

Attaining GDPR compliance in MiVoice MX-ONE

DESCRIPTION



NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2018, Mitel Networks Corporation

All rights reserved

1 GENERAL

1.1 WHAT IS GDPR?

The European Union (EU) **General Data Protection Regulation (GDPR)** effective from May 25, 2018, replaces the previous EU Data Protection Directive 95/46/EC.

The intent of GDPR is to harmonize data privacy laws across Europe so that the data privacy of EU citizens can be ensured. GDPR requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. GDPR also addresses the export of personal data outside of the EU. Any business that processes personal information about EU citizens within EU must ensure that they comply with GDPR. Under GDPR, 'processing' means any operation performed on personal data, such as collecting, recording, erasing, usage, transmitting, and disseminating.

1.1.1 WHAT DO BUSINESSES NEED TO KNOW ABOUT GDPR?

GDPR applies to businesses with a presence in any EU country, and in certain circumstances, to businesses that process personal data of EU residents even if the businesses have no presence in any EU country.

In order to achieve GDPR compliance, businesses must understand what personal data is being processed within their organization and ensure that appropriate technical and organizations measures are used to appropriately safeguard such data. This document explains what personal data is processed by Mitel's MiVoice MX-ONE system ("MX-ONE") and highlights available security features to safeguard such data.

2

PERSONAL DATA COLLECTED BY MX-ONE

The MiVoice MX-ONE is made available as both on-premise and hosted offerings. Both offerings only process personal data which is required for the delivery of communication services including billing services and technical support services. There are no opt-in consent mechanisms implemented in MiVoice MX-ONE.

Note: The MiVoice MX-ONE does not collect or store any really sensitive personal data.

During the course of installation, provisioning, operation, and/or maintenance, MiVoice MX-ONE collects data related to several types of natural persons, including:

- **End users** of Mitel products and services, typically Mitel customer employees using Mitel phones and collaboration tools.
- **Customers of Mitel customers** – for example, call recordings contain personal content of all parties in the call; personal contact lists contain personal data of business contacts.
- **System administrators and technical support personnel** – Logs and audit trails contain records of the activities of system administrators and technical support personnel.

To summarize what GDPR means for a technical system like MiVoice MX-ONE, it is to:

- Be able to protect personal data from unauthorized readers, or from being manipulated by unauthorized users.
- Be able to extract personal data for review.
- Be able to erase personal data, on request.

2.1

PERSONAL DATA PROCESSED BY MIVoice MX-ONE

The MiVoice MX-ONE system processes the following types of data to enable its communication features:

- **Provisioning Data:** The end user's name, business extension phone number, mobile phone number, business address, department, and email address.
- **Maintenance, Administration, and Technical Support Activity Records:** System backups, content backups, logs, and audit trails.
- **End User Activity Records:** Call history and call detail records.
- **End User Personal Content:** Voice mail, call recordings, and personal contact lists.

2.2

PERSONAL DATA TRANSFERRED BY MIVoice MX-ONE

Depending on the customer's configuration, and specific use requirements, the personal data collected may be processed and/or transferred between the MiVoice MX-ONE and other related systems and applications (such as directory systems, voice mail systems, and billing systems.)

For example:

- User provisioning data such as the user's first name, last name, office phone number, and mobile phone number may be shared between Microsoft Active Directory, MiVoice MX-ONE Provisioning Manager, MiCollab and CMG and management systems such as the Mitel Performance Analytics (MPA) system.
- Voice quality logs, phone inventory, user name, and phone number may be read by the MPA system and may be transferred to third-party systems.
- System logs, login and logout audit logs for the desktop tools, voice quality logs, customer databases, call detail records (CDR/SMDR), and voice quality statistics may be transferred to Mitel product support, or transferred to customer authorized log collecting systems.
- Call Detail Records (SMDR) may be transferred to third-party call accounting systems.
- When MiVoice MX-ONE is part of a Hospitality solution (hotels or similar) the system may be configured to transfer the end user's personal data to other customer-authorized Property Management Systems.

