

Advisory: Privacy Features of Oracle Cloud Infrastructure

How Oracle Cloud Infrastructure Helps Customers
Align with Common Data Privacy Principles

November 2021, version 2.1
Copyright © 2021, Oracle and/or its affiliates
Public

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document is not part of your 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 assessing your use of Oracle cloud services in the context of the requirements applicable to you under various privacy frameworks. This may 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 as the information in this document 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.

This document does not make any 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.

Table of Contents

Introduction	4
Document Purpose	4
About Oracle Cloud Infrastructure	4
The Cloud Shared Management Model	4
Roles	5
Customer Data	5
Data Privacy Principles	6
Transparency—Openness	6
Data Minimization—Collection Limitation	6
Purpose Specification—Notice and Consent	7
Purpose Limitation	7
Accuracy—Data Quality	8
Availability	8
Security Safeguards	10
Sensitive Information	10
Breach Notification—Incident Response	11
Least Privilege	12
Storage Limitation	12
Data Subject (End User) Requests	13
Cross-Border Data Transfers	13
Subprocessors	13
Privacy Officer	13
Oracle Cloud Infrastructure Compliance	13
Other Resources	14
Conclusion	14

Introduction

Many jurisdictions around the world have implemented data privacy regulations. Examples of such regulations are the European Union General Data Protection Regulation (GDPR), the Australian Data Privacy Act, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the Japan Act on the Protection of Personal Information, and the South Korean Personal Information Protection Act (PIPA). These regulations define rules for the collection and processing of the personal information of individuals.

Document Purpose

This paper describes how the features and functionality of Oracle Cloud Infrastructure (OCI) can help you address some of the requirements that arise from data privacy regulations found across the world.

The information contained in this document does not constitute legal advice. 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 OCI in regard to their legal and regulatory requirements.

The following policies and documents are referenced throughout this paper:

- Oracle Services Privacy Policy at oracle.com/legal/privacy/services-privacy-policy.html
- Oracle General Privacy Policy at oracle.com/legal/privacy/privacy-policy.html
- Data Processing Agreement for Oracle Services (DPA) at oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing

About Oracle Cloud Infrastructure

Oracle Cloud Infrastructure (OCI) is a set of collaborative cloud services that enable you to build and run a 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 your on-premises network. OCI offers platform as a service (PaaS) and infrastructure as a service (IaaS) that delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI services, see docs.oracle.com/en-us/iaas/Content/home.htm.

OCI continues to invest in features and services that can help our customers more efficiently address their security and compliance needs. For more information about how OCI services and features can help with your compliance and reporting requirements, see oracle.com/cloud/compliance/.

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 partially under the management 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 its 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, infrastructure security patching, and so on. Customers are responsible for securely configuring and using their cloud resources. For more information, see oracle.com/security.

