ORACLE

# Oracle Cloud and the US CLOUD Act

Frequently asked questions from customers and prospective customers

April, 2023, Version 2.0

Public

ORACLE

# Disclaimer

Please note that the relevant contract(s) between you and Oracle determine the scope of services provided and the related legal terms. These FAQs are provided on an "AS-IS" basis without warranty and are subject to change. Also note that the information in this document may not be construed or used as legal advice about the content, interpretation, or application of any law, regulation, or regulatory guideline. Customers and prospective customers must obtain their own legal advice to understand the applicability of any law or regulation on the processing of their data, including through the use of any vendor's products or services.

ORACLE

# Purpose

At Oracle, we are committed to helping customers operate globally in a fast-changing business environment and address the challenges of an increasingly complex regulatory environment.

This FAQ document provides responses to frequently asked questions ("FAQs") about the US CLOUD Act and Oracle Cloud services.

Fundamentally, the CLOUD Act does not change the way that Oracle handles disclosure requests from law enforcement. As a cloud provider, Oracle generally has no insight into the data that customers store and process in our Cloud services. Customers manage the information that they collect, decide how it's processed, and decide the data regions where it is stored. In addition, Oracle continues to invest in features and services that help customers address their security, compliance, and privacy needs efficiently.

# Frequently Asked Questions

## What is the US CLOUD Act?

The US Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") is a United States federal law passed in 2018 that amends the US Stored Communications Act.

The CLOUD Act provides a legal framework for providers of 'electronic communication services' and 'remote computing services' to respond to requests from US law enforcement to disclose subscriber and other related data hosted on their servers, regardless of whether these servers are located within the US or abroad. The CLOUD Act applies to such service providers, including non-US-headquartered service providers, that are subject to US jurisdiction, for example, because they contract for services with US customers or have an establishment in the US.

The CLOUD Act also enables the US government to conclude executive agreements with qualifying foreign governments. On October 3, 2019, the US and the UK signed an executive agreement on cross-border law enforcement demands for data from service providers, which entered into force on October 3, 2022. Notably, the agreement lays down additional privacy safeguards, such as data minimization controls, data use restrictions, and transparency requirements.

Oracle will continue monitoring any ongoing developments in this area, including the negotiations of a bilateral CLOUD Act Agreement between the US and Canada, the EU-US negotiations for an executive agreement governing cross-border access to electronic evidence for judicial cooperation in criminal matters, and the European Commission e-evidence initiative and regulation.

### Read more

CLOUD Act (Summary and Text)

US Department of Justice White Paper ("DoJ White Paper") on "Ensuring Lawful Access to Data of the Department of Justice White Paper on the Purpose and Impact of the CLOUD Act," April 2019

BSA White Paper on the US CLOUD Act: Myths vs. Facts, February 2019

Recommendation for a Council Decision (EU and USA negotiations on cross-border access to electronic evidence)

E-evidence Regulation

Access to Electronic Data for the Purpose of Countering Serious Crime, dated October 3, 2019

US Department of Justice announcement on US – UK Cross-Border Data Access Agreement

United States and Canada Welcome Negotiations of a CLOUD Act Agreement

## Does the CLOUD Act give US law enforcement indiscriminate access to data on cloud service provider systems?

The CLOUD Act does not enable indiscriminate access to data by US law enforcement. Disclosure requests are subject to legal process requirements and restrictions and independent judicial oversight. Requests are limited to data that may be responsive in connection with a criminal investigation.

The CLOUD Act also introduces new safeguards designed to protect the privacy of individuals and specifically provides an avenue for challenging disclosure requests on the basis of a conflict under a foreign – i.e., non-US – country's applicable law.

Further information can be found in Section I of the DoJ White Paper, specifically:

- Question 12. Do CLOUD Act agreements allow the US government to acquire data that it could not before?
- Question 19. What is necessary under the Stored Communications Act to obtain a warrant for the stored content?
- Question 20. Will a warrant issued under the Stored Communications Act allow the US to scoop up large amounts of data indiscriminately?
- Question 29. Does the CLOUD Act require providers to decrypt data in response to law enforcement requests?

### Read more

US Department of Justice White Paper ("DoJ White Paper") on "Ensuring Lawful Access to Data of the Department of Justice White Paper on the Purpose and Impact of the CLOUD Act", April 2019

BSA White Paper
"*The CLOUD Act provides businesses a substantial basis to challenge court orders for the production of EU citizens' data' and 'The CLOUD Act authorizes law enforcement access only through transparent, robust, publicly accountable judicial proceedings with strong oversight.*"

## Does the CLOUD Act change the preference for US law enforcement to request data directly from the customer itself?

The US Department of Justice has stated that "the CLOUD Act does not change US law or practice with regard to enterprise customer data."

The Department of Justice has also added that this is consistent with their 2017 guidance note, which advises that "*prosecutors should seek data directly from the enterprise, if practical, and if doing so will not compromise the investigation. Therefore, before seeking data from a provider, the prosecutor, working with agents, should determine whether the enterprise or the provider is the better source for the data being sought*."

