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.

Note that this Privacy Data Sheet is a supplement to the Cisco Privacy Statement.

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.

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 cached only long enough to complete each authentication)	- Account creation and activation - Service authentication and login - Deliver, support, improve security functionality, upgrade and improve the services

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	• 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)	• 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

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, Germany, Australia, Japan, and Singapore.

- Customers using a U.S. based phone number during sign-up will automatically be placed on U.S.-based AWS hosting.

- Customers using a Canadian based phone number during sign-up will automatically be placed on Canadian-based AWS hosting.
- Customers using a phone number based in the ANZ region[1] during sign-up will automatically be placed on Australian-based AWS hosting.
- Customers using a phone number based in Japan during sign-up will automatically be placed on Japan based AWS hosting.
- Customers using a phone number based in the ASEAN region[2] during sign-up will automatically be placed on Singapore-based AWS hosting.
- Customers using a phone number based in any other region where Duo is authorized to provide services will automatically be placed on European-based AWS hosting.
- Customers may request that their production hosting be on any country-specific AWS location utilized by Duo.

Data Center Locations	Infrastructure Provider	Description
United States	• AWS	• The infrastructure for the Duo services runs on Amazon Web Services (AWS) in multiple regions in the United States and spans multiple availability zones (AZs).
Canada	• AWS	• The infrastructure for the Duo services runs on Amazon Web Services (AWS) in a single region in Canada and spans multiple availability zones (AZs).
Ireland	• AWS	• The infrastructure for the Duo services runs on Amazon Web Services (AWS) in a single region in Ireland and spans multiple availability zones (AZs).
Germany	• AWS	• The infrastructure for the Duo services runs on Amazon Web Services (AWS) in a single region in Germany and spans multiple availability zones (AZs).
Australia	• AWS	• The infrastructure for the Duo services runs on Amazon Web Services (AWS) in a single region in Australia and spans multiple availability zones (AZs).
Japan	• AWS	• The infrastructure for the Duo services runs on Amazon Web Services (AWS) in a single region in Japan and spans multiple availability zones (AZs).
Singapore	• AWS	• The infrastructure for the Duo services runs on Amazon Web Services (AWS) in a single region in Singapore and spans multiple availability zones (AZs).

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)
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

5.Access Control

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

---

[1] ANZ region includes 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.

[2] ASEAN region includes Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Phillippines, Singapore, Thailand, and Vietnam.

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
	Duo	Support the services in accordance with its data access and security controls process
Administrator Registration Information	Duo	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
	Duo	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
	Duo	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
	Duo	Deliver, support, upgrade and improve the services

6.Data Portability

Customers can access data through the Duo administrator panel. Requests to extract and export such data can also be made by contacting Duo at privacy@cisco.com.

7.Data Deletion & Retention

A customer may request deletion of personal data at any time by sending a notice to privacy@cisco.com. When a customer makes a request for deletion of personal data stored by Duo, Duo will purge or anonymize the requested data from its systems to the extent required by applicable law and may retain administrative data required for legitimate business purposes (e.g., billing records) as identified below.

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. A copy of this data is also retained to support the security, quality, and improved functionality of the service. When used for these purposes, all personal data is pseudonymized (except for IP addresses, which are needed in original form for threat detection and related security reasons). Once

		the specified retention period has expired (or 1 year from collection in the case of IP Addresses), all personal data used for these purposes will be deleted or anonymized, as there will be no remaining production data or account information allowing for re-identification. *Note that Active Directory passwords for Duo-hosted SSO are only cached long enough to complete each authentication.
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. A copy of this data is also retained to support the security, quality, and improved functionality of the service. When used for these purposes, all personal data is pseudonymized (except for IP addresses, which are needed in original form for threat detection and related security reasons). Once the specified retention period has expired (or 1 year from collection in the case of IP Addresses), all personal data used for these purposes will be deleted or anonymized, as there will be no remaining production data or account information allowing for re-identification.
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. A copy of this data is also retained to support the security, quality, and improved functionality of the service. When used for these purposes, all personal data is pseudonymized (except for IP addresses, which are needed in original form for threat detection and related security reasons). Once the specified retention period has expired (or 1 year from collection in the case of IP Addresses), all personal data used for these purposes will be deleted or anonymized, as there will be no remaining production data or account information allowing for re-identification.
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. A copy of this data is also retained to support the security, quality, and improved functionality of the service. When used for these purposes, all personal data is pseudonymized (except for IP addresses, which are needed in original form for threat detection and related security reasons). Once the specified retention period has expired (or 1 year from collection in the case of IP Addresses), all personal data used for these purposes will be deleted or anonymized, as there will be no remaining production data or account information allowing for re-identification. *Certain 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. A copy of this data is also retained to support the security, quality, and improved functionality of the service. When used for these purposes, all personal data is pseudonymized (except for IP addresses, which are needed in original form for threat detection and related security reasons). Once the specified retention period has expired (or 1 year from collection in the case of IP Addresses), all personal data used for these purposes will be deleted or anonymized, as there will be no remaining production data or account information allowing for re-identification.
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.

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.

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 established since calendar year 2018.
Administrator Registration Information	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts established since calendar year 2018.
End-User Device Metadata	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts established since calendar year 2018.
Events and Usage Data	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts established since calendar year 2018.
Authentication and Activity Logs	Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts established since calendar year 2018.

Duo is actively working towards enabling encryption at rest for accounts created before 2018 (encryption at rest for such accounts may be requested by contacting support@duosecurity.com). Regardless of whether or not the data is encrypted, 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.

9. 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	Cloud based infrastructure and hosting, analytics, data storage	US, Canada, Ireland, Germany, Australia, Japan, Singapore

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 enrolled in Duo Beyond	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	SMS and push notifications for authentication	US
Microsoft	End-User Registration/Authentication Information, End-User Device Metadata, Administrator Registration Information, Events and Usage Data, Authentication & Activity Logs	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	US
Skilljar	Administrator Registration Information	Integrated training platform	US
Salesforce	Administrator Registration Information	Deliver, support, and improve the services	US
Mulesoft	Administrator Registration Infomration	Assist with Salesforce integration	US
Marketo	Administrator Registration Information	Automated account management	US

10. Information Security Incident Management

Breach and Incident Notification Processes

The Data Protection & Privacy 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).

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.

11. 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 privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 4, Cisco has the following:

- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework

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

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 ask to 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:

Chief Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES		
Americas Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES	**APJC Privacy Officer** Cisco Systems, Inc. Bldg 80, Lvl 25, Mapletree Biz City, 80 Pasir Panjang Road, Singapore, 117372 SINGAPORE	**EMEAR Privacy Officer** Cisco Systems, Inc. Haarlerbergweg 13-19, 1101 CH Amsterdam-Zuidoost NETHERLANDS

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.