3

HOW MIVOICE MX-ONE SECURITY FEATURES RELATE TO GDPR

Security Feature	Feature Details	Documentation
System and Data Protection, Identification and Authentication	<p>Access to personal data is limited with administrative controls on accounts.</p> <p>Access to the system is limited by allowing only authorized access that is authenticated using username/password combinations.</p> <p>System administrator users can be associated with different profiles. Failed logins are logged and restricted to a maximum of three attempts.</p> <p>Communication to the system is performed over authenticated connections, using SSH version 2 or HTTPS (TLS).</p> <p>A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs) and firewalls.</p> <p>In all cases, physical access to systems should be restricted by the customer.</p> <p>All data stored at rest (system logs, audit files, and backups) are protected with administrative controls on accounts.</p> <p>Personal data included in Call Detail Records can be masked or anonymized.</p>	<p>Details can be found in the documents called, <i>MiVoice MX-ONE Security Description</i> and <i>Security Guidelines</i>, <i>Provisioning Manager Description</i>, <i>Service Node Manager Description</i> and in the MiVoice MX-ONE Provisioning Manager Help files.</p> <p>User management setup: In the MX-ONE Service Node go to <i>mxone_maintenance</i> to set up user accounts.</p> <p>In the MiVoice MX-ONE Provisioning Manager go to the: <i>Security Profiles</i> to configure Administrative access controls users.</p> <p>Call Detail Record (CDRs/SMDR) setup details can be found in the document Call Information Logging Operational Directions.</p>

Security Feature	Feature Details	Documentation
<p>Communication Protection</p>	<p>Encryption is highly recommended to be used for communications protection.</p> <p>The following controls are available in MiVoice MX-ONE:</p> <p>Data protection MiVoice MX-ONE Service Node</p> <ul style="list-style-type: none"> - SSH version 2 is used to access MiVoice MX-ONE. - HTTPS is used between MX-ONE and SIP phones to protect VDP (Visitor Desktop/hot-desking) data transmission. <p>MiVoice MX-ONE Service Node Manager and MiVoice Provisioning Manager</p> <ul style="list-style-type: none"> - HTTPS is used to protect data transmission in MiVoice MXONE Service Node Manager and MiVoice MX-ONE Provisioning Manager. - HTTPS may be used to protect data transmission between Provisioning Manager and Mitel applications as well as third-party applications. <p>Voice Call Signaling Only authenticated devices may connect to the MiVoice MX-ONE. Call signaling between the MiVoice MX-ONE and IP phones may be secured with TLS. Note that TLS 1.2 is the preferred option to encrypt call signaling when it is supported by the terminal. Legacy analog and digital trunks and devices do not support encryption.</p>	<p>Details can be found in the document called, <i>MiVoice MX-ONE Security Description</i> and <i>Security Guidelines</i>, <i>Provisioning Manager Description</i>, <i>Service Node Manager Description</i> and in the MiVoice MX-ONE Provisioning Manager Help files.</p> <p>Data protection MiVoice MX-ONE Service Node SSH version 2 is enabled by default in MiVoice MXONE. To enable HTTPS to protect VDP data, go to <i>mxone_maintenance > certificate management</i></p> <p>MiVoice MX-ONE Service Node Manager and MiVoice Provisioning Manager</p> <p>To enable HTTPS to protect management data go to <i>mxone_maintenance > webmanagement</i> After that, enable HTTPS in the proper Provisioning Manager subsystem.</p> <p>Voice Call Signaling, Voice Streaming, and CSTA traffic To enable encryption in the MX-ONE Service Node, go to <i>mxone_maintenance > certificate management</i>. After that, correctly configure the application that will use encryption; for example, SIP extensions, SIP trunks, or CSTA.</p>

