ORACLE

Advisory: Oracle Cloud Infrastructure and the General Data Protection Regulation (GDPR)

How Oracle Cloud Infrastructure Helps Customers Align with GDPR Principles

July 2023, Version 1.4

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 assessing your use of Oracle cloud services in the context of the requirements applicable to you under the General Data Protection Regulation (GDPR). This information 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 on in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remain at the sole discretion of Oracle.

The General Data Protection Regulation (GDPR) is subject to periodic changes or revisions by the European Commission. The current version of the GDPR is available at ec.europa.eu/info/law/law-topic/data-protection_en. This document is based on information available at the time of drafting. It is subject to change at the discretion of Oracle and may not always reflect changes in the regulations.

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**

Lawfulness, Fairness and Transparency 6

Purpose Limitation 7

Data Minimization 8

Accuracy 8

Storage Limitation 10

Integrity and Confidentiality 10

Conclusion **12**

Additional Resources **12**

Introduction

The European Union (EU) General Data Protection Regulation (GDPR) applies broadly to entities based in the EU and elsewhere that collect and process the personal information of individuals in the EU. This document explains how the features and functionality of Oracle Cloud Infrastructure (OCI) can assist you in assessing your use of Oracle cloud services in the context of the requirements applicable to you under the GDPR. This document doesn't provide an exhaustive discussion of the GDPR requirements, nor does it give legal or compliance advice. Customers are advised to seek their own legal counsel to develop and implement their GDPR compliance program in relation to cloud services and to assess the features and functionality provided by Oracle in regard to their specific legal and regulatory requirements.

Document Purpose

This document is intended to provide relevant information related to OCI to assist you in determining the suitability of using OCI in relation to GDPR.

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

The following policies and documents are referenced throughout this paper:

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

About Oracle Cloud Infrastructure

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

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

The Cloud Shared Management Model

From a security management perspective, cloud computing is fundamentally different from on-premises computing. On-premises customers are in full control of their technology infrastructure. For example, they have physical control of the hardware and full control over the technology stack in production. In the cloud, however, customers use components that are 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 enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in Oracle cloud services. By design, Oracle provides security functions for cloud infrastructure and operations, such as cloud operator access controls and infrastructure security patching. Customers are responsible for securely configuring and using their cloud resources. For more information, see the cloud service documentation.

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

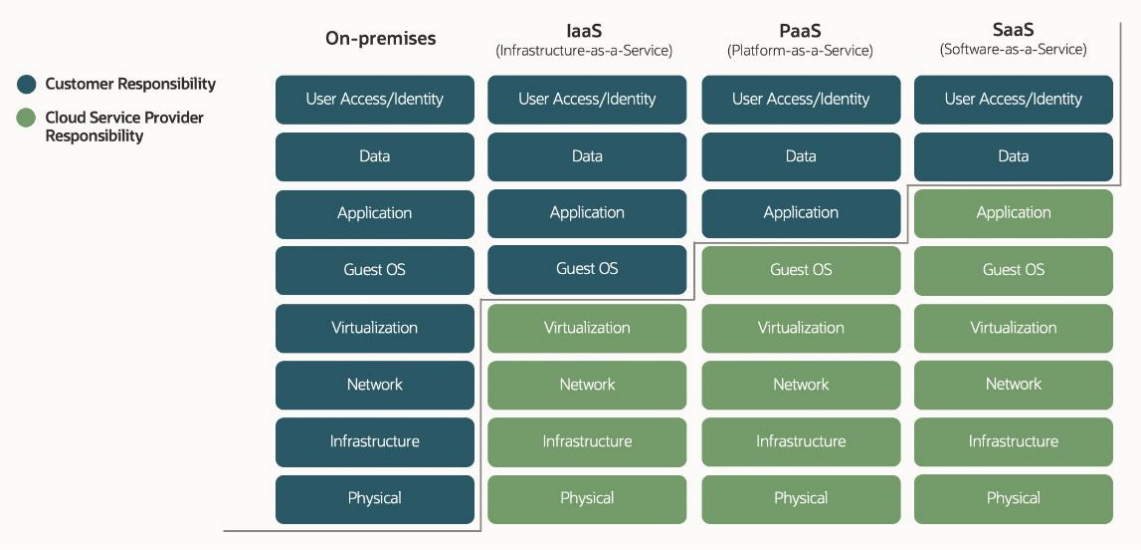

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Roles

The GDPR defines three key roles:

- **Data subject**: An individual whose personal data is gathered and processed by the controller.
- **Controller**: An entity that determines the purposes and means by which the data is processed.
- **Processor**: An entity that only processes data at the controller's command.

