Duo

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

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

Cisco will process personal data from Duo 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 Duo in order to provide its functionality.

1. Overview of Cisco Duo Capabilities

Duo is a cloud-based software service that provides customers additional layers of security designed to protect access to proprietary and third party applications. Most applications only require a username and password prior to allowing a user to login. When protected with Duo, the username and password will first be verified on the customer/application side (or with the assistance of Duo-hosted SSO, depending on customer's settings) before triggering Duo's two-factor workflow by requiring the user to take additional action before the login process can be completed (e.g. confirming login via Duo's mobile app, SMS, phone call, or hardware token). Customers can further check the security hygiene of user devices before granting access and block, notify, or restrict access for users with risky devices. Duo also allows customers to control which internal applications are accessible by different groups of users to limit exposure to sensitive information and enforce policies at an application level.

You may be asked to provide your personal data in order to use the service. The following paragraphs describe Cisco's processing of personal data in connection with the delivery of Duo, the location and transfers of that data, and how it is secured in accordance with privacy principles, laws, and regulations. If you choose to use the Duo services, you will need to disclose personal data to Cisco. Cisco will use your personal data consistent with this Privacy Data Sheet.

Please see the following link for more details on Duo: https://duo.com/docs.

The following paragraphs describe which personal data Duo processes to deliver its services, the location of that data, and how it is secured in accordance with privacy principles, laws, and regulations.

Your use of Duo may include the option to use Cisco Identity Intelligence (CII). CII is an API-driven, cloud-native, and agentless platform that provides a unified view of all the identities within, and interacting with, an organization and then helps remediate risks at scale. Please see the Addendum for information on this capability and how it processes personal data.

2. Personal Data Processing

The table below lists the personal data used by Duo to carry out the services and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
End-User Registration/Authentication Information	• Username • Telephone number • Email address • Organization name • A user's Active Directory username & password for those users authenticating via Duo-hosted SSO (password is processed only long enough to complete each authentication and not retained after authentication) • A user's password if created for use with Duo Directory[1] • Custom Attributes defined and configured by Customer in Duo Directory (e.g., an employee's	• Account creation and activation • Service authentication and login • Deliver, support, improve security functionality, upgrade and improve the services

	role, nickname, username, or office location)	
Administrator Registration Information	• Name • Username • Telephone number • Email address • Billing and delivery address • One-way hashed representations of password(s) for the Duo Administrator Panel • Job title • Organization name	• Account creation and activation • Service authentication and login • Sending communications to you, including for marketing or customer satisfaction purposes, either directly from Cisco or from our partners • Deliver, support, improve security functionality, upgrade and improve the service
End-User Device Metadata[2]	• Type of device • Device operating system, device version, and other device characteristics (e.g., if a device is "jailbroken" or has a screen lock in place) • Connection information - such as encryption protocol(s) being used to access the Duo service • Browser type • IP address • Whether a Public Key Infrastructure Certificate is installed • Time zone • Time and date of authentication • Broad geographic area (country or city-level location) • Application that device is attempting to access • Whether device is utilizing certain plugins • The device's fully qualified domain name associated with the end-user • Device identifiers (e.g., device name, processor ID, serial numbers, UDIDs, UUIDs, DNS Hostname) • Snapshot of device location represented by hash value derived from visible SSID at time of capture	• Provide and maintain the services • Improve user experience • Improve security functionality • Improve quality of the services • Ensure secure devices and/or applications • Issue certificates verifying device is secure • Authenticate device • Conduct statistical analysis with pseudonymized and/or aggregate usage data to improve the services • Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, security risks, and criminal activity
Events and Usage Data	• How end-users access the services • Dates and times of access • IP address for determining where the services are accessed • Device events (e.g., crashes, system activity, hardware settings)	• Provide and maintain the services • Improve user experience • Improve security functionality • Improve quality of the services • Conduct statistical analysis with pseudonymized and/or aggregate usage data to improve the services • Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, security risks, and criminal activity

Authentication and Activity Logs	• Which end-users access the services • Which devices access the services • Applications protected by the services • Time when the services are accessed • End-user IP address when accessing the services	• Provide and maintain the services • Improve user experience • Improve security functionality • Improve quality of the services • Conduct statistical analysis with pseudonymized and/or aggregate usage data to improve the services • Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, security risks, and criminal activity
AI Assistant Data[3]	• Prompts and feedback typed into text fields by end-users including any personal data therein • Personal data fetched by the AI assistant in response to prompts, such as admin, user, or event data • Which end-user accesses the AI assistant	• Provide context for a large language model for the purpose of assisting customers in answering product-related questions.

