Citrix DaaS

Privacy & AI Governance

Data Sheet

version: December 19, 2025

Introduction

Cloud Software Group and its business units, including Citrix, endeavor to build products with privacy, data protection, and AI governance in mind, to comply with global *Data Protection by Design* legal obligations, to align with industry standard *Privacy by Design* principles, and, perhaps most importantly, to meet customers' expectations. This means Cloud Software Group products go through operationalized product privacy & AI governance reviews as part of the product development process.

Purpose

This product privacy data sheet's purpose is to provide information to assist Cloud Software Group customers and prospective customers assess Citrix DaaS's privacy/data protection and AI governance impacts.

Scope

This data sheet covers Citrix DaaS's personal data processing, from collection, transmission, use, and sharing, to storage, retention, and deletion. It also covers the product's data security controls and features. Finally, this data sheet incorporates an AI governance section.

Product Summary

Citrix Desktop as a Service (DaaS) is a cloud computing offering that delivers virtual apps and desktops from the cloud to any device. This managed desktop virtualization solution is used for provisioning SaaS and legacy applications, as well as full Windows-based virtual desktops and delivers them to the workforce.

Types of Personal Data Collected & Processed

With the Citrix DaaS offering, application servers remain under the customer's control, in a resource location consisting of the customer's own datacenter or a customer-provided account with a third-party cloud vendor such as Microsoft Azure, Amazon Web Service, or Google Cloud Platform. While Citrix provides management and monitoring capabilities for these servers, it does not have access to the data within the servers, including the

©2025, Cloud Software Group, Inc.

contents of user files, applications, and disk images (unless enabled by the customer, e.g., as part of customer support). Citrix DaaS does not collect, inspect, or transfer Customer Content files (for example, Microsoft Word and Excel files) from the virtual machines that end users access. End users' virtual machines are under the customer's control.

Citrix DaaS collects and processes the following categories and types of personal data for the following purposes:

Data Category	Personal Data Captured? Y/N	Personal Data Element(s) Captured	Purpose(s) for Processing Personal Data
Product Admin User Data	Yes	Administrator Login email, First Name, Last Name, Partner Name (if applicable) Plus other elements that customer-managed IDP transmits to Citrix DaaS for authentication	To operate and administer the product, including user authentication
End User Data	Yes	User unique identifier, user security identifier, user principal name, username, full name, user domain name, session host name, IP address, device ID, and product version, product ID, hardware ID associated with session Plus other elements that customer-managed IDP transmits to Citrix DaaS for authentication	To operate and administer the product, including user authentication
Customer Content (e.g., customer data on physical and virtual hard drives)	No	Not applicable (customer managed)	Not applicable
Logs: Usage Data/Telemetry	Yes	Access ID, time, authorization granted or denied, diagnostic data such as trace and crash files, and other relevant information and activity.	To (i) provide, secure, manage, measure and improve the product; (ii) bill customer, manage customer account, run internal reports, and develop product strategy; and (iii) comply with contractual obligations, policies, applicable law, regulation, or valid government request.
Logs: Security	Yes	IP address, user domain name, username	To perform security operations and monitoring for the product environment and detect any anomalies

Legal Bases for Personal Data Processing

Cloud Software Group processes personal data based on the following legal bases:

- consent from product users;
- compliance with legal obligations;
- legitimate interests, which may include but are not limited to: product and data security, product license

compliance, product improvement, and development of new products and product features

Third-Party Vendors and Subprocessors

To provide Citrix DaaS, Cloud Software Group has engaged the following third parties:

Vendor Name	Subprocessor Status[1]	Services Performed	HQ Location(s)	Office Locations	Contact for Inquiries	Vendor's Subprocessors
Akamai Technologies	Subprocessor	Content Delivery and monitoring	United States	https://www.akamai.com/company/locations	Akamai Technologies, Inc. 145 Broadway Cambridge, MA 02142 USA privacy@akamai.com	https://www.akamai.com/legal/compliance/privacy-trust-center/list-of-sub-processors
Amazon Web Services	Subprocessor	Machine learning service	United States	https://www.amazon.jobs/en/locations/	Amazon.com LLC 410 Terry Avenue North Seattle, WA 98109-5210 USA aws.amazon.com/contact-us/compliance-support/	https://aws.amazon.com/compliance/sub-processors/
Firebase(Google Cloud Platform)	Subprocessor	Traffic/event analysis	United States	about.google/intl/en_us/locations/	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA support.google.com/policies/contact/general_privacy_form	https://firebase.google.com/terms/subprocessors
Functional Software, Inc. (dba Sentry)	Subprocessor	Monitor logs and events	United States	https://sentry.io/about/	Functional Software, Inc. 45 Fremont Street 8th Floor San Francisco, CA 94105	https://sentry.io/legal/subprocessors/

[1] A subprocessor is a vendor that processes personal data on behalf of Cloud Software Group.

					USA security@sentry.io	
Google Chronicle	Subprocessor	Security monitoring, logging and analytics	United States	about.google/intl/en_us/locations/	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA support.google.com/policies/contact/general_privacy_form	https://cloud.google.com/terms/secops/subprocessors
Google Cloud Platform	Subprocessor	Traffic logging and analysis	United States	about.google/intl/en_us/locations/	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA support.google.com/policies/contact/general_privacy_form	https://cloud.google.com/terms/subprocessors
Grafana Cloud	Subprocessor	Monitoring	United States	https://grafana.com/docs/grafana-cloud/account-management/regional-availability/	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA support.google.com/policies/contact/general_privacy_form	https://grafana.com/docs/grafana-cloud/security-and-account-management/regional-availability/
Microsoft Azure	Subprocessor	Storage and diagnostics	United States	https://www.microsoft.com/en-us/about/office-locations	Microsoft Corporation One Microsoft Way Redmond, Washington 98052 USA privacy.microsoft.com/en-US/privacystatement#mainhowtocontact	https://www.microsoft.com/en-gb/trust-center/privacy/data-access

					usmodule	
Pendo	Subprocessor	In-App communications and analytics	United States	Israel, Japan, United Kingdom	Pendo.io 150 Fayetteville St. Raleigh, NC 27601 USA gdpr@pendo.io	https://trust.pendo.io/subprocessors
SendGrid (Twilio)	Subprocessor	Email Service Provider	United States	https://sendgrid.com/careers/locations/	Twilio Inc. 375 Beale Street Suite 300 San Francisco, CA 94105 USA Or Twilio Inc. 25 N Wall Quay, North Wall Dublin 1, D01 H104 Ireland privacy@twilio.com	https://www.twilio.com/en-us/legal/sub-processors
Splunk	Subprocessor	Security monitoring, logging and analytics	United States	https://www.splunk.com/en_us/about-splunk/contact-us.html#office-locations	Splunk Inc. 270 Brannan Street San Francisco, California 94107 USA dpo@splunk.com	https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet&search_keyword=splunk#/19756406092799239
Wiz	Subprocessor	Application security	United States	https://www.wiz.io/contact	One Manhattan West 52nd Floor New York, NY 10001 USA privacy@wiz.io	https://www.datocms-assets.com/75231/1743575496-wiz-subprocessor-list-april-02-2025.pdf

Data Security and Certifications

As of the publication of this data sheet, Citrix DaaS certifications include the following:

- **System and Organization Controls (SOC) 2 reports.** Citrix DaaS undergoes regular SOC 2 assessments by a licensed CPA firm that issues a resulting SOC 2 report. The SOC 2 report is used to verify the design and operating effectiveness of Citrix internal controls. The report provides detailed information and assurance about the protections relevant to the security, availability, and confidentiality of customer data.

- **ISO/IEC 27001.** Citrix DaaS has services certified with the internationally recognized ISO/IEC 27001 standard. This is part of the ISO 27000 series of standards that focuses on information security, risk management, and privacy management which, when combined, creates a globally recognized framework applicable to organizations of all sizes and sectors.
- **HIPAA.** Citrix DaaS offers HIPAA configurations for certain services and Business Associate Agreements for those customers who need to store or process covered health information in the cloud. Citrix DaaS undergoes an annual independent assessment evaluating our services and controls under the HIPAA Security, Privacy, and Breach Notification Rules.
- **IRAP.** Citrix DaaS has services accredited at the "Protected" level with the Australian Information Security Registered Assessors Program (IRAP) standard.
- **PCI DSS.** Citrix DaaS has services that are certified with Payment Card Industry Data Security Standard (PCI DSS), a mandatory global set of security standards developed by the PCI Security Standards Council for all entities that process, store, or transmit cardholder data. Its purpose is to protect cardholder data and reduce credit card fraud by establishing technical and operational requirements for maintaining a secure payment environment.

Beyond the above product security certifications, Citrix DaaS includes the following baseline security features:

- **Encryption.** Citrix maintains a Certificate, Credential, and Secret Management policy which covers authentication and credential lifecycles, including the requirements for encryption key management.
    - In transit. All data in transit is encrypted using TLS 1.2 or higher. Citrix Cloud authenticates administrators and stores user tokens as needed (by prompting the administrator explicitly) on encrypted storage.
    - At rest. Citrix Cloud storage is encrypted during the provisioning process (e.g., Storage Accounts, Microsoft Azure SQL databases, etc.). Encryption keys are AES-256 bit or higher.

  Hypervisor passwords have a second level of encryption with keys managed by Citrix.

- **Key management.** Citrix has key management policies in place to ensure the protection of all customer data, and Citrix does not bind keys to identifiable owners. Citrix manages the unique encryption of customer data in the Citrix Cloud platform by leveraging cloud native key management. Depending on the customer's choice of control plane, Azure Key Vault or Google Cloud Platform Secret Manager is used for key management in Citrix Cloud in accordance with Citrix's Global Security Assurance policies and standards. The customer can manage encryption of the data in the resource domain that they control. For DevOps engineers that administer the services, the keys that have access to the services are rotated at a regular frequency. Per Citrix's security encryption standards, database administrators do not have access to keys stored in databases.

Data Storage

Citrix DaaS customer data is hosted on Azure or Google Cloud, based on customer preference. When a Citrix DaaS customer is onboarded to a Citrix cloud service, they are asked to choose one of the following regions for the location of the data center that will host their cloud services environment: United States, European Union, and Asia Pacific South.

Citrix cloud services use the customer's designated region to store customer content and logs, except with select logs collected by Citrix sub-processors or for which non-regional storage is necessary for performance of the service. This covers support or troubleshooting, monitoring performance, security, auditing, and cross-region authentication (such as when an EU-based support engineer needs to access a US-based environment). Customer content and logs may be accessed on a global basis as necessary to perform these services.

See Geographical Considerations for more details.

For all Cloud services, logs and customer content may be backed up to a disaster recovery datacenter and mirrored in real time to a secondary server location to ensure service can be quickly resumed in case of a disruption at the primary location. Backups may be stored in different data centers for redundancy, but are located in the same region as the production environment.

