

Oracle Cloud Infrastructure Privacy and Security Features and PIPEDA

Canadian Personal Information Protection and Electronic Documents Act

ORACLE WHITE PAPER | DECEMBER 2018





Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, functionality, or certification or compliance status and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality, certification or compliance status described for Oracle's products remains at the sole discretion of Oracle.

You can find the most recent versions of the Oracle Cloud Infrastructure white papers at <https://cloud.oracle.com/iaas/technical-resources>.



Table of Contents

Overview	4
Customer Data	4
Principles	5
Accountability	5
Identifying Purposes	6
Consent	6
Limiting Collection	6
Limiting Use, Disclosure, and Retention	6
Accuracy	7
Safeguards	8
Openness	11
Individual Access	11
Challenging Compliance	12
Certifications and Third-Party Audit Reports	12
Oracle Cloud Infrastructure Resources	12
Other Resources	12



Overview

The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) is a data privacy law in Canada that applies to many organizations based in Canada that collect and process the personal information of individuals.

This paper describes how features and functionality of Oracle Cloud Infrastructure can help our Canadian customers comply with PIPEDA principles. This paper 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 you store in Oracle Cloud Infrastructure or your particular legal requirements for the processing of your data. This paper is not legal advice and customers are advised to seek their own legal counsel to develop and implement their privacy compliance program and to assess the features and functionality provided by Oracle Cloud Infrastructure in regards to their legal and regulatory requirements.

Oracle Cloud Infrastructure is an infrastructure as a service (IaaS) product in which responsibility for data security and data privacy is shared between Oracle Cloud Infrastructure and customers (for more details about security, see the [Oracle Cloud Infrastructure Security white paper](#)).

Customer Data

Generally speaking, Oracle Cloud Infrastructure may handle two broad categories of data in the context of its interactions with its customers:

- **Data about our customers:** This is the information needed to operate your Oracle Cloud Infrastructure 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 the Oracle Cloud Infrastructure, such as files, documents, and databases. Your data might include personal information, but Oracle does not have insight into the contents of this data or how you collect or use it, nor whether it is subject to Canadian or any other specific data privacy regulations. Additionally, it is important to note that Oracle does not have a direct relationship with your end users—the individuals that you might collect personal information from. You manage this data, make decisions about its processing, and decide in which [region](#) it is stored. Oracle's handling of this data is described by the [Oracle Services Privacy Policy](#) and the [Data Processing Agreement](#).

This paper focuses on the data that our customers store in the Oracle Cloud Infrastructure and any personal information that it might contain.



Principles

PIPEDA sets out 10 [fair information principles](#) that organizations must adhere to:


- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, and Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

The following sections outline how Oracle Cloud Infrastructure customers can take advantage of product features to help them align with these principles when using Oracle Cloud Infrastructure services. This paper also explains how Oracle and its customers may share the responsibilities for these principles.

Accountability

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. [PIPEDA Principle 1](#)

- The Oracle Services Privacy Policy explains that a Global Data Protection Officer has been appointed to field inquiries about any privacy matter such as Oracle Cloud Infrastructure's compliance with Oracle's obligations as a processor of your customer data.
- All Oracle customers have several options to resolve their privacy concerns in regards to Oracle's obligations. Oracle Cloud Infrastructure complies with the [Oracle Services Privacy Policy](#), which provides the following information:
 - Explains how to contact Oracle's Global Data Protection Officer about any privacy compliance matter
 - Points to a data privacy Inquiry form
 - Outlines a privacy and security dispute resolution process

- 
- The [Data Processing Agreement](#) between Oracle and its customers describes Oracle's data protection practices and indicates that Oracle requires its Affiliates and any third-party subprocessors to adhere to such practices.

Identifying Purposes

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

- As cloud provider, Oracle generally has no insight into your purposes for collecting personal data from individuals.

Consent

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

- As cloud provider, Oracle does not establish or maintain a relationship with your end users or with other individuals about whom you may store personal data. As such, Oracle does not provide notices to or obtain consents from your end users for you to obtain their personal data.

Limiting Collection


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. [PIPEDA Principle 4](#)

- As cloud provider, Oracle generally has no insight into the personal information that you may collect from your end users and process in Oracle Cloud Infrastructure, or for what purposes it was collected.