[1] Duo adheres to industry best practices for password security by using strong hashing algorithms, high iteration counts, unique random salts for each password before hashing, and a secret per-customer pepper. Duo stores password hashes and salts in databases with strict access controls that are encrypted at rest.

[2] Duo Passwordless does not record or collect user biometric data in any way. Where available, it can request use of device biometric capabilities in a way that does not involve any biometric data leaving the device.

[3] End-users should not include any confidential information or personal data that they do not want processed into AI Assistant prompts.

3. Data Center Locations

Duo is headquartered in the United States and operates internationally. Duo uses Amazon Web Services (AWS) data centers in the United States, Canada, Ireland, France, Germany, Switzerland, Australia, Japan, Singapore, Indonesia, the United Kingdom, India, and the UAE.

Hosting region is automatically selected based on the country of the phone number during sign-up (or based on country selected during certain methods of provisioning). The countries that are selected for each hosting region are listed in the table below.

Customers may also request that their production hosting be in any region listed below.

If you use the CII functionality of Duo, your personal data from this functionality will be hosted in accordance with Section 3 of the Addendum.

Region	Infrastructure Provider	Automatically selected during sign-up for phone numbers from these countries	Data Center Locations
United States	AWS	United States	Multiple regions and availability zones in the United States.
Canada	AWS	Canada	Multiple regions and availability zones in Canada.
EU	AWS	All other countries not listed	Single regions and multiple availability zones in France and Ireland.
DACH	AWS	Germany, Austria, Switzerland, Denmark, Finland, Iceland, Norway, and Sweden	Single regions and multiple availability zones in Germany and Switzerland.

ANZ	AWS	Australia, Cook Islands, Fiji, French Polynesia, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, New Caledonia, New Zealand, Niue, Pitcairn, Samoa, Solomon Islands, Tokelau, Tonga, Tuvalu, Vanuatu, Wallis and Futana	Multiple regions and availability zones in Australia.
Japan	AWS	Japan	Multiple regions and availability zones in Japan.
ASEAN	AWS	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam	Single regions and multiple availability zones in Singapore and Indonesia.
United Kingdom	AWS	United Kingdom, British Overseas Territories	A single region and multiple availability zones in the United Kingdom.
India	AWS	India	Multiple regions and availability zones in India.
UAE	AWS	Bahrain, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, UAE	A single region and multiple availability zones in the UAE

4. Cross-Border Data Transfer Mechanisms

Duo's support staff throughout the world may have access to personal data stored in the United States or elsewhere. Additionally, certain personal data (e.g. phone numbers) may be transferred across borders to Duo's third party vendors for purposes related to providing the Services, such as sending text messages with authentication codes or making automated VOIP-based calls that verify logins wherever the end-user is located.

Duo has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- 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

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

Personal Data Category	Who has Access	Purpose of the Access
End-User Registration / Authentication Information	Customer administrator	Modify and control access to the services and other administrator information
	Cisco	Support the services in accordance with its data access and security controls process
Administrator Registration Information	Customer administrator	Modify and control access to the services and other administrator information
	Cisco	Deliver, support, upgrade and improve the services
End-User Device Metadata	Customer administrator	Set policies for customer network, monitor customer network, and limit or approve access to users and applications
	Cisco	Deliver, support, upgrade and improve the services
Events and Usage Data	Customer administrator	Set policies for customer network, monitor customer network, and limit or approve access to users and applications
	Cisco	Deliver, support, upgrade and improve the services

Authentication and Activity Logs	Customer administrator	Set policies for customer network, monitor customer network, and limit or approve access to users and applications
	Cisco	Deliver, support, upgrade and improve the services
AI Assistant Data	Customer Administrator	Receive assistance with answering product questions
	Cisco	Deliver, support, upgrade and improve the services

6. Data Retention

A user may request deletion of personal data at any time by contacting their Organization/Controller. Duo Account Administrators can reference the following article to process individual deletion requests: https://help.duo.com/s/article/2162?language=en_US.

Duo only keeps personal data for as long as it has an ongoing legitimate business need to do so. This includes retaining such personal data at all times that a customer has at least one active account for the services. However, customers do have the ability to delete user/administrator registration information and logs, as set forth below (note that it may take up to 30 days for certain manually deleted data to fully purge from Duo's systems).

The Duo multi-tenant service is architected to provide strong guarantees around data integrity and availability of customer data. A core component of this architecture requires a balance between the need to purge data associated with previously deleted customers while ensuring that data associated with remaining active customers is properly maintained and protected.