©2025, Cloud Software Group, Inc.
www.cloud.com

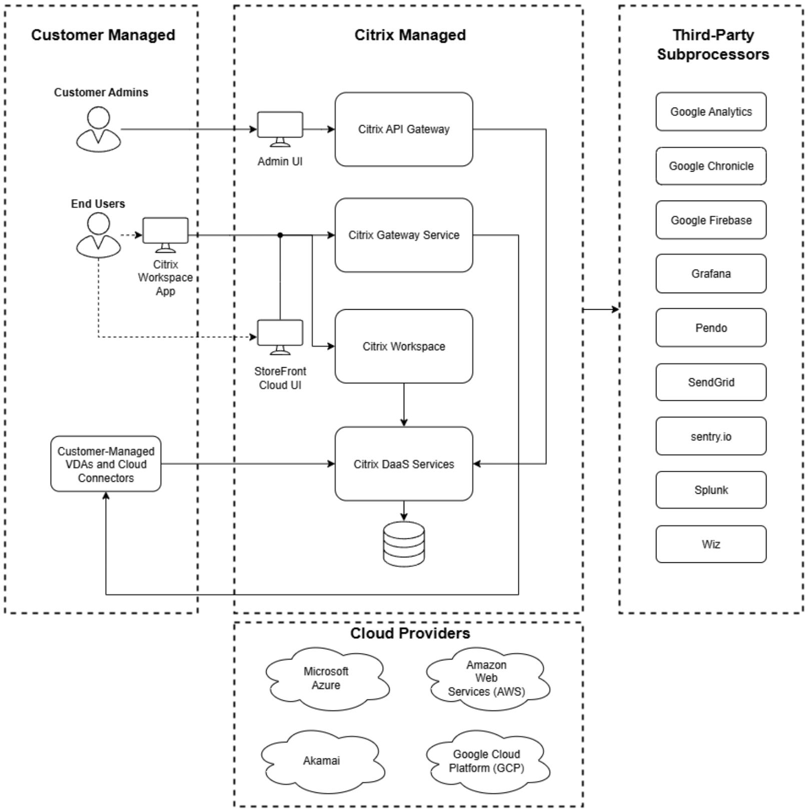
Data Retention, Disposal & Return

Cloud Software Group retains data in line with its customer data retention standards for periods specified below.

Data Category	Data Retention Period	Disposal Mechanism	Data Return Options
Product Admin User Data	Deleted within 90 days of end of contract	Removal of data	N/A
End User Data	Deleted within 90 days of end of contract	Removal of data	N/A
Customer Content (e.g., customer data on physical and virtual hard drives)	N/A	N/A	N/A
Logs: Usage Data/Telemetry	up to 90 days	Removal of data	N/A
Logs: Security	12 months	Removal of data	N/A

Data Flow Diagram

DaaS Data Flow Diagram



©2025, Cloud Software Group, Inc.
www.cloud.com

Other Information Relating to Citrix DaaS's Privacy & Data Protection Impacts

- **Data Minimization**. Citrix DaaS only processes personal information for specific limited purposes. Upon termination or expiration of the contract, data (including personal information) is deleted in accordance with our End User Agreement.
- **Data Subject Rights (DSR) Requests**. Citrix DaaS customers can delete, correct, and/or access their Customer Content during the course of their active subscription, through self-serve features. Citrix DaaS admin and end users can update their account-related personal information upon request. Other data subjects who are non-Citrix DaaS users may submit a product-related DSR request with the relevant Citrix DaaS customer, who bears primary responsibility for responding to such a request. Additionally, Cloud Software Group has operationalized a DSR request process, which advises individuals to forward product-related DSR requests to the responsible customer to handle.
- **Cross-Border Data Transfers**. Customers may configure their Citrix DaaS instance and pick between the following regional instances: US, EU, APS, Japan. Cloud Software Group relies on Standard Contractual Clauses (SCCs) to transfer personal information from the EU and the UK. Cloud Software Group also operationalizes transfer impact assessments with regard to such transfers. In our agreements with subprocessors, we also include EU Standard Contractual Clauses for transfers to countries not deemed to provide an adequate level of protection.

AI Governance

As of the publication date of this data sheet, Cloud Software Group does not provide any covered AI systems[2] through Citrix DaaS.

Related Resources

- Citrix DaaS Product Documentation
- Cloud Software Group Services Security Exhibit
- Cloud Software Group Privacy Statement
- Cloud Software Group Subprocessors List
- Cloud Software Group Data Processing Agreement

About This Data Sheet

Please note that the information provided within this product privacy & AI governance data sheet concerning technical or professional subject matter is for general awareness only. It may be subject to change without notice and does not constitute legal or professional advice, warranty of fitness for a particular purpose, or compliance with applicable laws. Customers are responsible for conducting their privacy/data protection and AI governance assessments of this product as implemented in their environment(s).

[2] An **AI system** means "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments." EU AI Act, Art. 3(1).

cloud™
SOFTWARE GROUP

©2025, Cloud Software Group, Inc.