Cisco DNA Spaces – Privacy and Data Protection

Cisco DNA Spaces and Data Privacy

Cisco® DNA Spaces is an indoor location services cloud platform that provides wireless customers with rich location-based services, including location analytics, business insight, customer experience management, asset tracking, Bluetooth Low Energy (BLE) management, and API.

It provides a single point of entry for all location technology and intelligence through a single dashboard interface. Cisco DNA Spaces delivers the industry's most scalable location-based marketing platform, all while being compatible across existing Cisco Catalyst or Meraki infrastructure.

Following are key stakeholders who develop, support, host, and consume the functionalities of the Cisco DNA Spaces solution:

- **Individual** (also referred as "**data subject**") – The data subject is an identifiable natural person to whom the data relates. The data subject is the final consumer of the Cisco DNA Spaces features and functionality.
- **Customer** (also referred as "**data controller**") – The data controller can be a person, organization, or an entity that owns and exercises control over the personal data that is collected. A data controller can determine how the data is collected and the manner in which the data will be processed. For the Cisco DNA Spaces solution, the customer is the data controller.
- **Cisco** (also referred as "**data processor**") – The data processor is an entity or an organization that processes the collected data on behalf of the data controller. For the Cisco DNA Spaces solution, Cisco is the data processor, which processes the da-ta on behalf of the customer. At Cisco, the DevOps and the engineering teams are involved in the data processing and operational activities.
  - **DevOps** – The primary responsibility of the DevOps team is to manage and monitor the cloud infrastructure and the platform hosted in the Amazon Web Services (AWS) cloud.
  - **Engineering** – The engineering team is responsible for creating the solution architecture, technical design and implementation, testing, and deployment of the Cisco DNA Spaces solution. The team currently follows the Cisco Secure Development Lifecycle (CSDL) process, which is designed to increase the resiliency and trustworthiness of Cisco offerings, while developing new applications or making enhancements to the existing applications. The Quality Assurance (QA) team, which is part of the engineering team is responsible for testing the product functionality and performing security testing of the Cisco DNA Spaces solution.

© 2019 Cisco and/or its affiliates. All rights reserved.

Personal data records and its use, collection, and retention

Personal data is any information relating to an identified or identifiable natural person (end user). Information can include a name, location data, or one or more factors specific to the physical, genetic, mental, economic, cultural, or social identity of that natural person.

What data does Cisco DNA Spaces collect?

Personal data collection and its purpose is solely determined by the customer (data controller), who provides the data to Cisco (data processor) for processing. Cisco collects and processes the non-sensitive personal data on behalf of customer. The Cisco DNA Spaces solution:

- Does not collect any special category of personal data, such as race, ethnic background, political opin-ions, genetic data, biometric data, health data, etc.
- Does not intentionally collect any personal data from minors, as minors are disallowed from using the Cisco DNA spaces solution.
- Collects only the non-sensitive personal data through the network (MAC address). This data collection is optional and in certain cases, the customer may decide to collect additional data from users.

What does Cisco DNA Spaces do with the collected data?

The non-sensitive personal data collected via the Cisco DNA Spaces platform is essential for implementing the customer solution, such as report generation, trend and data analytics, etc. The underlying restrictions on the purposes of the collected data are applied as per the agreements with the data controller. Restrictions are bound by the commitments provided to the customer (data controller) with respect to the use and retention of the non-sensitive personal data. The data retention activity is based on the agreements with the customer, and as governed by local laws and compliance with prevailing regulations.

Privacy compliance by Cisco DNA Spaces

- Cisco DNA Spaces customers expect and rely upon Cisco to protect their data and privacy. Hence, it is mandatory to provide data protection and implement privacy controls on the collected data.
- The Cisco DNA Spaces solution has adopted the Cisco Secure Development Lifecycle (CSDL) process, which helps to ensure the Cisco DNA Spaces cloud solution adheres to predefined Cisco security requirements and standards.
- The Cisco DNA Spaces solution has achieved Cloud Approval To Operate (CATO) compliance as per the process outlined in the Cloud Security Progression Plan.
- One of the keys to maintaining CATO compliance is to ensure that the data protection and secure operations of the Cisco DNA Spaces solution adheres to industry standards and certifications, such as ISO 27001, GDPR compliance, etc.
- CATO makes sure all the secure operations of the Cisco DNA Spaces solution follow:
  - Adherence to industry standards and best practices
  - Include cyber security controls such as privacy impact assessments
  - Implement privileged access control mechanisms
  - Implement authentication and authorization mechanisms
  - Manage security incident responses
  - Adopt cryptography controls and encryption mechanisms
  - Implement secure development process
  - Monitor logging and auditing control mechanisms

© 2019 Cisco and/or its affiliates. All rights reserved.

Legal information

The specifications and information regarding the products in this manual are subject to change without notice. all statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. users must take full responsibility for their application of any products.

The software license and limited warranty for the accompanying product are set forth in the information packet that shipped with the product and are incorporated herein by this reference. if you are unable to locate the software license or limited warranty, contact your Cisco representative for a copy.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided "as is" with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C11-742079-01 06/19