Advisory: Oracle Cloud Infrastructure and the South African Protection of Personal Information Act, 2013

Partial Descriptions of Oracle Cloud Infrastructure Security Practices in the Context of the Protection of Personal Information Act (POPIA), 2013, General Conditions of Lawful Processing of Personal Information in Chapter 3, Part A

January 2023, version 1.1

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 assessing your use of Oracle Cloud services in the context of the requirements applicable to you under the Protection of Personal Information Act (POPIA), 2013, general conditions of lawful processing of personal information in Chapter 3, Part A. This document might also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document, which is not intended and may not be used as legal advice about the content, interpretation, or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

The general conditions of lawful processing of personal information in Chapter 3, Part A of the Protection of Personal Information Act (POPIA), 2013 are subject to periodic changes or revisions by the Information Regulator (South Africa). The current version is available at popia.co.za/protection-of-personal-information-act-popia/chapter-3-2/.

This document is based on information available at the time of drafting. It is subject to change at the sole discretion of Oracle Corporation and might not always reflect changes in the regulations.

Revision History

The following revisions have been made to this document.

DATE	REVISION
January 2023	Updated
November 2021	Initial publication

Table of Contents

Introduction

The Protection of Personal Information Act (POPIA) is a South African law intended to “promote the protection of personal information processed by public and private bodies.” POPIA sets general conditions for public and private entities to lawfully process South African data subjects’ personal information. For more information, see popia.co.za/act/.

Document Purpose

This document is intended to provide relevant information related to Oracle Cloud Infrastructure (OCI) to assist you in determining the suitability of using OCI in relation to POPIA’s eight conditions for lawful processing of personal information in general (Chapter 3, Part A). For more information about these conditions, see popia.co.za/protection-of-personal-information-act-popia/chapter-3-2/chapter-3/.

The information contained in this document doesn’t constitute legal advice. Customers are advised to seek their own legal counsel to develop and implement their compliance program and to assess the features and functionality provided by Oracle regarding their specific legal and regulatory requirements.

About Oracle Cloud Infrastructure

Oracle’s mission is to help customers see data in new ways, discover insights, and unlock possibilities. Oracle provides several cloud solutions tailored to customers’ needs. These solutions provide the benefits of the cloud, which is designed to run all your workloads in global, secure, and high-performance environments. The cloud offerings discussed in this document include OCI.

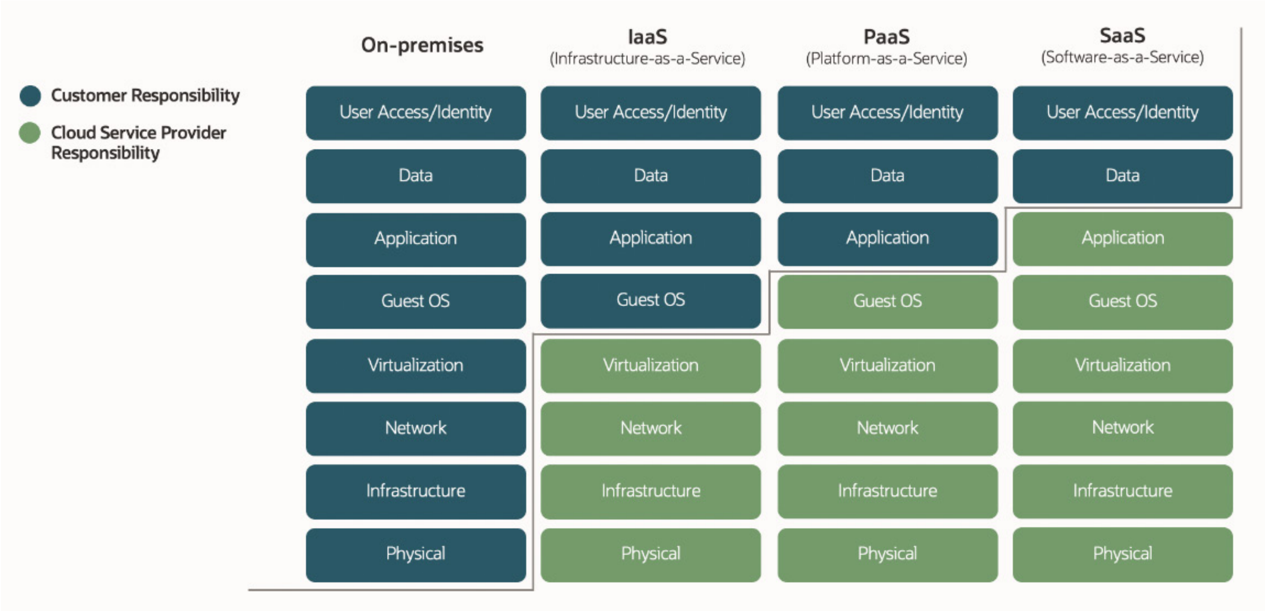
OCI is a set of complementary cloud services that enable you to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI offers high-performance computing capabilities and storage capacity in a flexible overlay virtual network that is easily accessible from an on-premises network. OCI also delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI, see docs.oracle.com/en-us/iaas/Content/home.htm.

