

Oracle Cloud Infrastructure and the GDPR

European Union General Data Protection Regulation

ORACLE WHITE PAPER | APRIL 2018





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, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.



Table of Contents

Disclaimer	2
Overview	4
Roles	4
Customer Data	5
Principles	5
Lawfully, Fairly, and Transparently	6
Purpose Limitation	7
Accuracy	9
Integrity and Confidentiality	10
Certifications and Third-Party Audit Reports	12
Oracle Cloud Infrastructure Documentation	12
Additional Oracle GDPR Documentation	12
Other Resources	13



Overview

The European Union (EU) General Data Protection Regulation (GDPR) is a new, comprehensive data protection law that goes into effect on May 25, 2018. It applies broadly to organizations based in the EU and elsewhere that collect and process the personal information of individuals residing 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 security is shared between Oracle Cloud Infrastructure and the customer. For details, see the [Oracle Cloud Infrastructure Security white paper](#). Likewise, privacy compliance is also a shared responsibility between Oracle Cloud Infrastructure and the customer. This paper explains this shared responsibility in the context of the GDPR and Oracle Cloud Infrastructure.

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 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 subject 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 subject users. 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 subject users.

Principles

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

- Processed lawfully, fairly, and transparently
- Collected and processed for a limited purpose (purpose limitation)
- The minimum amount necessary for the purpose (data minimization)
- Accurate
- 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 some of these principles.



Lawfully, Fairly, and Transparently

“Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject...” Article 5(1)(a)

Processed Lawfully


- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructure does not have a direct relationship with the data subject users, nor does it have insight into the data that the customer has collected from the data subject users.
- **Customers:** Customers 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 subject users.

Data Breach Notification

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructure has incident response mechanisms and processes in place designed to detect potential data breaches within the security environment that we implement. Oracle notifies customers of data breaches following the terms described in the [Data Processing Agreement for Oracle Cloud Services](#).
- **Customers:** 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 customer should monitor the environment that they set up in Oracle Cloud Infrastructure by using the [Oracle Cloud Infrastructure Audit service](#). The customer may want to implement other monitoring software, depending on the functionality that they have implemented on the Oracle Cloud Infrastructure platform. Also, as a controller, the customer may be required to follow data breach notification regulations and notify their data subject users, regulators, or both when regulations demand.

Processed Fairly

- **Oracle Cloud Infrastructure:** The [Oracle Services Privacy Policy](#) gives transparency to customers about Oracle’s overall approach to data handling as a processor.
- **Customers:** Only customers themselves can be transparent to their data subject users about how they process their data subject users’ 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 users 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:** 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.
- **Customers:** 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 user, nor does Oracle have any direct relationships with data subject users. Therefore, only the customer can inform their data subject users about the geographical location details of their personal data storage if it is determined by the customer to be necessary.

Audit

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructure offers an [audit service](#) that logs calls to the Oracle Cloud Infrastructure public application programming interface (API). These read-only logs can help with the transparency of user data access.
- **Customers:** The audit logging occurs automatically. The customer can [set up the audit log retention period](#).

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
- Tagging



Compartments

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructure offers its customers the ability to [create compartments](#) under their initial root compartment (or [tenancy](#)). This type of planning can help them organize and isolate their cloud resources in a way that aligns with their data management goals of enforcing purpose limitation of any personal information that they collect, as determined by the customer.
- **Customers:** Customers may need to determine and assess the purposes for which they are collecting and using their data subject users' personal information.

Virtual Cloud Networks

- **Oracle Cloud Infrastructure:** 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:** 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

Tagging

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructure offers a flexible [tagging](#) operation to label resources with similar purposes. Tagging can help users enforce specific processing on resources within a tagging group.
- **Customer:** Tagging can help the customer aggregate resources with similar purposes. Tagging allows the customer to run bulk operations on resources with the same tag. The customer's administrators control tagging within the customer's tenancy.



Accuracy

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

Data Storage

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructure offers Object Storage, Block Volume, and File Storage services that customers can leverage to help accurately store customer data.
 - 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.
 - 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.
 - 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.
- **Customer:** The customer can use the Object Storage, Block Volume, and File Storage services in Oracle Cloud Infrastructure to keep accurate copies of their data. These data storage options may also be used by the customer for business continuity, disaster recovery, and long-term archiving.

Availability Domains and Replication

- **Oracle Cloud Infrastructure:** 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](#). These availability domains can be used by the customer to build replicated systems.
- **Customer:** The customer can choose to build their systems in Oracle Cloud Infrastructure across availability domains in the same region. This choice allows for system replication, which in turn helps to more effectively maintain the accuracy of the data being stored in Oracle Cloud Infrastructure.