The following table explains Duo's default personal data retention policies, the length of time that data needs to be retained, and why we retain it, which will apply in all cases that a customer does not take other action available within the Duo Admin Panel:

Personal Data Category	Retention Period After Account Deletion	Reason for Retention
End-User Registration/Authentication Information	1 year (unless deleted sooner by customer)*	This retention period was selected because it provides a balance between the need to purge data associated with previously deleted customers and ensuring that data associated with remaining active customers is properly maintained and protected.
Administrator Registration Information	1 year (unless deleted sooner by customer)	This retention period was selected because it provides a balance between the need to purge data associated with previously deleted customers and ensuring that data associated with remaining active customers is properly maintained and protected.
End-User Device Metadata	1 year (unless deleted sooner by customer)	This retention period was selected because it provides a balance between the need to purge data associated with previously deleted customers and ensuring that data associated with remaining active customers is properly maintained and protected.
Events and Usage Data	1 year (unless deleted sooner by customer)*	This retention period was selected because it provides a balance between the need to purge data associated with previously deleted customers and ensuring that data associated with remaining active customers is properly maintained and protected. *Debug logs may reside in Duo's systems for up to 90 days after their creation for customer support purposes, security review, and to monitor and alert on patterns of system performance.
Authentication and Activity Logs	1 year (or less, depending on customer's log retention settings)	This retention period was selected because it provides a balance between the need to purge data associated with previously deleted customers and ensuring that data associated with remaining active customers is properly maintained and protected.

AI Assistant Data	1 year (unless deleted sooner by customer)	This retention period was selected because it provides a balance between the need to purge data associated with previously deleted customers and ensuring that data associated with remaining active customers is properly maintained and protected.
Services Backups	3 years beyond the timeframes identified above	Backups are generated on a daily basis, encrypted, and moved into cold storage as a means of providing data integrity and resiliency for the services. This retention period was selected because it is sufficient to cover the majority of scenarios wherein customers may request access to their historical data to serve their own legal discovery or forensics needs.
Data related to Duo's financial, audit or other legal obligations	As long as necessary to meet the relevant obligations	Duo may need to retain certain data related to evidencing financial transactions, audit requirements or for other legal obligations. The retention of any such data will be tied to the timeline under which Duo is required to retain any such data in line with its legal obligation and Cisco's Enterprise Record Retention Schedule.

Pseudonymized Data: Duo additionally may retain copies of the data above for the purpose of supporting the security, quality, and improved functionality of the service. In these copies, all personal data listed above is pseudonymized (except for IP addresses, which are needed in original form for threat detection and related security reasons). After the retention periods above have expired (or 1 year from collection in the case of IP Addresses) from as there will be no remaining production data or account information allowing for re-identification.

Global Threat Intelligence Research: To continually secure Cisco's product portfolio, certain Cisco products share data with the global threat intelligence team, including Cisco Talos and other trusted Cisco security and support personnel, which then processes the data for global threat intelligence and product improvement purposes. If the threat intelligence team determines the data is not malicious, it is deleted on the schedule set forth in this section. Any data that is determined to be malicious, as well as aggregated and de-identified data, including IP addresses, is retained by the threat intelligence team.

7. 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.

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. See AWS' documentation for more information. More details about Duo's physical security can be found within Duo's information security policy, which is available subject to a non-disclosure agreement.

Personal Data Category	Type of Encryption
End-User Registration/Authentication Information	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.
Administrator Registration Information	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.
End-User Device Metadata	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.
Events and Usage Data	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.
Authentication and Activity Logs	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.

AI Assistant Data	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts.

Duo uses multiple techniques to protect customer data, including, but not limited to: network segmentation between datastores and other components of the Duo platform, least privilege access to datastores based upon roles or responsibilities, and hardening of production assets to minimize attack surface.

