Privacy Data Sheet

Duo

THIS PRIVACY DATA SHEET WILL BECOME EFFECTIVE UNDER CISCO'S PRIVACY STATEMENT ON OCTOBER 28, 2019

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

1. Overview of Cisco Duo Capabilities

Cisco Duo ("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 require a username and password prior to allowing a user to login. When protected with Duo, an application will first internally determine whether the entered username and password are correct before triggering Duo's workflow by requiring the user to take an additional action before the login process can be completed (e.g., confirming login via Duo's mobile app, SMS, phone call, or hardware token). Duo differentiates itself from many competitors in that, for security reasons, it does not store any user's primary credentials to protected applications. This is designed to force an attacker to compromise multiple systems prior to gaining improper access to customer applications. 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 remote users to limit exposure to personal information and enforce policies at an application level.

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 Information	• Username • Telephone number • Email address • Organization name	• 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 • Deliver, support, 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 identification numbers (e.g., serial numbers, UDIDs, 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 aggregate statistical analysis with pseudonymized usage data to improve the services • Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, 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 aggregate statistical analysis with pseudonymized usage data to improve the services • Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, and criminal activity
Authentication 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 aggregate statistical analysis with pseudonymized usage data to improve the services • Prevent, detect, respond and protect against potential or actual claims, liabilities, prohibited behavior, and criminal activity

3. Cross-Border Transfers

Duo is headquartered in the United States and operates internationally. It uses Amazon Web Services (AWS) data centers: four are located in the United States (two East and two West), one is located in Canada, one is located in Ireland, and one is located in Germany. Customers using a phone number based in Europe, the Middle East, or Africa (collectively, EMEA) will automatically be placed on an EMEA based AWS instance. Customers using any non-EMEA based phone number will automatically be placed on a U.S. based AWS instance. Customers may request for their production instance to be on any country-specific AWS location utilized by Duo.

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. More details can be found within Duo's information security policy, which is available subject to a non-disclosure agreement.

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 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
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses

4. Access Control

Personal Data Category	Who has access	Purpose of the access
End-User Registration Information	Customer administrator	Modify and control access to the services and other admin 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 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

5. Data Portability

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

6. Data Deletion & Retention

A customer may request deletion of personal data by sending a notice to privacy@cisco.com. When a customer makes a request for deletion of their Duo related personal data, Duo will purge 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 data at all times customer has at least one active account for the services. The following table explains Duo's personal data retention policies upon expiration or termination of the services.

Personal Data Category	Retention Period After	Reason for Retention

	Account Deletion	
End-User Registration Information	1 year	The Duo multi-tenant service is architected to provide strong guarantees around data integrity and availability of customer data. The architecture and data storage techniques employed do not allow for data associated with specific customer accounts to be selectively deleted without impact to the integrity or availability of data associated with other customers. 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	The Duo multi-tenant service is architected to provide strong guarantees around data integrity and availability of customer data. The architecture and data storage techniques employed do not allow for data associated with specific customer accounts to be selectively deleted without impact to the integrity or availability of data associated with other customers. 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 in identifiable format	The Duo multi-tenant service is architected to provide strong guarantees around data integrity and availability of customer data. The architecture and data storage techniques employed do not allow for data associated with specific customer accounts to be selectively deleted without impact to the integrity or availability of data associated with other customers. 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	The Duo multi-tenant service is architected to provide strong guarantees around data integrity and availability of customer data. The architecture and data storage techniques employed do not allow for data associated with specific customer accounts to be selectively deleted without impact to the integrity or availability of data associated with other customers. 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.
Authentication Logs	1 year (or less as set by Administrator in the Duo Admin Panel)	The Duo multi-tenant service is architected to provide strong guarantees around data integrity and availability of customer data. The architecture and data storage techniques employed do not allow for data associated with specific customer accounts to be selectively deleted without impact to the integrity or availability of data associated with other customers. 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 timeframe 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.

7. Personal Data Security

Personal Data Category	Type of Encryption
End-User Registration Information	Encryption in transit over Transport Layer Security (TLS), encryption at rest may be requested by contacting Duo at privacy@duosecurity.com
Administrator Registration Information	Encryption in transit over TLS, encryption at rest may be requested by contacting Duo at privacy@duosecurity.com
End-User Device Metadata	Encryption in transit over TLS, encryption at rest may be requested by contacting Duo at privacy@duosecurity.com
Events and Usage Data	Encryption in transit over TLS, encryption at rest may be requested by contacting Duo at privacy@duosecurity.com
Authentication Logs	Encryption in transit over TLS, encryption at rest may be requested by contacting Duo at privacy@duosecurity.com

These data categories are encrypted at rest for all customer accounts established in calendar year 2018 or later. Duo is actively working towards enabling encryption at rest for all customer accounts. 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.

8. Third Party Service Providers (Sub-processors)

Duo partners with service providers who 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 Duo service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
AWS	End-User Registration Information, End-User Device Metadata, Administrator Registration Information, Events and Usage Data, Authentication Logs	Cloud based infrastructure and hosting, analytics, data storage	US, Canada, Ireland, Germany
Certified Security Solutions d/b/a Keyfactor	End-User Registration 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 Information	Telephone and SMS for authentication	US
Nexmo Inc.	End-User Registration Information	Telephone and SMS for authentication	US
Clickatell, Inc.	End-User Registration Information	Telephone and SMS for authentication	US
Google	End-User Registration Information	SMS and push notifications for authentication	US, Ireland
Apple	End-User Registration Information	SMS and push notifications for authentication	US
Rackspace Inc.	End-User Registration Information, End-User Device Metadata, Administrator Registration Information, Events and Usage Data, Authentication Logs	Data storage, Hosting cold backups	US
Microsoft	End-User Registration Information, End-User Device Metadata, Administrator Registration Information, Events and Usage Data, Authentication 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

9. Information Security Incident Management

Breach and Incident Notification Processes
The Security team within Duo coordinates the data incident response process and manages the Duo response to data-centric incidents. The Duo team works with the Cisco Incident Commander which directs and coordinates Duo'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), where applicable and necessary to a particular incident.

PSIRT along with the Duo 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. 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.*

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. Cisco and its underlying processes are designed to meet Cisco's obligations under the EU General Data Protection Regulation (GDPR) and other privacy laws around the world. In addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security.

11. General Information and GDPR FAQ

For more general information and FAQs related to Cisco's Security Compliance Program and Cisco's GDPR readiness 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, please see https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html.