Security Feature	Feature Details	Documentation
	<p>CSTA traffic MiVoice MX-ONE may be configured to encrypt all CSTA traffic with TLS 1.2.</p> <p>Call Privacy (restrict user identity) Only authenticated devices may connect to the MiVoice MX-ONE. MX-ONE offers options to restrict user identity as well as presentation of the phone number during a call.</p> <p>Other setups A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs) and firewalls.</p>	<p>Call Privacy (Restrict user identity) There are category parameters that are used to configure the following features in MX-ONE Service Node:</p> <ul style="list-style-type: none"> - Request A-number from the PSTN - Use Number Presentation Restriction - Number Presentation Restriction is Permitted per Call - Calling Line Identification Presentation Restriction Override - Never Display Number from PSTN <p>Configure the Common Service Profile or the category as needed.</p> <p>To restrict name presentation (user identity) in calls in the MiVoice MX-ONE Service Node Manager, go to the <i>Telephony > Extension > Common Service Profiles</i> and select/edit a CSP Number Presentation.</p>
<p>Access and Authorization</p>	<p>Access to the MiVoice MX-ONE system is restricted by a login password.</p> <p>All personal data processing is protected with role-based access and authorization controls. This includes personal data processing by data subjects, administrators, and technical support.</p> <p>All system data processing and all access to databases, files, and operating systems, are protected with role-based access and authorization controls.</p> <p>A customer can further limit access over the network using standard network security techniques such as VLANs, ACLs, and firewalls. In all cases, physical access to systems should be restricted by the customer.</p>	<p>Details can be found in the document called, MiVoice MX-ONE Security Description and Security Guidelines, Provisioning Manager Description, Service Node Manager Description and in the MiVoice MX-ONE Provisioning Manager Help files.</p> <p>Linux accounts are managed in the MX-ONE Service Node (<i>mxone_maintenance</i>).</p> <p>System administrators and technical support personnel can:</p> <ul style="list-style-type: none"> - Set/reset the password - Enable/disable the Login banner <p>Provisioning Manager administrators and end users can manage their account settings in the end user information task. They can:</p> <ul style="list-style-type: none"> - Set/reset the password - Set/reset PIN for extensions <p>In the MX-ONE Service Node, the following task is used to establish role-based access controls:</p> <ul style="list-style-type: none"> - <i>mxone_maintenance, user task</i> <p>In the MiVoice MX-ONE Provisioning Manager, the following task is used to establish role-based access controls:</p> <ul style="list-style-type: none"> - Security Profile task (when using the System Setup Admin account). This task is used to create, modify, and delete user security profiles that are required to access the following MiVoice MX-ONE management interfaces: - Provisioning Manager, Administration Portal - Service Node Manager

Security Feature	Feature Details	Documentation
Data Deletion	<p>The system provides the administrator with the ability to delete a user, or to delete a user and all phone services including MiCollab, CMG, and MiCollab Advanced Messaging services associated with that user.</p> <p>Deleting a User and Phone Services MiVoice MX-ONE allows the administrator to delete a user, the user and all of the user's associated phone services.</p> <p>Deleting Logs Certain types of logs cannot be deleted on a per user basis such as Call Detail Record logs. However, MiVoice MXONE provides the administrator with the ability to delete the entire contents from almost all logs, except the audit log in Service Node.</p> <p>Note: Logs that are transferred to external or third-party systems are not deleted by this step. For information on how to delete logs from these systems, refer to the vendor's documentation.</p>	<p>Details can be found in the document MiVoice MX-ONE Security Description and Security Guidelines, Provisioning Manager Description, Service Node Manager Description and in the MiVoice MX-ONE Provisioning Manager Help files.</p> <p>Deleting a user in MX-ONE Service Node In the MiVoice MX-ONE Service Node, command line interface (CLI) is used to delete user data; basically, first name, last name, extension number, function keys, and VDP (visitor desktop/ hot desking) data.</p> <p>Deleting a user in MX-ONE Provisioning Manager In Provisioning Manager, the extension task is used to delete a user or to delete a user and all associated phone services, including MiCollab, CMG, and MiCollab Advanced Messaging.</p> <p>Deleting Logs The System Administrator can delete system logs from the MiVoice MX-ONE using the root account or mxone_admin account. However, Linux audit logs cannot, for other security reasons, be deleted.</p>