8. Sub-processors

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

Sub-processor	Personal Data	Service Type	Location of Data Center
AWS	End-User Registration/Authentication Information, End-User Device Metadata, Administrator Registration Information, Events and Usage Data, Authentication & Activity Logs, AI Assistant Data	Cloud based infrastructure and hosting, analytics, data storage	US, Canada, Ireland, Germany, Australia, Japan, Singapore, the United Kingdom, India, and the UAE
Certified Security Solutions d/b/a Keyfactor	End-User Registration/Authentication Information Device IDs (e.g. serial numbers)	PKI service that issues and manages certificates to devices	US
Twilio, Inc.	End-User Registration/Authentication Information	Telephone and SMS for authentication	US
Nexmo Inc.	End-User Registration/Authentication Information	Telephone and SMS for authentication	US
Clickatell, Inc.	End-User Registration/Authentication Information	Telephone and SMS for authentication	US
Bandwidth Inc.	End-User Registration/Authentication Information	Telephone and SMS for authentication	US
Google	End-User Registration/Authentication Information	SMS and push notifications for authentication	US, Ireland
Apple	End-User Registration/Authentication Information	Cloud backup and restore	US
Microsoft	End-User Registration/Authentication Information, End-User Device Metadata, Administrator Registration Information, Events and Usage Data, Authentication & Activity Logs, AI Assistant Data	Allowing customer integration with select Microsoft Azure services to add layers of protection to customer managed cloud applications and synchronization between customer managed Azure AD user directories and the Duo product Hosted large language models for AI assistant functionality	US
Skilljar	Administrator Registration Information	Integrated training platform	US
Salesforce	Administrator Registration Information	Deliver, support, and improve the services	US

Mulesoft	Administrator Registration Information	Assist with Salesforce integration	US
Marketo	Administrator Registration Information	Automated account management	US
Datadog	Events and Usage Data	Monitor infrastructure and service activity, aggregate administrative logs, perform service troubleshooting and diagnostics	US
Amplitude	Events and Usage Data	Analyze feature usage and product functionality	US
Databricks	AI Assistant Data	Analyze AI assistant usage and product functionality	US

9. Information Security Incident Management

Breach and Incident Notification Processes

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), the Advanced Security Initiatives Group (ASIG), and Cisco Legal.

Duo's security team, in collaboration with the Cisco PSIRT team, manages the receipt, investigation, and public reporting of security vulnerabilities related to Duo products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Duo products and networks. Duo's Security Response procedures and the Cisco Security Center detail 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.

10. Certifications and Compliance with Privacy Laws

The Security and 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 security and privacy in mind and is designed so that it can be used by Cisco customers in a manner consistent with global security and privacy requirements.

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations and certifications to demonstrate our commitment to information security and privacy, including a SOC2 Type II audit report and two FedRAMP Authorized editions of the service.

11. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, data portability and / or deletion of the personal data processed by the Service as well as object to processing by contacting their Organization's Administrator. Administrators, please reference the knowledge article in Section 7 for instructions about completing such rights requests. Customers can access data through the Duo administrator panel, as well as programmatically through Duo's administrative APIs.

Additional privacy inquiries or Data Subject Rights support can be sent to Cisco 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.

12. General Information

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

This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement. To the extent this document differs from the Cisco Online Privacy Statement, this document will take precedence. If there is a difference in translated, non-English versions of this document, the U.S.-English version will take precedence.

Cisco frequently evolves and updates its offerings. Cisco Privacy Data Sheets are subject to change, and are reviewed and updated on an annual basis, or as reasonably needed to reflect a material change in the processing of Personal Data. 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.

Cisco Identity Intelligence Addendum

This Privacy Data Sheet Addendum describes how Cisco Identity Intelligence (CII) processes personal data.

1. Overview of Cisco Identity Intelligence

Cisco Identity Intelligence (CII) is an API-driven, cloud-native, and agentless platform that provides a unified view of all the identities within, and interacting with, an organization and then helps remediate risks at scale.

This Addendum only addresses the CII feature. This capability is configurable and may be turned off at any time, in which case none of the data mentioned in this addendum is stored nor processed by Cisco. For information regarding the processing of personal data by Duo please see the Duo Privacy Data Sheet to which this Addendum 1 is attached.

2. Personal Data Processing

The table below describes how personal data may be processed and stored by Cisco when a customer is using CII.

Personal Data Category	Types of Personal Data	Purpose of Processing
Admin Personal Data	• Username • Name • City • Country	• Account creation and activation • Service authentication and login • Sending communications to you, including for marketing or customer satisfaction purposes, either directly from Cisco or from our partners • Deliver, support, improve security functionality, upgrade and improve the service
Admin Audit Log	• Login History • Action History	• Service availability and support
Subject Data	• Name • Username • Telephone number • Email address • Login History (including city and county) • Employment information (including directory role, directory organization, directory reporting structure, directory title, directory department, directory location)	• Account creation and activation • Service authentication and login • Deliver, support, improve security functionality, upgrade and improve the services

3. Data Center Locations

CII uses Amazon Web Services (AWS) data centers in the United States, Germany, Australia, and Japan.

Hosting region is selected based on the country of the customer's primary identity provider or where parties mutually agree. The countries that are selected for each hosting region are listed in the table below.