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

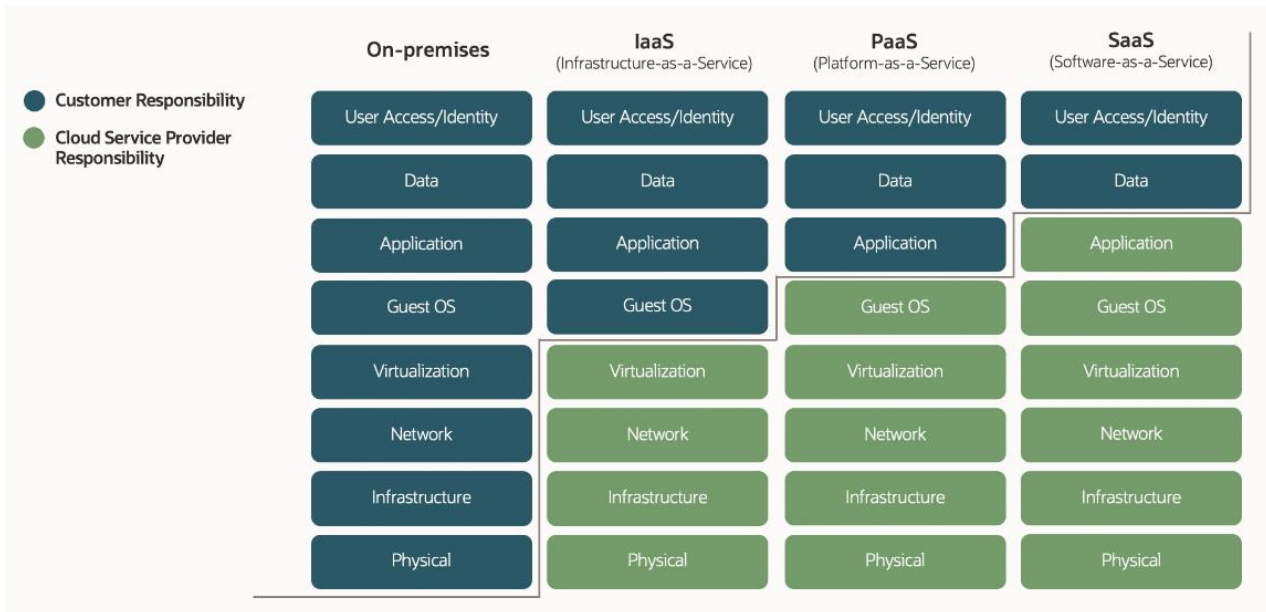


Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Roles

As a cloud service vendor that hosts personal information on behalf of our customers, Oracle takes on the role of a *processor*. Processors carry out the instructions of the *controller*. You, our direct customers who build applications by using the features and functionality of OCI, typically assume the role of controller. As controller, you decide for what purposes your data is processed. Your own customers are the *end users* of the applications that you create. In many situations, your end users are also referred to as *data subjects* or *individuals*.

Data subjects (end users) ↔ Controller (Oracle customer) ↔ Processor (Oracle)

Within the context of the service, Oracle does not have a direct relationship with your end users or data subjects—the individuals whose personal information you might process. You manage any personal information that you collect, decide how it's processed, and decide which data center region stores it.

OCI is an infrastructure as a service (IaaS) product in which responsibility for data security and data privacy is shared between Oracle and its customers.

Customer Data

Generally speaking, OCI handles two broad categories of data in its interactions with customers:

- **Data about our customers:** 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:** 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's 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 paper provides general information about the features and services available to Oracle customers for the handling of the data that they store in their OCI services and tenancies and any personal information that the data might contain.

Data Privacy Principles

The following sections outline how OCI customers can use the features of the service to help them comply with many key data privacy principles. The sections also explain how Oracle and its customers share the responsibilities for these principles. The definitions provided at the beginning of each section are from the IAPP Glossary of Privacy Terms at iapp.org/resources/glossary/.

Transparency—Openness

Transparency: Taking appropriate measures to provide any information relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language.

Transparency of Processing

The Oracle Services Privacy Policy and Data Processing Agreement for Oracle Services provide transparency about Oracle's overall approach to the handling of your data. However, as 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 individual. In this context, Oracle has no relationship with your end users and therefore does not inform them about any of your data processing details. Only you can be transparent to your end users about how the data is processed.

Location Transparency

OCI is transparent about where your data is processed and stored. This transparency is important because some data privacy regulations define requirements for cross-border data transfers. When setting up your account, you choose a *home region* in which to initially locate your *tenancy*. Your data stays within that region unless you choose to move it outside the region. OCI offers powerful services that might operate cross-tenancy or cross-region. Through the Oracle Cloud Console user interface and API documentation, you will always be informed when your actions might cause data to move to another region or tenancy. Depending on the terms of your agreements with Oracle, Oracle may process data globally to fulfill the services.

See Regions and Availability Domains at docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htm and Setting Up Your Tenancy at docs.cloud.oracle.com/iaas/Content/GSG/Concepts/settinguptenancy.htm.

Data Localization

Data localization laws, also known as data residency laws, may require certain categories of data to be stored in a specific country. Familiarize yourself with the requirements of the data localization laws or regulations that may apply to your data, and then determine what steps you must take to comply.

Oracle generally has no insight into the data that you store and process in OCI or whether it falls in categories covered by data localization laws. The location transparency described in the previous section may help with data localization because you always know the geographic location of your data in OCI. Oracle continues to open new data center regions in countries around the world, which allows more of its customers to store their data within their own country.

See Oracle Cloud Infrastructure Data Center Regions at oracle.com/cloud/architecture-and-regions.html.

Data Minimization—Collection Limitation

Data minimization principle: The idea that one should only collect and retain that personal data which is necessary.

As cloud provider, Oracle generally has no insight into the data that you store and process in OCI or 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.

Purpose Specification—Notice and Consent

Purpose specification: The purposes for which personal data are collected should be specified no later than at the time of data collection.

As cloud provider, Oracle generally has no insight into the data that you store and process in OCI or 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.

Purpose Limitation

Purpose limitation: The purposes for which personal data are collected should be specified no later than at the time of data collection and the subsequent use of that personal data is limited to the fulfillment of those purposes.

