

Cisco Umbrella Privacy Data Sheet

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Umbrella.

1. Overview of Cisco Umbrella Capabilities

Cisco Umbrella is a cloud-delivered security platform that provides the first line of defense against threats on the Internet by blocking requests to malicious destinations (domains, IPs, URLs) before a connection is established. Leveraging DNS as the first point of inspection, Umbrella provides protection against threats over all ports and protocols, and can protect Internet access across all devices on your network, all office locations, and roaming users. Using a diverse dataset of billions of daily DNS requests and live views of the connections between different networks on the Internet, Umbrella applies statistical models and human intelligence to identify attackers' infrastructures. Additionally, Cisco Umbrella Investigate provides access to Cisco's threat intelligence about malicious domains, IPs, networks, and file hashes. Investigate data can be accessed via a web-based console or an API. Umbrella offers various license options including Professional, Insights, Platform, WLAN, and Investigate. Please consult the Umbrella Documentation for further information on its technical specifications, configuration requirements, features and functionalities.

More details at offer description:

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/Omnibus_Cloud_Security_OD.pdf

Because Umbrella processes, stores and analyzes DNS traffic, and where applicable, processes and stores active directory information, it processes certain personal data of the users. The processed data is used for reporting purposes to the customer and for internal security research. Cisco's security research includes aggregating the processed data to track and predict threats, and using such data to provide predictive threat intelligence for its customers. The following paragraphs describe which personal data Cisco 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 tables below list the personal data used by Umbrella to carry out the services and describe why we process that data.

Personal Data processed by Cisco Umbrella Generally	Purpose of Processing
Registration Information Administrator email address, activation code, Administrator first and last name, password, Company name, billing contact name	<ul style="list-style-type: none"> • Activation of service • Billing/invoicing • Future notification of features/updates • Remote access support • Authentication/Authorization
Usage information: (i) DNS query data (domain, DNS record type, DNS response, IP address), (ii) Device ID	<ul style="list-style-type: none"> • DNS query data is initially processed to direct end user to domain being queried. • DNS query data is used to conduct analytics and statistical analysis in aggregate form to track and predict threats, for internal security research, and for reporting purposes to customer.

Additional Personal Data processed by Active Directory add-on	Purpose of Processing
Usage information: Active Directory identity (optional if using Active Directory) and Device ID.	<ul style="list-style-type: none"> • If Active Directory is used, Umbrella may also collect names of individuals and/or user device IDs, depending upon how customer admins upload data to the service. Customer's administrator can manually upload Active Directory information that is non-identifying in Umbrella systems. For example, rather than using employees' names or Machine ID's for tracking purposes, the admin can anonymize on the customer's end by using a string of numbers that only the admin could associate with a person's name/machine ID.

Additional Personal Data processed by Intelligent Proxy add-on	Purpose of Processing
Usage information: HTTP Traffic (optional if using the Intelligent Proxy or Block Page Bypass features) and HTTP Header info (e.g. URL), but excluding HTTP body content	<ul style="list-style-type: none"> • If using Intelligent Proxy, HTTP Traffic and Header info is collected to provide granular protection at URL and file level.

Personal Data processed for technical assistance and support	Purpose of Processing
Support Information First name, Last name, Email, Phone number of the employee appointed to open the service request, Customer information, etc.	<ul style="list-style-type: none"> • Remote access support • Review of the support service quality • Troubleshooting • Analysis of service

3. Cross-Border Transfers:

Cisco Umbrella is co-located in tier-1 data centers that feature state of the art physical and cyber security and highly reliable designs. Based on dynamic Anycast routing decisions, each customer's DNS traffic can be routed to any data center facility listed on our network map (set forth below), although normally the data center in which the traffic is routed will be the closest physical location to the individual initiating the DNS query. Additionally, the DNS query and associated IP address is then sent to San Jose, CA for additional processing. This is necessary for the delivery of Umbrella services, as big data analytics requires the examination of worldwide data in real time.

