Cisco Secure Email Gateway

(formerly, “Cisco Email Security Appliance” or “ESA”)

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) that is transmitted to Cisco by the Cisco Secure Email Gateway (the “Service”) it is configured to do so.

The Cisco Secure Email Gateway is an on-premise solution and is not hosted or operated by Cisco. Cisco does not access or process any personal data from Cisco Email Security Appliance unless it is configured to transmit personal data to Cisco to provide additional functionality. If the Service is configured to transfer personal data to Cisco, Cisco will process personal data from it in a manner that is consistent with this Privacy Data Sheet.

Cisco will process personal data from Cisco Secure Email Gateway 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 Gateway in order to provide its functionality.

1. Overview of Cisco Secure Email Gateway

Cisco Secure Email Gateway is an on-premise email security solution that blocks spam and security threats from the Internet and, depending on the features licensed, prevents the accidental or intentional leakage of customer data.

The following functionalities are available depending on the licensed features purchased:

- Anti-spam
- Intelligent Multi-Scan Anti-spam
- Anti-virus
- Outbreak Filters
- Advanced Malware Protection
- Safe Unsubscribe
- Image Analysis
- Email Encryption Service
- Data Loss Prevention

This Service is made available by Cisco to companies or persons (“Customers,” “you,” or “your”) who acquire it for use for inbound protection and outbound control of your email traffic.

The Service is not hosted or operated by Cisco and therefore, Cisco does not access or process any personal data to provide the Service’s functionality unless the Service is configured to do so. You may choose to purchase the Cisco Secure Email and Web Manager which enables reporting, tracking and quarantine features. The Cisco Secure Email and Web Manager is also an on-premise solution, and Cisco will not process any personal data when delivering this service.

Your Cisco Secure Email Gateway license makes available integrations with various Cisco products, enables automated workflows, and more. For more information regarding the processing of personal data by integrations, please refer to the applicable Privacy Data Sheet.

For more information about Cisco Secure Email Gateway, please see: https://cisco.com/go/emailsecurity.

2. Personal Data Processing

The table below lists the personal data processed by Cisco Secure Email Gateway and transferred to Cisco when configured to do so to carry out additional services and describes why we process that personal data.

Certain data listed below may not always qualify as personal data by itself, but for the purposes of this Privacy Data Sheet, Cisco shall treat it as personal data.

Important note: *Cisco Secure Email Gateway is an on-premise product that processes certain personal data which resides within Cisco Secure Email Gateway and the customer's data centers. The following table covers the personal data that may be transferred to Cisco for processing as described below only when Cisco Secure Email Gateway is configured to do so.*

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Customer Name • Email Address • Phone Number • Physical Address • Smart Account Usernames/IDs	• Creating an account • Validating license entitlements • Enable product operations and functionality
Service Logs Data (Optional)	• Global Unique ID (GUID) for email message • IP address • Secure Malware Analytics disposition (e.g., malicious, neutral, unknown) • Message metadata (e.g., date, sender, recipient) • Filename	• Global threat intelligence research *Only processed if Customer has not disabled Service Logs*
Sender Domain Reputation Data (Optional)	• GUID for email message • Message ID • Email sender IP address • SMTP envelope fields (e.g., sender email addresses) • Display Name • List-Unsubscribe headers • Message ID header • SPF Result • DKIM Result • DMARC Result • Header data (e.g., marketing header, List-Unsubscribe header, reply-to header domain) • Fully qualified domain name	• Global threat intelligence research *The "Additional Attributes" feature of Sender Domain Reputation can optionally be disabled by Customer to restrict sending the full sender email address, display name, etc.*
Sender IP Reputation Data (Optional)	• IP address of the sending email server • Sender IP address	• Global threat intelligence research. *Only processed if Customer has not disabled Sender IP Reputation*
URL Reputation Data (Optional)	• GUID for email message • Sender IP address • URL in the email being queried	• Global threat intelligence research • Used to develop and deploy URL exploit detection models *Only processed if customer has enabled URL Reputation*
Email Submission Data (Optional)	• Email Envelope Header • Email Data Header • Email Body (email body and/or attachment)	• If Customer chooses to send false positive/false negative email samples to Cisco TAC or Talos, Cisco may share with appropriate Cisco product teams and the third party subprocessors listed below for further analysis. • Global threat intelligence research and machine learning • Technical Support *Only processed if Customer has enabled Email Submission Data or if Customer directly submits to Cisco for further analysis*
Submitted Attachment Data (Optional)	• Any personal data that may be contained in the files	• If Customer chooses to send erroneously blocked file attachments to Cisco TAC, TAC may share with Threat Intelligence teams and the third party subprocessors listed below for further analysis

		• Technical support • Global threat intelligence research
IronPort Anti-Spam Engine (IPAS) Data **(Optional)**	• GUID for email message • Filename to the extent it includes personal data • IPAS results (spam score, rule hits, sender IP address)	• Global threat intelligence research *Only processed if Customer has enabled IronPort Anti-Spam Data*
Email Metadata for Integration with Cisco Secure Email Phishing Defense (Optional)	• Email Envelope Header (Sender, Recipient, Host/IP address) • Email Data Header (From, To, Subject, Reply-to Headers)	• Enable integration between Cisco Secure Email Gateway and Secure Email Phishing Defense for customers with both products. For further information please refer to the Cisco Secure Email Phishing Defense Privacy Data Sheet *Only processed if both Cisco Secure Email Gateway and Secure Email Phishing Defense has been integrated by Customer*

Cisco Secure Email Gateway further collects "System Information" to assist Cisco with understanding product usage and enabling product improvements. Customers have the option of disabling the transmission of Systems Information. For more information, see the Systems Information brief.

