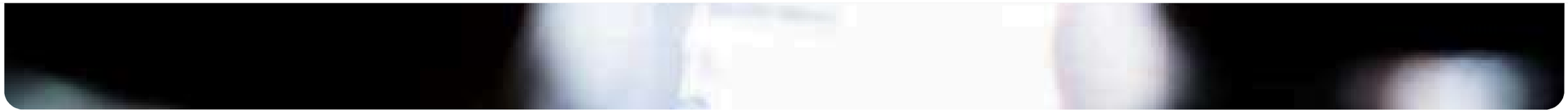
# Cisco Online Privacy Statement



## The Trust Center

Cisco is committed to maintaining strong protections for our customers, products and company. We believe in building and maintaining trust, reducing risk and simply doing what is right.

Learn more

Cisco Systems, Inc. and its subsidiaries (collectively "Cisco") are committed to protecting your privacy and providing you with a positive experience on our websites and while using our products and services ("Solutions").

This Privacy Statement applies to Cisco websites and Solutions that link to or reference this Privacy Statement and describes how we handle Personal Data and the choices available to you regarding collection, use, access, and how to update and correct your Personal Data. Additional information on our Personal Data practices with respect to Cisco Solutions may be provided in Solution specific privacy data sheets and maps, offer descriptions, or other notices provided prior to or at the time of data collection. Certain Cisco websites and Solutions may have their own privacy documentation describing how we handle Personal Data for those websites or Solutions specifically. To the extent a specific notice for a website or Solution differs from this Privacy Statement, the specific notice will take precedent. If there is a difference in translated, non-English versions of this Privacy Statement, the U.S.-English version will take precedence.

### What is Personal Data?

"Personal Data" is any information that can reasonably be used to identify an individual, or otherwise make an individual identifiable, and may include name, address, email address, phone number, login information (such as account number and password), social media account information, or payment card number.

The types of Personal Data we may process depend on the business context and the purposes for which it was collected. It may include:

- Contact, subscription, and account/registration details, as well as online identifiers
- Login credentials where we require an account be made
- Communications content (such as audio, video, text), social media and discussion forum, or other communications details when you interact with Cisco
- Financial Information (such as bank account details or credit card information)

- Details of an individual's business and other interests and opinions (such as information held in a customer relationship management database)
- Information about the user and usage of our websites and Solutions, including System Information such as device identifiers and telemetry (such as IP or MAC address) when such data is linked or tied to a specific individual's device

If we link other data with your Personal Data, we will treat that linked data as Personal Data.

## Collection and use of your Personal Data

We may collect data, including Personal Data, about you as you use our websites and Solutions and interact with us. We also acquire Personal Data from trusted third-party sources and engage third parties to collect Personal Data on our behalf, in accordance with applicable laws.

We may use your Personal Data for the purposes of operating and helping to ensure the security of our business; delivering, improving, and customizing our websites and Solutions; sending notices, marketing, and other communications; and for other legitimate purposes permitted by applicable law.

We collect Personal Data for a variety of business reasons, such as:

- Customer relationship management and administration
- Order processing, including billing and payment
- Asset recovery and product returns and replacements
- Creating and managing user accounts
- Provisioning websites and Solutions and enabling the use of certain features
- Analyzing, personalizing, improving accuracy, and enhancing user experience, communications, and interactions
- Sending communications to you, including for marketing or customer satisfaction purposes, either directly from Cisco or from our partners
- Managing communications preferences. You can modify your communication preferences at any time. See Your choices and selecting your communication preferences below
- Contract performance, Solution delivery, and customer service
- Managing job applications
- Administering online education, testing, and certifications
- Facilitating conferences, webinars, and other events
- Protecting Cisco, our users, websites and Solutions, and others

If you choose to provide Cisco with a third party's Personal Data (such as name, email, and phone number), you represent that you have the third party's permission to do so. Examples include forwarding reference or marketing material to a friend or sending job referrals. Third parties may unsubscribe from any future communication following the link provided in the initial message or by submitting a Privacy Request.

In some instances, Cisco and the third parties we engage may automatically collect data through cookies, web logs, web beacons, and other similar applications. Please read the Use of cookies and similar technologies section below for more information.

