

Personal Data Usage and Protection

All Mediatrix Products

DGW 49.2.2941

2023-08-09

Table of Contents

Personal Data Exposure	3
Personal Data Collection	3
Personal Data Processing	4
Personal Data Transfers	4
Personal Data Protection	5
System and Data Protection	5
Communications Protection (VoIP Calls)	5
Access and Communications	6
Data Deletion	6
Audit	6
Copyright Notice	7

Personal Data Exposure

Personal Data Collection

Mediatrix products collect the basic personal data required for the proper delivery of the telecommunication service. The actual collected data depends on the type of users and how the Mediatrix products are administrated.

Type of users	Collected Personal Information	Collected Activity Information
End-Users	Name and phone number used to register to the telecommunication provider service.	Calls history for billing purposes and call details and recordings for troubleshooting purposes. For example: • Call date/time and duration • IP address • Voice or video stream • Fax or modem data stream • In-call digits dialled (DTMF) • E911 geo-localisation • Voicemail PIN • etc.
System Administrators and Technical Support	Account name and password used to access the product for administrative and troubleshooting purposes.	• Logs of the administration and troubleshooting activities. • Audit trails of the administration and troubleshooting activities.

Personal Data Processing

Personal data is processed in Mediatrix products through the following activities:

- Configuring and storing end-user data
- Recording voice and fax calls
- Logging call history (CDR)
- Logging administration audit trails
- Access of the personal data by an authorised system administrator
- Provisioning data
- Maintenance, administration and technical support records
- Audit trails
- End-user activity records
- End-User personal content
- Recording voice and fax calls for troubleshooting

Personal Data Transfers

The following collected personal data may be transferred to other systems, depending on how the device administrators configure the Mediatrix products.

- Call Details Records (CDR) may be sent to an external call accounting system.
- Logs may be sent over an external monitoring system for live troubleshooting.
- Administration activity logs may be sent over an external monitoring system for auditing.
- Backups of the Mediatrix products, containing collected personal data, may be retrieved by an authorised system administrator.
- Network captures from the Mediatrix products, containing collected personal data, may be retrieved by an authorised system administrator for troubleshooting purposes.

Personal Data Protection

System and Data Protection

To protect the end-user personal data stored inside the Mediatrix devices, the device administrator should control and restrict access to the management interfaces by:

- Forcing the use of a strong authentication password
- Authorising LAN access only
- Using the device firewall service to limit the remote access to the device to only authorized peers and authorised services
- Using an external firewall
- Enabling IEEE 802.1x authentication of Ethernet link

The device administrator may also enforce the use of encryption and authentication for a secure administration of the Mediatrix devices:

- Authenticated Management Interfaces:
 - Web Interface: HTTPS with trusted certificates
 - CWMP: HTTPS with trusted certificates
 - CLI: SSH
- Secure Management Operations:
 - Consult or retrieve the stored personal data: HTTPS with trusted certificates
 - Provisioning: HTTPS with trusted certificates
 - Firmware upgrades: HTTPS with trusted certificates
 - Backup/restore: HTTPS with trusted certificates

Communications Protection (VoIP Calls)

The device administrator may configure the encryption of the data that transits through Mediatrix products:

- Call signalling: SIP over TLS with trusted certificates
- Media packets: SRTP

Access and Communications

The Mediatrix products have three (3) default account roles:

- Administrator
- User (no password access)
- Observer (read-only)

All the management interfaces are restricted to authorised accounts only, verified by username and password. Refer to the [System and Data Protection](#) (p.5) section for the list of management interfaces and how to protect them.

The account credentials may be stored locally in the Mediatrix devices or in an external RADIUS authentication server.

In all cases, the device administrator should restrict the physical access to the Mediatrix products.

Data Deletion

The Mediatrix products allow an authorised system administrator to delete end-user registration information (name and number).

A system administrator should also delete any temporary logs that may have been stored locally during a troubleshooting session such as:

- call history
- call recordings
- network captures

A factory reset can be performed by a system administrator to revert a Mediatrix device back to its default factory state through a factory reset, thus erasing all the collected data and configuration.

Audit

Audit trail logs of the system administrator activities may be enabled by the device administrator. These audit logs may be temporarily stored locally or sent through syslog to an external monitoring system.

Copyright Notice

Copyright © 2023 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.



media5corp.com