Furthermore, the Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime explains in its Section 17 that "*The Agreement does not compel the CSP (cloud service provider) to remove the encryption and is encryption neutral*." Also, additional

### Read more

US Department of Justice White Paper ("DoJ White Paper") on "Ensuring Lawful Access to Data of the Department of Justice White Paper on the Purpose and Impact of the CLOUD Act," April 2019

DoJ Guidance Note on Seeking Enterprise Customer Data Held by Cloud Service Provider

information can be found in Section I of the DoJ White Paper - Question 26. Will US law enforcement go directly to service providers to obtain information of an employee of an enterprise when the enterprise is not otherwise suspected of committing a crime?

Customers have direct access to their data stored in their cloud services environments, and customers are generally in a better position to identify and access their own data in response to a data access request.

## Does the CLOUD Act require service providers to decrypt customer data?

The US Department of Justice has confirmed that CLOUD Act does not create any requirements compelling service providers to decrypt customer data. This point is also reinforced in the Explanatory Memorandum to the US-UK executive agreement on cross-border law enforcement demands for data from service providers.

From a technical perspective, Oracle offers security services and features, such as Transparent Data Encryption ("TDE"), which may help customers keep track of their encryption keys and to apply safeguards such as TDE master encryption key reset.

### Read more

Oracle Cloud Hosting & Delivery Practices

Oracle Corporate Security Practices (Data Security)

Oracle Help Center > Introduction to Transparent Data Encryption

## How does Oracle handle disclosure requests?

Customers have direct access to their data stored in their cloud services environments, and customers are generally in a better position to identify and access their own data in response to a data access request.

However, if Oracle does receive a disclosure request directly from a law enforcement authority, Oracle observes the following process:

- Oracle assesses on a case-by-case basis whether the request is legally binding and valid under applicable law.
- Oracle will challenge any request that is not binding and valid under applicable law. The US CLOUD Act provides multiple avenues for service providers to challenge access requests.
- 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.
- Oracle will request an extension to enable the customer's and Oracle's data protection authorities to take a view on the validity of the request.
- If applicable law expressly prohibits Oracle from informing the customer (e.g., to preserve the confidentiality of a criminal

### Read more

The Data Processing Agreement for Oracle Services (Sections 2.1, 2.2, and 11)

Oracle's Binding Corporate Rules for Processors (BCR-p: Section 3.4) incorporated by reference the Data Processing Agreement for Oracle Services

Oracle's Services Privacy Policy (Section III.1)

Oracle's Frequently Asked Questions about Data Flows and Oracle Services, Section Notifying and challenging legal access requests

Oracle Law Enforcement Requests

investigation), Oracle will request a waiver of this prohibition. Oracle will also document that it has asked for such a waiver.

- Oracle will provide only the information that responds to a legal access request based on a reasonable interpretation of the request.

In order to adhere to these commitments, Oracle maintains and enforces a policy for Oracle staff and contractors explaining how to deal with government access requests. The policy explains the legal oversight by global and regional teams, procedural steps, and training on GDPR principles.

Oracle also publishes a biannual transparency report, listing the requests Oracle receives from law enforcement agencies, judicial authorities, and government agencies from around the world. In particular, the report provides information about the type of request (e.g., administrative subpoena issued by a government agency, judicial request, take down notice, or request for assistance by a law enforcement agency) and the number of requests received.

The most current version of the report is available here.

## Where can I find more information on the privacy and security controls for Oracle Cloud's services?

Oracle offers its cloud services with industry-leading security and privacy controls. These controls are embedded in our cloud services and cloud data centers in every major region around the world, including in Europe.

To address demanding data residency, security, and latency requirements, Oracle also offers several sovereign deployment models, from public cloud to private, dedicated cloud models. For customers who wish to take advantage of a cost-effective public cloud model, Oracle is introducing the Oracle EU Sovereign Cloud, which is a cloud service located, fully operated, and supported in the European Union. Additionally, Oracle offers a private Dedicated Region option, allowing customers to host their own private cloud region(s) on-premises in a physical location of their choice. Finally, Oracle Cloud Isolated Regions are designed to support highly-classified workloads and customer accreditations and compliance requirements that cannot be met through internet-connected cloud regions.

For further information on Oracle sovereign cloud solutions, please visit https://www.oracle.com/cloud/sovereign-cloud and https://www.oracle.com/security/saas-security/data-sovereignty.

We also invite you to review our privacy and security policies that apply to the Oracle cloud service offerings you have purchased or are evaluating. Many of these policies are available online through www.oracle.com/contracts and http://www.oracle.com/privacy and include clear purpose-limitation restrictions, security controls and safeguards around legally required disclosure requests from law enforcement entities. If you have further questions about this document or about Oracle's privacy & security policies and practices, please consult your Oracle Sales representative.

ORACLE

## 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