TRIANZ℠

# Cloud Interoperability and Portability Policy

TRIANZ INTERNAL

trianz.com

## Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

## Information Classification

| | |
|---|---|
| ☐ | Public |
| ☒ | Internal |
| ☐ | Confidential |
| ☐ | Restricted |

# Table of Contents

# 1. Purpose

The purpose of this policy is to provide interoperability and portability requirements and guidelines required to be considered for rendering Cloud Service Provider (CSP) Services or consuming the CSP's services as Cloud Service Customer (CSC)

# 2. Objectives

- The objective of Cloud Interoperability & Portability Policy is to facilitate effective implementation and validation of the interoperability & portability of Cloud hosted data.
- Intent of the policy is to ensure transparency for CSC to assess effort required to interoperable with other environments & to achieve portability
- The policy is to support GDPR Free flow of Personal Data & regulation on free flow of non-personal data within EU

# 3. Scope

This policy document covers the Cloud Interoperability & portability requirements where Trianz act as an CSC or CSP.

# 4. Policy Statement

## 4.1 Basic Definitions:

***Interoperability –*** *ability* of two or more systems or applications to exchange information and to mutually use the information that has been exchanged

***Syntactic Interoperability –*** interoperability such that the formats of the exchanged information can be understood by the participating systems

***Semantic Data Interoperability –*** interoperability such that the meaning of the data model within the context of a subject area is understood by the participating systems

***Data Portability –*** ability to port data from one cloud service to another service or between a CSC system to Cloud

***Data Syntactic Portability –*** Data portability using data formats that can be decoded in the target systems

***Data Semantic Portability –*** Data portability such that the meaning of the data model within the context of a subject area is understood by the target systems

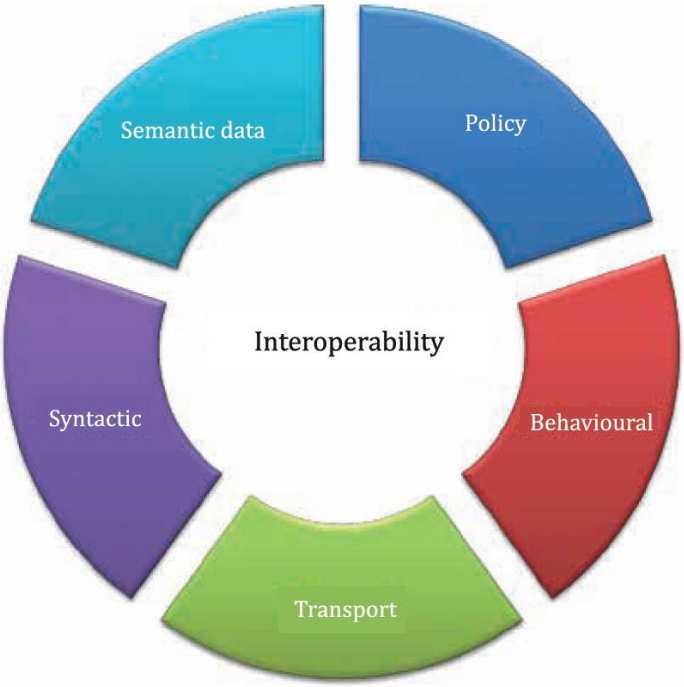
***Application Portability –*** ability to migrate an application from source to target systems between the cloud or from CSC Systems

***Application Instruction Portability –*** Application portability such that the application instruction set executes on the target

***Application Instruction Portability –*** Application portability such that the application metadata is retained and understood on the target

## 4.2 Interoperability:

### 4.2.1 Cloud Interoperability Facets:




Interoperability is not a binary (Yes/No) concept. Interoperability is to be implemented based on number of elements. The interoperability facet model described by ISO/IEC 19941:2017 defines five facets within the context of cloud interoperability. These five facets are transport, syntactic, semantic data, behavioral and policy. Description of each facet including the requirements and examples are detailed in this section.

Trianz Associates who are implementing or evaluating a Cloud solution would need to consider detailed facets during execution

### 4.2.2 Facets of Cloud Interoperability:

Transport interoperability is about common communication infrastructure established to exchange data between systems. Cloud transport interoperability is the transfer mechanism between various cloud computing components, either between CSC components and CSP components or between CSP components of different cloud services. Few examples of the Standard Transport Interoperability protocols are REST based HTTP/S, SOAP, Advanced Message Queuing Protocol (AMQP) and Message Queuing Telemetry Transport (MQTT).

