



Oracle Cloud Infrastructure Privacy Features



How Oracle Cloud Infrastructure helps customers align with
common data privacy principles

October 26, 2020 | Version 1.1
Copyright © 2020, 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 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.

Table of Contents	
Overview	3
Roles	3
Customer Data	3
Data Privacy Principles	4
Transparency - Openness	4
Data Minimization – Collection Limitation	5
Purpose Specification – Notice and Consent	5
Purpose Limitation	5
Accuracy—Data Quality	6
Availability	7
Security Safeguards	8
Sensitive Information	8
Breach Notification—Incident Response	9
Least Privilege	10
Storage Limitation	10
Data Subject (End User) Requests	11
Cross-Border Data Transfers	11
Subprocessors	11
Privacy Officer	11
Internationally Recognized Third-Party Attestations	12
Other Resources	13

OVERVIEW

Many jurisdictions around the world have regulations that govern the collection and use of personal information of individuals, such as the European 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. This paper describes how the features and functionality of Oracle Cloud Infrastructure (OCI) can help you address some of the requirements that arise from these and other data privacy regulations.

The information contained in this paper 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 Oracle Cloud Infrastructure in regards to their legal and regulatory requirements.

NOTE - The following policies and documents are referenced throughout this paper:

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

ROLES

As a cloud service vendor hosting 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 Oracle Cloud Infrastructure, 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; end users are often referred to as data subjects or individuals.

End users or data subjects ↔ Controller (Oracle customer) ↔ Processor (Oracle)

Note that within the context of the service, Oracle does not have a direct relationship with your end users—the individuals that you might collect personal information from. You manage any personal information that you collect, make decisions about its processing, and decide in which data center region it is stored.

Oracle Cloud Infrastructure 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, 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 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 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, 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 paper focuses only on providing general information about features and services available to our customers for the

handling of the data that our customers store in the Oracle Cloud Infrastructure services and tenancies and any personal information that it might contain.

DATA PRIVACY PRINCIPLES

The following sections outline how Oracle Cloud Infrastructure 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 <https://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 Oracle Cloud Infrastructure, or whether it is personal data that belongs to a particular end user. 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 their data is processed.

Location Transparency

Oracle Cloud Infrastructure is transparent about where your data is processed and stored. This is important because some data privacy regulations lay down 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. Oracle Cloud Infrastructure offers powerful services that might operate cross-tenancy or cross-region. Through the Oracle Cloud Infrastructure Console user interface and API documentation, you will always be made aware 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 <https://docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htm>, and Setting Up Your Tenancy at <https://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. Only you can take steps to familiarize yourself with the requirements of the data localization laws or regulations which 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 Oracle Cloud Infrastructure, 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 will always know the geographic location of your data in Oracle Cloud Infrastructure. Oracle continues to open new **data center regions** in countries around the world which will allow more of its customers to store their data within their own country.

See Oracle Cloud Infrastructure Data Center Regions at <https://www.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 Oracle Cloud Infrastructure, 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 the customer's 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 Oracle Cloud Infrastructure, 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 left for you to determine.

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 Oracle Cloud Infrastructure, why it was collected, or whether it is being processed beyond any purpose that you have communicated to your end users. However, Oracle Cloud Infrastructure has the following features designed to help customers 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 <https://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 a compartment for their human resources department, and another for the finance department. This would effectively separate the cloud resources, which in turn would help keep separate the data, for the two departments.

See Managing Compartments at

<https://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 the same route table and security list within a common subnet

See the following OCI networking-related websites for more about VCNs:

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

- **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 across multiple availability domains. It actively monitors technical data integrity using checksums intended to automatically detect and repair damaged data. Object Storage actively monitors and provides data redundancy. If a redundancy loss is detected, Object Storage is designed to automatically create 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

<https://docs.cloud.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm>, and

Overview of Archive Storage at

<https://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 is 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 <https://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

<https://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 Oracle Cloud Infrastructure features help with data availability:

Availability Domains and Fault Domains

A customer's tenancy is created in the available home region of their choice. Many Oracle Cloud Infrastructure regions are composed of physically isolated and fault-tolerant availability domains. Customers 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 at launch time. This allows you to distribute your compute instances so that they are not on the same physical hardware within a single availability domain.