## Your privacy rights

We need your help to keep your Personal Data accurate and up to date. We provide options to access, correct, suppress, or delete your Personal Data:

- You can view or edit your Cisco.com Personal Data and preferences online by using the Cisco Profile Management Tool.
- When Cisco is acting as a **"data controller,"** you can exercise your rights of access and request corrections, suppression, objection, and deletion under applicable data protection laws directly with Cisco as described in the specific website and Solution documentation or by submitting a request through the Privacy Request form.
- When Cisco is acting as a **"data processor,"** and you wish to exercise your rights of access and request corrections, suppression, or deletion, Cisco will direct you to the data controller under the applicable data protection laws.
- If you need additional assistance, or help with accessing, correcting, suppressing, or deleting your Personal Data, please feel free to contact us directly. We will respond to your request within 30 days or as appropriate under applicable data protection laws. If we are unable to honor your request or need more time, we will provide you with an explanation.

## Your choices and selecting your communication preferences

We give you the option to receive a variety of information related to our business, programs, websites, and Solutions. You can manage your communication preferences at any time through the following methods:

- By following the instructions included in each promotional email from us to unsubscribe from that mailing
- By completing and submitting this form or by contacting us via mail at: Cisco Systems, Inc., Privacy Office, 170 West Tasman Dr., San Jose, CA 95134, USA. Please be sure to include your name, email address, the communication received, method of delivery (such as post, email, phone call, text), and any additional information about the material you no longer wish to receive.
- For short message service (“SMS”) messages, reply "STOP," "END," or "QUIT" to the SMS text message you have received

These choices do not apply to service notifications or other required communications that are considered part of certain programs, websites, and Solutions which you may receive periodically unless you cancel or stop use in accordance with its terms and conditions. With your permission, your Personal Data may be shared with third

parties (such as Cisco business partners or vendors) so that they may inform you about websites, programs, products, or services that may be of interest to you. To opt out of Cisco sharing with third parties for their marketing purposes, please submit a Privacy Request.

By using or engaging with our websites or Solutions, or otherwise providing Personal Data to us, you agree that we may communicate with you regarding security, privacy, and administrative issues relating to your use. For example, if we learn of a security system's breach, we may attempt to notify you by posting a notice on our websites, sending an email, or otherwise contacting you.

## Disclosing your Personal Data

Personal Data may be processed by third parties for the purposes of operating our business; delivering, analyzing, improving, securing, and customizing our websites and Solutions; sending marketing and other communications related to our business; and for other legitimate purposes permitted by applicable law(s); or otherwise with your consent.

Personal Data may be disclosed in the following ways:

- Within Cisco and any of our worldwide subsidiaries for the purposes of data processing, such as marketing, business operations, compliance, security, website or Solution functionality, or storage
- With business partners, service vendors, authorized third-party agents, or contractors to provide a requested website, Solution, service, or transaction. Examples include processing of orders and credit card transactions, hosting websites, hosting seminar registration, assisting with sales-related efforts or pre/post-sales support, and providing customer support.
- With Cisco business partners or vendors, so that they may share information with you about their products or services. To opt out of Cisco sharing with third parties for their marketing purposes, please submit a Privacy Request.
- In connection with, or during negotiations of, any merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of our business by or to another company
- In response to a request for information by a competent authority or third party if we believe disclosure is in accordance with, or is otherwise required by, any applicable law, regulation, or legal process
- With law enforcement officials, government authorities, or other third parties as necessary to comply with legal process or meet national security requirements; protect the rights, property, or safety of Cisco, our business partners, you, or others; or as otherwise required by applicable law
- In aggregated, anonymized, and/or de-identified form that cannot reasonably be used to identify you
- If we otherwise notify you and you consent to the sharing

## Security of your Personal Data

We take reasonable and appropriate steps to protect the Personal Data entrusted to us and treat it securely in accordance with this Privacy Statement. Cisco implements physical, technical, and organizational safeguards designed to protect your Personal Data from accidental or unlawful destruction, loss, alteration, and unauthorized disclosure or access. We also contractually require that our suppliers protect such information from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

## Retention and disposal of Personal Data

We will retain your Personal Data as needed to fulfill the purposes for which it was collected. We will retain and use your Personal Data as necessary to comply with our business requirements and legal obligations, resolve disputes, protect our assets, and enforce our rights and agreements.