Limiting Use, Disclosure, and Retention

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. [PIPEDA Principle 5](#)

- As cloud provider, Oracle generally has no insight into your purposes for collecting personal data from individuals. However, Oracle Cloud Infrastructure has features that



may help customers with purpose limitation (tagging) and data retention and deletion (Object Lifecycle Management).

Tagging

Oracle offers a flexible [tagging](#) operation for their customers. Tagging can help you label and aggregate resources (even across [compartments](#)) with similar purposes and run bulk processing on those resource groups. Your tenancy administrators can plan and implement a resource tagging strategy that may help enforce the purposes for which the data you are processing was collected.

Object Lifecycle Management

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


Accuracy

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. [PIPEDA Principle 6](#)

- As cloud provider, Oracle generally has no insight into whether you store personal information and its accuracy with respect to individuals. However, Oracle Cloud Infrastructure offers the Object Storage, Block Volume, and File Storage services to help you store accurate copies of your data. These data storage options can also be used for business continuity, disaster recovery, and archiving. Regardless of the data storage services that you select, you always choose which [region or regions](#) to store your data in.

Data Storage

- The [Object Storage service](#) allows you to store unstructured data of many content types. Object Storage actively monitors data integrity by using checksums to automatically detect and repair corrupt data. Object Storage actively monitors for data redundancy. If a redundancy loss is detected, Object Storage automatically creates additional data copies.
- The [Block Volume service](#) allows a block volume to be used 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 help protect against data loss, and can also be backed up if the customer chooses.

- 
- The [File Storage service](#) allows you to manage shared file systems, mount targets, and create file system snapshots. The File Storage service uses [synchronous replication and high availability failover](#) for resilient data protection.

Safeguards

Personal information must be protected by appropriate security relative to the sensitivity of the information.

[PIPEDA Principle 7](#)

- Oracle Cloud Infrastructure has received ISO 27001 audits and SOC 1 and SOC2 reports (see [Oracle Cloud Compliance](#)). Some of the security-related features offered in Oracle Cloud Infrastructure are discussed in the following sections.

Least Privilege

The least privilege approach requires access on a “need-to-know” basis as one control for protecting personal data. Access control in Oracle Cloud Infrastructure is based on the concept of least privilege. New resources (for example, block storage volumes or compute instances) are “secure by default”—only users in the administrator group are initially given access when the resource is created. Access for other users must be explicitly given by your administrators by use of [policies](#). Your cloud administrators must take explicit actions, by use of these policies, to expand access to those who “need to know.”

Encryption

Note: The encryption described in this section occurs regardless of the nature of the underlying data. Oracle Cloud Infrastructure does not have insight into the nature of the customer’s data, whether it is personal data, sensitive data, or otherwise.

Encryption may be used as one method to help protect data. Data encryption is provided with the Block Volume, Object Storage, and File Storage services by default, regardless the type of data stored.

- [Block Volume service encryption](#): Block Volume storage is encrypted at rest by default, and the backups are also encrypted in Object Storage.
- [Object Storage service encryption](#): Each object is encrypted with its own key. Encryption is enabled by default.
- [File Storage service encryption](#): Customer data is encrypted at rest by default.



Compartments

Oracle Cloud Infrastructure offers the ability to [create compartments](#) in your [tenancy](#). Compartments 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. Your administrators can plan and create compartments in your tenancy. This planning should organize cloud resources in a way that aligns with your data-management goals and can help enforce the purpose limitation of any personal information to be processed.

Virtual Cloud Networks

Oracle Cloud Infrastructure customers can set up [virtual cloud networks](#) (VCNs) to allow communication with their 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 may act as a type of purpose limitation among similar compute instance resources.

You must carefully plan your VCN architecture so that its potential network isolation supports the necessary security and purpose limitation of your data, whether that isolation comes from either of the following configurations:

- Compute instances in a private subnet that are not reachable from the Internet
- Compute instances that share the same route table and [security list](#) within a common subnet

Secure Communications to Existing Customer Networks

Oracle Cloud Infrastructure gives you two ways to communicate from your VCN in Oracle Cloud Infrastructure to an existing on-premises network:

- [IPSec VPN](#)
- [FastConnect](#), which offers a private connection where traffic does not traverse the Internet

You can follow the steps outlined in the [Access to Your On-Premises Network](#) documentation to set up an IPSec VPN or FastConnect connection from an on-premises network to your VCN in Oracle Cloud Infrastructure.



