ORACLE

Advisory: Oracle Cloud Infrastructure and PIPEDA

Recommendations for Oracle Cloud Infrastructure Customers Related to the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)

April 2021, Version

Public

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Table of contents

Introduction

The Canadian Personal Information Protection and Electronic Document Act (PIPEDA) "applies to private-sector organizations across Canada that collect, use, or disclose personal information in the course of a commercial activity." Under the act, covered businesses "must follow 10 fair information principles to protect personal information." For more information about PIPEDA, see https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.

This document describes how the features and functionality of Oracle Cloud Infrastructure ("OCI") can help customers ("you") address some of the technical requirements and principles that arise from PIPEDA. It also describes some Oracle practices that might be relevant in your assessment of OCI.

This document does not provide an exhaustive discussion of PIPEDA requirements, nor does it give compliance advice. Generally, Oracle has no insight into the content of the data that you store in OCI or your particular legal requirements for the processing of your data.

The information contained in this document does not constitute legal advice. You should seek your own legal counsel to develop and implement your compliance program and to assess the features and functionality provided by OCI in regard to your specific legal and regulatory requirements.

The following policies and documents are referred to throughout this document:

- Oracle Services Privacy Policy https://www.oracle.com/legal/privacy/services-privacy-policy.html
- Oracle General Privacy Policy: https://www.oracle.com/legal/privacy/privacy-policy.html
- Data Processing Agreement for Oracle Services: https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing

The Cloud Shared Responsibility Model

From a security management perspective, cloud computing is fundamentally different from on-premises computing. On premises, you are in full control of your technology infrastructure; for example, you have physical control of the hardware and full control over the technology stack in production. In the cloud, however, you use components that are under the control of the cloud service provider. As a result, the management of security in the cloud is a shared responsibility between the cloud customer and the cloud service provider.

Oracle Cloud Infrastructure offers best-in-class security technology and operational processes to secure its enterprise cloud services. However, for you to securely run your workloads in OCI, you must be aware of your security and compliance responsibilities. By design, Oracle provides security of cloud infrastructure and operations (cloud operator access controls, infrastructure security patching, and so on). You are responsible for securely configuring your cloud resources. For more information, see https://docs.oracle.com/iaas/Content/Security/Concepts/security_overview.htm.

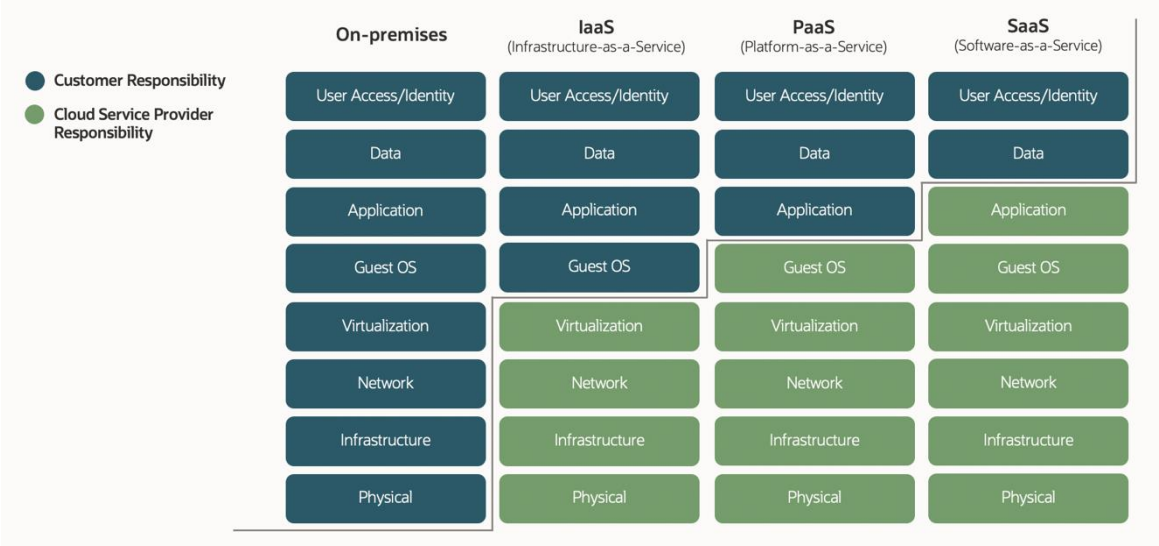

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Customer Data

Generally speaking, Oracle Cloud Infrastructure handles two broad categories of data in its interactions with customers:

- **Data about our customers:** This is the contact and related information needed to operate your OCI account and bill you for services. The use of any personal information that Oracle gathers from you for purposes of account management is governed by the Oracle General Privacy Policy.
- **Data stored by our customers:** This is the data that you store in OCI, such as files, documents, and databases. Your data might include personal information, but Oracle does not have insight into the contents of this data, how you collect or use it, or whether it is subject to any specific data privacy regulations. Oracle's handling of this data is described by the Oracle Services Privacy Policy and the Data Processing Agreement for Oracle Services.