We will not retain Personal Data in identifiable form when the purpose(s) for which the Personal Data was collected have been achieved and there is no legal or business need to retain such Personal Data. Thereafter, the data will either be destroyed, deleted, anonymized, and/or removed from our systems.

## Use of cookies and similar technologies

Cisco uses automatic data collection tools, such as cookies, embedded web links, pixels, tags, and web beacons. These tools collect certain standard information that your browser sends to us (such as Internet Protocol [IP] address, MAC address, clickstream behavior, and telemetry).

These tools help make your visit to our websites and Solutions easier, more efficient, and personalized. We also use the information to improve our websites and Solutions, provide greater service and value, better understand your potential interest in our websites and Solutions, and provide you with more relevant ads and other content.

We partner with third parties to display advertising on our website and to manage our advertising on other sites. Our third-party partners may use cookies or similar technologies to provide you with advertising based on your browsing activities and interests. Where this type of third party advertising is disabled, generic, non-personalized ads will continue to be displayed.

For more information, or if you would like to opt out of interest-based advertising, see How Cisco Uses Automatic Data Collection Tools.

To update your cookie preferences, click the "Cookies" link at the bottom of any page on this website. Additionally, you may be able to use other tools to control cookies and similar technologies. For example, you may have controls in your internet browser to limit how the websites you visit are able to use cookies.

## Automated decision-making

We process Personal Data using both manual and automated methods of processing. Automated methods are often used to assist our manual methods in accordance with applicable laws. Where an individual's rights and legitimate interests may be impacted by such automated decision-making, we will provide the impacted individual the opportunity to inquire about the decision or request manual review. Manual review may be conducted by Cisco employees or trusted third-party business partners working on Cisco's behalf.

## Linked websites

We may provide links to other third-party websites and services that are outside Cisco's control and governed by the respective third party's privacy policy, not by this Privacy Statement. We encourage you to review the privacy statements posted on the websites you visit and in the applications you use.

## Forums and chat rooms

If you participate in a discussion forum, local communities, or chat room on a Cisco website, you should be aware that the information you provide there (such as your public profile and comments) will be made broadly available to others and could be used to contact you, to send you unsolicited messages, or for purposes neither Cisco nor you have control over. Also, please recognize that individual forums and chat rooms may have additional rules and conditions. Cisco is not responsible for the Personal Data or any other information you choose to submit in these forums. To request removal of your Personal Data from our blog or community forum, please submit a Privacy Request. In some cases, we may not be able to remove all Personal Data and comments. In such cases, we will provide you with a response and explanation.

## Children's privacy

Cisco encourages parents and guardians to take an active role in their children's online activities. Cisco does not knowingly collect Personal Data from children without appropriate parental or guardian consent. If you believe that we may have collected Personal Data from someone under the applicable age of consent in your country without proper consent, please let us know using the methods described in the Questions, comments, and how to contact us section and we will take appropriate measures to investigate and address the issue promptly.

## International transfer, processing, and storage of Personal Data

As Cisco is a global organization, Personal Data may be transferred to Cisco in the United States of America, to any Cisco subsidiary worldwide, or to third parties and business partners as described above that are located in various jurisdictions around the world. Similarly, Personal Data may be accessed from countries where Cisco or its subsidiaries have operations. Cisco will transfer your Personal Data in accordance with approved transfer mechanisms as well as any applicable local legal requirements.

By using our websites and Solutions or providing any Personal Data to us, where applicable law permits, you acknowledge and accept the transfer, processing, and storage of such information outside of your country of residence where data protection standards may be different.

Cisco safeguards and enables the global transfer of Personal Data in a number of ways:

- ### APEC Privacy Certification

  Cisco's global privacy program, described in this Privacy Statement, complies with the Asia Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system (CBPRs) and Privacy Recognition for Processors (PRP). The APEC CBPR system and PRP provides a framework for organizations to ensure protection of Personal Data

transferred among participating APEC economies. More information about the APEC Privacy Framework, CBPRs, and PRP can be found on the CBPRs site. Our certification applies to our business processes across our global operations that process and transfer Personal Data to/from our affiliates around the world. To view our certifications, please see the APEC CBPR System Directory and the APEC PRP Directory.