Region	Infrastructure Provider	Countries Supported	Data Center Locations
United States	AWS	United States	US-east-2 (Ohio)
Canada	AWS	Canada	CA- central-1 (Toronto)
Europe	AWS	All Europe and all other countries not listed	EU-central-1 (Frankfurt)
UK	AWS	UK	EU-west-2 (London)

ANZ	AWS	Australia	AP-southeast-2 (Sydney)
Japan	AWS	Japan	AP-northeast-1 (Tokyo)
ASEAN	AWS	Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam	AP-southeast-1 (Singapore)

4. Cross-Border Data Transfer Mechanisms

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

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC 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

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

Personal Data Category	Who has Access	Purpose of the Access
Admin Personal Data	Customer administrator, Customer Support	Deliver, support, upgrade and improve the services
	Cisco	Support the services in accordance with its data access and security controls process
Admin Audit Log	Customer administrator, Customer Support	Deliver, support, upgrade and improve the services
	Cisco	Support the services in accordance with its data access and security controls process
Subject Data	Customer administrator, Customer Support	Deliver, support, upgrade and improve the services
	Cisco	Support the services in accordance with its data access and security controls process

6. Data Retention

A user may request deletion of personal data at any time by contacting their Organization/Controller. Cisco Identity Intelligence has set up an automatic tool to remove customer data and can be accessed by opening a Cisco support ticket.

CII only keeps personal data for as long as it has an ongoing legitimate business need to do so. This includes retaining such personal data at all times that a customer has at least one active account for the services. However, customers do have the ability to delete user/administrator registration information and logs, as set forth below (note that it may take up to 30 days for certain manually deleted data to fully purge from Cisco Identity Intelligence's system.)

The following table explains personal data retention policies, the length of time that data needs to be retained, and why we retain it, which will apply in all cases that a customer does not take other action.

Personal Data Category	Retention Period	Reason for Retention

Admin Personal Data	Deleted upon customer request	This retention period was selected because it provides a balance between the need to purge data associated with previously deleted customers and ensuring that data associated with remaining active customers is properly maintained and protected.
Admin Audit Log	1 year (unless deleted sooner by customer)	This retention period was selected because it provides a balance between the need to purge data associated with previously deleted customers and ensuring that data associated with remaining active customers is properly maintained and protected.
Subject Data	Deleted upon customer request	This retention period was selected because it provides a balance between the need to purge data associated with previously deleted customers and ensuring that data associated with remaining active customers is properly maintained and protected.

7. 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.

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. See AWS' documentation for more information.

Personal Data Category	Type of Encryption
Admin Personal Data	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts (AES-256)
Admin Audit Log	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts (AES-256)
Subject Data	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts (AES-256)

8. Sub-processors

CII partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for Cisco Identity Intelligence is below:

Sub-processor	Data Processed	Service Type	Location of Data Center
AWS	Subject Data and Admin Personal Data	Cloud based infrastructure and hosting, analytics, data storage	US, Germany, UK, Australia, Canada,Japan, and Singapore
Snowflake	Subject Data and Admin Personal Data	Data Storage and analytics	Colocated with AWS account
Datadog	Subject Data and Admin Personal Data	Data Storage and analytics	US1

9. Information Security Incident Management

Breach and Incident Notification Processes

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), the Advanced Security Initiatives Group (ASIG), and Cisco Legal.

Cisco Identity Intelligence team, in collaboration with the Cisco PSIRT team, manages the receipt, investigation, and public reporting of security vulnerabilities. The team works with customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues. Cisco Security Center detail 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.

10. Certifications and Compliance with Privacy Laws

The Security and 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 security and privacy in mind and is designed so that it can be used by Cisco customers in a manner consistent with global security and privacy requirements.

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations and certifications to demonstrate our commitment to information security and privacy, including a SOC2 Type II audit report.

11. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, data portability and / or deletion of the personal data processed by the Service as well as object to processing by contacting their Organization's Administrator. Administrators, please reference the knowledge article in Section 7 for instructions about completing such rights requests. Customers can access data through the Cisco Identity Intelligence dashboard, as well as programmatically through administrative APIs.

Additional privacy inquiries or Data Subject Rights support can be sent to Cisco 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.

12. General Information

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

If there is a difference in translated, non-English versions of this document, the U.S.-English version will take precedence.

Cisco frequently evolves and updates its offerings. Cisco Privacy Data Sheets are subject to change, and are reviewed and updated on an annual basis, or as reasonably needed to reflect a material change in the processing of Personal Data. 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.