The identified network/transport protocols need to meet industry accepted cryptographically security standards.

### 4.2.3 Syntactic Interoperability:

Syntactic interoperability is the ability of two or more cloud systems or services to understand the structure of exchanged information, which is an encoding of the domain concepts as defined by the semantic data facet. Few examples of encoding syntaxes include JSON, XML and ASN.1.( Abstract Syntax Notation 1) syntaxes

### 4.2.4 Semantic Data Interoperability:

Semantic data interoperability is the ability for the systems exchanging information to understand the meaning of the data model within the context of a subject area.

At the infrastructure level, this concerns virtual machines (VMs), containers, storage and networking concepts and their management.

At the application level, the domain concepts are dictated by the application itself, such as Customer Service Management (CSM), Human Capital Management (HCM), Customer Relationship Management (CRM) etc.,

At the business domain level, semantic data interoperability concerns the ability for discrete domain concepts to be shared and understood between applications. Example approaches include the construction of ontologies using, for example, OWL, and the use of semantic query languages like SPARQL

### 4.2.5 Behavioral Interoperability:

Behavioral interoperability of a cloud service is defined in the service description. The service description includes a declaration of the interface provided by the service which is commonly referred to as an API. The API interface declaration describes the service in terms of a set of operations provided by the service and the inputs and outputs for each operation.

The behavioral interoperability requires additional information to be supplied in terms of the expected results of each operation, including elements such as pre-conditions, post-conditions and any sequences of operations that are necessary for successful use of the API service.

The behavioral interoperability facet abstracts from implementation details and describe the behavior of software components in a representation-independent way.

If the result of an operation against an interface is coherent with the customer expectations for two different cloud services, the cloud services

are considered interoperable, assuming identical policies have been applied.

As an example, if the CSC's current order processing system automatically waits for approval of a submitted order by a listed authority, while a new system assumes that such an order is already approved, the behavior is very different and problems will arise, although both process the same order data otherwise correctly.

CSCs should be enabled to retrieve data programmatically using API like interfaces based on the business requirements and the business agreement with the Service Provider.

### 4.2.6 Policy Interoperability:

Policy interoperability is defined as the ability of two or more systems to interoperate while complying with the legal, organizational and policy frameworks applicable to the participating systems.

This facet concerns governmental laws and regulations by regulatory bodies, CSP and CSC policy terms and conditions and organizational policies covering the interactions.

Policy interoperability includes regulations or policies which relate to specific capabilities of the cloud services. One of the principal capabilities of concern is security.

There can be specific security requirements based on the nature of the data and the processing involved, for example, where credit card information is concerned, the cloud service can be required to meet the requirements of the PCI-DSS standard. There can be more general security requirements demanded by policies of the CSC, such as a requirement for

the cloud service to be certified against a standard such as ISO/IEC 27001 or ISO/IEC 27017.

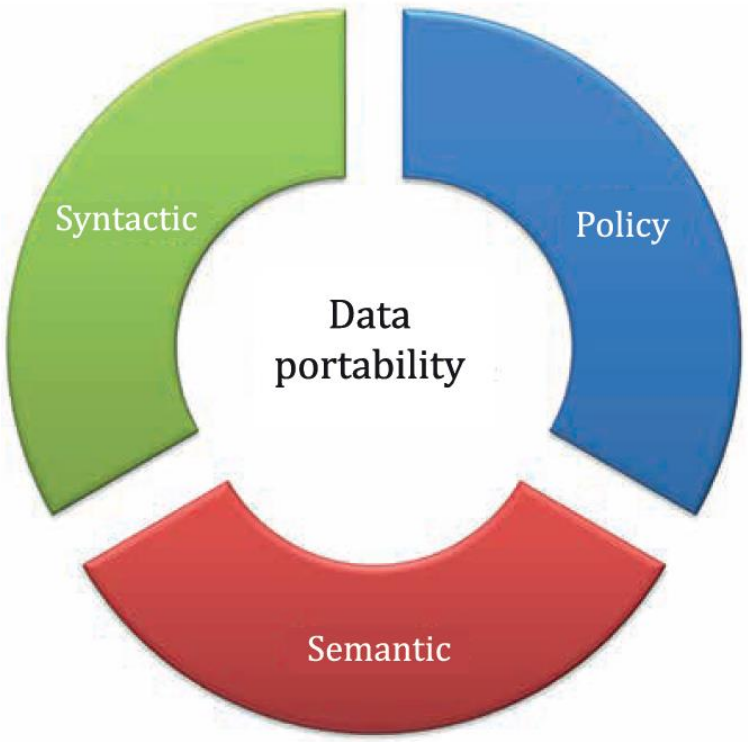
### 4.2.7 Summary of Cloud Interoperability Facts:

| Facets | Purpose | Requirements | Examples |
|---|---|---|---|
| Transport | Data transfer between Systems | Data transfer Protocols | REST based HTTPs, SOAP, MQTT |
| Syntactic | Data in a common understood format | Standardized Data exchange formats | JSON, XML, ASN.1 |
| Semantic | Data in understood data model | Data model common interpretation | OData, OWL |
| Behavioral | Expected outputs on service requests | Behavioral models for the Cloud service | API Pre & Post Conditions, Constraint specifications & UML Models |
| Policy | Assurance that interoperating systems follow | Control for use & access | Customer Security policies, Standards, Cross |

| | | | |
|---|---|---|---|
| | applicable government / regulatory policies | | border data transfer restrictions, PII regulations |

## 4.3 Cloud Data Portability:

### 4.3.1 Cloud Data Portability Facet Model:




Cloud data portability is the ability to transfer data from one cloud service to another cloud service or between a CSC's system to a cloud service using a machine-readable format.

Like interoperability, data portability can be observed from different facets, where each facet focuses on a single dimension. To achieve data portability, all facets need to be understood and mutually agreed upon or sufficiently understood so that it is clear what facet might need attention when porting data.

These facets are called data policy, data syntactic and data semantic as shown in Figure 5. This model is based on the cloud interoperability model in 5.2.1, adapted to focus on the different concerns of cloud data portability.

Trianz Associates who are implementing or evaluating a Cloud solution would need to consider detailed facets during execution. Also, would need to ascertain the contracts between the CSC & CSP is clearly stating the status of the data post termination of the contract which includes standardized data formats, duration until which CSP will hold that data, data deletion policy post contract termination etc.,

### 4.3.2 Data Syntactic Portability:

Data syntactic portability is defined as transferring data from a source system to a target system using data formats that can be decoded on the target system, using a particular syntax for encoding the data, such as XML or encapsulating the data in a packaging format, such as Open Virtualization Format (OVF) or Zip.

### 4.3.3 Data Semantic Portability:

Data semantic portability is defined as transferring data to a target such that the meaning of the data model is understood within the context of a

subject area by the target. A data model (Metadata) expresses the data items, attributes, logical structures and relationships between data items. Data models in a cloud context are dictated by the type of cloud service offering. At the infrastructure level, data models concern VMs, containers, storage and networking metadata. At the application level, the domain concepts and data model will be dictated by the application itself viz., CSM, CRM or ERP.

### 4.3.4 Data Policy Portability:

Data policy portability is defined as the ability to transfer data between a source and a target while complying with the legal, organizational and policy frameworks applicable to the source and target. This includes regulations on data locality, rights to access, use and share data, and mutual responsibilities with respect to security and privacy between a CSP and a CSC.

### 4.3.5 Summary of Cloud Data Portability Facts:

| Facets | Purpose | Requirements | Examples |
|---|---|---|---|
| Data Syntactic | Receive data in structured, commonly used & machine-readable format | Common machine-readable data format | XML, CSV, JSON |
| Data Semantic | Assured meaning of data | Mutually understood ontologies & metadata | OWL, Dublin Core Schema |

| | | | |
|---|---|---|---|
| Data Policy | Adhering to all applicable regulations & organizational polices | Agreed set of applicable regulations & organizational policies | Confidentiality levels, privacy rights & cross border data transfer |

## 4.4 Cloud Application Portability:

### 4.4.1 Cloud Application Portability Facet Model:


Cloud application portability is the ability to migrate an application from one cloud service to another cloud service or between a CSC's system to a cloud service.

The objective is that once ported, the application provides equivalent functionality in the target environment as it did on the source environment.

The five facets of cloud application portability are application syntactic, application instruction, application metadata, application behaviour and application policy.

Trianz Associates who are implementing or evaluating a Cloud solution would need to consider detailed facets during execution.

### 4.4.2 Application Syntactic Portability:

Application syntactic portability is migrating an application from a source system to a target system in a format that can be decoded on the target system. Application artefacts and metadata are structured according to a domain model for applications and are encoded using a particular syntax and packaging format.

### 4.4.3 Application Instruction Portability:

Application instruction portability is migrating an application from a source system to a target system so that its instruction set executes on the target system. Once ported, the software artefacts, orchestration instructions and other scripts that comprise an application need to be executed on an infrastructure that appears to the application as similar to the system for which it was designed. This means ensuring all the necessary interpreters and execution engines are available.

