Cisco Secure Email Encryption Service (formerly, "Cisco Registered Envelope Service" or "CRES")

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Secure Email Encryption Service.

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

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

1. Overview

Cisco Secure Email Encryption Service (the "Service") helps customers secure their email communications. This Service allows a customer to send encrypted messages via secure messages. Secure message is an encyrypted email which may also be password-protected. If the envelope is password-protected, it can only be opened by authorized recipients who authenticate themselves.

For more information about Cisco Secure Email Encryption Service, visit here.

The Service processes certain personal data of its users. The following paragraphs describe which personal data Cisco processes to deliver the Service, 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 processed by Cisco Secure Email Encryption Service to provide its services and describes why the data is processed. For more information on data management and the purpose of processing, please see our Trust Center on How We Manage Data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Email address • Company Name	• Account creation • License entitlement validation • General product support and administration
Admin Information	• Admin Information (e.g., name, email)	• Provide the Service • Allow Customer to access admin interface, set configurations, operate the Service
Email Information	• Sender email • Recipient email • Subject	• Provide the Service • Troubleshooting customer issues • Diagnose technical issues
Encryption Key	• Unique Encryption Key per email	• Provide the Service • Unique message identifier used to allow appropriate sender and recipient to open encrypted message
IP Address	• IP Address of end-user's device	• Provide the Service • IP is used to maintain user session connectivity to the service and security monitoring

Encrypted Envelope	• Full email in encrypted format	• Provide the Service • Optional cloud storage for customers of encrypted envelope if customer enables the "Easy Open" feature (Cisco does not decrypt the envelope)

Integrations
The Service may integrate with various Cisco products. Please see the applicable Privacy Data Sheet for details regarding processing of personal data by the Cisco product receiving personal data from the Service. In addition, the Service may integrate with third-party products. Protection of data within the applicable third-party system is governed by the contract(s) and policies of the applicable third party.

TAC
If a customer contacts the Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from Cisco Secure Email Gateway and from the Customer, and may share such data with appropriate Cisco product teams as set forth herein. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data.

3. Data Center and Point of Presence Locations

Cisco Secure Email Encryption Service leverages third party cloud hosting providers to provide services globally.

Cisco Secure Email Encryption Service does not use PoPs.

Data Center	Description	Location
Amazon Web Services (AWS)	Cisco Email Encryption Services is hosted in Amazon's public cloud infrastructure	Virgina, USA (us-east-1) Oregon, USA (us-west-2)

Note: Cross border transfers occur with respect to data processed by Cisco Secure Email Encryption Service. When a new customer purchases a subscription, that customer's account information is always created, processed and stored in the United States. All subsequent data from such customer that is associated with the Cisco Secure Email Encryption Service product function will be processed in the United States in the data centers listed above. All data are encrypted in transit.

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 Secure Email Encryption Service to carry out the service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
Registration Information	Customers	Product administration
	Cisco	Provide the Service; support
Admin Information	Customers	Product administration and operations

	Cisco	Provide the Service; support
Email Information	Customer	Product administration; report generation
	Cisco	Provide the Service Security Monitoring Configuration; support and maintenance
Encryption Key	Cisco	While Cisco operates the Service, Cisco will not access this data
IP Address	Cisco	Provide the Service; support; security monitoring
Encrypted Envelope	Cisco	While Cisco operates the Service, Cisco will not access this data.

6. Data Retention

The table below lists the personal data used by Cisco Secure Email Encryption Service, the length of time that data needs to be retained, and why we retain it.

Personal Data Category	Retention Period	Reason for Retention
Registration Information	Deleted upon request	Administrative purposess
Admin Information	Deleted upon request	Service delivery
Email Information	Deleted upon request	Service delivery (e.g., allow recipient to access encrypted email) Sender email/recipient email used for user registration
Encryption Key	Retention period in AWS can be configured for up to 5 years, or data will be deleted upon request to delete the account	Service delivery (e.g., allow recipient to access encrypted email) End users cannot open and read the existing secure messages after the key retention period expires Note: Encryption keys generated prior to AWS migration will continue to have a 10-year retention period Customer has the ability to lock encryption keys or to set the encryption keys to expire
IP Addresses	90 days	Security Monitoring
Encrypted Envelope	Up to 30 days (Configurable)	To provide a method for mobile devices to open envelopes without the need for an application or software on the device Note: Encrypted envelopes stores prior to AWS migration will have a 14 day rention period

Deletion

Customer account admins can now configure the time period for which the encryption keys are stored. By default, the key retention period is set for 1 year. Customer can configure the key retention period for up to 5 years. End users cannot open and read an existing secure message after the key retention period expires. However, encryption keys generated prior to AWS migration will have a 10 year retention period.

After the retention period expires, Cisco will automatically purge all Email Information and Encryption Keys from Cisco Secure Email Encryption Service. Encryption Keys that are set to lock or expire are still subject to the configured deletion period; they will not be deleted sooner.

Notwithstanding the foregoing, customers may open a Cisco TAC request to request that Cisco delete their Cisco Secure Email Encryption Service user accounts. Customers cannot delete the IP Addresses that are part of an audit log. Cisco will purge IP Addresses after the expiration of the retention period listed above.

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. These technical and organizational measures include the following:

Personal Data Category	Controls and Measures
Registration Information	Data encrypted at rest disk level (SAN encryption) Data encrypted in transit (TLS encryption)
Admin Information	Data encrypted at rest disk level (SAN encryption) Data encrypted in transit (TLS encryption)
Email Information	Data encrypted at rest disk level (SAN encryption) Data encrypted in transit (TLS encryption)
Encrypted Envelope	Data encrypted at rest (payload encrypted using AES-256) Data encrypted at rest (key stored on the key server is hashed value of encryption key and the salt combined)
Encryption Key	Data encrypted at rest disk level (SAN encryption) Data encrypted in transit (TLS encryption)
IP Address	Data encrypted at rest disk level (SAN encryption) Data encrypted in transit (TLS encryption)

8. Sub-processors

Cisco partners with service providers that act as sub-processors of personal data and contract to provide the same level of data protection and information security provided to you by Cisco. The current list of sub-processors is set out below. Sub-processors may change from time to time and this Privacy Data Sheet will be updated to reflect those changes.

Sub-processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Equinix	Admin Information; Email Information; Encryption Key; IP Address; Encrypted Envelope	Cisco Secure Email Encryption Service leverages the Equinix data center to help provide a global service footprint, security assurance, service elasticity and resilience	California, USA	ISO 27001, SSAE 18 SOC 1 Type II, SOC 2 Type II
Switch	Admin Information; Email Information; Encryption Key; IP Address; Encrypted Envelope	Cisco Secure Email Encryption Service leverages the Switch data center to help provide a global service footprint, security assurance, service elasticity and resilience	Nevada, USA.	SSAE 18 SOC I Type 2, SOC II Type 2
Amazon*	Admin Information; Email Information; Encryption Key; IP Address; Encrypted Envelope	Cisco Secure Email Encryption Service leverages the AWS data centers to help provide a global service footprint, security assurance, service elasticity and resilience	Virginia, USA (us-east-1) Oregon, USA (us-west-2)	ISO 27001, SSAE 18 SOC 1 Type II, SOC 2 Type II

*on 20 April 2024, Amazon will replace Equinix and Switch as sub-processor for Cisco Secure Email Encryption Service.

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

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

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

10. Certifications and Compliance with Privacy Requirements

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

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

11. Exercising Data Subject Rights

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

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

Requests can also be made by submitting a request via:

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

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

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

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

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