Key Management Service

Oracle Cloud Infrastructure [Key Management](#) provides centralized management of the encryption of customer data with keys that you control. It can be used to 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, and use keys for encryption and decryption to safeguard data.

Multi-Factor Authentication

Oracle Cloud Infrastructure customers can use multi-factor authentication (MFA) through the [Oracle Identity Cloud Service \(IDCS\)](#) to further safeguard accounts (customer tenancies are now automatically federated with IDCS). For details, see [IAM Federation](#) and [Identity Providers and Federation](#).

Audit

The [Audit service](#) logs calls to the Oracle Cloud Infrastructure public application programming interface (API). Data from logged events can help you safeguard your data by enabling you to monitor activity within your tenancy. This logging occurs automatically and you can set up the [Audit log retention period](#).


Database Security

Specific security recommendations for managing your Oracle Cloud Infrastructure Database instances can be found in the [Securing Database documentation](#). Those recommendations include using the following tools:

- Transparent Data Encryption (TDE) and the Oracle Key Vault
- Database Security Assessment Tool (DBSAT)
- Audit Vault and Database Firewall (AVDF)

The Oracle Database Security Guides (available through the [Oracle Database Documentation portal](#)) explain how to use the following features to help enforce the access and privacy of your data in the Oracle databases that you choose to run in Oracle Cloud Infrastructure:

- Virtual Private Database (VPD) enables you to create security policies or group policies to control database access at the row and column level. It allows multiple users to access a single schema while preventing them from accessing data which is not relevant to them.
- Oracle Label Security (OLS) controls access to the contents of a row by comparing that row's label with a user's label and privileges. It provides the ability to define data



classification labels to match specific business and compliance requirements like controlling access to sensitive data.

- [Data Masking and Subsetting](#) enables entire copies or subsets of data to be extracted from an Oracle database, its sensitive data discovered and obfuscated, and then shared with partners inside and outside of the business or used for testing in non-production environments.

Cloud Access Security Broker

The [Oracle Cloud Access Security Broker \(CASB\)](#) for Oracle Cloud Infrastructure monitors the following items and alerts you about detected security issues:

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

Openness


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

- The [Oracle Services Privacy Policy](#) and [Data Processing Agreement](#) provide transparency about Oracle's overall approach to the handling of your data. However, as cloud provider, Oracle generally has no insight into data that you store and process in Oracle Cloud Infrastructure or whether it is personal data that belongs to a particular end user. Oracle has no relationship with your end users to inform them about any of your data processing details.

Individual Access

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. [PIPEDA Principle 9](#)

- As cloud provider, Oracle generally has no insight into what personal information is collected from your individual end users and processed in Oracle Cloud Infrastructure. However, the [Data Processing Agreement](#) describes assistance Oracle may be able to provide in instances where the Oracle Cloud Infrastructure service does not provide you with the necessary access.



Challenging Compliance

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. [PIPEDA Principle 10](#)

- Oracle Cloud Infrastructure complies with the [Oracle Services Privacy Policy](#), which provides the following information:
 - Explains how to contact Oracle's Global Data Protection Officer about any privacy compliance matter
 - Points to a data privacy Inquiry form
 - Outlines a privacy and security dispute resolution process

Certifications and Third-Party Audit Reports

Oracle has successfully completed the following audits for Oracle Cloud Infrastructure:

- ISO/IEC 27001:2013
- Service Organization Control: SOC 1 and SOC 2
- PCI-DSS
- Assessment for relevant HIPAA controls

See [Oracle Cloud Compliance](#) for details.

Oracle Cloud Infrastructure Resources

- [Oracle Cloud Infrastructure documentation](#)
- [Oracle Cloud Infrastructure and the European Union General Data Protection Regulation white paper](#)
- [Oracle Cloud Infrastructure Security white paper](#)
- [Other Oracle Cloud Infrastructure technical white papers](#)

Other Resources

- [Privacy at Oracle](#)
- [Oracle Cloud Services Contracts](#)




Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

 blogs.oracle.com/oracle

 facebook.com/oracle

 twitter.com/oracle

 oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 1218

Oracle Cloud Infrastructure Security and Privacy Features and PIPEDA
December 2018



Oracle is committed to developing practices and products that help protect the environment.