ORACLE
Cloud Infrastructure

Oracle Cloud Infrastructure Privacy Features

ORACLE WHITE PAPER | OCTOBER 2019

ORACLE

Disclaimer

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

You can find the most recent versions of the Oracle Cloud Infrastructure white papers at https://docs.cloud.oracle.com/iaas/Content/General/Reference/aqswhitepapers.htm.

Table of Contents

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 can help you address some of the requirements that arise from these 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.

Roles

As a cloud service vendor handling 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 (for details about security, see the Oracle Cloud Infrastructure Security white paper).

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 the latter category—data that our customers store in the Oracle Cloud Infrastructure 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.

All of the definitions provided in this section are from the IAPP Glossary of Privacy Terms.

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.

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 left for you to determine.

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 does not establish or maintain a relationship with your end users or other individuals about whom you might store personal information. As such, Oracle does not give notice to your end users about the purposes for which their personal data might be collected, nor does Oracle obtain consent from your end users that allows you to process their personal information. Any notice or consent requirements related to your use of Oracle Cloud Infrastructure are for you to determine and address.

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 with 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.

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. This planning 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.

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

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.

Backups

The following flexible data storage backup options are available:

- Block Volume backups: 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.
- Copies of objects in Object Storage: Copies of objects can be made to other buckets in the same region or across regions.
- Exadata DB System backup: You can back up your Exadata database to Object Storage.
- Bare metal and virtual machine DB backup: You can back up to Object Storage or local storage.

For more information about the high-availability solutions in the following Oracle Cloud Infrastructure services, see the Best Practices for Deploying High Availability Architecture on Oracle Cloud Infrastructure white paper:

- Compute, Storage, Database
- Networking (VCNs, FastConnect, and IPSec VPN)
- Load Balancing

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, File Storage, and Database 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.
- 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. Volumes are automatically replicated to help protect against data loss, and can also be backed up.
- 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.
- Oracle Data Guard lets you replicate standby databases for your Oracle Cloud Infrastructure bare metal and virtual machine DB systems.

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.

Security Compliance

Oracle Cloud Infrastructure security controls have been assessed by the following audits and reports:

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

For details, see the Oracle Cloud Compliance web page.

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).
- You, the customer, are responsible for securing your workloads and securely configuring services (such as compute, network, storage, and database).

Security Services and Features

Oracle Cloud Infrastructure's many security services and features are documented online and in the Oracle Cloud Infrastructure Security white paper.

Security Practices

Oracle Cloud Infrastructure security practices are explained online and in the Oracle Cloud Infrastructure Security white paper.

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 encryption: Block Volume storage is encrypted at rest by default, and the backups are also encrypted in Object Storage.
- Object Storage encryption: Each object is encrypted with its own key. Encryption is enabled by default.
- File Storage encryption: Customer data is encrypted at rest by default.
- Bare metal and virtual machine DB system encryption: Encryption is enabled by default by using Transparent Data Encryption (TDE).

Key Management Service

Oracle Cloud Infrastructure Key Management provides centralized management of the encryption of customer data with keys that you control. It can be used 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 and Object Storage both integrate with Key Management to let you control who and what services have access to your data. The Audit service lets you track administrative actions on your keys and vaults.

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 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. 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.

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.

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. Policies only allow access; they cannot deny it.

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:

- Deleting block volumes
- Deleting an object from an Object Storage bucket
- Deleting Object Storage buckets
- Deleting Compute instances and NVMe storage
- Deleting a file system in File Storage

Object Lifecycle Management

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

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,” in the Oracle Cloud Hosting and Delivery Policies.

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.

The Oracle Services Privacy Policy explains that a Global Data Protection Officer has been appointed to field inquiries about any privacy matter. All Oracle customers have several options for

resolving their privacy concerns in regards to Oracle's obligations. Oracle Cloud Infrastructure is subject to the Oracle Services Privacy Policy, which provides the following information:

- Explains how to contact Oracle's Global Data Protection Officer
- Points to a data privacy inquiry form
- Outlines a privacy and security dispute resolution process

Internationally Recognized Third-Party Assurance

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. The scope of these certificates is global.
- 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. The scope of this attestation is global.
- 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). The scope of this attestation is global.
- 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). The scope of the AOC is global.
- 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 United Kingdom.

Oracle Cloud Infrastructure Resources

- Oracle Cloud Infrastructure service documentation
- Oracle Cloud Infrastructure and the European Union General Data Protection Regulation
- Oracle Cloud Infrastructure white papers

Other Oracle Resources

- Oracle Cloud Compliance
- Privacy at Oracle
- Oracle Cloud Services Contracts

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services

Oracle Cloud Infrastructure Privacy Features
October 2019