### 4.4.4 Application Metadata Portability:

Application metadata portability is migrating an application from a source system to a target system so that the application metadata is understood on the target system.

The domain model for an application needs to be mutually understood if an application is ported from one system to another.

The domain model for an application typically includes metadata about the application, including what resources the application needs, how it might be configured, initialization data, etc.

### 4.4.5 Application behavior Portability:

Application behaviour portability is migrating an application from a source to a target so that execution on the target produces equivalent results to those produced on the source.

An application ported from one system to another might not exactly exhibit the same behaviour in the target system due to the differences in the execution environment.

This issue might occur if the application is getting ported from legacy to cloud native environment.

### 4.2.1 Application Policy Portability:

Application policy portability is defined as migrating an application from a source system to a target system while complying with the applicable legal, organizational and policy frameworks of both the source and target systems.

Examples of policy portability challenges are lack of payment for the cloud service, lack of a license to run the application in the target system, regulations preventing running an application in a certain geography, etc.

### 4.2.2 Summary of Cloud Application Portability Facts:

| Facets | Purpose | Requirements | Examples |
|---|---|---|---|
| Application Syntactic | Received application in an understandable format | Common packaging format | Zip, tar, jar |
| Application Instruction | Ability to execute application in equivalent manner | Supported runtime environment | Java Runtime, C++, C# |
| Application Metadata | Understanding of environment dependencies for application execution | Shared metadata model | XML, JSON, YAML |
| Application Behavior | Application execution ability to produce expected results | Shared assumptions on environment | Application Test suites |

| | | | |
|---|---|---|---|
| Application Policy | Agreed set of regulatory & organizational policy constraints for application use | Conditions & controls for use & access | Licenses, applicable regulations & enterprise policies |

## 5. Roles & Responsibilities

| Roles | Responsibilities | Internal/External |
|---|---|---|
| Project/Platform/Product Engineering, Cloud, Infra management team | Adhere to the Interoperability & Portability policy based on the Customer/Provider role for the engagement | Internal |
| Product Owner /Project Manager/Operations Manager | Validate the Interoperability & Portability controls are implemented as the policy | Internal |
| InfoSec & Compliance Team | Validate the Interoperability & Portability Process & responsibilities are adhered as per the policy | Internal |

## 6. Applicable Standards

- CCM v4.0
- SWIPO Code of Conduct

- ISO/IEC 19941:2017
- IEEE P2302

## 7. Exception(s)

There is no exception to this policy.

## 8. ISO Control Mapping(s)

| Category of Control | ISO 27001:2022 Control | Document Name as per ISO 27001:2022 |
|---|---|---|
| Organizational Control | 5.23 Information security for use of cloud services | Cloud Interoperability & Portability Policy |

# Document Control

| **Owner:** | CISO | **Release ID:** | IPY-POL-0175 |
|---|---|---|---|

## For Trianz Process Improvement Group (TPIG) Purpose Only

### Version History

| Ver. No. | Date | Author | Reviewer | Approver | Reason for Change | Change Description |
|---|---|---|---|---|---|---|
| 0.1 | 24th Jun 22 | Divya | Balu Nair | Siva N | Initial Version | None |
| 1.0 | 01st July 22 | Divya | Balu Nair | Siva N | Amendments | Changes post peer review |
| 1.0 | 11th Aug 22 | Divya | Balu Nair | Siva N | Approval | Approved and Baselined |
| 1.0 | 25-April-2023 | Krutideepta | Vijaya R | | For Review | Reviewed with no changes |
| 1.1 | 12-May-2023 | Rama Madhavan | Vijaya | | For Review | Migrated to new template |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2.0 | 12-May-2023 | Rama Madhavan | Vijaya | Srikanth M | For approval | Approved and Baselined |
| 2.1 | 15-Feb-24 | Vijaya | Vijaya and Bala | | For Review | Mapped to ISO 27001, 2022 control 5.23 |
| 3.0 | 23-Feb-24 | Vijaya | Vijaya and Bala | Srikanth | For approval | Approved and Baselined |
| 3.1 | 5-May-2025 | Vijaya | Balu | | For Review | Migrated to new template |
| 4.0 | 14-May-2025 | Vijaya | Balu | Srikanth | For approval | Approved and Baselined |

## Contact Information

Name

Email

Phone

# Thank You

infosec@trianz.com