The Cloud Shared Management Model

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

Oracle provides best-in-class security technology and operational processes to secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in Oracle cloud services. By design, Oracle provides security functions for cloud infrastructure and operations, such as cloud operator access controls and infrastructure security patching. Customers are responsible for securely configuring and using their cloud resources. For more information, see the cloud service documentation.

The following figure illustrates this division of responsibility at a high level.


● Customer Responsibility
● Cloud Service Provider Responsibility

On-premises	IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
User Access/Identity	User Access/Identity	User Access/Identity	User Access/Identity
Data	Data	Data	Data
Application	Application	Application	Application
Guest OS	Guest OS	Guest OS	Guest OS
Virtualization	Virtualization	Virtualization	Virtualization
Network	Network	Network	Network
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

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

Summary of the Eight General Conditions for Lawful Processing of Personal Information in Chapter 3, Part A

This section summarizes the eight conditions for the lawful processing of personal information in general in Chapter 3, Part A of POPIA and describes OCI operational and security practices and services in the context of the conditions.

Condition 1: Accountability

> "The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself."

As a cloud provider, Oracle generally has no insight into the data that you store and process in OCI, nor whether it constitutes the minimum necessary to accomplish the purpose agreed to with your end users. Any assessment of whether the minimum amount of data was collected from your end users is your responsibility.

You decide for what purposes your data is processed. Your own customers are the end users of the applications that you create (*end users* are also referred to as *data subjects* or *individuals*). You manage any personal information that you collect, decide how it will be processed, and decide which data center region stores it. You are solely responsible for determining the suitability of a cloud service in the context of this requirement.

OCI provides many features and functions that can help you meet this requirement, as outlined throughout this paper.

Condition 2: Processing Limitation

"Personal information must be processed— (a) lawfully; and (b) in a reasonable manner that does not infringe the privacy of the data subject."

Oracle customers are responsible for their own personal information collection and processing practices, including when customers use Oracle products or services to process their personal information. As a cloud provider, Oracle generally has no insight into the data that you store and process in OCI, nor whether it constitutes the minimum necessary to accomplish the purpose agreed to with your end users. An assessment of your compliance with applicable laws and of whether the minimum amount of data was collected from your end users is your responsibility. You are solely responsible for determining the suitability of a cloud service in the context of this requirement.

However, OCI provides the Data Catalog service, which might help you meet this requirement. Data Catalog is a metadata management service that helps data professionals discover data and support data governance. Designed specifically to work in the Oracle ecosystem, it provides an inventory of assets, a business glossary, and a common metastore for data lakes. This service provides more insight into data with the glossary and enrichments to improve trust in data in the Oracle ecosystem. For more information, see docs.oracle.com/iaas/data-catalog/home.htm.