Security Feature	Feature Details	Documentation
Audit of logs	<p>The system provides the administrator with the ability to delete a user, or to delete a user and all phone services including MiCollab, CMG, and MiCollab Advanced Messaging services associated with that user.</p> <p>Deleting a User and Phone Services MiVoice MX-ONE allows the administrator to delete a user, the user and all of the user's associated phone services.</p> <p>Deleting Logs Certain types of logs cannot be deleted on a per user basis such as Call Detail Record logs. However, MiVoice MXONE provides the administrator with the ability to delete the entire contents from almost all logs, except the audit log in Service Node.</p> <p>Note: Logs that are transferred to external or third-party systems are not deleted by this step. For information on how to delete logs from these systems, refer to the vendor's documentation.</p>	<p>Details can be found in the document MiVoice MX-ONE Security Description and Security Guidelines, Provisioning Manager Description, Service Node Manager Description and in the MiVoice MX-ONE Provisioning Manager Help files.</p> <p>Audit logs In the MX-ONE Service Node, the audit logs are enabled by default and these logs can be accessed only by the root account. In the MiVoice MX-ONE Provisioning Manager and Service Node Manager, the <i>Audit Trails Logs</i> task provides a historical record of changes made to the system from the MX-ONE Management tools.</p> <p>CIL logs In the MX-ONE Service Node, the Call Information Logging is configured via the command-line interface (CLI).</p>
End Customer Guidelines	<p>MiVoice MX-ONE Security Guidelines are available to assist with installation, upgrades, and maintenance.</p>	<p>The MiVoice MX-ONE Security Guidelines provide detailed recommendations on how the MiVoice MX-ONE security based features can be used within the customer GDPR compliance initiatives.</p> <p>The MiVoice MX-ONE Security Guidelines can be found in the MiVoice MX-ONE CPI documentation.</p>

4 QUERY/PRINTING OF PERSONAL DATA

4.1 QUERY/PRINTING OF END USER'S DATA

The query/printing of an End User's personal data in an MX-ONE system is done via MX-ONE Provisioning Manager or via MX-ONE O&M commands for the query/printing of extensions, names, PBX operators, voice mailboxes, diversion data, call list data, personal number data, etc.

See applicable Operational Directions and MX-ONE Provisioning Manager on-line help text. See also third party documentation if applicable (e.g. for Voice Mail systems).

4.2 QUERY/PRINTING OF CUSTOMER'S DATA

The query/printing of a Mitel customer's personal data for a customer, in an MX-ONE system, is done via MX-ONE Service Node Manager, MX-ONE Provisioning Manager, or via MX-ONE O&M commands for the query/printing of such customer data. Of course the related End User data for that customer can be printed as well.

See applicable Operational Directions and MX-ONE Provisioning Manager on-line help text.

4.3 QUERY/PRINTING OF SYSTEM ADMINISTRATORS OR TECHNICAL SUPPORT PERSONNEL

The query/printing of a system Administrator's or Technical support personnel's personal data in an MX-ONE system is done via the *mxone_maintenance* tool.

See the *mxone_maintenance* tool's on-line instructions.

5 REMOVAL OF PERSONAL DATA

5.1 REMOVAL OF END USER'S DATA

The removal of an End User's personal data in an MX-ONE system is done via MX-ONE Provisioning Manager or via MX-ONE O&M commands for the removal of extensions, names, PBX operators, voice mailboxes, diversion data, call list data, personal number data, etc.

See applicable Operational Directions and MX-ONE Provisioning Manager on-line help text. See also third party documentation if applicable (e.g. for Voice Mail systems).

5.2 REMOVAL OF CUSTOMER'S DATA

The removal of a Mitel customer's personal data for a customer, in an MX-ONE system, is done via MX-ONE Service Node Manager, MX-ONE Provisioning Manager, or via

MX-ONE O&M commands for the removal of such customer data. Of course the related End User data for that customer shall have been removed before.

See applicable Operational Directions and MX-ONE Provisioning Manager on-line help text.

5.3

REMOVAL OF SYSTEM ADMINISTRATORS OR TECHNICAL SUPPORT PERSONNEL

The removal of a system Administrator's or Technical support personnel's personal data in an MX-ONE system is done via the *mxone_maintenance* tool.

See the *mxone_maintenance* tool's on-line instructions.

6

PRODUCT SECURITY INFORMATION

6.1

MITEL PRODUCT SECURITY VULNERABILITY

The Product Security Policy discusses how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how the reporting of security vulnerabilities is performed.

Mitel's Product Security Policy is available at:

www.mitel.com/mitel-product-security-policy

6.2

MITEL PRODUCT SECURITY PUBLICATIONS

Mitel Product Security Publications are available at:

www.mitel.com/security-advisories