This document provides general information about the features and services available to you for handling the data that you store in OCI services and tenancies and any personal information that it might contain.

Data Privacy Principles

The 10 information principles set forth by PIPEDA are as follows:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure, and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

Accountability

PIPEDA Principle 1: An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.

Oracle does not have insight into the contents of the data that you store in our infrastructure. As a result, you are solely responsible for meeting the "Accountability" principle in PIPEDA.

Identifying Purposes

PIPEDA Principle 2: The purposes for which personal information is being collected must be identified by the organization before or at the time of collection.

Oracle does not have insight into the contents of the data that you store in our infrastructure. As a result, you are solely responsible for meeting the "Identifying Purposes" principle in PIPEDA.

Consent

PIPEDA Principle 3: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

As cloud provider, Oracle does not establish or maintain a relationship with your end users or with other individuals about whom you might store personal data. As such, Oracle does not provide notices to or obtain consent from your end users for you to obtain their personal data. As a result, you are solely responsible for meeting the "Consent" principle in PIPEDA.

Limiting Collection

PIPEDA Principle 4: The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.

Oracle does not have insight into the contents of the data that you store in our infrastructure. As a result, you are solely responsible for meeting the "Limiting Collection" principle in PIPEDA.

Limiting Use, Disclosure, and Retention

PIPEDA Principle 5: Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.

Oracle does not have insight into the content of the data that you store in our infrastructure. As a result, you are solely responsible for meeting the "Limiting Use, Disclosure, and Retention" principle in PIPEDA.

However, Oracle Cloud Infrastructure provides technical features that might help with purpose limitation (compartments and tagging) and data retention and deletion (Object Lifecycle Management).

Compartments

Oracle Cloud Infrastructure gives you the ability to create compartments under your initial root compartment (or tenancy). Your administrators can plan and create compartments in your tenancy to enable you to organize cloud resources (for example, block volumes and compute instances) and the data that they contain so that only specific groups can access them. Compartments can help you organize and isolate your cloud resources in a way that aligns with the data management goal of enforcing the purpose limitation of any personal information to be processed. For example, an enterprise could create one compartment for their human resources department and another for their finance department. This would effectively separate the cloud resources for the two departments, which in turn would help separate their data.

See "Managing Compartments": https://docs.oracle.com/iaas/Content/Identity/Tasks/managingcompartments.htm

Tagging

Oracle Cloud Infrastructure offers a flexible tagging operation to label resources with similar purposes. Your tenancy administrators can plan and implement a resource tagging strategy to help enforce the purposes for which the data you are processing was collected. Tagging can help with the following tasks:

- Enforce specific processing on resources within a tagging group
- Aggregate resources with similar purposes
- Run bulk operations on resources with the same tag

See "Tagging Overview": https://docs.oracle.com/iaas/Content/Tagging/Concepts/taggingoverview.htm

Virtual Cloud Networks

Oracle Cloud Infrastructure enables you to set up virtual cloud networks (VCNs) to allow communication with your attached compute instance resources. These VCNs contain one or more subnets, which are a unit of configuration within a VCN. A subnet can be designated as public (default) or private. Private subnets preclude any compute instance attached to them from having a public IP address. Therefore, those compute instances are not reachable from the internet. All compute instances within the same subnet use the same route table and security lists, which can act as a type of purpose limitation among similar compute instance resources.

You should carefully plan your VCN architecture so that its potential network isolation supports the necessary security and purpose limitation of your data. That isolation can come from either of the following configurations:

- Compute instances in a private subnet that are not reachable from the internet
- Compute instances that share a route table and security list within a common subnet

See "VCNs and Subnets": https://docs.oracle.com/iaas/Content/Network/Tasks/managingVCNs.htm

See "Security Lists": https://docs.oracle.com/iaas/Content/Network/Concepts/securitylists.htm

See "Connectivity Choices": https://docs.oracle.com/iaas/Content/Network/Concepts/overview.htm#connectivity

Object Lifecycle Management

Oracle offers Object Lifecycle Management to help automate the archiving, retention, and deletion of data objects. You can use Object Lifecycle Management to help define the end of life for data objects within the same Object Storage bucket, including whether to archive or delete the objects.

