ORACLE

Oracle Cloud Infrastructure and the GDPR

European Union General Data Protection Regulation

February 3, 2021 | Version 1.2

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

The European Union (EU) General Data Protection Regulation (GDPR) applies broadly to organizations based in the EU and elsewhere that collect and process the personal information of individuals in the EU. This paper explains how the features and functionality of Oracle Cloud Infrastructure can help customers meet some of their GDPR requirements. This paper does not provide an exhaustive discussion of the GDPR requirements, nor does it give compliance advice. Customers are advised to seek their own legal counsel to develop and implement their GDPR compliance program.

Oracle Cloud Infrastructure is an Infrastructure as a Service (IaaS) product in which responsibility for managing security is shared between Oracle Cloud Infrastructure and the customer, see https://docs.oracle.com/iaas/Content/Security/Concepts/security_overview.htm#Shared_Security_Model.

Likewise, managing the security controls to meet compliance and privacy requirements is also a shared responsibility between Oracle Cloud Infrastructure and the customer. This paper explains some of this shared responsibility in the context of the GDPR and Oracle Cloud Infrastructure.

Note: The following policies and documents are referenced throughout this paper:

- Data Processing Agreement for Oracle Services (DPA) at https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing
- 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

ROLES

The GDPR defines three key actors:

- 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

As a cloud service vendor, Oracle takes the role of a *processor*. Our direct Oracle Cloud Infrastructure customers (those who build applications by using the features and functionality of Oracle Cloud Infrastructure) typically assume the role of *controller*. These customers, in turn, have users of their Oracle Cloud Infrastructure-built applications, which makes these users *data subjects*. Recasting the preceding relationships, we then have the following:

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

CUSTOMER DATA

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

- **Customer account information:** Information needed to operate the customer's Oracle Cloud Infrastructure 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, Oracle Cloud Infrastructure acts as a *controller* in this narrow instance.

- **Customer services data:** Data that customers choose to store within Oracle Cloud Infrastructure, which may include personal information gathered from data subjects (users). Oracle does not have insight into the contents of this data or the customer's decisions regarding its collection and use. Additionally, it is important to note that Oracle does not 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 paper focuses on customer services data and any personal information that it may contain from the customer's data subjects.

PRINCIPLES

GDPR Article 5 defines the key "principles related to processing of personal data." In this regard, personal data must be:

- 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 Oracle Cloud Infrastructure 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

Oracle Cloud Infrastructure does not have a direct relationship with the data subjects (users), nor does it have insight into the data that the customer may have collected from the data subjects. Therefore, the customer may need to 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

Oracle Cloud Infrastructure has incident response mechanisms and processes in place designed to detect potential data breaches within the security environment that Oracle implements. Oracle notifies customers of data breaches following the terms described in the Data Processing Agreement for Oracle Services. See also Oracle Corporate Incident Response at https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html.

Customers may have responsibilities for data 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 Cloud Guard and Audit services can help the customer monitor the environment they have set up in Oracle Cloud Infrastructure. The customer may want to implement other monitoring software, depending on the functionality that they have implemented in their tenancy. Also, as a controller, the customer may be required to follow data breach notification regulations and notify their data subjects, regulators, or both when regulations demand.

See “Cloud Guard” at https://docs.oracle.com/en-us/iaas/cloud-guard/using/index.htm.

See “Overview of Audit” at https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm.

Processed Fairly

The Oracle Services Privacy Policy gives transparency to customers about Oracle’s overall approach to data handling as a processor.

Only customers themselves can be transparent to their data subjects about how they process their data subjects’ personal data, and the purposes for which they process that data. Oracle has no insight into the data that its customers store and process in Oracle Cloud Infrastructure, or whether it is 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.

Location Transparency

Oracle Cloud Infrastructure is transparent with its customers about where the customer’s data is processed and stored. When a customer sets up their Oracle Cloud Infrastructure account, they choose a home region in which to initially locate their tenancy. The customer’s data stays within that region unless the customer chooses to move the data outside the region. Oracle Cloud Infrastructure offers powerful services that may operate cross-tenancy or cross-region. Oracle Cloud Infrastructure remains transparent (in the console user interface and API documentation) so that the customer will always be made aware when their actions may cause data to move to another region or tenancy.