The following list may be updated from time to time and a current list can be found at:

www.cisco.com/go/dataprivacy

Location	Provider	Certification
Amsterdam, Netherlands	Telecity (Equinix)	Equinix ISO 27001 Certificate (valid to 28-06-2019)
Ashburn, VA	Equinix	SOC 2 Type 2 Equinix (NA IBX) - 2015; Equinix (NA - IBX) - 2015 SOC 1 Type 2
Berlin, Germany	e-Shelter	DIN EN ISO 9001; DIN ISO/IEC 27001
Bucharest, Romania	GTT	ISO 9001; ISO 27001
Chicago, IL	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
Copenhagen, Denmark	GTT	Global connect_ISAE3402_General DC certification; Global Connect_ISAE3402_Cloud_DC certification
Dallas, TX	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
Dubai, United Arab Emirates	Equinix DX1	SSAE16/ISAE3402 SOC-1 Type II; ISO 27001; PCI-DSS; FACT; ISO 9001-2008
Frankfurt am Main, Hessen, Germany	Equinix	Equinix (EMEA) - 2015 SOC 1 Type 2
Hong Kong	iAdvantage	ISO27001
Johannesburg, South Africa	EOH JB1	ISO 9001; ISO 27001
London, UK	Telehouse	ISO/IEC 27001
Los Angeles, CA	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
Miami, FL	Terremark	Verizon 2015 SOC 2
Mumbai, India	TATA BKC (Bandra Kurla Complex)	ISO 27001 and ISO 20000
New York, NY	NTT-GIN	Zayo Group LLC 2015 SOC 1 Type 2 Report
Paris, France	GTT	BSI - ISO 27001; Telehouse - BSI 9001 FS 612057; Telehouse - BSI ISO 14001 EMS 612059
Prague, Czech	GTT	ISO 27001, ISO 1800, ISO 14001, ISO 9001
San Jose, CA	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
San Jose, CA	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
Seattle, WA	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
Singapore	Equinix	Equinix (APAC) - 2015 SOC 1 Type 2
Sydney, Australia	Equinix	Equinix (APAC) - 2015 SOC 1 Type 2
Tokyo, Japan	Equinix	Equinix (APAC) - 2015 SOC 1 Type 2
Toronto, Canada	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015

Version 1; February 2, 2018

© 2018 Cisco Systems, Inc. All rights reserved.

Printed and soft copies are uncontrolled. For the latest version see: www.cisco.com/go/dataprivacy

Vancouver, BC	Cologix	Cologix 9-30-15 Multi-Site SOC 1
Warsaw, Poland	Linx Telecom	LINX WRW ISO 27001 2013 valid to Dec 2016; Cert ISO 9001 WRW LINX 2015

Umbrella also leverages Amazon Web Services (AWS) data centers in the AWS West region of the United States with future plans to leverage AWS data center in the AWS East Region of the United States, Frankfurt, and Ireland. 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/>.

Certain administrative data and support data may also be processed and stored in the US. Umbrella uses Salesforce and Zendesk for the processing and storage of limited customer administrative data and support data (if any) and the Salesforce and Zendesk data center locations are based in the US. Additionally, Umbrella employs support personnel globally, so a customer support agent based outside of the EU may need access to certain personal administrative data to assist the customer in troubleshooting the service.

4. Access control

Personal Data processed by Cisco Umbrella	Who has access	Purpose of the access
Registration Information	Customer administrator	Modify and control certain admin information
	Cisco Umbrella	Provision customer's account; billing/invoicing; supporting the service in accordance with our data access and security controls process
Usage Information	Cisco Umbrella	Support of the service; improvement of the service
	Customer administrator (only to customer's DNS logs, not to all Cisco Umbrella DNS logs)	Set policies on customer network; monitor customer network
Support Information	Cisco Umbrella	Provide support for the service and troubleshoot customer issues
	Customer administrator	Provide feedback, point out technical issues

