ORACLE

Frequently Asked Questions about

Data Flows and Oracle Services

How Oracle is responding to the CJEU Schrems II ruling[1] and guidance from EU privacy authorities

DATA TRANSFER MECHANISMS

Does Oracle rely on the Privacy Shield?

No. Effective October 21, 2020, Oracle has withdrawn from the EU-U.S. and Swiss-U.S. Privacy Shield programs.

Prior to that, Oracle was EU-U.S. and Swiss-U.S. Privacy Shield certified, but did not rely on Privacy Shield as a transfer mechanism in its standard services contracts with customers and partners.

Does Oracle provide an adequate transfer mechanism?

Oracle has and continues to rely on appropriate data transfer safeguards such as its Binding Corporate Rules for Processors (BCR-p) and Standard Contractual Clauses, where and as applicable to transfers of EU/EEA, Swiss and UK personal information.

The services agreement between You and Oracle references the applicable version of the Oracle Data Processing Agreement, which provides further details on the relevant data transfer mechanism that applies to Your order for Oracle services. The BCR-p are incorporated by default into the European DPA Addendum attached to Oracle's Data Processing Agreement for Services, effective June 26, 2019[2].

Oracle will also continue to monitor ongoing developments with regard to these transfer mechanisms, such as potential updates to WP257 guidelines for Binding Corporate Rules, and the European Commission's proposal for new EU Standard Contractual Clauses.

Have Oracle's Binding Corporate Rules been reviewed for alignment with the GDPR?

Yes. Oracle's BCR-p have received EU/EEA-wide authorization from the competent EU/EEA data protection authorities, and have been updated to reflect the GDPR requirements for BCRs.

Among other things, Oracle's BCR-p include provisions on data subject rights and remedies (Section 11.1 and 11.4 BCR-p), purpose-limitation provisions and data transfer descriptions (Section 4), as well as accountability requirements (Sections 8, 9 and 10).

[1] CJEU July 16, 2020 decision invalidating the EU-U.S. Privacy Shield program

[2] Note that different terms may apply to selected services, such as Oracle CrowdTwist. Please contact your Sales representative if you have any questions about the terms that apply to these services.

For further information on how Oracle's BCR-p meet applicable GDPR requirements, please refer to the BCR and DPA Statement of Changes.

DATA LOCATIONS AND DATA TRANSFERS

Where is customer data hosted for Oracle services?

This depends on the Oracle service(s).

For example, the applicable data center region (e.g. 'Europe') for Oracle Cloud Applications is typically specified in the top section of the applicable order for Cloud services. For Oracle Cloud Infrastructure, customers can select a default data region, depending on available regions for those services. For Oracle Cloud@Customer services, the data is hosted in the customer's data center.

For more information about applicable hosting locations for the services you have ordered, please contact your Oracle Sales representative.

Is customer data accessed from regions or countries outside the data (center) region, as applicable?

Again, this depends on the Oracle service(s). In general, Oracle provisions its services from delivery locations globally[3].

A list of *Oracle affiliates* that may assist with the provision of Oracle services, including the location of such Oracle affiliates, is available here.

Some services also rely on *third party subprocessors*. To confirm the identify and location of such third party subprocessors (if any), customers can consult the relevant Third Party Subprocessor List(s) available on My Oracle Support or other primary support tool for their services. Third Party subprocessors are subject to privacy and security provisions consistent with those applicable to Oracle and Oracle affiliates, including compliance with applicable data transfer safeguards, and transparency about data processing locations[4].

DATA ACCESS AND SUPPLEMENTARY MEASURES

Has Oracle implemented any supplementary measures to restrict access to customer data?

Oracle understands that customers are seeking additional information and reassurances about how their data is secured and protected when relying on Oracle services. We are confident that our comprehensive security and privacy features and measures are responsive to our customers' needs.

Below is an overview of some of the key technical, contractual and organization safeguards that Oracle makes available to customers. Please note that different services may have different (technical) controls, and that the relevant contract terms are specified in the Oracle services agreement.

Encryption and Key Management controls

Oracle employs robust data security controls, including encryption for data at rest and in transit. Service-specific information about encryption and key management controls is available to customers in the Privacy and Security Feature documentation on My Oracle Support and the Cloud security portal.