For more information on the scope of our participation, or to submit a privacy inquiry through BBB National Programs, our Accountability Agent, please click on the official seal below:


- EU Binding Corporate Rules–Controller

  Cisco's global privacy program and policies have been approved by the Dutch, Polish, Spanish, and other relevant European privacy regulators as providing additional safeguards for the protection of privacy, fundamental rights, and freedoms of individuals for transfers of Personal Data protected under European law. Cisco's Binding Corporate Rules–Controller (BCR-C) provide that international transfers made worldwide by Cisco entities bound by these rules as a controller of European Personal Data benefit from appropriate safeguards.

  A copy of our BCR-C can be found in our Global Privacy Policy. More information about BCRs can be found on the European Commission site.

- EU-U.S. Data Privacy Framework, the U.K. Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework

  EU/U.K. (and Gibraltar)/Swiss - U.S. transfer of Personal Data

  When we transfer Personal Data out of the European Union (“EU”), European Economic Area (“EEA”), the United Kingdom (“U.K.”)(and Gibraltar), and Switzerland to countries that do not benefit from an adequacy decision, we may rely on Standard Contractual Clauses, Binding Corporate Rules–Controller, or other legal transfer mechanisms with appropriate safeguards in place to protect Personal Data. Additionally, Cisco Systems, Inc. and its U.S. based subsidiaries (collectively "Cisco-U.S.") comply with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the U.K. Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) for transfers of Personal Data from the EU, EEA, U.K. (and Gibraltar), and Switzerland to the U.S.

Data Privacy Framework

Cisco-U.S. has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. DPF Principles with regards to the processing of Personal Data received from the EU and EEA in reliance on the EU-U.S. DPF and from the U.K. (and Gibraltar) in reliance on the U.K. Extension to the EU-U.S. DPF. Cisco-U.S. has also certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. DPF Principles with regards to the processing of Personal Data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this Online Privacy Statement and the EU-U.S. DPF Principles, the U.K. Extension to the EU-U.S. DPF Principles, and/or the Swiss-U.S. DPF Principles, the DPF Principles shall govern. For more information about the DPF program, and to view our certification, please visit the DPF Website.

Pursuant to the DPF Principles, Cisco-U.S. commits to the following:

- Cisco-U.S. is responsible for the processing of Personal Data it receives under the DPF, and subsequently may transfer it to third parties acting as agents on its behalf. Cisco-U.S. complies with the DPF Principles for all onward transfers of Personal Data from the EU, EEA, U.K. (and Gibraltar), and Switzerland (for examples of such transfers, see Disclosing your Personal Data ), including the onward transfer liability provisions. In certain situations, Cisco-U.S. may be required to disclose Personal Data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. Further, Cisco-U.S. is committed to protecting Personal Data received from EU and EEA member countries, Switzerland, and the U.K. (and Gibraltar) (see Collection and use of your Personal Data for examples of the Personal Data Cisco processes when you use our websites and Solutions and interact with us) in accordance with the DPF's applicable Principles and to help ensure Personal Data collected from individuals is accessible to them as part of their individual rights when Cisco is the Controller of the Personal Data (see Your privacy rights). Furthermore, Cisco acknowledges the right of EU, EEA, U.K. (and Gibraltar), and Swiss individuals to request access to their data while it is in the U.S. and to correct, amend, and supplement inaccurate or incomplete data. Said individuals also have the right to request erasure of personal information that has been handled in violation of the DPF Principles. Subject individuals interested in accessing their data should see Disclosing your Personal Data for information on how to contact us, or submit a Privacy Request online.
- In compliance with the EU-U.S. DPF Principles, the U.K. Extension to the EU-U.S. DPF Principles, and/or the Swiss-U.S. DPF Principles, Cisco-U.S. commits to resolve complaints about your privacy and our collection or use of your Personal Data transferred to the U.S. pursuant to the DPF Principles. EU, EEA, U.K. (and Gibraltar), and Swiss individuals with DPF inquiries or complaints, or any questions or concerns regarding Cisco-U.S. processing or international transfer of their Personal Data should first contact Cisco-U.S. by submitting a Privacy Request online.
- Cisco-U.S. has further committed to refer unresolved privacy complaints under the DPF Principles to a U.S.-based independent third-party dispute resolution mechanism, DPF Services, operated by BBB National Programs. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://bbbprograms.org/programs/all-programs/dpf-consumers/ProcessForConsumers for more information and to file a complaint. This service is provided free of charge to you.
- If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See https://www.dataprivacyframework.gov/s/article/G-Arbitration-Procedures-dpf?tabset-35584=2.
- Cisco-U.S. is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.