Condition 3: Purpose Specification

"…records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed…

"The destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form."

As a cloud provider, Oracle generally has no insight into the data that you store and process in OCI, nor whether it constitutes the minimum necessary to accomplish the purpose agreed to with your end users. Any assessment of whether the minimum amount of data was collected, retained, or destroyed on behalf of your end users is for you to determine. You are solely responsible for determining the suitability of a cloud service in the context of this requirement.

If you determine that your data must be deleted, OCI provides deletion capability in all its data storage services. For more information about each service, see the following resources:

- **Block Volume**: "Deleting a Volume" at docs.cloud.oracle.com/iaas/Content/Block/Tasks/deletingavolume.htm
- **Object Storage**: "To delete objects" at docs.cloud.oracle.com/iaas/Content/Object/Tasks/managingobjects.htm
- **File Storage**: "To delete a file system" at docs.cloud.oracle.com/iaas/Content/File/Tasks/managingfilesystems.htm

Oracle also offers Object Lifecycle Management to help automate the archiving and deletion of data objects. See docs.cloud.oracle.com/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm.

Condition 4: Further Processing Limitation

“Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of section 13 [Collection for a specific purpose].”

As a cloud provider, Oracle generally has no insight into the data that you store and process in OCI, nor whether it is processed in accordance with the purpose for which it was collected. Any assessment of whether the minimum amount of data was collected from your end users is for you to determine.

Oracle processes your data only at your request and uses it only for the purposes specified in your agreement with Oracle. You are solely responsible for determining the suitability of a cloud service in the context of this requirement.

However, OCI provides the following features and functions that might help you meet this requirement:

- **Tagging** lets you add metadata to resources, which enables you to define keys and values and associate them with resources. You can use tags to organize and list resources based on your business needs. For more information, see docs.cloud.oracle.com/iaas/Content/Tagging/Concepts/taggingoverview.htm.
- **Compartments** let you organize and isolate your cloud resources in a way that aligns with your data management goals of enforcing the purpose limitation of any personal information to be processed. For more information, see docs.oracle.com/iaas/Content/Identity/Tasks/managingcompartments.htm.
- **Virtual cloud networks** (VCNs) are virtual, private networks that you set up in Oracle data centers. You can plan your VCN architecture so that its potential network isolation supports the necessary security and purpose limitation of your data. For more information, see docs.cloud.oracle.com/iaas/Content/GSG/Tasks/creatingnetwork.htm.

Condition 5: Information Quality

“(1) A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

“(2) In taking the steps referred to in subsection (1), the responsible party must have regard to the purpose for which personal information is collected or further processed.”

As a cloud provider, Oracle generally has no insight into the data that you store and process in OCI, nor whether it is complete, accurate, or misleading, or updated where necessary. An assessment of whether the minimum amount of data was collected from your end users is your responsibility. You are solely responsible for determining the suitability of a cloud service in the context of this requirement.

However, Oracle provides the following features and functions that might help you in meet these requirements:

- **Block Volume** lets you use a block volume as a regular hard drive when it’s attached and connected to a compute instance. Volumes can be disconnected and attached to another compute instance without the loss of data. Data durability is enhanced by automatically replicating volumes to help protect against data loss. Data is encrypted at rest by default, and the backups are also encrypted in Object Storage. For more information, see docs.cloud.oracle.com/iaas/Content/Block/Concepts/overview.htm.
- **Object Storage** lets you store unstructured data of many content types. Object Storage is a regional service that stores data redundantly across multiple storage servers and multiple availability domains. Encryption is enabled by default, with each object encrypted with its own key. It’s a fully programmable, scalable, and durable cloud storage service. For more information, see docs.oracle.com/iaas/Content/Object/home.htm.