5. Retention Period

Umbrella follows the below retention policies:

Type of Personal Data	Retention Period	Criteria for the retention
Raw DNS query data (domain, DNS record type, DNS response, IP address) and Device ID	30 days or less	Automatically deleted after no later than 30 days

Administrator email address, activation code, Administrator first and last name, password, Company name, billing contact name	No official retention period, data is not deleted unless requested	n/a
Active Directory identity (optional if using Active Directory) and Device ID.	No official retention period, data is not deleted unless requested	n/a
HTTP Traffic (optional if using the Intelligent Proxy or Block Page Bypass features) and HTTP Header info (e.g. URL), but excluding HTTP body content	30 days or less	Automatically deleted after no later than 30 days
Summarized log data	Up to 2 years	Automatically deleted no later than 2 years after creation of logs

6. Deletion

A customer may request deletion of Personal Data by sending a notice to Cisco umbrella support or privacy@cisco.com. When customer makes a request for deletion, Cisco will purge 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).

7. Personal Data Security

For additional information on Umbrella's data security program, please refer to Section 9 below.

Personal Data processed by Cisco Umbrella	Type of Encryption
Raw DNS query data (domain, DNS record type, DNS response, IP address) and Device ID	AES 128 encryption in transit.
Administrator email address, activation code, Administrator first and last name, password,	Backups are encrypted with GPG.

Company name, billing contact name	
Active Directory identity (optional if using Active Directory) and Device ID.	Encryption in transit over TLS 1.2 (full Cipher list available upon request).
HTTP Traffic (optional if using the Intelligent Proxy or Block Page Bypass features) and HTTP Header info (e.g. URL), but excluding HTTP body content	Encryption in transit.

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 Cisco Umbrella's third party service providers having access to customer data can be provided upon request. Sub-processors include, for example, third party colocation data centers (DNS infrastructure), AWS (hosting infrastructure), CRM (Salesforce), and support (Zendesk).

List of Third Parties	Personal Data	Purpose of Sharing	Location
<ul style="list-style-type: none"> Data centers, as set forth in Section 3 above 	<ul style="list-style-type: none"> IP address contained in DNS query data 	<ul style="list-style-type: none"> To resolve DNS queries 	<ul style="list-style-type: none"> See map in Section 3 above
<ul style="list-style-type: none"> AWS 	<ul style="list-style-type: none"> Customer network logs 	<ul style="list-style-type: none"> Holds customer logs 	<ul style="list-style-type: none"> AWS US and EMEA
<ul style="list-style-type: none"> Salesforce 	<ul style="list-style-type: none"> Administrative and support data 	<ul style="list-style-type: none"> To provision the service and provide support 	<ul style="list-style-type: none"> Dallas, TX, USA Phoenix, AZ, USA
<ul style="list-style-type: none"> Zendesk 	<ul style="list-style-type: none"> Support data 	<ul style="list-style-type: none"> To provide support 	<ul style="list-style-type: none"> West Coast, USA Backup site in East Coast, USA

9. Data Protection and GDPR FAQ

Is there a cross-border transfer of personal data when using Cisco Umbrella?

Yes. Please see Section 3 above.

How does Cisco Umbrella comply with European data protection laws?

In addition to implementing a comprehensive privacy and data security program, Umbrella complies with applicable privacy laws and endeavors to follow best practices set out in relevant guidance, including the Directive 94/46 of the European Parliament of the Council of October 24, 1995. This regards the protection of individuals when processing personal data and the free movement of data (the "Privacy Directive"), as implemented into local laws, Switzerland's Federal Act on Data Protection of June 19, 1992, Germany's Federal Data Protection Act of December 20, 1990 as amended on September 14, 1994, and the nonbinding Opinion May, 2012 on Cloud Computing released by the Article 29 Working Party on July 1, 2012.

What is GDPR and who does it affect?