The following diagram shows the relationship between these roles:

Data subject ←→ Controller ←→ Processor

OCI customers (those who build applications by using the features and functionality of OCI) assume the role of the *controller* for the personal data collected by or through their applications. The users of such OCI-supported applications are *data subjects*. As a cloud service provider, Oracle takes the role of a *processor* with respect to such data. Adding these definitions recasts the preceding relationship as follows:

Data subject (Users) ←→ Controller (Oracle Customers) ←→ Processor (Oracle)

Customer Data

Generally speaking, OCI handles two types of data in the context of its interactions with its customers:

- **Customer account information**: Information needed to operate the customer's OCI account. This information is primarily used to contact and bill the customer. The use of any personal information that Oracle gathers from the customer for purposes of account management is governed by the Oracle General Privacy Policy. With customer account information, OCI acts as a *controller* in this instance.

- **Customer services data**: Data that customers choose to store within OCI, which may include personal information gathered from data subjects (users). Typically, Oracle doesn't have insight into the types of this data or the customer's decisions regarding its collection and use. Also, Oracle doesn't have a direct relationship with the data subjects. As mentioned earlier, the customer is the *controller* in this situation and manages the data. Oracle is the *processor* that acts on the commands of the customer.

The remainder of this document focuses on customer services data and any personal information that it may contain from the customer's data subjects.

Data Privacy Principles

GDPR Article 5 defines the key "principles related to processing of personal data," summarized in this section. In this regard, personal data must be treated as follows:

- Processed lawfully, fairly, and transparently (lawfulness, fairness and transparency)
- Collected and processed for a limited purpose (purpose limitation)
- The minimum amount necessary for the purpose (data minimization)
- Accurate (accuracy)
- Stored only as long as necessary (storage limitation)
- Processed securely (integrity and confidentiality)

The following sections outline how OCI and its customers allocate or share the responsibilities for these principles.

Lawfulness, Fairness and Transparency

"Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject…" Article 5(1)(a)

Processed Lawfully

As controllers, OCI customers determine whether they have a lawful basis (as defined in the GDPR) to process personal data that is gathered from their data subjects.

Data Breach Notification

The customer is responsible for incident and personal information breach detection within the security environment that they control. By contrast, OCI can't detect whether a user's login to a customer's tenancy was unauthorized. Oracle Cloud Guard and the OCI Audit service can help customers monitor the environment that they have set up in OCI. Customers may want to implement other monitoring software, depending on the functionality that they have implemented on the OCI platform.

Oracle will evaluate and respond to any event when Oracle suspects that Oracle-managed customer data has been unproperly handled or accessed. Oracle's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to security events and incidents. In the event that Oracle determines that a confirmed security incident involving information processed by Oracle has taken place, 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 and incident history are not shared externally.

As a controller, the customer must determine whether any of its data subjects (users) or regulators must be notified of a personal information breach.

See “Cloud Guard” at docs.oracle.com/iaas/cloud-guard/home.htm.

See “Overview of Audit” at docs.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm.

See Oracle Corporate Security Practices, “Incident Response” at oracle.com/corporate/security-practices/corporate/security-incident-response.html.

Processed Fairly

Only customers can be transparent with their data subjects about how customers process their data subjects’ personal data and the purposes for which they process that data. As a cloud provider, Oracle generally has no insight into the data that its customers store and process in OCI, or whether it’s personal data that belongs to a particular data subject. Oracle has no relationship with data subjects to inform them about any of the customer-controller’s data processing details. Only the customer can provide that information.

The Oracle Services Privacy Policy and Data Processing Agreement for Oracle Services give transparency to customers about Oracle’s overall approach to data handling as a processor.

Location Transparency

A customer’s tenancy is created in the home region of their choice. The data that the customer brings into their tenancy to process with OCI services stays within that home region unless the customer subscribes to another region and then explicitly chooses to move data to that other region. OCI offers services that can operate cross-region, but it's the customer's choice, as the data controller, to use them.

See “Regions and Availability Domains” at docs.oracle.com/iaas/Content/General/Concepts/regions.htm.

See “Setting Up Your Tenancy” at docs.oracle.com/iaas/Content/GSG/Concepts/settinguptenancy.htm.

Purpose Limitation

> “Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes…” Article 5(1)(b)

The customer remains the controller at all times. Oracle processes data only at the customer’s request and uses it only for the purposes specified in the customer’s agreement with Oracle.

OCI has the following features designed to help customers effectively manage purpose limitation.

Compartments

OCI offers its customers the ability to create compartments under their initial root compartment (or tenancy). Compartments are a fundamental component of OCI, and customers can use them to separate resources for the purposes of measuring usage and billing, access (through the use of policies), and isolation (separating the resources of one project or business unit from another). These separate compartments may help customers support their purpose-limitation requirements for the data that they collect and process by isolating their cloud resources.

Customers determine and assess the purposes for which they are collecting and using their data subjects’ personal information. They can take steps to plan and create compartments under their initial root compartment (or tenancy). This planning can organize their cloud resources in a way that aligns with their data management goals and helps them support purpose-limitation requirements for the personal data that they may collect.