Oracle has no insight into the data that its customers store in Oracle Cloud Infrastructure or whether it is personal information that belongs to a particular data subject, nor does Oracle have any direct relationships with data subjects. Therefore, only the customer can inform their data subjects about the geographical location details of their personal data storage if it is determined by the customer to be necessary.

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

See “Setting Up Your Tenancy” at https://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)

From a technical perspective, purpose limitation can be supported by the use of compartments, virtual cloud networks, or tagging.

Compartments

Oracle Cloud Infrastructure offers its customers the ability to create compartments under their initial root compartment (or tenancy). Compartments are a fundamental component of Oracle Cloud Infrastructure and can be used 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 may need to 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 should 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 collect.

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

Virtual Cloud Networks

Oracle Cloud Infrastructure 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 table and security lists, which acts as a type of purpose limitation among similar compute instance resources.

Customers should 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 the same route table and security list within a common subnet

See "VCNs and Subnets" at https://docs.oracle.com/iaas/Content/Network/Tasks/managingVCNs.htm.

See "Security Lists" at https://docs.oracle.com/iaas/Content/Network/Concepts/securitylists.htm.

See "Connectivity Choices" for a discussion of public and private subnets at https://docs.oracle.com/iaas/Content/Network/Concepts/overview.htm#connectivity.

Tagging

Oracle Cloud Infrastructure offers a flexible tagging operation to label resources with similar purposes. Tagging can help customers:

- 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 https://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)

As cloud provider, Oracle generally has no insight into the data that customers store and process in Oracle Cloud Infrastructure, nor whether it constitutes the minimum necessary to accomplish the purpose agreed to with their data subjects (users). Any assessment of whether the proportionate amount of data was collected from data subjects is left to the customer to determine.

Accuracy

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

Data Storage

Oracle Cloud Infrastructure offers Object Storage, Block Volume, File Storage, and Database services that customers can leverage to help accurately store customer data. Customers can also use these data storage options for business continuity, disaster recovery, and long-term archiving.

- The **Object Storage** service 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 actively monitors and ensures data redundancy. If a redundancy loss is detected, Object Storage automatically creates additional data copies.

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

- The **Block Volume** service allows a block volume to be used as a regular hard drive when it is 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 https://docs.oracle.com/iaas/Content/Block/Concepts/blockvolumebackups.htm.

- The **File Storage** service allows the customer to manage shared file systems, mount targets, and create file system snapshots. The File Storage service uses synchronous replication and high availability failover for resilient data protection.

  See "Overview of File Storage" at https://docs.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm.

- **Bare Metal and Virtual Machine Database Systems** can use Object Storage or local storage for backups. Data Guard can also be used for data protection and availability.

  See "Backing up a Database" at https://docs.oracle.com/iaas/Content/Database/Tasks/backingup.htm.

  See "Using Oracle Data Guard" at https://docs.oracle.com/iaas/Content/Database/Tasks/usingdataguard.htm.

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

  Read about Exadata backups managed by Oracle Cloud Infrastructure at https://docs.oracle.com/iaas/Content/Database/Tasks/exabackingup.htm.

  Read about Exadata backups managed by the customer at https://docs.oracle.com/iaas/Content/Database/Tasks/exabackingupBKUPAPI.htm.

  Read about using Data Guard for Exadata backups at https://docs.oracle.com/iaas/Content/Database/Tasks/exausingdataguard.htm.

Availability Domains, Replication, and Fault Domains

A customer's tenancy is created in the home region of their choice. An Oracle Cloud Infrastructure 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 at launch time. This allows customers to distribute their compute instances so that they are not on the same physical hardware. This is especially useful within single availability domain regions.