## Complaint resolution

Cisco commits to resolve complaints and concerns about your privacy and our collection and use of your Personal Data. If you have concerns or complaints about your privacy and our collection and use of your Personal Data, please contact us via the Privacy Request Form.

For complaints or concerns about your privacy and our collection or use of your Personal Data transferred to the U.S. pursuant to the DPF Principles, please see Data Privacy Framework.

Alternatively, you can contact the data protection supervisory authority in your jurisdiction for assistance. (Note, Cisco's main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch Autoritiet Persoonsgegevens.)

## Your California privacy rights

## California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)

For business purposes in the last 12 months, Cisco may have collected, used, and shared Personal Data about you as described in this Privacy Statement. Each category of data that may be used by Cisco or shared with third parties is categorically outlined in this Privacy Statement.

California consumers have a right to: (1) request access, correction, and deletion of their Personal Data, (2) opt out of the sale or sharing of their Personal Data, and (3) not be discriminated against for exercising one of their California privacy rights.

All individuals have the right to request access to and deletion of the information Cisco holds about them either online via the Cisco Privacy Request Form or by mail to Cisco Systems, Inc., Privacy Office, 170 West Tasman Dr., San Jose, CA 95134, USA.

In addition, California residents may also submit a request by calling direct 408-906-2726 or toll free 833-774-2726 (833-PRI-CSCO).

Cisco does not sell the Personal Data of California consumers.

Cisco does not discriminate against individuals for exercising their privacy rights.

View the Cisco CCPA Metrics Report.

## California Shine the Light

Residents of the State of California, under California Civil Code § 1798.83, have the right to request from companies conducting business in California a list of all third parties to which the company has disclosed Personal Data during the preceding year for direct marketing purposes. Alternatively, the law provides that if the company has a privacy policy that gives either an opt out or opt in choice for use of your Personal Data by third parties (such as advertisers) for marketing purposes, the company may instead provide you with information on how to exercise your disclosure choice options.

Cisco has a comprehensive Privacy Statement and provides you with details on how you may either opt-out or opt-in to the use of your Personal Data by third parties for direct marketing purposes. Therefore, we are not required to maintain nor disclose a list of the third parties that received your Personal Data for marketing purposes during the preceding year.

## Updates to this Cisco Privacy Statement

We may update this Privacy Statement from time to time. If we modify our Privacy Statement, we will post the revised version here with an updated revision date. If we make material changes to our Privacy Statement, we may also notify you by other means, such as by posting a notice on our websites or sending you a notification. By continuing to use our website after such revisions are in effect, you accept and agree to the revisions and to abide by them.

## The Cisco Privacy Statement was revised and effective as of September 26, 2023.

Click here for the previous version of the Privacy Statement.

## Questions, comments, and how to contact us

We value your opinion. Should you have questions or comments related to this Privacy Statement, please submit a Privacy Request or send mail to:

**Chief Privacy Officer**
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

**Americas Privacy Officer**
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

**Europe, Middle East, and Africa (EMEA) Privacy Officer**
Cisco Systems International BV
Haarlerbergweg 13-19,
1101 CH Amsterdam-Zuidoost, Netherlands

**Asia Pacific, Japan, and China (APJC) Privacy Officer**
Cisco Systems (USA) Pte Ltd
80 Pasir Panjang Road

Level 25, Maple Tree Business City 2,
Singapore 117372

## Privacy Statement

### Summary version

Select Language - English

For information on additional Cisco offers, see the Privacy Data Sheets on the Cisco Trust Center.

## How to Contact Us

### Privacy Request Form

Mail: Cisco Systems, Inc.
Legal Department
170 West Tasman Dr.
San Jose, CA 95134 USA

**Quick Links**

About Cisco

Contact Us

Careers

Connect with a partner

## Resources and Legal

Feedback

Help

Terms & Conditions

Privacy

Cookies / Do not sell or share my personal data

Accessibility

Trademarks

Supply Chain Transparency

Newsroom

Sitemap