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

Virtual Cloud Networks

OCI customers 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 the 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 by the internet. All compute instances within the same subnet use the same route tables and security lists, which acts as a type of purpose limitation among similar compute instance resources.

Customers can carefully plan their VCN architecture so that its potential network isolation supports the necessary purpose limitation, 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 “VCNs and Subnets” at docs.oracle.com/iaas/Content/Network/Tasks/managingVCNs.htm.

See “Security Lists” at docs.oracle.com/iaas/Content/Network/Concepts/securitylists.htm.

For a discussion of public and private subnets, see “Connectivity Choices” at docs.oracle.com/iaas/Content/Network/Concepts/overview.htm.

Tagging

OCI offers a flexible tagging operation to label resources with similar purposes. Tagging can help customers with the following actions:

- Enforce specific processing on resources within a tagging group
- Aggregate resources with similar purposes
- Run bulk operations on resources with the same tag

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

Data Minimization

“Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed…” Article 5(1)(c)

OCI customers perform the relevant assessment of whether the proportionate amount of data was collected from data subjects. As cloud provider, Oracle generally has no insight into the data that customers store and process in OCI, nor whether such data constitutes the minimum necessary to accomplish the purpose agreed to by customers with their data subjects.

Accuracy

“Personal data shall be accurate…” Article 5(1)(d)

Although OCI customers are responsible for maintaining accuracy of the personal information of their data subjects, including while in storage, OCI offers the following features to help customers store accurate copies of data.

Data Storage

OCI offers Object Storage, Block Volume, File Storage, and Database services that customers can use to help them store accurate copies of their data subjects' data. Customers can also use these data storage options for business continuity, disaster recovery, and long-term archiving.

- **Object Storage** allows the customer to store unstructured data of any content type. Object Storage actively monitors data integrity by using checksums, and automatically detects and repairs corrupt data. Object Storage monitors and ensures data redundancy. If a redundancy loss is detected, Object Storage automatically creates more data copies.

  See "Overview of Object Storage" at docs.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm.

- **Block Volume** allows the customer to use a block volume as a regular hard drive when it's attached and connected to a compute instance. Volumes can also be disconnected and attached to another compute instance without the loss of data. Volumes are automatically replicated to protect against data loss, and can also be backed up if the customer chooses.

  See "Overview of Block Volume Backups" at docs.oracle.com/iaas/Content/Block/Concepts/blockvolumebackups.htm.

- **File Storage** allows the customer to manage shared file systems, 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.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm.

- **Bare metal and virtual machine database systems** have many options for database backup and recovery. See docs.oracle.com/iaas/dbcs/doc/backup-and-recovery.html.

  Oracle Data Guard can also be used for data protection and availability. See docs.oracle.com/iaas/dbcs/doc/use-oracle-data-guard-db-system.html.

- **Exadata Cloud Service** has many database backup options. See docs.oracle.com/iaas/exadatacloud/exacs/ecs-managing-db-backup-and-recovery.html.

  Read about using Data Guard for Exadata backups at docs.oracle.com/iaas/exadatacloud/exacs/using-data-guard-with-exacc.html.

Availability Domains, Replication, and Fault Domains

A customer's tenancy is created in the home region of their choice. An OCI region is composed of physically isolated and fault-tolerant availability domains. Customers can choose to build replicated systems across availability domains in the same region for both high availability and disaster recovery.

Fault domains are groupings of hardware and infrastructure within an availability domain. Customers can optionally specify the fault domain for a new compute instance when it's created. Fault domains allow customers to distribute their compute instances so that they are not on the same physical hardware, and are especially useful in single availability domain regions.

Read about regions, availability domains, and fault domains at docs.oracle.com/iaas/Content/General/Concepts/regions.htm.

Storage Limitation

"Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary..." Article 5(1)(e)

If a customer determines that the purposes for processing data have passed and that the data must be deleted, OCI offers the following methods designed to allow the customer to delete such data.

Data Deletion

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

- "Deleting a Volume" at docs.oracle.com/iaas/Content/Block/Tasks/deletingavolume.htm
- "Managing Objects" at docs.oracle.com/iaas/Content/Object/Tasks/managingobjects.htm
- "Managing File Systems" at docs.oracle.com/iaas/Content/File/Tasks/managingfilesystems.htm
- "Terminating an Instance" at docs.oracle.com/iaas/Content/Compute/Tasks/terminatinginstance.htm

Object Lifecycle Management

The Object Storage service offers Object Lifecycle Management to help automate the archiving and deletion of data objects. Customers 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.

See "Using Object Lifecycle Management" at docs.oracle.com/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm.

