Duo

This Privacy Data Sheet describes the processing of personal data (or 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 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.

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

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. 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.

<table>
<thead>
<tr>
<th>Personal Data Category</th>
<th>Types of Personal Data</th>
<th>Purpose of Processing</th>
</tr>
</thead>
</table>
| 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  
● Deliver, support, improve security functionality, upgrade and improve the service |
3. Cross-Border Transfers

Duo is headquartered in the United States and operates internationally. Duo uses Amazon Web Services (AWS) data centers in the United States, Canada, Ireland, and Germany. Customers using a U.S. or Canadian based phone number during sign-up will automatically be placed on a U.S. based AWS instance. Customers using a phone number based in any other region where Duo is authorized to provide services will automatically be placed on a European-based AWS instance. Customers may request that their production instance 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. 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.

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.

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)

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
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
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

4. Access Control

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

5. 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.

6. 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 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, which will apply in all cases that a customer does not take other action available within the Duo Admin Panel:

<table>
<thead>
<tr>
<th>Personal Data Category</th>
<th>Retention Period After Account Deletion</th>
<th>Reason for Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-User Registration/Authentication Information</td>
<td>1 year (unless deleted sooner by customer)*</td>
<td>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.</td>
</tr>
<tr>
<td>Administrator Registration Information</td>
<td>1 year (unless deleted sooner by customer)</td>
<td>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.</td>
</tr>
<tr>
<td>End-User Device Metadata</td>
<td>1 year (unless deleted sooner by customer)</td>
<td>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.</td>
</tr>
<tr>
<td>Events and Usage Data</td>
<td>1 year (unless deleted sooner by customer)*</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Authentication and Activity Logs**

- **Retention Period:** 1 year (or less, depending on customer’s log retention settings)
- **Description:** 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**

- **Retention Period:** 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**

- **Retention Period:** 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

<table>
<thead>
<tr>
<th>Personal Data Category</th>
<th>Type of Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-User Registration/Authentication Information</td>
<td>Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts established since calendar year 2018.</td>
</tr>
<tr>
<td>Administrator Registration Information</td>
<td>Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts established since calendar year 2018.</td>
</tr>
<tr>
<td>Events and Usage Data</td>
<td>Encryption in transit over Transport Layer Security (TLS). Encryption at rest for all customer accounts established since calendar year 2018.</td>
</tr>
</tbody>
</table>

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.

### 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:
<table>
<thead>
<tr>
<th>Sub-processor</th>
<th>Personal Data</th>
<th>Service Type</th>
<th>Location of Data Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>End-User Registration/Authentication Information, End-User Device Metadata, Administrator Registration Information, Events and Usage Data, Authentication &amp; Activity Logs</td>
<td>Cloud based infrastructure and hosting, analytics, data storage</td>
<td>US, Canada, Ireland, Germany, Australia</td>
</tr>
<tr>
<td>Certified Security Solutions d/b/a Keyfactor</td>
<td>End-User Registration/Authentication Information Device IDs (e.g. serial numbers)</td>
<td>PKI service that issues and manages certificates to devices enrolled in Duo Beyond</td>
<td>US</td>
</tr>
<tr>
<td>Twilio, Inc.</td>
<td>End-User Registration/Authentication Information</td>
<td>Telephone and SMS for authentication</td>
<td>US</td>
</tr>
<tr>
<td>Nexmo Inc.</td>
<td>End-User Registration/Authentication Information</td>
<td>Telephone and SMS for authentication</td>
<td>US</td>
</tr>
<tr>
<td>Clickatell, Inc.</td>
<td>End-User Registration/Authentication Information</td>
<td>Telephone and SMS for authentication</td>
<td>US</td>
</tr>
<tr>
<td>Bandwidth Inc.</td>
<td>End-User Registration/Authentication Information</td>
<td>Telephone and SMS for authentication</td>
<td>US</td>
</tr>
<tr>
<td>Google</td>
<td>End-User Registration/Authentication Information</td>
<td>SMS and push notifications for authentication</td>
<td>US, Ireland</td>
</tr>
<tr>
<td>Apple</td>
<td>End-User Registration/Authentication Information</td>
<td>SMS and push notifications for authentication</td>
<td>US</td>
</tr>
<tr>
<td>Rackspace Inc.</td>
<td>End-User Registration/Authentication Information, End-User Device Metadata, Administrator Registration Information, Events and Usage Data, Authentication &amp; Activity Logs</td>
<td>Data storage, Hosting cold backups</td>
<td>US, UK</td>
</tr>
<tr>
<td>Microsoft</td>
<td>End-User Registration/Authentication Information, End-User Device Metadata, Administrator Registration Information, Events and Usage Data, Authentication &amp; Activity Logs</td>
<td>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</td>
<td>US</td>
</tr>
</tbody>
</table>

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 in collaboration with incident response teams within Cisco, including the Cisco Product Security Incident Response Team (PSIRT) and the Cisco Security Incident Response Team (CSIRT) where applicable and necessary to a particular incident.

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 phone calls). 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, including a SOC2 Type II audit report and two FedRAMP Authorized editions of the service.

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.