See Fault Domains at <https://docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htm#fault>, and Editing the Fault Domain for an Instance at <https://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

<https://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 (Object Storage) Replication at

<https://docs.cloud.oracle.com/iaas/Content/Object/Tasks/usingreplication.htm>, and

Copying Objects at <https://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, see . Data Guard can also be used for data protection and availability.

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

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/backingup.htm>, and

Using Oracle Data Guard (Bare Metal/VM) at

<https://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 Managing Exadata Database Backups (Oracle-managed) at

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/exabackingup.htm>,

Managing Exadata Database Backups by Using bkup_api at

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/exabackingupBKUPAPI.htm>, and

Using Oracle Data Guard with Exadata Cloud Service at

<https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/exausingdataguard.htm>.

Learn more about high-availability solutions for Oracle Cloud Infrastructure at:

<https://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.

Shared Responsibility

Security in Oracle Cloud Infrastructure is a shared responsibility between you and Oracle:

- Oracle is responsible for the security of the underlying cloud infrastructure (such as data center facilities, and hardware and software systems). See Oracle Corporate Security Practices at <https://www.oracle.com/corporate/security-practices/>.
- 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 https://docs.cloud.oracle.com/iaas/Content/Security/Concepts/security_overview.htm#Shared_Security_Model.

Security Services, Features and Best Practices

Oracle Cloud Infrastructure's many security services, features, and best practices are documented in

- Security Services and Features at https://docs.cloud.oracle.com/iaas/Content/Security/Concepts/security_features.htm,
- Oracle Cloud Infrastructure Security Architecture white paper at <https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf>, and
- Security Best Practices at https://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 Oracle Cloud Infrastructure or whether it is sensitive information. Any assessment of whether data contains sensitive information and must undergo special processing is left for you to determine and should include an evaluation of whether a particular service and or region is suitable for your workload and data. However, Oracle provides encryption 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. Oracle Cloud Infrastructure 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 at

<https://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

<https://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

<https://docs.cloud.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm#encryption>.

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

See Transparent Data Encryption (Bare Metal/VM DB) at

https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/configuringDB.htm#Transparent_Data_Encryption

- **Exadata Cloud Service:** All new tablespaces created by the customer in the Exadata Cloud Service database are encrypted by default.

See Managing Tablespace Encryption (Exadata) at

https://docs.cloud.oracle.com/iaas/Content/Database/Tasks/exaconfiguring.htm#Managing_Tablespace_Encryption.

Vault

Oracle Cloud Infrastructure 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

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 lets you control who and what services have access to your keys. The Audit service (see next section) lets you track administrative actions on your keys and vaults.

See Overview of Vault at <https://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 Cloud Infrastructure has incident response mechanisms and processes in place designed to detect and respond to (potential) security incidents within the security environment that we implement. Oracle notifies you, the customer, if a security incident was confirmed to have led to a personal information breach, following the terms described in the "Incident Management and Breach Notification" section of the Data Processing Agreement for Oracle Cloud Services.

As a controller, it is left for you to determine whether any of your end users or regulators must be notified of a personal information breach.

Customers may have responsibilities for incident and personal information breach detection within the security environment that they control. For example, Oracle Cloud Infrastructure cannot detect whether a user's login to a customer's tenancy was unauthorized. **Cloud Guard** and the **Audit service** (see the following section) can help you monitor the environment that you have set up in the Oracle Cloud Infrastructure. You might want to implement other monitoring software, depending on the functionality that you have implemented on the Oracle Cloud Infrastructure platform.

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

Audit Service

The Audit service logs calls to the Oracle Cloud Infrastructure public application programming interface (API), whether those calls originate from the console UI, 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 activity within your tenancy. This logging occurs automatically, and you can set up the Audit log retention period.

See Overview of Audit at <https://docs.cloud.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm>, and Setting Audit Log Retention Period at <https://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 Oracle Cloud Infrastructure 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. Resource access for other users can only be given by administrators through existing or new **policies, groups, and compartments**. Policies only allow access; they cannot deny it.

See Getting Started with Policies at <https://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 Oracle Cloud Infrastructure, whether the purposes for processing that data have passed, nor whether the data needs to be deleted. If you determine that your data must be deleted, Oracle Cloud Infrastructure offers services designed to permanently delete data.