- **File Storage** lets you manage shared file systems, mount targets, and create file system snapshots. File Storage uses synchronous replication and high availability failover for resilient data protection. For more information, see docs.cloud.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm.
- **Archive Storage** is another available storage class tier for data objects that must be retained for long periods of time but are rarely accessed. For more information, see docs.cloud.oracle.com/iaas/Content/Archive/Concepts/archivestorageoverview.htm.

Condition 6: Openness

> "A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act."
>
> "(1) If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of— (a) the information being collected and where the information is not collected from the data subject, the source from which it is collected; (b) the name and address of the responsible party; (c) the purpose for which the information is being collected; (d) whether or not the supply of the information by that data subject is voluntary or mandatory…"

As a cloud provider, Oracle generally has no insight into the data that you store and process in OCI, or whether it's personal data that belongs to a particular end user. In this context, Oracle has no relationship with your end users and doesn't inform them about any of your data processing details. It is your responsibility to be transparent with your end users about how their data is processed. You are solely responsible for determining the suitability of a cloud service in the context of this requirement.

The Oracle Services Privacy Policy and the Data Processing Agreement for Oracle Services describe Oracle's overall approach to the handling of your data, which might help you meet this requirement. For more information about Oracle's contracts and policies, see the Privacy Policies section at oracle.com/corporate/contracts/data-services/privacy-policies.html and Data Processing Agreement at oracle.com/be/corporate/contracts/cloud-services/contracts.html#data-processing.

Condition 7: Security Safeguards

> "A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent— (a) loss of, damage to or unauthorised destruction of personal information; and (b) unlawful access to or processing of personal information."

You are solely responsible for determining the suitability of a cloud service in the context of this requirement and ensuring that your use of the cloud service and business processes meet these requirements.

Oracle provides the following features and functions that might help you meet these requirements:

- **Cloud Guard** is a cloud native service that is designed to help customers monitor, identify, achieve, and maintain a strong security posture on OCI. Use the service to examine your OCI resources for security weakness related to configuration, and your OCI operators and users for insecure activities. Upon detection, Cloud Guard can suggest, assist with, or take corrective actions, based on your configuration. For more information, see docs.oracle.com/iaas/cloud-guard/home.htm.
- **Vulnerability Scanning** helps improve your security posture by routinely checking your cloud resources for potential security risks. The service generates reports with metrics and details about these vulnerabilities. For more information, see docs.oracle.com/iaas/scanning/home.htm.

To learn about the security services in OCI that provide customer isolation, identity management, authorization, data encryption, vulnerability detection, and monitoring, see docs.oracle.com/iaas/Content/Security/Concepts/security_features.htm.

Condition 8: Data Subject Participation

> "A data subject, having provided adequate proof of identity, has the right to— (a) request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and (b) request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information…"

As a cloud provider, Oracle generally has no insight into what personal information you collect from your data subjects (end users) and process in OCI. You control access to your "Services Personal Information" (as defined in the Oracle Services Privacy Policy) by your end users, and your end users should direct any requests related to their Services Personal Information to you. You are solely responsible for determining the suitability of a cloud service in the context of this requirement.

However, the "Privacy Inquiries and Requests from Individuals" section in the Data Processing Agreement for Oracle Services describes the assistance that Oracle might be able to provide you to handle data subject requests, such as requests to access, delete, erase, restrict, rectify, receive and transmit (data portability), block access to, or object to processing of specific personal information.

Oracle provides the following features and functions that might help you meet these requirements:

- **Tagging** lets you add metadata to resources, which enables you to define keys and values and associate them with resources. You can use the tags to organize and list resources based on your business needs. For more information, see docs.cloud.oracle.com/iaas/Content/Tagging/Concepts/taggingoverview.htm.
- **Object Lifecycle Management** can help automate the archiving and deletion of data objects. For more information, see docs.cloud.oracle.com/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm.

Conclusion

Oracle is committed to helping customers operate in a fast-changing global business environment and address the challenges of local privacy regulations. The capabilities and features of Oracle Cloud Infrastructure can help organizations that operate in South Africa meet their business and compliance objectives.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle