Cisco Cloudlock

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Cloudlock.

Cisco Cloudlock is a cloud-based security solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from Cisco Cloudlock in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the customer relationship. Cisco is the Data Processor for the personal data processed by Cisco Cloudlock in order to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

Cisco Cloudlock is a cloud-based Cloud Access Security Broker (CASB) and cloud cybersecurity platform that helps organizations securely leverage use of applications in the cloud such as Office 365, Salesforce, Box and others ("Covered SaaS Environments"). Cisco Cloudlock delivers visibility and control for cloud application environments across users, data, and applications.

For additional information on Cisco Cloudlock subscriptions, please see the Offer Description applicable to Cisco Cloudlock (the "Offer Description") available at: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html

Depending upon the applicable Cisco Cloudlock subscription, customers may be afforded the right on an opt-in basis to access and use Cisco Umbrella features as part of their Cisco Cloudlock subscription, including by way of example, DNS monitoring, Umbrella App Discovery and Umbrella Cloud Malware. Please see the Cisco Umbrella Privacy Data Sheet for information regarding the processing of personal data by Cisco Umbrella.

For information regarding the processing of personal data for the delivery of support, please see the Cisco Technical Assistance (TAC) Service Delivery Privacy Data Sheet by visiting the Cisco Trust Portal.

2. Personal Data Processing

Cisco Cloudlock analyzes user activities and scans data residing on Covered SaaS Environments to look for sensitive information based on policies selected by the customer, suspicious user activity and connected applications as described above. Therefore, Cisco Cloudlock processes personal data associated with the user in order to associate a particular user with that user's account (or that user's ID or e-mail address) and that user's data, actions and applications. This processing of personal data is required to provide the security and controls to a customer that are enabled through Cisco Cloudlock. The following paragraphs describe which personal data Cisco processes to deliver the Cisco Cloudlock services, the location of that data and how it is secured in accordance with privacy principles, laws and regulations.

It is important to note that while the DLP feature scans data residing on Covered SaaS Environments, the content scanned by Cisco Cloudlock is encrypted in transit to Cisco Cloudlock, is scanned only in active memory, and does not persist in Cisco Cloudlock. As further described below in Section 7, Cisco Cloudlock retains and stores only administrative registration data and service metadata needed to allow a customer's IT and security staff to identify and review incidents, alerts, and events raised by the service as well as reports generated by the service.

The tables below list the personal data processed by Cisco Cloudlock to provide its services and describes why the data is processed.

Personal Data Category	Types of Personal Data	Purpose of Processing

Registration Data	• First and Last Name • Email Address • Company name	• Activation of Service • Billing/invoicing • Future notification of features/updates • Authentication/Authorization/License Management
DLP	• User ID and/or e-mail address • User first and last name • Any personal data that may be stored on the Covered SaaS Environment including in any file, posting, attachment, record or other assets scanned by Cisco Cloudlock	• This feature and the personal data processed are necessary to allow Cisco Cloudlock (and customer's Cisco Cloudlock administrators) to discover, monitor and control sensitive information (including personal data) stored in files and application fields by a customer's users in the applicable Covered SaaS Environments. • Detection of sensitive information is done through the use of customer-selected or customer-defined policies, such as a policy that looks for a pattern or expression matching a credit card number or social security number. When a policy identifies a potential violation, an incident record is established. • The content of files inspected by Cisco Cloudlock is not stored. See Section 7 for the Cisco Cloudlock Metadata that is stored by the service.
	For Webex customers that have authorized Cloudlock for meetings DLP: • Meeting title • Meeting host email ID • Meeting attendees email IDs • Meeting date, duration • Meeting transcript	• The meeting transcript is scanned in active memory for policy violations but is not stored.
	• OAuth Keys including username and password of admin that authorized access	• Authentication and authorization to Covered SaaS Environment to be scanned for DLP • Enables Cloudlock to inspect the file metadata and content of files stored in the applicable Covered SaaS Environment and assess violations with SaaS API-based DLP configured DLP criteria.
UEBA	• User ID and/or e-mail address • User first and last name • IP Address • Browser and operating system version information • Geolocation • Associated actions and events on the Covered SaaS Environments, including names of files or assets created, modified or accessed by user	• For customers that elect to use this feature, processing is necessary to perform user activity anomaly detection and user activity logging and reporting. UEBA employs statistical analysis and heuristics to assess user activity and identify anomalous behavior. Events represent end user activities, such as login attempts and failures, login locations, administrative actions, changes in privilege, and other events depending on the protected platform. • As is the case with DLP, Cisco Cloudlock processing results in the creation of incidents identifying events that violate policies established in Cisco Cloudlock by the customer's organization, as well as sequences of events that trigger anomaly detection and other automated threat detectors established by Cisco Cloudlock. • The event data as described above is stored by Cisco Cloudlock for the purposes of providing display, search, filter, reporting and export capabilities in the product to enable forensic research across all user activities.

Apps Firewall	• User ID and/or e-mail • Address • User first and • Last name, • IP Address and associated cloud applications installed via OAuth access through the Covered SaaS Environment	• Processing is necessary to provide visibility into applications connected to a customer's environment by its users via an OAuth connection through the Covered SaaS Environments. Apps Firewall provides a risk rating for individual applications as well as the ability to ban or approve apps based on risk profile and access scope. Apps Firewall enables the customer to increase employee awareness with e-mail alerts and to revoke application use in bulk across the user base.
Audit Logs	• Admin email associated with Cloudlock account • Actions audited (e.g. log-in, log-out) • Time stamp	• Audit actions of Admin taken on the CloudLock service
Incident Metadata	A combination of the event (DLP, UEBA or Apps Firewall) and a policy match or violation. Please see Section 7 for a list of the incident metadata retained by Cloudlock.	• Incident metadata is processed in order to allow customers to determine whether a policy match or violation has occurred, for purposes of security and threat detection.

3. Data Center Locations

Cisco Cloudlock uses Amazon Web Services (AWS) data centers in the AWS East/West regions of the United States. AWS offers robust controls to maintain security and data protection. Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC reports provide additional details on the specific control activities executed by AWS. More details can be found at: https://aws.amazon.com/compliance/ and https://aws.amazon.com/security/.

Data is transmitted to Cisco Cloudlock from Covered SaaS Environments exclusively via secure HTTPS connections protected by standard internet encryption protocols. If a customer's Covered SaaS Environment data is stored outside of the United States (for example, if the customer's salesforce.com data resides in an EU based data center), then such data is transferred from the EU to Cisco Cloudlock in the United States. Such data is scanned in active memory for the purposes described above but does not persist in Cisco Cloudlock except for registration information and Cisco Cloudlock metadata as described in Section 7 below.

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- Global Cross-Border Privacy Rules
- Global Privacy Recognition for Processors
- EU Standard Contractual Clauses
- EU-U.S. Data Privacy Framework and the U.K. Extension to the EU-U.S. Data Privacy Framework
- Swiss-U.S. Data Privacy Framework

5. Access Control

Cisco Cloudlock provides the minimum set of secure access methods and interfaces necessary for both Cisco Cloudlock staff access and for customer access. These access methods are created according to the principle of least privileged access. Cisco Cloudlock staff require access in order to administer the system. Customers require access in order to configure, manage and operate the service. These interfaces are secured using several methods including encrypted channels, strong multi-factor authentication, jump server proxy hosts, role-based access controls and detective and preventive security controls via network and host security systems.

The table below lists the personal data used by Cisco Cloudlock to carry out the service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access

Registration Information	Cisco Cloudlock	Activation, billing, support (see Section 2, Personal Data Processing)
DLP **UEBA** **Apps Firewall**	Cisco Cloudlock	Access provided on a need-to-know basis. Prior authorization required. Access required to deliver, support, upgrade and improve services, and perform code deployment.
Audit Logs **Incident Metadata**	Customer Administrators	Set policies, view incidents and alerts, take actions, review audit logs
OAuth Keys	Cisco Cloudlock	Enable authentication to Covered SaaS Environments; encrypted storage
	Customer Administrators	Revoke OAuth keys

6. Data Portability

Data Portability requirements are not applicable to this product.

7. Data Deletion & Retention

Cisco Cloudlock metadata ("Cisco Cloudlock Metadata") is stored on Cisco Cloudlock AWS environments in the United States. Cisco Cloudlock Metadata may include items from the following list, which applies to documents, objects, and assets, depending on the protected platform. A detailed list of metadata fields is available on request.

Policies Implemented by Customer

- Personal data, if any, included in the Customer policies (for example, a policy may state that all users other than John Smith should be monitored)

For protected Documents, Objects, or Assets, Cisco Cloudlock stores:

- Name of the document, object, or asset
- Document or Object ID
- Owner's email address
- Collaborators' email addresses and access rights
- Attributes (for example, file type, object type, last modification time, creation time, size, etc.)
- Redacted snippet of data in violation of a policy (for example, upon detection of a credit card number ending in "6899", the following would be recorded: "XXXXXXXXXXXX6899")

For Webex customers that have authorized Cloudlock for meetings DLP, Cisco Cloudlock also stores:

- Meeting title
- Meeting host email ID
- Meeting attendees email IDs
- Meeting date, duration

For UEBA events, Cisco Cloudlock stores:

- Time of event
- Username, user's email address, first and last name
- IP address and geolocation
- User-agent string, including device type, operating system and browser versions
- Full name for Folder, File or Asset created, modified or accessed by user in activity
- Username, email, first and last name for other users affected by user's activity
- Other attributes (for example: target system and subsystem accessed; type of activity; related events etc.)

For incidents, Cisco Cloudlock stores:

- Audited actions performed on an object triggering an incident (the object itself is not stored by Cisco Cloudlock)

For Covered SaaS Environments, Cisco Cloudlock stores:

- Domain, organization name and subdomain names, if any.
- Usernames associated with the domain, including internal and external collaborators; first and last names
- Groups, Organization Units, and the associated users
- Authorization keys enabling platform integration (OAuth Keys)

See the table below for retention periods.

Type of Personal Data	Retention Period	Reason for Retention
Registration Data	• Retained during customer subscription and for 180 days after a customer's subscription ends ("Post Subscription Retention Period"). Deleted promptly upon expiration of Post Subscription Retention Period.	• Retention of administrative data required for legitimate business purposes (e.g., billing, notifications, support, managing entitlements and renewals) records
Cisco Cloudlock Metadata and OAuth Key - DLP	• Retained during customer subscription and for Post Subscription Retention Period. Deleted promptly upon expiration of Post Subscription Retention Period. • Customers can revoke the Oauth Keys at any time at their discretion. Revocation of the keys will disable Cisco Cloudlock's access to the applicable cloud environment.	• Ongoing feature usage and reporting
Cisco Cloudlock Metadata - UEBA Events	• Retained in UI for 90 days and in database for 180 days.	• Ongoing feature usage and reporting
Cisco Cloudlock Metadata - Apps Firewall	• Retained during customer subscription and for Post Subscription Retention Period. Deleted promptly upon expiration of Post Subscription Retention Period.	• Ongoing feature usage and reporting
Cisco Cloudlock Metadata - Audit Logs	• Retained for 12 months during customer's subscription (deleted on rolling 12 month basis). Deleted after the customer's subscription end promptly upon expiration of the Post Subscription Retention Period.	• Ongoing feature usage and reporting
Cisco Cloudlock Metadata - Incident Metadata	• Resolved incidents retained for 12 months during customer's subscription (deleted on rolling 12 month basis). • All other incident records (new, dismissed, in progress) retained during customer's	• Ongoing feature usage and reporting,

	subscription and for Post Subscription Retention Period. Deleted promptly upon expiration of the Post Subscription Retention Period.	

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Data is encrypted in transit to Cisco Cloudlock. OAuth keys enabling access to the Covered SaaS Environments are encrypted in storage.

9. Sub-processors

Cisco partners with service providers that act as sub-processors of personal data and contract to provide the same level of data protection and information security provided to you by Cisco. A current list of sub-processors for the Cisco Cloudlock service is below:

Sub-processor	Service Type	Personal Data	Location of Data Center
Amazon Web Services, Inc.	Cloud Service Infrastructure	See Section 2 and Section 7	United States (East and West regions)
Datadog	Administrative system logs	User email, File ID, geolocation,	United States

10. Information Security Incident Management

The Information Security team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

11. Certifications and Compliance with Privacy Laws

The Security & Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security.

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security. Cisco Cloudlock security related certifications include:

FedRAMP: Cisco Cloudlock has received a FedRAMP ATO (authorization to operate) in partnership with their sponsor, the GSA, for the Cisco Cloudlock federal environment. The Cisco Cloudlock federal environment complies with required additional security controls under the FedRAMP program, a description of which are available to Government customers

SSAE16 – SOC 2 Type 2 Certified: Cisco Cloudlock is SOC 2 Type 2 certified for both the federal and commercial Cisco Cloudlock environments. The SOC 2 report provides a description of the Cisco Cloudlock controls, environment and external audit of Cisco Cloudlock controls that meet the AICPA Trust Services Security Principle and Criteria.

SOC 3 Certified – Trust Services Report for Service Organizations: Cisco Cloudlock has met the AICPA Trust Services Security Principle and Criteria.

12. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

We will confirm identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller, may be redirect to their employer for a response.

Requests can be made by submitting a request via:

1) the Cisco Privacy Request form
2) by postal mail:

<table>
<tr><td colspan="3">Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td><td>APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td>EMEA Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Zuidoost NETHERLANDS</td></tr>
</table>

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data processed or transferred by Cisco remains unresolved, contact Cisco's US-based third-party dispute resolution provider. Alternatively, you can contact the data protection supervisory authority in your jurisdiction for assistance. Cisco's main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch Autoritiet Persoonsgegevens.

13. General Information

For more general information and FAQs related to Cisco's Security and Privacy Program please visit The Cisco Trust Center.

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.

To receive email notifications of updates to the Privacy Data Sheet, click the "Subscribe" link in the upper right corner of the Trust Portal.