Data Deletion

Oracle Cloud Infrastructure 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 <https://docs.cloud.oracle.com/iaas/Content/Block/Tasks/deletingavolume.htm>
- **Object Storage:** See Deleting an Object at https://docs.cloud.oracle.com/iaas/Content/Object/Tasks/managingobjects.htm#To_delete_an_object, and

To Delete a Bucket at <https://docs.cloud.oracle.com/iaas/Content/Object/Tasks/managingbuckets.htm>

- **Compute instances and NVMe storage:** See Terminating an Instance at <https://docs.cloud.oracle.com/iaas/Content/Compute/Tasks/terminatinginstance.htm>
- **File Storage:** See To Delete a File System at <https://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 Lifecycle Management at <https://docs.cloud.oracle.com/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm>.

Service Termination

If you terminate your Oracle Cloud Infrastructure service subscription, Oracle will make your data, residing 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,” see Oracle Cloud Hosting and Delivery Policies at <https://www.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 Oracle Cloud Infrastructure. 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 and 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 (DPA) and “Cross-Border Data Transfers - Oracle Processor Code” 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 (DPA) 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 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 Oracle Cloud Infrastructure services.

Privacy Officer

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

Oracle Cloud Infrastructure 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

INTERNATIONALLY RECOGNIZED THIRD-PARTY ATTESTATIONS

Oracle Cloud Infrastructure engages independent auditors and assessors to test and provide opinions about security, confidentiality, and availability controls that are relevant to data protection laws, regulations, and industry standards.

- Ernst & Young CertifyPoint BV (EYCP) audits Oracle Cloud Infrastructure's Information Security Management System (ISMS) and has issued an ISO/IEC 27001:2013 certificate. In addition, EYCP has issued an ISO/IEC 27017:2015 certificate addressing information security controls for cloud services and an ISO/IEC 27018:2014 certificate addressing relevant aspects of protection for personally identifiable information (PII) in public clouds acting as PII processors. Oracle Cloud Infrastructure's scope for its ISMS is global in nature for both services and regions. Newly deployed services and regions are brought into the ISMS scope upon deployment and are audited by EYCP within our 6 months audit cadence, producing certificate updates by June and December each year.
- Ernst & Young LLP examines Oracle Cloud Infrastructure in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements 18 (SSAE 18) and the International Auditing and Assurance Standards Board (IAASB) International Standard on Assurance Engagements 3000 (ISAE 3000), and issues a System and Organization Control 2 (SOC 2) Type 2 report covering AICPA Trust Services Criteria for controls relevant to security, confidentiality, and availability. Oracle Cloud Infrastructure's scope under these assurance programs is global in nature for both services and regions. Newly deployed services and regions are aligned with the appropriate security, confidentiality, and availability requirements upon deployment and are audited by Ernst & Young LLP within our 6 months audit cadence, producing assurance reports by June and December each year.
- In addition, Ernst & Young LLP examines Oracle Cloud Infrastructure in accordance with ISAE 3000 and issues a report addressing relevant criteria found in the Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Controls Catalog (C5). Oracle Cloud Infrastructure's scope under these assurance programs is global in nature for both services and regions. Newly deployed services and regions are aligned with the appropriate C5 requirements upon deployment and are audited by Ernst & Young LLP within our 6 months audit cadence, producing assurance reports by June and December each year.
- Schellman & Company LLC assesses Oracle Cloud Infrastructure as a Level 1 service provider in accordance with the Payment Card Industry Data Security Standard (PCI DSS). Oracle Cloud Infrastructure's PCI DSS Attestation of Compliance (AOC) covers all 12 PCI DSS requirements in relation to in-scope infrastructure as a service (IaaS). Oracle Cloud Infrastructure's scope under PCI is global in nature for both services and regions. Newly deployed services and regions are meet all applicable PCI DSS requirements upon deployment and are audited by Schellman & Company LLC within our 6 months audit cadence, producing an AOC by June and December each year.
- Secarma Ltd. performed an independent assessment of Oracle Cloud Infrastructure's cybersecurity practices and issued a Cyber Essentials Plus certificate. The scope of this certificate covers the services and regions within the United Kingdom.

OTHER RESOURCES

- Oracle Cloud Infrastructure Documentation: <https://docs.cloud.oracle.com/iaas/Content/GSG/Concepts/baremetalintro.htm>
- Oracle Services Privacy Policy: <https://www.oracle.com/legal/privacy/services-privacy-policy.html>
- Oracle Cloud Services Contracts: <https://www.oracle.com/corporate/contracts/cloud-services/>

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 © 2020, 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

Oracle Cloud Infrastructure Privacy Features
October, 2020
Author: Jim Feltis