The European Union General Data Protection Regulation, or EU GDPR, will become law on May 25, 2018, and affects organizations that process EU personal data. Aimed at protecting the fundamental right to privacy, the new regulations are broad, strict, and require adherence from organizations all over the world.

Will Cisco Umbrella make an organization GDPR compliant?

No single product will make an organization GDPR compliant. GDPR is the legislative embodiment of privacy best practices and calls for transparency, fairness, and accountability when processing personal data. GDPR pushes the concepts of Privacy by Design and by Default: privacy and data protection have to be built-in and integrated in all data processing activities performed by the entity (the data controller) or by external organizations on its behalf (the data processor). This is about respecting individual rights, secure processes, and managing risk. Well-applied technology solutions can help underpin success. For example, Cisco Umbrella can help the customer raise their security levels by blocking suspicious domains that might be compromised.

Does personal data need to remain in the EU?

No. People often assume that the EU GDPR requires data localization and that personal data must remain in the EU. GDPR provides that EU personal data should be processed in the EU unless you have approved mechanisms that allow for the international transfer of data. For example, Cisco has certified compliance with the EU-US and Swiss-US Privacy Shield which commits Cisco to a set of privacy principles and practices aligned to EU law when processing EU personal data in the US. The Shield framework has been deemed “adequate” by the European Commission – meaning EU personal data can flow to Shield-certified companies and hence can flow to Cisco Umbrella.

If necessary, Cisco also offers a Data Processing Agreement to customers that incorporates the EU Standard Contractual Clauses, which contractually binds Cisco to adhere to EU privacy standards. The use of EU Standard Contractual Clauses has been approved by the European Commission to allow transfers of EU personal data outside of the EU. We do not require our customers to agree to the clauses but offer this option to give our customers an additional path to meeting requirements under applicable data protection laws.

What is Cisco’s stance on data privacy in general?

Cisco respects and is committed to protecting personal information. Our privacy statements reflect current global principles and standards on handling personal information: notice and choice of data use, data access and integrity, security, onward transfer and enforcement/oversight.

Cisco is certified under the EU-US and Swiss-US Privacy Shield frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, processing, and cross-border transfer of personal data from the EU and Switzerland. Cisco is also certified under the APEC Cross Border Privacy Rules system (www.cbprs.org) which has been endorsed by the 21 member economies of the Asia Pacific Economic Cooperation (APEC) organization as providing an appropriate baseline for privacy and data protection. To read Cisco’s full privacy statement visit:

<https://www.cisco.com/c/en/us/about/legal/privacy.html>.

What does the Cisco Umbrella privacy and data security program entail?

Cisco takes a systematic approach to data protection, privacy, and security. We believe a comprehensive security and privacy program requires executive sponsorship and active involvement of cross-functional stakeholders, ongoing education, internal and external assessments, and instilment of best practices within the organization.

Cisco has established formal policies and supporting procedures concerning the privacy, security, review, and management of our products and services. The Cisco Chief Security and Trust Officer, Chief Privacy Officer (including EMEAR, APAC and Americas Privacy Officers), Chief Information Security Officer, and Global Data Protection & Privacy Counsel maintain overall responsibility for the program, which is evaluated on a regular basis. This helps ensure it is up to date and follows modern security standards and best practices, as well as compliance with applicable privacy regulations. The Cisco Security and Trust Organization's Information Security and Data Protection and Privacy programs include technical and organizational measures designed to help ensure physical and cyber security, data integrity, privacy, and transparency.

The Umbrella service is designed for top-tier security and data privacy, and follows industry leading best practices for security and privacy. As set forth in Section 3 above, Cisco Umbrella data centers are certified by various industry recognized standards. These data centers feature state of the art physical and cyber security and highly reliable designs.

You can view the following resources for more information:

- <https://blogs.cisco.com/security/gdpr-cisco-and-you>
- <https://www.cisco.com/c/en/us/about/trust-center/privacy-podcast.html>
- <https://www.cisco.com/c/en/us/products/security/general-data-protection-regulation.html>