLR01 - the procedure to determine the testing of the mechanisms and schedule of a transfer, based on the CSC's business needs, security risks, and technical and support capabilities expected of each of the *Infra. CSP* and the CSC. Testing should include both the testing of the mechanisms used for porting data to and from a cloud service and also of the APIs used to access and to manage the data when stored within the cloud service. Further guidelines on testing of the mechanisms including APIs may be adopted by the relevant governance body of the Code. Acceptance of the testing should be made with the CSC, in the frame of a transparent test process. CSC should be recommended by the *Infra. CSP* to have a test suite.

[CSP to provide details of mechanisms for testing the porting of data to and from a cloud service.]
[Example Checklist (informative):
- *Identify any known test suites that are available to customers.*
- *Identify any APIs supported by the CSP that are available to help test the porting and switching process.*
- *Provide other details of assistance given to CSCs to support their processes.]*

PLR02 - what constitutes appropriate duration for the transfer of the data using current best practices and available technology, including any solutions not using a network;

[CSP to specify what timeframes it supports for the transfer of data.
CSP to provide a reference to materials that help customers plan appropriate durations for the transfer of their data using current best practices and available technology.
CSP to include references to any non-networked solutions.]
[Example Checklist (informative):
- *Have details of typical transfer rates and or durations using current best practice and available technology been provided?*
- *Declare if physical (non-network) transfer capabilities are offered, and if so document shipment options, timescales and costs.*
- *Is there any other information that can be provided to help a CSC plan the transfer?]*

PLR03 - for the anticipated volume of Infrastructure Artefacts the appropriate mechanisms, availability periods and price for the transfer;

[CSP to declare if there are different mechanisms are available for different volumes of infrastructure artefacts, and the details for each mechanism including availability periods and cost.]
[Example Checklist (informative):
- *List all transfer mechanisms.*
- *For each mechanism, provide durations, costs and other conditions that are applicable, and advise for what volumes the mechanism is appropriate for.]*

PLR04 - allocation of responsibility and methods for providing security for the data to ensure, for example, access control, authentication of users, confidentiality and integrity through the process;

[CSP to set out the respective responsibilities for the security of data during the transfer process.
CSP to provide references to materials that explain the methods available for securing data through the data transfer process.]
[Example Checklist (informative):
- *Are the respective responsibilities between the CSC and CSP for the security of data during the transfer process been laid out?*
- *Has material that explain the methods available and the steps customers can take to secure data during the data transfer process been provided?*
- *Are the any specific support functions available to the CSC to support secure transfers processes?]*

PLR05 - the period during which the CSC data will remain available for transfer once the termination of the source service is required by the CSC, and the nature of clear and timely warnings issued before CSC data is deleted.

[CSP to set out the duration that a CSC's infrastructure artefacts will be retained following termination of the service.
CSP to detail any warnings that the customer will receive prior to removal of the data.]
[Example Checklist (informative):
- *Declare how long infrastructure artefacts are available (for download) after contract termination.*
- *Document if the CSC will be given warnings, and how and at what frequency these warnings are given before deletion of artefacts.*
- *Document what happens to backups as well as the primary source of artefacts.]*

2.1.5 Cloud Service Agreement Requirements

From Section 6.2 of the IaaS Code.

FR1 - The CSA shall be documented (including in electronic form) and legally binding between the *Infra. CSP* and the CSC.

> [CSP to set out all terms and conditions for using a cloud service, including the terms under which data portability, cloud service switching, and termination are delivered.]
> *[Example Checklist (informative):*
> - *Is it clear to the CSC what CSA is applicable?*
> - *Under what jurisdiction is the CSA legally binding?]*

FR2 - The CSA may take any form, including but not limited to:

a) a single contract;

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

c) standard online terms and conditions.

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

> [CSP to define what form the CSA takes.]
> *[Example Checklist (informative):*
> - *Have all constituent materials (documents, policies etc) of the CSA been identified?*
> - *Provide references to standard terms and conditions.*
> - *Has this transparency statement been referenced?]*

2.1.6 Transparency Requirements

From Section 7 of the IaaS Code.

TR01 - The terms and conditions necessary to meet this Code (including those referenced in clauses 5 of this Code) shall be described to potential CSC in clear terms and with an appropriate level of detail in a pre-contractual CSP transparency statement between the CSC and the *Infra. CSP*. 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).