See "Using Object Lifestyle Management":
https://docs.oracle.com/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm

Accuracy

PIPEDA Principle 6: Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.

Oracle does not have insight into the contents of the data that you store in our infrastructure. Oracle has no insight into whether you store personal information and its accuracy with respect to individuals. As a result, you are solely responsible for meeting the "Accuracy" principle in PIPEDA.

However, Oracle Cloud Infrastructure provides technical features that might help you meet this principle. The Object Storage, Block Volume, and File Storage services help you store accurate copies of your data. These data storage options can also be used for business continuity, disaster recovery, and archiving.

- The **Object Storage** service can store unstructured data of any content type. It actively monitors data integrity by using checksums, and automatically detects and repairs corrupt data. Object Storage actively

monitors and ensures data redundancy. If a redundancy loss is detected, then more data copies are created automatically. Archive Storage is another available storage class tier for data objects that must be retained for long periods of time but are rarely accessed.

See "Overview of Object Storage": https://docs.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm

See "Overview of Archive Storage": https://docs.oracle.com/iaas/Content/Archive/Concepts/archivestorageoverview.htm

- The **Block Volume** service lets you use a block volume as a regular hard drive when it is attached and connected to a compute instance. Volumes can also be disconnected and attached to another compute instance without the loss of data. Volumes are automatically replicated to protect against data loss, and can also be backed up.

  See "Overview of Block Volume Backups": https://docs.oracle.com/iaas/Content/Block/Concepts/blockvolumebackups.htm

- The **File Storage** service lets you manage shared file systems and mount targets, and create file system snapshots. It uses synchronous replication and high availability failover for resilient data protection.

  See "Overview of File Storage": https://docs.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm

- **Bare metal and virtual machine database systems** can use Object Storage or local storage for backups. Data Guard can also be used for data protection and availability.

  See "Backing up a Database": https://docs.oracle.com/iaas/Content/Database/Tasks/backingup.htm

  See "Using Oracle Data Guard": https://docs.oracle.com/iaas/Content/Database/Tasks/usingdataguard.htm

- **Exadata Cloud Service** database backups can be managed or unmanaged. Data Guard can also be used for data protection and availability.

  See "Managing Exadata Database Backups": https://docs.oracle.com/iaas/Content/Database/Tasks/exabackingup.htm

  See "Managing Exadata Database Backups by Using bkup_api": https://docs.oracle.com/iaas/Content/Database/Tasks/exabackingupBKUPAPI.htm

  See "Using Oracle Data Guard with Exadata Cloud Service": https://docs.oracle.com/iaas/Content/Database/Tasks/exausingdataguard.htm

Safeguards

PIPEDA Principle 7: Personal information must be protected by appropriate security relative to the sensitivity of the information.

With Oracle Cloud Infrastructure, Oracle provides security of cloud infrastructure and operations (cloud operator access controls, infrastructure security patching, and so on). You are responsible for securely configuring your cloud resources in a way that is appropriate relative to the sensitivity of the information. OCI provides many security services, features, and recommendations. See the following topics:

- "Security Services and Features": https://docs.oracle.com/iaas/Content/Security/Concepts/security_features.htm
- "Security Overview": https://docs.oracle.com/iaas/Content/Security/Concepts/security_overview.htm
- "Oracle Cloud Infrastructure Security Architecture": https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf

- "Oracle Cloud Infrastructure Security Guide": https://docs.oracle.com/iaas/Content/Security/Concepts/security_guide.htm

The following sections discuss some of OCI's security features and principles.

Least Privilege

The least privilege approach requires access on a "need-to-know" basis as one control for protecting personal data. Access control in OCI is based on the concept of least privilege. New resources (for example, block storage volumes or compute instances) are "secure by default," which means that only users in the administrator group are given access when the resource is created. Access for other users must be explicitly given by administrators through the use of policies, groups, and compartments. You can create service-level administrators to further scope administrative access.

See "How Policies Work": https://docs.oracle.com/iaas/Content/Identity/Concepts/policies.htm

See "Create Service-level Admins for Least Privilege": https://docs.oracle.com/iaas/Content/Security/Reference/iam_security.htm#Security_Policy_Examples

Encryption

The encryption described in this section occurs by default regardless of the nature of the underlying data. OCI does not have insight into the nature of your data, whether it is personal data, sensitive data, or otherwise.