Service Termination

When customers terminate an OCI service subscription, any data that resides in the production Cloud Services environment will be available for retrieval from Oracle. After the retrieval period, the data is deleted. Details about available retrieval functionality and the applicable retrieval period are described in section 6, "Oracle Cloud Suspension and Termination Policy," in the Oracle Cloud Hosting and Delivery Policies at oracle.com/contracts/cloud-services/.

Integrity and Confidentiality

"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage..." Article 5(1)(f)

The security of the cloud environments in which customer data is hosted can be enhanced by using the following methods:

- Least-privilege access control and policies
- Encryption
- Vault key management service
- Secure communications to existing customer networks
- Multifactor authentication

Least Privilege

Access control in OCI is based on the concept of *least privilege*. New resources (for example, block volumes or compute instances) are configurable so that only users in the customer's administrator group are given access when the resource is created. Access for other existing users must be explicitly given by the customer's administrators through the use of policies, groups, and compartments. New users who are created in a customer's tenancy must also explicitly be given access to resources by the customer's administrators through the use of policies, groups, and compartments. Customers can also create service-level administrators to further reduce the scope of administrative access.

- See "How Policies Work" at docs.oracle.com/iaas/Content/Identity/Concepts/policies.htm.
- See "Create Service-level Admins for Least Privilege" at docs.oracle.com/iaas/Content/Security/Reference/iam_security_topic-Security_Policy_Examples.htm.

Tagging can be used to scope resource access. See docs.oracle.com/iaas/Content/Tagging/Tasks/managingaccesswithtags.htm.

Oracle Managed Access allows the customer to manage requests for temporary access to their organization's cloud resources (for troubleshooting purposes) from authorized operators. See docs.oracle.com/iaas/Content/managed-access/overview.htm

Encryption

Note: The encryption described in this section occurs regardless of the nature of the underlying data. OCI doesn't generally have insight into the nature of the customer's data, whether it's personal, sensitive, or otherwise.

GDPR Article 32(1) lists the encryption of personal data as a possible technical measure "to ensure a level of security appropriate to the risk." Customer data is encrypted through the following services:

- **Block Volume** encrypts volumes and backups at rest by default, and the backups are also encrypted in Object Storage. See docs.oracle.com/iaas/Content/Block/Concepts/overview.htm.
- **Object Storage** encrypts each object with its own key. Encryption is enabled by default and can't be turned off. See docs.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm and docs.oracle.com/iaas/Content/Object/Tasks/encryption.htm.
- **File Storage** encrypts data at rest by default, and the encryption can't be turned off. See docs.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm.
- **Bare metal and virtual machine database systems** encrypt all user-created tablespaces, enabled by default, using Transparent Data Encryption (TDE). See docs.oracle.com/iaas/dbcs/doc/network-time-protocol-and-transparent-data-encryption.html.
- **Exadata Cloud Service** encrypts all new tablespaces created by the customer by default. See docs.oracle.com/iaas/exadatacloud/exacs/exa-conf-db-features.html.

Vault

The Vault key management service provides centralized management of the encryption of customer data with keys that the customer controls. It can be used for the following purposes:

- 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

Many services are integrated with Vault, including Block Volume, Object Storage, and File Storage. See docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.

Secure Communications to Existing Customer Networks

OCI gives customers two ways to securely communicate from their virtual cloud network (VCN) to their existing on-premises network:

- **Site-to-Site VPN**, also known as IPSec VPN (virtual private network). See docs.oracle.com/iaas/Content/Network/Tasks/managingIPsec.htm.
- **FastConnect**, which offers a private connection where traffic doesn't traverse the internet. See docs.oracle.com/iaas/Content/Network/Concepts/fastconnect.htm.

Multifactor Authentication

The Identity and Access Management service (IAM) offers multifactor authentication (MFA) to customers for their user accounts.

For IAM without Identity Domains, see "Managing Multifactor Authentication" at docs.oracle.com/iaas/Content/Identity/Tasks/usingmfa.htm.

For IAM with Identity Domains, see "Managing 2-Step Verification" at docs.oracle.com/iaas/Content/Identity/mfa/manage-2-step-verification.htm.

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. OCI provides several security and privacy features that help organizations implement the technical controls that may be required to operate under the GDPR.

Additional Resources

- OCI Security Overview: docs.cloud.oracle.com/iaas/Content/Security/Concepts/security_overview.htm
- OCI Security Guide: docs.oracle.com/iaas/Content/Security/Concepts/security_guide.htm
- OCI Privacy Features: oracle.com/a/ocom/docs/oci-privacy-features.pdf
- OCI Security Architecture: oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf
- Oracle Cloud Services Contracts: oracle.com/contracts/cloud-services/
- Oracle Cloud Compliance: oracle.com/corporate/cloud-compliance/
- Official EU portal on Data Protection: commission.europa.eu/law/law-topic/data-protection_en

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