[CSP to complete this transparency statement and make available to potential customers, and to make it binding in applicable CSAs.]
[Example Checklist (informative):

- *Has this transparency statement been completed for the applicable services?*
- *Declare under what conditions and NDA is required in order to supply a transparency statement to a potential CSC.]*

TR02 - The description provided for in TR01 shall provide an appropriate level of details including:

a) all aspects of compliance with this Code;

b) all documentation, available support and tools to transfer the CSC data from one *Infra. CSP* to another;

c) a description of the overall data porting process and supported capabilities including any data back-up and recovery processes adopted for the purpose of protecting the data while undertaking the porting of the data, security measures, record management and, if agreed upon, the deletion of the CSC's data after the data porting is successfully completed (if the CSC intends to terminate the cloud service contract). If the deletion capability is provided to the CSC by the *Infra. CSP*, the CSC can do the deletion on its own. The deletion shall be completed by the source *Infra. CSP*, in the case where such capability is not provided to the CSC;

d) the status and procedures for handling the CSC data on the *Infra. CSP's* infrastructure after termination including CSC instructions on any data retention, preservation or restoration obligations stipulated by applicable law or regulation;

e) a clear description of any and all third-parties that have access to the data through the process;

f) a clear description of the policies and process for accessing data in the event of *Infra. CSP*'s bankruptcy or acquisition by another entity. These policies and process shall include CSC information without undue delay once a bankruptcy procedure has been started with the competent public authorities; and,

g) if a third-party service provider is needed to convert, translate or transfer CSC's Infrastructure Artefacts, it should be explicitly mentioned in the CSP transparency statement.

[CSP to provide descriptions, through the completion of this transparency statement, of:

a) all aspects of compliance with this Code;

b) the documentation, available support and tools to transfer the CSC data;

c) a description of the overall data porting process and supported capabilities including:
   - any data back-up and recovery processes available whilst porting,
   - security measures,
   - Any record management and,
   - if agreed upon, the responsibility for deletion of the CSC's data after the data porting is successfully completed (if the CSC intends to terminate the cloud service contract;

d) the status and procedures for handling the CSC data on the CSP's infrastructure after termination including CSC instructions on any data retention, preservation

e) a description of any and all third parties that have access to the data through the process;

f) available policies and process for accessing data in the event of CSP's bankruptcy or acquisition by another entity. These policies and process shall include CSC information without undue delay once a bankruptcy procedure has been started with the competent public authorities; and,

g) if a third-party service provider is needed to convert, translate or transfer CSC's Infrastructure Artefacts, it should be explicitly mentioned in the CSA.

[Example Checklist (informative):

- *Has all required and relevant information been provided or referenced in this transparency statement been provided to demonstrate compliance with all aspect of the code?*
- *Have references to the following been provided:*
  - *documentation,*
  - *available support*
  - *tools, APIs and test suites*

  to enable to transfer of customer infrastructure artefacts?
- *Is there a description of the overall data porting process and supported capabilities including?:*
  - *any data back-up and recovery processes available whilst porting,*
  - *security measures,*
  - *any record management and,*
  - *if agreed upon, the responsibility for deletion of the CSC's data after the data porting is successfully completed (if the CSC intends to terminate the cloud service contract;*
- *Is there a description of the procedures for handling customer artefacts on the CSP's infrastructure after termination including CSC instructions on any data retention, preservation?*
- *Is there a description of any and all third parties that have access to the data through the process?*
- *Is there a description of the available policies and process for accessing data in the event of CSP's bankruptcy or acquisition by another entity?*
  - *These policies and process shall include CSC information without undue delay once a bankruptcy procedure has been started with the competent public authorities*
- *Is it documented if a third-party service provider is needed to convert, translate or transfer CSC's Infrastructure Artefacts?]*

TR03 - Before the CSC accepts the CSA, the *Infra.* CSP shall provide to the CSC a CSP transparency statement describing the mechanism(s) related to the porting of CSC data:

a) from a CSC's on-premise facilities to a *Infra. CSP*'s cloud service
b) from another cloud service to the *Infra. CSP* 's cloud service

And:

c) to the CSC's on-premise facilities from the *Infra. CSP* 's cloud service
d) to another cloud service from the *Infra. CSP* 's cloud service

The description shall provide an appropriate level of details including:

e) procedures, terms and conditions, policies and costs, associated with such a data porting;

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

g) if applicable, an explanation of the data model, data schema and data semantics and any policy facet considerations adopted by the *Infra. CSP* as these apply to the CSC data, and how these aspects are handled when considering data portability.

h) All related costs areas that would be charged by the *Infra. CSP*.

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

[CSP to provide references materials that set out how to port customer data into the service. CSP to provide references to materials that set out how to port customer data out of the service. The materials MUST address porting to or from both a customer's on-premise facilities AND another provider's service. Or otherwise illustrate that the mechanisms are agnostic on the source and or destination. The materials MUST provide an appropriate level detail or reference other material that provide the necessary information including procedures, T&C, and costs. The materials MUST provide an appropriate level detail or reference other material that provide the necessary information on the relevant technical, physical measures necessary to undertake data porting. The materials SHOULD provide an explanation of any data model(s), schema(s) and semantics as well as any policy facets applied to the customer's data if applicable.

