Collection and Storage of Personal Data from Cisco DNA Spaces Networks in Russia

First Published: October 22, 2020
Last Updated: November 3, 2020

Table of Contents

Introduction

Russian legislation on personal data requires that information that can be considered as personal data of Russian citizens (PII data), when collected, shall be recorded by the personal data operator in databases in Russia and stored in Russia. Cisco DNA Spaces installed in Russia, as well as the Cisco DNA Spaces Dashboard/Captive Portal web interface used by Russian customers, under certain circumstances, can collect PII data and send them to the Cisco DNA Spaces data center (DC) located in the European Union (EU).

Since Cisco DNA Spaces does not have a DC located in Russia, the following solution may be used to enable customer's compliance with Russian legislation on personal data:

Cisco has developed a DNA Spaces Firehose Archiver for the DNA Spaces Dashboard/Captive Portal that enables customers and/or partners to extract PII data collected directly by DNA Spaces and via the DNA Spaces Dashboard/Captive Portal web interface and store such data on local servers in Russia. For purposes of this informational document, a partner that implements the DNA Spaces Firehose Archiver is called a "PII partner."

PII Partner should have all the necessary licenses and certificates required by Russian law on personal data security.

The PII partner should store personal data as long as it is required by Russian law or longer in case of special agreements with Cisco DNA Spaces customers, but not less than the storage period in the Cisco DNA Spaces DC in the EU.

Data in the Cisco DNA Spaces DC in the EU is stored for the duration of Customer's active license term to the Service, or until such time that Customer or PII data owner requests deletion of this data by reaching out to Cisco technical support for Cisco DNA Spaces.

Customers may implement the Cisco DNA Spaces Firehose Archiver I solution in two ways: (1) a Cisco DNA Spaces customer located in Russia may conclude a direct contract with a PII Partner for storing PII data in Russia (on behalf of the customer), in which case such PII partner may include payment or other conditions for the storage in such direct contract with the customer, or (2) a customer may implement the Cisco DNA Spaces Firehose Archiver solution directly itself and without the assistance of a PII partner.

Data Flows

For Wi-Fi Client Devices

1. The initial collection of PII data is carried out by the Customer (using Cisco DNA Spaces on-prem components installed on the Customer's site in Russia).
2. The collected PII data is stored in Russia at the facilities of the customer or the PII Partner and is also sent for additional processing to Cisco DNA Spaces servers located in the EU.

3. For Russia deployments, the customer or the PII partner using the Cisco DNA Spaces Firehose Archiver receives a complete set of PII data collected by Cisco DNA Spaces and stores it in Russia. The same set of data is also stored in the DC in the EU.

For Cisco DNA Spaces Dashboard Web Interface

1. PII data collected via the Cisco DNA Spaces Dashboard/Captive Portal web interface is stored in Russia at the facilities of the customer or PII Partner and is also processed by Cisco DNA Spaces servers in the EU.
2. The customer or the PII partner using the Cisco DNA Spaces Firehose Archiver stores in Russia the set of customer data collected via the Cisco DNA Spaces web interface, which is also stored in the Cisco DNA Spaces DC in the EU.

Data Collection

Option # 1: Cisco DNA Spaces Captive Portal web interface is not used for registration, authentication and authorization of end users.

The table below shows the data collected by Cisco DNA Spaces devices. Data can be visualized using the Cisco DNA Spaces Dashboard.

Table 1

Personal Data Category	Types of Personal Data
System Administrator Account Information	▪ First and last name ▪ E-mail address ▪ Password
End User Information	▪ MAC address ▪ Employee username

In this case, the data collected may be recognized as personal data and it is necessary to use the Cisco DNA Spaces Firehose Archiver solution for the processing and storage of such data.

At the same time, since the PII data shown in the Table 1 are data that may be known to the Client since he is the employer of the subject of such data, then the use of the Cisco DNA Spaces Firehose Archiver solution may not be required, since the localization of the specified data has already been carried out by the Client under his employment relationship with the PII data owner.

Option #2: The Cisco DNA Spaces Captive Portal web interface is used for registration, authentication and authorization of end users.

The list below shows the data collected by the Cisco DNA Spaces and Captive Portal web interface. Data can be visualized using the Cisco DNA Spaces Dashboard.

Table 2

Personal Data Category	Types of Personal Data
System Administrator Account Information	▪ First and last name ▪ E-mail address ▪ Password
End User Information	▪ MAC address (collected by default) ▪ Employee username The customer has the opportunity to enable through the authorization portal the collection and processing of additional types of personal data, namely: Any other categories added by the customer: ▪ First and last name ▪ Floor ▪ E-mail address ▪ Phone number ▪ Position ▪ Postcode ▪ Work tags (customer-assigned tags / categories for end users) ▪ Age range ▪ Social Media ID

In this case, the data collected may be recognized as personal data and it is necessary to use the Cisco DNA Spaces Firehose Archiver for the processing and storage of such data.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

Legal Information

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.

Cisco Trademark

Cisco Copyright