GDPR Notice

AudioCodes Mediant SBC Devices

This document describes the support of Mediant SBC devices for the EU General Data Protection Regulation (GDPR).

Note: GDPR aspects that are not listed in this document are considered not relevant to the operation of the SBC products.

1 Overview and Definitions

GDPR defines 'personal data' as any information related to an identifiable person. This person may be identified directly (i.e. by name) or indirectly through any other identifier which is unique to that person. For the Mediant SBC products, individuals can be indirectly identified through phone numbers that are processed by the SBC. The SBC generates three data sets which may contain personal data:

a) CDR records: Call Detail Records (CDR) contain information on calls made from the device. Information that may be defined as private information in CDR records could include, for example, the caller phone number and called phone number.
The device can generate and report CDRs at various stages of the call - end of call, or only at the start and end of call. In addition, CDRs can be generated for SIP signaling and/or media. The device can send CDRs to any of the following:

I. Syslog server: The CDR Syslog message complies with RFC 3164 and is identified by Facility 17 (local1) and Severity 6 (Informational).
II. RADIUS server for CDR in RADIUS format.
III. CDRs stored locally on the device.

b) Syslog notifications: Syslog is an event notification protocol that enables a device to send event notification messages across IP networks to event message collectors, also known as Syslog servers. Information that may be defined as private information in syslog events could include, for example, a caller phone number and called phone number.
The device contains an embedded Syslog client, which sends error reports / events that it generates to a remote Syslog server using the IP / UDP protocol. This information is a collection of error, warning, and system messages that records every internal operation of the device.

AudioCodes Inc.
80 Kingsbridge Road Piscataway, NJ 08854
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Israel
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

c) **Debug Recording:** The device can send debug recording packets to a debug capturing server. Information that may be defined as private information in a debug recording could include, for example, a caller phone number and called phone number. When the debug recording is activated, the device duplicates all messages that are sent and/or received by it and then sends them to an external server defined by IP address. The debug recording can be done for different types of traffic such as RTP/RTCP, T.38, and SIP.

Under normal operation, the device treats the above types of information as 'write only' and may cache it temporarily before sending it out, if ordered by a privileged user, to 3rd party tools that are external to the SBC where the information can be further processed outside of the scope of the SBC device.

Any 'personal information', as defined above, that was generated by the above sources of information is treated in a constant fashion:

a) The information may be temporarily cached on the device

b) A privileged user can extract the information from the device into a 3rd party system

c) The temporarily cached information is deleted either explicitly by a user command or automatically by the device's normal operation

Once the information is sent to 3rd party tools that are external to the SBC, GDPR compliance with regards to further processing these data sets depends on the third-party tools being used and is beyond the scope of control of AudioCodes SBCs.

The rest of this document describes the compliance of SBC handling of 'personal data' records per the corresponding GDPR sections.

Apart of the above data sets, the Mediant SBCs do not collect and retain any other 'personal data' as defined above.

2 Right of Access (Art 15)

Access to the CDR, syslog notification and debug recording on the SBC is limited to admin level users and requires valid administrator credentials.

Once appropriate credentials are provided, locally cached information can be retrieved from the SBC to a 3rd party system, using a standard SFTP client, allowing for a secure retrieval of the information into a 3rd party file system. The information can then be further processed as needed, for example: it can be searched using a simple text search so that a 3rd party system can filter/identify specific records matching any requested 'personal data' that is defined in this document.

When the SBC is configured to send the CDR records, Syslog notifications or Debug Recording to a 3rd party server, the information is sent to the external server shortly after it is captured. Once sent, this information can be further processed by the a 3rd party system, for example: it can be searched using a simple text search so that a 3rd party system can filter/identify

AudioCodes Inc.
80 Kingsbridge Road Piscataway, NJ 08854
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Israel
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

specific records matching any requested 'personal data' that is defined in this document. This processing is outside the scope of the SBC product.

Detailed information on how to connect the SBC to a Syslog server, a RADIOUS server, or a debug information capture server and instructions for retrieving the CDR stored locally via SFTP can be found in the product's user manual.

3 Right to Rectification (Art 16)

All information collected via CDR records, Syslog notifications or Debug Recording is treated as 'read only' information once stored on the SBC. There is no mechanism that allows a user to edit or modify the information once captured and stored as part of normal operation, and there are no actions that the product takes based on the information captured in CDR records, Syslog notifications or debug recordings.

4 Right to be Forgotten (Art 17)

Information collected as part of the sub-systems described in section 1 is treated in the following way: the information is stored in a 'cyclic buffer' and is overridden over time. this means that the cached information will be deleted as part of normal device operation as new information is cached on the device over time. No user action is needed to enable this as this is the default normal way of handling the information.

For CDR local storage (1)(a)(iii), the SBC admin can define a retention policy of the information (for how long it will be kept), and in addition use the SBC CLI to order the product to delete any existing CDR records from its local persistent storage.

Detailed information on how to specify a CDR retention policy and how to delete all CDR local storage records can be found in the product's user manual.

5 Right to Data Portability (Art 20)

Access to the CDR, syslog notification and debug recording is limited to admin level users. The admin user needs to provide valid credentials to access the information.

Once appropriate credentials are provided, the full information can be retrieved, and moved from the SBC to a 3rd party system, where the information can then be identified, processed, filtered, and aggregated upon user request.

The information removed from the SBC product is provided using an open standard format that is portable to any modern computer system.

As an example, a simple text search can be performed using the 3rd party system to filter/identify specific records matching the requested user. The exact processing is beyond the scope of the SBC product.

AudioCodes Inc.
80 Kingsbridge Road Piscataway, NJ 08854
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Israel
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

Detailed information on how to connect the SBC to a Syslog server, a RADIOUS server, and instructions for retrieving the CDR stored locally using a standard SFTP client can be found in the product's user manual.

6 Retention

For CDR local storage (a)(iii), the SBC admin can define the retention policy of the information (for how long it will be kept), and in addition use the SBC CLI to delete any existing CDR records from its local persistent storage.

Detailed information on how to specify a CDR retention policy and how to delete all CDR local storage records can be found in the product's user manual.

7 Disposal Process

To remove any personal information from the system before disposal, an admin level user can perform a 'return to a Factory Snapshot' operation on the device.

This operation erases all data from the device and returns it to its initial state, removing all 'personal data' as defined in this document.

Detailed information on how to return the device to the default factory settings can be found in the product's user manual.

8 Security

The device provides security measures that only allow authorized users to have access to the device information and settings, these measures include a secured HTTPS device log-in, user access levels, and user activity Logs. The CDR information can be retrieved from the device in a secure way using SFTP and both signaling and media information can be configured to use encrypted communications.

AudioCodes Inc.
80 Kingsbridge Road Piscataway, NJ 08854
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
Naimi Park, 6 Ofra Haza Street, Israel
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com