You remain the controller at all times. Oracle processes your data only at your request and uses it for no purposes other than those specified in your agreement with Oracle.

As cloud provider, Oracle generally has no insight into data that you store and process in OCI, why it was collected, or whether it's being processed beyond any purpose that you have communicated to your end users. However, OCI has the following features designed to help you effectively manage purpose limitation.

Tagging

Oracle offers a flexible tagging operation to 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 to help enforce the purposes for which the data you are processing was collected.

See Tagging Overview at docs.cloud.oracle.com/iaas/Content/Tagging/Concepts/taggingoverview.htm.

Compartments

Oracle 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. These features can help 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 example, an enterprise could create one compartment for their human resources department and another compartment for the finance department. Doing so would effectively separate the cloud resources, which in turn would help keep separate the data, for the two departments.

See Managing Compartments at docs.cloud.oracle.com/iaas/Content/Identity/Tasks/managingcompartments.htm.

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 might act as a type of purpose limitation among similar compute instance resources.

You can 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 a route table and security list within a common subnet

See the following OCI Networking documentation pages for more about VCNs:

- Creating a Virtual Cloud Network at docs.cloud.oracle.com/iaas/Content/GSG/Tasks/creatingnetwork.htm
- VCNs and Subnets at docs.cloud.oracle.com/iaas/Content/Network/Tasks/managingVCNs.htm
- Security Lists at docs.cloud.oracle.com/iaas/Content/Network/Concepts/securitylists.htm

Accuracy—Data Quality

Accuracy: Organizations must take every reasonable step to ensure the data processed is accurate and, where necessary, kept up to date.

As cloud provider, Oracle generally has no insight into whether you store personal information or its accuracy regarding individuals. However, OCI offers the Object Storage, Block Volume, and File Storage services to help you store accurate copies of your data.

- **Object Storage** lets you store unstructured data of many content types. Object Storage is a regional service in which data is stored redundantly across multiple storage servers and multiple availability domains. It actively monitors technical data integrity by using checksums that automatically detect and repair damaged data. Object Storage actively monitors and provides data redundancy. If a redundancy loss is detected, Object Storage automatically creates more data copies. **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 at

docs.cloud.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm and Overview of Archive Storage at docs.cloud.oracle.com/iaas/Content/Archive/Concepts/archivestorageoverview.htm.

- **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.

See Overview of Block Volume at docs.cloud.oracle.com/iaas/Content/Block/Concepts/overview.htm.

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

See Overview of File Storage at

docs.cloud.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm.

Availability

Availability: Data is “available” if it is accessible when needed by the organization or data subject.

The following OCI features help with data availability.

Availability Domains and Fault Domains

Your tenancy is created in the available home region of your choice. Many OCI regions are composed of physically isolated and fault-tolerant availability domains. You can use these availability domains to build replicated systems.

Fault domains are a grouping of hardware and infrastructure within an availability domain. You can optionally specify the fault domain for a new compute instance when it's created. This allows you to distribute your compute instances so that they aren't on the same physical hardware within a single availability domain.

See Fault Domains at docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htm#fault and Editing the Fault Domain for an Instance at docs.cloud.oracle.com/iaas/Content/Compute/Tasks/edit-fault-domain.htm.

Backups

The following flexible data storage backup options are available:

- **Block Volume:** Block Volume backups can be manual or scheduled, incremental or full. Cross-region backups can be used for business continuity, disaster recovery, and application migration and expansion. Policy-based backups have different backup frequencies and retention periods. These backups are encrypted in Object Storage.

See Overview of Block Volume Backups at

docs.cloud.oracle.com/iaas/Content/Block/Concepts/blockvolumebackups.htm.

- **Object Storage:** Object Storage replication aids in disaster recovery efforts, and addresses data redundancy compliance requirements. Copies of objects can be made to other buckets in the same region or across regions.

See Using Replication at docs.cloud.oracle.com/iaas/Content/Object/Tasks/usingreplication.htm and

Copying Objects at docs.cloud.oracle.com/iaas/Content/Object/Tasks/copyingobjects.htm.

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

See Backing Up a Database (Bare Metal/VM) at

docs.cloud.oracle.com/iaas/Content/Database/Tasks/backingup.htm and Using Oracle Data Guard (Bare Metal/VM) at docs.cloud.oracle.com/iaas/Content/Database/Tasks/usingdataguard.htm.

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

See the following resources:

- Managing Exadata Database Backups (Oracle-managed) at docs.cloud.oracle.com/iaas/Content/Database/Tasks/exabackingup.htm
- Managing Exadata Database Backups by Using bkup_api at docs.cloud.oracle.com/iaas/Content/Database/Tasks/exabackingupBKUPAPI.htm
- Using Oracle Data Guard with Exadata Cloud Service at docs.cloud.oracle.com/iaas/Content/Database/Tasks/exausingdataguard.htm

Learn more about high-availability solutions for OCI at docs.oracle.com/en/solutions/design-ha.

Security Safeguards

Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

You, the customer, are responsible for securing your workloads and securely configuring services (such as compute, network, storage, and database). See Shared Security Model at docs.cloud.oracle.com/iaas/Content/Security/Concepts/security_overview.htm#Shared_Security_Model.

OCI's many security services, features, and recommended practices are documented in the following resources:

- Security Services and Features at docs.cloud.oracle.com/iaas/Content/Security/Concepts/security_features.htm
- Oracle Cloud Infrastructure Security Architecture at oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf
- Security Best Practices at docs.cloud.oracle.com/iaas/Content/Security/Reference/configuration_security.htm

Sensitive Information

Sensitive personal information: Data which is more significantly related to the notion of a reasonable expectation of privacy, such as medical or financial information.

As cloud provider, Oracle generally has no insight into the data that you store and process in OCI or whether it's sensitive information. Any assessment of whether data contains sensitive information and must undergo special processing is left for you to determine. Such an assessment should include an evaluation of whether a particular service and or region is suitable for your workload and data. However, Oracle offers encryption capabilities and a key management service to help protect your data including, where appropriate, sensitive data.

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's 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 at docs.cloud.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 at docs.cloud.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm#features.
- **File Storage:** Customer data is encrypted at rest by default.
See Encryption (File Storage) at docs.cloud.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm#encryption.
- **Bare metal and virtual machine database systems:** Encryption of user-created tablespaces is enabled by default using Transparent Data Encryption (TDE).
See Transparent Data Encryption (Bare Metal/VM DB) at docs.cloud.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 (Exadata) at docs.cloud.oracle.com/iaas/Content/Database/Tasks/exaconfiguring.htm#Managing_Tablespace_Encryption.

Vault

The Vault key management 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

The **Block Volume**, **Object Storage**, **File Storage**, and **Streaming** services integrate with Vault to support the encryption of data in those services. The integration of Vault with Identity and Access Management (IAM) lets you control who and what services have access to your keys. The Audit service (see the next section) lets you track administrative actions on your keys and vaults.

See Overview of Vault at docs.cloud.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.

Breach Notification—Incident Response

Breach disclosure: The requirement that an organization notify regulators and/or victims of incidents affecting the confidentiality and security of personal data.

Oracle evaluates and responds to any event when Oracle suspects that Oracle-managed customer data has been improperly handled or accessed. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents.

If Oracle determines that a confirmed security incident involving personal information processed by Oracle has occurred, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts or suspected incidents is confidential to Oracle and is not shared externally. Incident history is also confidential to Oracle and is not shared externally. As a controller, you must determine whether any of your end users or regulators must be notified of a personal information breach.

You are responsible for incident and personal information breach detection within the security environment that you control. For example, OCI can't detect whether a user's login to a customer's tenancy was unauthorized.

Cloud Guard and the **Audit** service (see the next section) can help you monitor the environment that you have set up in OCI. You may want to implement other monitoring software, depending on the functionality that you have implemented on the OCI platform.

See Cloud Guard at docs.cloud.oracle.com/iaas/cloud-guard/using/index.htm.

Audit

The Audit service logs calls to the OCI public application programming interface (API), whether those calls originate from the Console, SDK, or command line interface (CLI). Audit log contents include the activity that occurred, the user who initiated it, the date and time of the request, the source IP address, the user agent, and the HTTP headers of the request. Data from these logged events can help you safeguard your data by enabling you to monitor the activity within your tenancy. This logging occurs automatically, and you can set up the Audit log retention period.

See Overview of Audit at docs.cloud.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm and Setting Audit Log Retention Period at docs.cloud.oracle.com/iaas/Content/Audit/Tasks/settingretentionperiod.htm.

Least Privilege

Least privilege: A security control where access is granted at the lowest possible level required to perform the function.

Access control in OCI is based on the concept of least privilege. New resources (for example, block volumes or compute instances) are restricted by default, which means that only users in the administrator group are initially given access to them. Only administrators can give resource access to other users, through existing or new policies, groups, and compartments. Policies only *allow* access to resources in a customer tenancy; they can't deny it.

See Getting Started with Policies at docs.cloud.oracle.com/iaas/Content/Identity/Concepts/policygetstarted.htm.