Read about regions, availability domains, and fault domains at https://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)

As cloud provider, Oracle generally has no insight into the data that customers 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 a customer determines that the purposes for processing their data have passed and that their 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 a Volume" at https://docs.oracle.com/iaas/Content/Block/Tasks/deletingavolume.htm
- "Managing Objects" at https://docs.oracle.com/iaas/Content/Object/Tasks/managingobjects.htm
- "Managing File Systems" at https://docs.oracle.com/iaas/Content/File/Tasks/managingfilesystems.htm
- "Terminating an Instance" at https://docs.oracle.com/iaas/Content/Compute/Tasks/terminatinginstance.htm

Object Lifecycle Management

Oracle 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 https://docs.oracle.com/iaas/Content/Object/Tasks/usinglifecyclepolicies.htm.

Service Termination

When customers terminate their Oracle Cloud Infrastructure service subscription, Oracle will make their data, residing in the production Cloud Services environment, available for retrieval. After the retrieval period, the data will be 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 https://www.oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html#hd.

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
- Multi-factor authentication

Least Privilege

Access control in Oracle Cloud Infrastructure is based on the concept of least privilege. New resources (for example, block storage volumes, compute instances) are "secure by default"; 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 by 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 admins to further scope down administrative access.

See "How Policies Work" at https://docs.oracle.com/iaas/Content/Identity/Concepts/policies.htm.

See "Create Service-level Admins for Least Privilege" at https://docs.oracle.com/en-us/iaas/Content/Security/Reference/iam_security.htm#Security_Policy_Examples.

Encryption

Note: The encryption described in this section occurs regardless of the nature of the underlying data. Oracle Cloud Infrastructure does not have insight into the nature of the customer's data, whether it is personal data, sensitive data, 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:

- The **Block Volume** service encrypts by default at rest, and the backups are also encrypted in Object Storage. See https://docs.oracle.com/iaas/Content/Block/Concepts/overview.htm#BlockVolumeEncryption.
- The **Object Storage** service encrypts each object with its own key. Encryption is enabled by default and cannot be turned off. See https://docs.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm#features.
- The **File Storage** service encrypts by default at rest and the encryption cannot be turned off. See https://docs.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm#encryption.
- **Bare Metal and Virtual Machine Database Systems** encrypts all user-created tablespaces by default, using Transparent Data Encryption (TDE). See https://docs.oracle.com/iaas/Content/Database/Tasks/configuringDB.htm#Transparent_Data_Encryption.
- **Exadata Cloud Service** encrypts by default all new tablespaces created by the customer. See https://docs.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 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 the Vault key management service including these storage services: Block Volume, Object Storage, and File Storage. See https://docs.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm

Secure Communications to Existing Customer Networks

Oracle Cloud Infrastructure gives the customer two ways to securely communicate from their virtual cloud network (VCN) to their existing on-premises network:

- **VPN Connect**, also known as IPSec VPN (virtual private network). See https://docs.oracle.com/iaas/Content/Network/Tasks/managingIPsec.htm.
- **FastConnect**, which offers a private connection where traffic does not traverse the internet. See https://docs.oracle.com/iaas/Content/Network/Concepts/fastconnect.htm.

Multi-Factor Authentication

The Identity and Access Management service (IAM) offers multifactor authentication (MFA) to customers for their user accounts. See https://docs.oracle.com/iaas/Content/Identity/Tasks/usingmfa.htm

Other Security

See the Oracle Cloud Infrastructure Security Guide at https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm#Oracle_Cloud_Infrastructure_Security_Guide.

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 CertifyPointBV (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 C5requirements 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 toin-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.

ORACLE CLOUD INFRASTRUCTURE RESOURCES

- Oracle Cloud Infrastructure Security Overview: https://docs.cloud.oracle.com/iaas/Content/Security/Concepts/security_overview.htm
- Oracle Cloud Infrastructure Documentation: https://docs.cloud.oracle.com/iaas/Content/GSG/Concepts/baremetalintro.htm
- Oracle Cloud Infrastructure Privacy Features: https://docs.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/oci-privacy-features.pdf
- Oracle Cloud Infrastructure Security Architecture: https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf

OTHER RESOURCES

- Oracle Cloud Services Contracts: https://www.oracle.com/corporate/contracts/cloud-services/
- Official EU portal on Data Protection: https://ec.europa.eu/info/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

Oracle Cloud Infrastructure and the GDPR
February, 2021
Author: Jim Feltis