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

- Least-privilege access control and policies
- Encryption
- API request authentication
- Secure communications to existing customer networks
- Multi-factor authentication via IDCS

Least Privilege

- **Oracle Cloud Infrastructure:** Access control in Oracle Cloud Infrastructure is based on the concept of *least privilege*. New resources (for example, block storage volumes, compute instances, and so on) 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](#). New users who are created in a customer’s tenancy must explicitly be given access to resources by the customer’s administrators, and must also be given access through the use of policies.
- **Customer:** Resource access is restricted and defaults to least privilege. The customer’s administrators must take explicit actions, by use of [policies](#), to open access to its users.

Encryption

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructure encrypts customer data through the following services:
 - [Block Volume service encryption](#): Block Volume storage is encrypted at rest, and the backups are also encrypted in Object Storage.
 - [Object Storage service encryption](#): Each object is encrypted with its own key. Encryption is enabled by default and cannot be turned off.
 - [File Storage service encryption](#): Data and metadata are encrypted at rest and the encryption cannot be turned off.

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.

- **Customer:** 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.” The customer gets encryption with the Block Volume, Object Storage, and File Storage services by default, regardless of the type of data they store.

API Request Authentication

- **Oracle Cloud Infrastructure:** All customer calls to Oracle Cloud Infrastructure public APIs must be done using secure, signed API requests. Otherwise, they fail.
- **Customer:** If the customer wants to securely call Oracle Cloud Infrastructure APIs, they must follow the [signing request steps](#) to sign their Oracle Cloud Infrastructure API requests.

Secure Communications to Existing Customer Networks

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructure gives the customer two ways to securely communicate from their virtual cloud network (VCN) in Oracle Cloud Infrastructure to their existing on-premises network:
 - [IPSec VPN](#)
 - [FastConnect](#), which offers a private connection where traffic does not traverse the internet
- **Customer:** The customer can follow the [Connectivity to Your On-Premises Network steps](#) to set up a secure IPSec VPN or FastConnect connection from their on-premises network to their VCN in Oracle Cloud Infrastructure.

Multi-Factor Authentication

- **Oracle Cloud Infrastructure:** Oracle Cloud Infrastructure customers can use multi-factor authentication (MFA) through the [Oracle Identity Cloud Service \(IDCS\)](#). For details, see [Multi-Factor Authentication with Oracle Identity Cloud Services](#).
- **Customer:** If the customer chooses to add the IDCS product, they can follow the [Federating with Oracle Identity Cloud Service steps](#) to federate their Oracle Cloud Infrastructure instance with IDCS, and subsequently enable MFA.

Certifications and Third-Party Audit Reports

Oracle has successfully completed ISO/IEC 27001 Stage 2 and Service Organization Control (SOC) 1, 2, and 3 audits for Oracle Cloud Infrastructure. The audits include the following services in the data center regions of Frankfurt, Germany; Phoenix, Arizona, USA; and Ashburn, Virginia, USA: Compute, Networking, Block Volume, Object Storage, Governance, Load Balancing, and Database.

- Conducted by EY/CertifyPoint, Oracle Cloud Infrastructure's ISO/IEC 27001:2013 Stage 2 audit provides assurance that Oracle Cloud Infrastructure has designed and implemented an Information Security Management System (ISMS) in accordance with information security standard ISO 27002:2013 (Information technology - Security techniques - Code of practice for information security management).
- Conducted by Ernst & Young, Oracle Cloud Infrastructure's SOC 1 Type 2 examination provides assurance that controls relevant to internal control over financial reporting are designed and operating effectively. The SOC 2 Type 2 examination provides assurance that controls relevant to the AICPA Trust Services Security and Availability Principles are designed and operating effectively, and the SOC 3 examination provides assurance that Oracle Cloud Infrastructure maintains effective controls relevant to the security and availability of its IaaS offerings.

Oracle Cloud Infrastructure Documentation

For more details about the services and features of Oracle Cloud Infrastructure, see the [Oracle Cloud Infrastructure Online Documentation](#).

Other Oracle Cloud Infrastructure white papers are located at https://cloud.oracle.com/en_US/iaas/technical-resources.

Additional Oracle GDPR Documentation

- Security
 - <https://go.oracle.com/gdpr-compliance>
 - <https://www.oracle.com/uk/corporate/features/gdpr.html>
- Database
 - <http://www.oracle.com/technetwork/database/security/wp-security-dbsec-gdpr-3073228.pdf>
- Cloud Applications
 - <https://www.oracle.com/applications/gdpr/index.html>

- 
- Marketing Cloud
 - <https://www.oracle.com/marketingcloud/about/events/gdpr.html>

Other Resources

- Privacy at Oracle: <https://www.oracle.com/legal/privacy/index.html>
- Oracle Cloud Services Contracts: <http://www.oracle.com/us/corporate/contracts/cloud-services/index.html>
- Official EU portal on Data Protection: https://ec.europa.eu/info/law/law-topic/data-protection_en







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

Copyright © 2018, 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. 0418

Oracle Cloud Infrastructure and the GDPR
April 2018
Author: Jim Feltis