Storage Limitation

Storage limitation: The principle that personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

As cloud provider, Oracle generally has no insight into the data that you store and process in OCI, whether the purposes for processing that data have passed, or whether the data needs to be deleted. If you determine that your data must be deleted, OCI offers services designed to permanently delete data.

Data Deletion

OCI provides deletion capability in all its data storage services. For more information about each service, see the following resources:

- **Block Volume:** See Deleting A Volume at docs.cloud.oracle.com/iaas/Content/Block/Tasks/deletingavolume.htm.
- **Object Storage:** See Deleting an Object at docs.cloud.oracle.com/iaas/Content/Object/Tasks/managingobjects.htm#To_delete_an_object and To Delete a Bucket at docs.cloud.oracle.com/iaas/Content/Object/Tasks/managingbuckets.htm.
- **Compute instances and NVMe storage:** See Terminating an Instance at docs.cloud.oracle.com/iaas/Content/Compute/Tasks/terminatinginstance.htm.
- **File Storage:** See To Delete a File System at docs.cloud.oracle.com/iaas/Content/File/Tasks/managingfilesystems.htm.

Object Lifecycle Management

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

Service Termination

If you terminate your OCI service subscription, Oracle makes your data that resides in the production cloud services environment available for you to retrieve. After the retrieval period, your data will be deleted. Details about this retrieval period are described in section 6, "Oracle Cloud Suspension and Termination Policy," of the Oracle Cloud Hosting and Delivery Policies at oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html#hd.

Data Subject (End User) Requests

Data subject: An identified or identifiable natural person.

As cloud provider, Oracle generally has no insight into what personal information you collect from your data subjects (end users) and process in OCI. 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 or erase, restrict, rectify, receive, transmit (data portability), block access to, or object to processing of specific personal information.

Cross-Border Data Transfers

Cross-border data transfers: The transmission of personal information from one jurisdiction to another.

The “Cross-Border Data Transfers” section in the Data Processing Agreement for Oracle Services and “Cross-Border Data Transfers – Oracle Processor Code” section in its European DPA Addendum explain the data transfer mechanisms that Oracle has put in place to support processing that involves transferring data across country borders.

Subprocessors

Outsourcing: Contracting business processes, which may include the processing of personal information, to a third party.

The “Oracle Affiliates and Third Party Subprocessors” section in the Data Processing Agreement for Oracle Services explains that Oracle requires its affiliates and any third-party subprocessors to adhere to Oracle’s data protection practices. The “Notice and Objection Right to New Oracle Affiliates and Third Party Subprocessors” section in the agreement’s European DPA Addendum explains how customers can view lists of the Oracle affiliates and third-party subprocessors that might process personal information to assist in the performance of the OCI services.

Privacy Officer

Privacy officer: A general term in many organizations for the head of privacy compliance and operations.

OCI is subject to the Oracle Services Privacy Policy, which explains that a Global Data Protection Officer has been appointed to field inquiries about any privacy matter. The policy also provides the following information:

- How to contact Oracle’s Global Data Protection Officer
- A data privacy inquiry form
- A privacy and security practices dispute resolution process

Oracle Cloud Infrastructure Compliance

Oracle is committed to helping customers operate globally in a fast-changing business environment and address the challenges of an increasingly complex regulatory environment. To that end, Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification for one or more of its services in the form of “attestations.” These attestations can assist in your compliance and reporting, providing independent assessment of the security, privacy, and compliance controls of the applicable Oracle Cloud services.

Also, Oracle provides general information and technical recommendations for the use of its cloud services in the form of “advisories.” These advisories are provided to help you determine the suitability of using specific Oracle Cloud services and to help you implement specific technical controls that may help you meet your compliance obligations.

For more information, see the Oracle Cloud Compliance site at oracle.com/cloud/compliance.

Other Resources

- Oracle Cloud Infrastructure documentation at docs.cloud.oracle.com/iaas/Content/GSG/Concepts/baremetalintro.htm
- Oracle Services Privacy Policy at oracle.com/legal/privacy/services-privacy-policy.html
- Oracle Cloud Services Contracts at oracle.com/corporate/contracts/cloud-services/

Conclusion

Oracle Cloud Infrastructure offers autonomous operations, integrated security, and truly elastic, serverless services in Oracle’s global public cloud regions or within your data center. Oracle Cloud Infrastructure provides several built-in security and privacy features that help organizations implement the technical controls required to operate under various regulatory frameworks.

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

Copyright © 2021, 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. 0120