Cisco Business Critical Services

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information), device data collection, data transfer and data storage by Cisco Business Critical Services (BCS).

Cisco will process personal data from Business Critical Services (BCS) 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 Business Critical Services in order to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

BCS helps customers overcome challenges like increased complexity, inefficiency, risk, and skills gap emanating from disparate technologies, manual processes, and digital innovations. It also helps businesses simplify complexity, optimize IT, reduce Operational Expenditure, and accelerate technology transitions.

BCS helps customers optimize value from their Cisco products and solutions today while creating a secure IT strategy for the future. BCS is expanding on this value to deliver even more innovative capabilities in analytics, automation, compliance, and security.

We provide a transformational framework of baseline deliverables and customizable capabilities which offer innovative capabilities that:

- Deliver analytics and operational insights from our cloud-based analytics platform.
- Speed case submission to minutes from hours without human intervention with the Automated Fault Management Service.
- Quickly test and deploy features to IT environments with new automation capabilities Network Replication and Test Automation Services.
- Automate Customer's compliance and remediation for recommended software and configuration upgrades and help Customer monitor against multiple regulatory standards (e.g., HIPAA, PCI, SOX, & ISO).
- Drive fast emergency response during a breach and proactive defense with Incident Response.

Please find the Service Description for Business Critical Services 3.0 here.

Note: Customer may integrate BCS with Customer's third party products. Cisco is not responsible for customer data once such data leaves BCS for a non-Cisco product. Protection of data within the applicable third party system is governed by the contract(s) and policies of such third party.

For more information about Business Critical Services, visit here.

2. Personal Data Processing

The table below lists the personal data processed by BCS to provide its services and describes why the data is processed.

Personal Data Category	Types of Personal Data	Purpose of Processing
Account and Registration Information	• CCO ID • First Name • Last Name • Email ID • Address • Phone • Preferred Language	We use Account and Registration Information to: • Authenticate and Authorize access to your account • Manage Customer Account and Services Activation • Provide access to CX Cloud • Assist and Notify during Data Collection Operations
Host and Usage Information	• IP Address • MAC Address • Hostname • BCS Portal logins • BCS Pages visited • BCS Functions executed • BCS Audit trails • BCS Data Collection health/status information	• Understand how the BCS Service is used • Improve user experience • Improve Data Collection Operations • Report Network Health

3. Device Data Processing

The following table shows the data collection methods and how data is used.

BCS processes data in order to provide operational insights. To collect data, Cisco deploys a Common Services Platform Collector (CSPC), or Operational Insights Collector (OIC) in the customer network to gather network data. Cisco does not monitor or collect network traffic data. No data about a specific person, their personal data, online activities, or online transactions is collected.

Cisco does not intentionally collect or process Personally Identifiable Information (PII) via CSPC or OIC.

Data Category	Types of Collected Data	Purpose of Processing
Device and Network Information	For illustrative purposes only, the list below includes the types of data that may be collected and processed from CX Collector or other collection methods for the purpose of providing support: • Serial numbers • Host Names • MAC Address • SNMP MIBs (ACLs, CDP) • Command Line Interface (CLI) (show commands, e.g., show version) • Device Configuration (e.g., running config and startup config, SNMP Strings (masked), Interface description) • Product identification numbers • Sysdescription (has device location) • IP addresses	We use Device and Network related Information to: • Display Insights and report network heath • Understand how the Service is used • Diagnose technical issues • Conduct analysis in aggregate form to improve the technical performance of the Service • Respond to Customer Support requests • Report enriched information back to authorized users

	• Operating System (OS) Feature Sets • OS Software Versions • Hardware Versions • Installed Memory • Installed flash • Boot Versions • Chassis series • Slot IDs • Card Types • Card families • Firmware versions • Syslog Data • DB records from Cisco Collaboration Products (if configured) • Log and image files (if configured)	• Analysis in aggregate form to improve the technical performance of the Service. • Analysis of customer systems to provide recommendations for remediation and optimization
Product Usage Telemetry Information	• Customer identity information • Product license information • Product features activation and usage data	• Improve contextual learning • Improve user experience

The following describes what is not collected as well as additional security attributes.

Data Not Collected

- No data is collected from network devices by default. Must be configured.
- Packet/traffic contents
- User/subscriber data

Masking

- Default masking is applied to customer personal data
- Customizable rules can be applied to mask command data or types of device configuration data

Data Security for Cisco Cloud

- Access to data is managed by Cisco IT and Customer Delivery team
- Uploaded data are secured and controlled by Cisco IT
- Data at rest are encrypted
- Listed public cloud infrastructures are used with restricted access to authorized Cisco users.
- All administration work on the database server requires explicit change management procedure

4. Data Center Locations

Cisco leverages its own data centers as well as third-party infrastructure providers to deliver the BCS globally.
The following table shows where these data centers are located, and the list below is for reference purposes only. All data are encrypted in rest and in transit. The customer may request which Data Center is used to store their Data.

Cisco Data Center Locations
Cisco Data Center location: Amsterdam, Netherlands
Cisco Data Center location: Richardson, Texas, USA
Cisco Data Center location: Allen, Texas, USA
Cisco Data Center location: Research Triangle Park, NC, USA
AWS Regions United States (East and West regions), Europe (Dublin, Frankfurt, Paris, Stockholm)
GCP Regions United States (East and West regions), Europe (Belgium, Frankfurt)

5. Cross-Border Data Transfer Mechanisms

Cisco has invested in a number of 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

6. Access control

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

Personal Data Category	Who has Access	Purpose of the Access
Account and Registration Information	Cisco	Support the Service in accordance with Cisco's data access and security controls process
Host and Usage Information	Cisco	Cisco analyzes collected data and usage data to improve and support the service in accordance with Cisco's data access and security controls process.
Device and Network Information	Cisco	Support the Service in accordance with Cisco's data access and security controls process.
Product Usage Telemetry Information	Cisco	Cisco analyzes collected data and usage data to improve and support the service in accordance with Cisco's data access and security controls process.

7. Data Portability

BCS provides capabilities to allow customers and authorized users to export displayed data. Customers may also access these reports by using APIs or by exporting the data through comma separated Value (CSV) format. Customers and users may view and export their Customer Data for their business needs.

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.

Personal Data Category	Security Controls and Measures
Account and Registration Information	Passwords are encrypted in transit. All data are protected by highly secure data center protection mechanisms and operational procedure.
Host and Usage Information	Encrypted in transit; documents containing customer data are encrypted at rest. All data are protected by highly secure data center protection mechanisms and operational procedure.
Device and Network Information	Encrypted in transit; documents containing customer data are encrypted at rest. All data are protected by highly secure data center protection mechanisms and operational procedure.
Product Usage Telemetry Information	Encrypted in transit; documents containing customer data are encrypted at rest. All data are protected by highly secure data center protection mechanisms and operational procedure.

9. Personal Data Deletion & Retention

Cisco retains personal data in a form that is personally identifiable for no longer than is necessary to accomplish the purpose(s), or other permitted purpose(s), for which the Personal Data was obtained. Customers can request deletion of personal data retained in the Cisco Data Center by sending a request to via the Privacy Request Form.

When a Customer or user makes a request for deletion, Cisco endeavors to delete the requested data from its systems within 30 days, unless the data is required to be retained for Cisco's legitimate business purposes.

10. Sub-processors

We may share information with service providers, contractors or other third parties to assist in providing and improving the Service. The data shared may include aggregate statistics or pseudonymized data. Cisco partners with service providers who contract to provide the same level of data protection and information security that you can expect from Cisco. We do not rent or sell your information.

Sub-processor	Service Type	Personal Data	Location of Data Center	Security Assurance
Amazon Web Services, Inc	Third party cloud-hosted application and data service	CCO id	AWS Regions US United States (East and West regions) AWS Regions Europe (Frankfurt) Customer may express preference regarding AWS locations.	For information regarding AWS compliance please refer to documentation online at https://aws.amazon.com/compliance
Google, LLC (GCP)	Third party cloud-hosted application and data service	CCO id	US (Iowa) UK (London) Europe (Belgium, Frankfurt) Asia Pacific (Singapore, Sydney) Canada (Montreal) Customer may express preference regarding GCP locations.	For information regarding GCP compliance please refer to documentation online at https://cloud.google.com/security/compliance
Okta, Inc.	Identity services management	Email Address	Standard USA EU Germany, Service – Cell – Ireland APAC Cell – Singapore, Australia.	Please see Okta's sub-processor disclosures for up-to-date information

11. Information Security Incident Management

Breach and Incident Notification Processes

The Incident Response 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.

12. 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 continually maintains third-party validations to demonstrate our commitment to information security. Cisco has received the following certifications:

- Cisco Services has received ISO 27001:2013 (Information Security) re-certification from TUV (a copy of the new certificate is available here).
- Cisco holds a Global ISO 9001 Certification and ISO 14001 Registration, managed by the Corporate Quality Compliance and Certifications program, which establishes and maintains policies that ensure quality management of processes and environmental responsibilities. Visit our Quality Certifications page to understand the scope of these compliance certifications and read more information.

13. 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 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 that 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.

14. General Information

For more general information and FAQs related to Cisco's Security and Privacy Program (including 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, go to the Personal Data Privacy section of the Cisco Trust Center.

For more general information related to BCS, please visit the Business Critical Services website.