Cisco and Third Party Integrations
In addition, Cisco Secure Email Gateway 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. If you utilize the Threat Defense Connector with the Cisco Secure Email Gateway, a copy of the customer email, including any attachments (referenced as "Journaled Email Data") is processed by Cisco as set forth in the Cisco Secure Email Threat Defense Privacy Data Sheet.

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.

Smart Licensing
Cisco Secure Email Gateway is Smart License enabled. Personal data may be provided to Cisco in the form of a user credential to associate it with a related Cisco.com account (i.e., CCO) or Smart License account. For more information regarding Smart License accounts and related data collection, please refer to the Smart Software Licensing Privacy Data Sheet.

3. Data Center and Point of Presence Locations

If a Personal Data Category above is processed for the purposes of "Global threat intelligence research," then the processing and storage of such personal data is conducted by Cisco's global threat intelligence teams, which have U.S. data centers described below and use the subprocessors in the locations set forth in Section 9 below.

Secure Email Gateway does not use PoPs.

Global Threat Intelligence Data Warehouse Centers

Location	Data Center	Security Assurance
US: California, Texas, Virginia	Equinix (co-location facility)	CA facility has SOC 2 Type II, ISO 27001 and SSAE16 SOC 1 Type 1 TX facility has NIST 800- 53/FISMA, ISO 27001, SOC 1 Type II, SOC 2 Type II, PCI DSS and HIPPA VA facility has NIST 800- 53/FISMA, ISO 27001, SOC 1 Type II, SOC 2 Type II, PCI DSS and HIPPA
US	AWS	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. The AWS SOC reports provide additional details on the specific control activities executed by AWS. More details can be found at: https://aws.amazon.com/compliance/ and https://aws.amazon.com/security/

With respect to data collected by the global threat intelligence teams, the Global Co-location Data Center Networks below use dynamic Anycast routing decisions to route each customer's Service Log Data, Sender Domain Reputation Data, Sender IP Reputation Data, URL Reputation Data and IPAS Data to any data center facility listed below (provided the features are enabled as described herein), although normally the data center in which the data is routed will be to the closest physical location to the Secure Email Cloud Gateway deployment. The data sent to the Global Co-location Data Center Network is transient in nature, and is not stored in those locations. This is necessary for the delivery of Secure Email Cloud Gateway, as threat intelligence analytics requires the examination of worldwide data in real time.

Global Co-location Data Center Network

Location	Provider	Certification
Amsterdam, Netherlands	Interxion	ISO27001/ISO22301
Ashburn, VA	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Atlanta, GA	Digital Reality	SOC2/SOC3/PCI-DSS/ISO 27001
Bucharest, Romania	NX DATA	ISO9001/ISO27001
Chicago, IL	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Copenhagen, Denmark	Interxion	ISO27001/ISO22301
Dallas, TX	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Denver, CO	CoreSite	ISO 27001/SOC 1 Type 2/SOC 2 Type 2/PCI DSS/HIPAA
Dubai, United Arab Emirates	Equinix	ISO27001/OHSAS/PCI/SOC1/SOC2
Dublin, Ireland	Interxion	ISO27001/ISO9001/ISO22301
Frankfurt, Germany	Equinix	ISO27001/PCI/SOC1/SOC2/ISO9001
Hong Kong	Equinix	ISO27001/PCI/SOC1
Johannesburg, South Africa	Teraco	ISO27001/PCI/ISO9001
London, UK	Equinix	ISO27001/PCI/SOC1/SOC2/ISO9001
Los Angeles, CA	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Melbourne, Australia	NEXT DC	ISO27001/ISO9001/UpTime Institute Certified Tier 4
Miami, FL	Coresite	ISO27001/HIPAA/PCI/SOC1/SOC2
Milan, Italy	Equinix	ISO27001/ISO9001/PCI
Mumbai, India	STT	ISO27001/ISO20000/ISO14001/TL9000/PCI-DSS
New York, NY	Coresite	ISO27001/HIPAA/PCI/SOC1/SOC2
Palo Alto, CA	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Paris, France	Equinix	ISO27001/ISO9001/SOC1/SOC2/PCI-DSS/ISO50001/ISO14001/OHSAS18001
Prague, Czech Republic	CECOLO	ISO27001/ISO14001/ISO18001(OHSAS)/ISO9001
Reston, VA	Coresite	ISO27001/HIPAA/PCI/SOC1/SOC2
Rio de Janeiro, Brazil	Equinix	ISO 22301, SOC 1 Type II, PCI-DSS, SOC 2 Type II, ISO 9001-2008, ISO 27001
San Jose, CA	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Sao Paulo, Brazil	Equinix	ISO27001/ISO9001/SOC1/SOC2
Seattle, WA	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Singapore	Equinix	ISO27001/PCI/SOC1/SOC2/SS564
Sydney, Australia	Equinix	ISO27001/PCI/SOC1/SCO2
Tokyo, Japan	Equinix	ISO27001/PCI-DSS/SOC1/SOC2
Toronto, Canada	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2

Vancouver, BC	Cologix	PCI/SOC1/SCO2/HIPAA
Warsaw, Poland	EdgeConneX	ISO27001/ISO9001/PCI-DSS

Registration Data is stored in the United States.

4. Cross-Border Transfers Mechanisms

Cisco 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
- 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 Gateway when it transmits personal data to Cisco to carry out additional services and who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
Registration Information	Customer	Administration and operations
	Cisco	Creating an account and validating license entitlements and general product support and operations
Service Logs Data	Customer	Administration and operations
	Cisco	Global threat intelligence research
Sender Domain Reputation Data	Customer	Administration and operations
	Cisco	Global threat intelligence research
Sender IP Reputation Data	Customer	Administration and operations
	Cisco	Global threat intelligence research
URL Reputation Data	Customer	Administration and operations
	Cisco	Global threat intelligence research
Email Submission Data	Customer	Administration and operations
	Cisco	Technical support; global threat intelligence research and machine learning;
Submitted Attachment Data	Customer	Administration and operations
	Cisco	Technical support; global threat intelligence research
IPAS Data	Customer	Administration and operations
	Cisco	Global threat intelligence research
Email Metadata for Integration with Cisco Secure Email Phishing Defense	Customer	Administration and Operations
	Cisco	Enable the integration

6. Data Retention

Customer may request a deletion of specific personal data sent to Cisco by Cisco Secure Email Gateway to provide additional services at any time by submitting a request via the Cisco Privacy Request Form.

Personal Data Category	Retention Period	Reason for Retention
Registration Information	• Data will be deleted upon request	Product registration and enablement, product use notifications, training, and support.
Service Logs Data	• Data will be deleted upon request	Global threat intelligence research
Sender Domain Reputation Data	• Data will be deleted upon request	Global threat intelligence research
Sender IP Reputation Data	• Data will be deleted upon request	Global threat intelligence research
URL Reputation Data	• Data will be deleted upon request	Global threat intelligence research
Email Submission Data	• Data will be deleted upon request	Global threat intelligence research; machine learning
Submitted Attachment Data	• Data will be deleted upon request	Global threat intelligence research to correct erroneous blocking/detection of the files as malicious
IPAS Data	• Data will be deleted upon request	Global threat intelligence research

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	Security Controls and Measures
Registration Information	• Encrypted in transit and at rest
Service Logs Data	• In transit: Data is SSL encrypted • At rest: Data at rest is stored unencrypted with strict access controls
Sender IP Reputation Data	• In transit: Data is SSL encrypted • At rest: Data at rest is stored unencrypted with strict access controls
Sender Domain Reputation Data	• In transit: Data is SSL encrypted • At rest: Data at rest is stored unencrypted with strict access controls
URL Reputation Data	• In transit: Data is SSL encrypted • At rest: Data at rest is stored unencrypted with strict access controls
Email Submission Data	• Data is Encrypted in transit and at rest
Submitted Attachment Data	• Data is Encrypted in transit and at rest
IPAS Data	• In transit: Data is SSL encrypted • At rest: Data at rest is stored unencrypted with strict access controls
Email Metadata for Integration with Cisco Secure Email Phishing Defense	• Encrypted in transit. For further encryption details, please see the Secure Email Phishing Defense Privacy Data Sheet

8. Third Party Service Providers (Sub-processors)

Cisco 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 service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
AWS	• Service Logs Data • Sender Domain Reputation Data • Sender IP Reputation Data • URL Reputation Data • Email Submission Data • IPAS Data	With respect to data collected for global threat intelligence, Cisco's threat intelligence teams leverage AWS cloud technology to assist in providing its capabilities	United States
Vade Secure	• Email Submission Data	Global threat intelligence research	France
Sophos	• Submitted Attachment Data	Global threat intelligence research	United Kingdom
McAfee	• Submitted Attachment Data	Global threat intelligence research	United States
BitDefender	• Submitted Attachment Data	Global threat intelligence research	Ireland Romania
Reversing Labs	• Submitted Attachment Data	Global threat intelligence research	Croatia
Google Cloud Translate	• Email Submission Data[1]	Translation services to assist with global threat intelligence research	United States

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.

[1] When analyzing Email Sample Data, Cisco may manually share a necessary portion of the email body text with Google Cloud Translate for the sole purpose of translation through the Google Cloud Translate API. Such text is retained by Google Cloud Translate for only enough time to perform the translation and then it is deleted.

11. Exercising Data Subject Rights

Users whose personal data is processed by Cisco to provide additional Cisco Secure Email Gateway functionality have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by Cisco for this additional functionality. Data portability requirements are not applicable to this product.

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 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	**EMEA 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.

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