The provider MUST make available or otherwise provide the materials describing the details of porting of Infrastructure Artefacts and cloud service switching to customers prior to their acceptance of an agreement.
This information is to be documented in, or referenced by, a completed transparency statement.
[Example Checklist (informative):

- *Have references to the materials that describe the mechanism for porting customer data been provided?*
- *Is the description or descriptions suitable for addressing both porting artefacts into the service AND porting artefacts out of the service?*
- *Is the description or descriptions suitable for addressing porting in or out of the service regardless of whether the source or (destination) is an on-premises environment or another Cloud service?*
- *Has the provider determined what is the appropriate level of detail to address typical use cases?*
- *Do the provider's descriptions provide reference to the relevant terms and conditions, policies and costs?*
- *Do the provider's descriptions provide reference to the relevant material on technical, physical and organizational measures necessary for porting?*
- *Has the provider advised whether any data models, schemas, semantics or associated policies are applicable? If so, has the provider made the necessary detail available?*
- *Has the provider demonstrated how the descriptions are made available prior to customers' acceptance of agreements?*
- *Has the provider demonstrated how they ensure information is kept up to date?*
- *Has all relevant and required information been provided in the transparency statement?]*

TR04 - The *Infra. CSP* shall inform the CSC in a timely manner of any changes to the mechanisms and conditions, including identified costs, that would materially alter the portability of the CSC data. The CSC should be given the right to terminate the agreement in advance.

[CSP to have a capability to inform affected customers of changes to the porting costs, mechanisms and conditions that would materially alter the portability of customer data.
[Example Checklist (informative):

- *Is there an established way of determining material impact to portability?*
- *Is there a detailed approach for informing customer?*
- *Is the CSC allowed to terminate a contract upon such changes, and are there extra or special conditions associated with such termination?*
- *Is there a timeframe that a CSC must act within to terminate?]*

TR05 - The *Infra. CSP* shall inform the CSC without undue delay if there are permanent changes in its Declaration of Adherence.

[CSP to specify how it will notify affected customers in the event there is a permanent change in the status of its declaration of adherence.]

[Example Checklist (informative):
- *Is there a detailed approach for informing customers?*
- *Does the approach ensure there is no undue delay?]*

2.2 Recommendations

The following recommendations have only to be completed if supported.

2.2.1 Portability Recommendations

From Section 5.2 of the IaaS Code.

DP02 – When exporting CSC Infrastructure Artefacts from a CSC to a cloud service, or between cloud services, the *Infra. CSP* should provide support to facilitate the interoperability between the CSC's capabilities including the user function, administrator function and business function[2] related to the cloud service.

[CSP to specify how it supports interoperability of its user function, administrator function and business function.]
[Example Checklist (informative):
- *How is interoperability of a cloud services user function supported?*
- *How is the interoperability of a cloud services administrator function supported?*
- *How is interoperability of a cloud services business function supported?]*

DP03 – The *Infra. CSP* should provide Application Programing Interfaces related to the cloud service and , if provided, they shall be fully documented. These APIs should enable the transfer of Infrastructure Artefacts between participating parties. If there are any associated code libraries or dependencies they should be documented and made available.

[CSP to specify what APIs are provided to enable the transfer of infrastructure artefacts. Any applicable APIs must be fully documented.
Any separate code libraries or other dependencies necessary to use the APIs must be documented and made available.]
[Example Checklist (informative):
- *List any APIs applicable to the transfer of Infrastructure Artefacts?*

- *For all of the APIs identified, is documentation detailing fully how to use the API, including all relevant prerequisites, methods, parameters and any reliance on separate code libraries been identified?]*

DP04 - The cloud service is not required under this Code to transform the CSC Infrastructure Artefacts where the destination environment requires the Infrastructure Artefacts to be in different formats than that offered by the source environment. Parties may agree otherwise in the CSA.

[CSP to specify if they provide transformation capabilities to convert between formats that a CSC or source/destination cloud service supports and the import/export formats supported by the cloud service. The CSP shall document if supported import formats are not supported for export [and thus will be transformed by the service.]
[Example checklist (informative):

- *If a format is not supported by a cloud service are other capabilities provided to transform the infrastructure artefacts?*
- *Is transformation through a different service (cloud service or otherwise) with different costs?*
- *If transformation capabilities are provided, is it clear to the customer that potential semantic information differences are possible, such as information loss?]*

DP05 – Transfer of CSC Infrastructure Artefacts to and from the cloud service should use open standards and open protocols for Infrastructure Artefacts movement.

[CSP to specify the standards and protocols used to support for transfer of infrastructure artefacts.]
[Example Checklist (informative):

- *What standards are supported for import/export and data transfer?*
- *What protocols are supported for import/export and data transfer?]*

DP07 – The *Infra. CSP* should provide a self-service interface that enables the CSC to carry out periodic retrieval of the CSC's data. This functionality can be subject to contract and may include additional costs.

[CSP to specify any self-service interfaces for data retrieval.
CSP to specify the technical details of such interfaces (For APIs see also DP03)
CSP to specify any contract terms, limitations and costs associated with the self-service interfaces for data retrieval.]
[Example Checklist (informative):

- *Have the self-service interfaces been identified?*

- *Is there documentation available on how to use such interfaces?*
- *Are limitations on the use of such interfaces, such a frequency and bandwidth specified?*
- *Have additional costs been declared?*
- *Does the self-service interface allow customers to periodically retrieve their data?]*