- **Block Volume**: Data is encrypted at rest by default, and the backups are also encrypted in Object Storage.

  See "Block Volume Encryption": https://docs.oracle.com/iaas/Content/Block/Concepts/overview.htm#BlockVolumeEncryption

- **Object Storage**: Each object is encrypted with its own key. Encryption is enabled by default.

  See "Object Storage Features": https://docs.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm#features

- **File Storage**: Customer data is encrypted at rest by default.

  See "Encryption": https://docs.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm#encryption

- **Bare metal and Virtual Machine DB Systems**: Encryption of user-created tablespaces is enabled by default using Transparent Data Encryption (TDE).

  See "Transparent Data Encryption": https://docs.oracle.com/iaas/Content/Database/Tasks/configuringDB.htm#Transparent_Data_Encryption

- **Exadata Cloud Service**: All new tablespaces that you create in the Exadata Cloud Service database are encrypted by default.

  See "Managing Tablespace Encryption": https://docs.oracle.com/iaas/Content/Database/Tasks/exaconfiguring.htm#Managing_Tablespace_Encryption

Secure Communications to Existing Customer Networks

OCI gives you two ways to communicate from your VCN to your existing on-premises network:

- **VPN Connect**, also known as IPSec VPN (virtual private network)

  See "VPN Connect": https://docs.oracle.com/iaas/Content/Network/Tasks/managingIPsec.htm

- **FastConnect**, which offers a private connection where traffic does not traverse the internet

See “FastConnect”: https://docs.oracle.com/iaas/Content/Network/Concepts/fastconnect.htm

Vault

The Vault service provides centralized management of the encryption of customer data with keys that you control. It can be used for the following tasks:

- Create master encryption keys and data encryption keys
- Rotate keys to generate new cryptographic material
- Enable or disable keys for use in cryptographic operations
- Assign keys to resources
- Use keys for encryption and decryption to safeguard data

Many services are integrated with the Vault service, including Block Volume, Object Storage, and File Storage.

See “Overview of Vault”: https://docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm

Multi-Factor Authentication

The Identity and Access Management (IAM) service offers multi-factor authentication (MFA) to customers for their user accounts.

See “Managing Multi-Factor Authentication”: https://docs.oracle.com/iaas/Content/Identity/Tasks/usingmfa.htm

Audit

The Audit service logs calls to the OCI public application programming interface (API). Data from logged events can help you safeguard your data by letting you monitor the activity in your tenancy. This logging occurs automatically, and you can set up your audit log retention period.

See “Overview of Audit”: https://docs.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm

See “Setting Audit Log Retention Period”: https://docs.oracle.com/iaas/Content/Audit/Tasks/settingretentionperiod.htm

Cloud Access Security Broker

The Oracle Cloud Access Security Broker (CASB) for OCI monitors the following items and alerts you about detected security issues:

- The security of resources in your tenancy
- Anomalous user behavior
- Other risks

See “Oracle Cloud Access Security Broker”: https://www.oracle.com/security/cloud-security/casb-cloud/

Openness

PIPEDA Principle 8: An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

Oracle does not have insight into the content of the data that you store in our infrastructure. Oracle has no relationship with your end users to inform them about any of your data processing details. As a result, you are solely responsible for meeting the “Openness” principle in PIPEDA.

Note that the Oracle Services Privacy Policy and Data Processing Agreement provide transparency about Oracle’s overall approach to the handling of your data.

Individual Access

PIPEDA Principle 9: Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Oracle does not have insight into the content of the data that you store in our infrastructure. As a result, you are solely responsible for meeting the "Individual Access" principle in PIPEDA.

Challenging Compliance

PIPEDA Principle 10: An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA, usually their Chief Privacy Officer.

Oracle does not have insight into the content of the data that you store in our infrastructure. You are solely accountable for your compliance with PIPEDA. As a result, you are solely responsible for meeting the "Challenging Compliance" principle in PIPEDA.

Other Resources

- Oracle Cloud Compliance: https://www.oracle.com/cloud/cloud-infrastructure-compliance/
- Oracle Cloud Infrastructure documentation: https://docs.oracle.com/iaas/Content/home.htm
- Oracle Cloud Infrastructure Privacy Features: https://docs.oracle.com/iaas/Content/Resources/Assets/whitepapers/oci-privacy-features.pdf
- Oracle Cloud Services Contracts https://www.oracle.com/corporate/contracts/cloud-services/