---

[3] Note that different terms may apply to selected services or service features, such as Government Cloud services or services with restricted access controls. Please contact your Sales representative if you have any questions about the availability and terms of these services.

[4] Also see Section 4.1 of the Data Processing Agreement for Oracle Services, Section 1.3 of the European DPA Addendum, and Section 7.1 of Oracle's BCR-p.

For example, Oracle Cloud Infrastructure services such as Block Volumes and Object Storage enable at-rest data encryption by default, by using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. In-transit control plane data is encrypted by using Transport Layer Security (TLS) 1.2 or later.

Oracle also provides key management services and products, such as Oracle Key Vault, designed to enable customers to securely manage and control their encryption keys.

Please contact your Oracle Sales representative if you have any additional questions about the availability, applicability and configuration options for these encryption services and features.

Anonymization and pseudonymization features

Similarly, Oracle customers are encouraged to consult the applicable security policies and Privacy and Security Feature documentation on My Oracle Support to review available privacy and security features that limit Oracle's access to customer data (or can be configured by customers to limit such access), such as anonymization, pseudonymization, data masking and truncation controls.

For example, for Oracle Support Services, Oracle offers guidance and tools that enable customers to remove personal information and sensitive information from their submissions to My Oracle Support.

Notifying and challenging legal access requests

Customers typically have direct access to their data stored in their services environments. Oracle therefore believes that customers are generally in a better position to identify and access their own data in response to a legal access request.

However, in the event Oracle does receive a disclosure request directly from a law enforcement or government authority, the Oracle Data Processing Agreement (Section 10) and Oracle's BCR-p (Section 3.4) provide for the following safeguards:

1. Oracle will assess on a case by case basis whether a disclosure request would be binding on Oracle and valid under applicable law;
2. Oracle will challenge any access request that is not binding and valid under applicable law. Some statutes, such as the U.S. CLOUD Act, provide for multiple avenues for service providers to challenge access requests;
3. Oracle will promptly notify the customer, as well as the customer's and Oracle's data protection authorities, without otherwise responding to the access request (subject to 5. below);
4. Oracle will request the authority that made the request for an extension to enable the customer's and Oracle's data protection authorities to take a view on the validity of the request;
5. In the event that Oracle would be expressly prohibited under applicable law to inform the customer, such as to preserve the confidentiality of a criminal investigation, Oracle will request the authority that made the request to waive this non-disclosure prohibition. Oracle will also document that it has asked for such a waiver;
6. In addition to publicly-available transparency reports (see below), Oracle will also provide annual transparency reports to its data protection authority about the number and types of requests it has received.

In order to enforce these commitments, Oracle maintains a Third Party Information Access Request policy which lays down requirements for all Oracle staff and contractors on how to deal with government access requests, including legal oversight by EU-based teams, procedural steps and training on GDPR principles.

Transparency reports

Oracle periodically publishes a transparency report to provide information regarding informational requests submitted to us by law enforcement agencies, judicial authorities and government agencies from around the world. In particular, the report provides information on the type of request (e.g. administrative

subpoena issued by a government agency, judicial request, take down notice, request for assistance by a law enforcement agency, etc), the number of requests, and Oracle's response to the request (i.e. full or partial response provided, declined to respond, or evaluating response).

The most current version of the report is available here.

Data minimization controls

Oracle applies role-based least privilege access control restrictions for all operational access to services data, such that Oracle user access is restricted to the resources required for users as necessary to perform their duties.

Oracle Software Security Assurance Program

Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. One of the primary goals of OSSA is to reduce the impact of security weaknesses in Oracle products. Oracle prohibits the introduction of features intended to allow a malicious attacker to bypass security functionality such as authentication, auditing, or access control (i.e., a 'backdoor').

Third party audit reports

Oracle meets a broad set of international and industry-specific compliance standards and regulations, such as ISO27001 and ISO 27018 for a whole host of Oracle Cloud Infrastructure and Oracle SaaS applications.

For many services, customers can access and retrieve available third party audit reports and certificates in My Oracle Support or other primary support tool.