# MiVoice MX-ONE – Personal Data Protection and Privacy Controls

MiVoice MX-ONE Release 7.6

70/1551-ANF 901 43 Uen C 2023-12-21

December 2023

## NOTICE



### Trademarks

# Contents

# List of Tables

# 1 Introduction

## 1.1 Overview

This document is one in a series of product-specific documents that discuss the product security controls and features available on Mitel products.

This document will be of interest to Mitel MiVoice MX-ONE customers that are putting security processes and security controls in place to comply with data security regulations.

This document is intended to assist Mitel MiVoice MX-ONE customers with their data security regulations compliance initiatives by:

- Identifying the types of personal data that are processed by MiVoice MX-ONE
- Listing the MiVoice MX-ONE Security Features that customers may require to achieve compliance with data security regulations
- Providing a description of the MiVoice MX-ONE Security Features
- Providing information about where the MiVoice MX-ONE Security Features are documented

This document is not intended to be a comprehensive product-specific security guideline. For information about product security guidelines, product engineering guidelines or technical papers, refer to Mitel's Web Site.

## 1.2 Reference Documents

Following internal documents have been referenced within this document and can be found in MX-ONE O&M Library:

- *SECURITY DESCRIPTION, Doc ID: 19/1551-ASP 113 01.*
- *SECURITY GUIDELINES, Doc ID: 9/154 31-ASP 113 01.*
- *PROVISIONING MANAGER DESCRIPTION, Doc ID: 15/1551-ANF 901 15.*
- *SERVICE NODE MANAGER DESCRIPTION, Doc ID: 16/1551-ANF 901 15.*
- *CALL INFORMATION AND QOS LOGGING Operational Description, Doc ID: 20/154 31-ANF 901 14.*

Following Mitel public web sites has been referenced within this document:

- *Mitel's Product Security Policy (https://www.mitel.com/support/security-advisories/mitel-product-security-policy )*
- *Mitel Product Security Publications (https://www.mitel.com/support/security-advisories )*

Following external documents has been referenced within this document and can be found at these web sites:

- General Data Protection Regulation (GDPR) (https://eur-lex.europa.eu/eli/reg/2016/679/oj)
- EU Data Protection Directive 95/46/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046)

## 1.3 What is New in this Release

From MX-ONE 7.6 release, only HTTPs should be used to transmit data between Provisioning Manager and Mitel and/or Third party applications.

# 2 Personal Data Collected by MiVoice MX-ONE

MiVoice MX-ONE is made available as both on-premises and hosted offerings. Both offerings process only personal data that is required for the delivery of communication services including call control, billing services, and technical support services. There are no end-user opt-in consent mechanisms implemented in MiVoice MX-ONE.

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

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

- **End-users of MiVoice MX-ONE** – typically Mitel customer employees using Mitel phones.
- **Customers of Mitel customers** – for example, voicemail recordings might contain personal content of both parties in a call; end-user personal contact lists may contain personal data of their 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.

# 3 Personal Data Processed by MiVoice MX-ONE

MiVoice MX-ONE processes the following types of data to enable its communications features:

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

# 4 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 configured to be shared between clustered MiVoice MX-ONE systems, Mitel MiCollab, and management systems such as the Mitel Performance Analytics system.
- Voice quality logs, phone inventory, user name, and phone number may be configured to be read by Mitel Performance Analytics system and other customer-authorized systems.
- System logs, login and logout audit logs for the desktop tool, voice quality logs, customer databases, call detail records (also known as CDR or SMDR), and voice quality statistics may be configured to be transferred to Mitel product support or transferred to customer-authorized log collecting systems.
- Call Detail Records may be configured to be transferred to third-party call accounting systems.
- When MiVoice MX-ONE is part of a Hospitality solution (hotel/motel) the system may be configured to transfer the end-user's personal data between the MiVoice MX-ONE system and other customer-authorized Property Management Systems.

# 5 How the Security Features Relate to Data Security Regulations

MiVoice MX-ONE provides security-related features that allow customers to secure user data and telecommunications data and to prevent unauthorized access to the user's data.

Table 1 summaries the security features Mitel customers can use when implementing both customer policy and technical and organizational measures that the customer may require to achieve compliance with data security regulations.

**Table 1: MiVoice MX-ONE Security Features that customers may require to achieve Compliance with Data Security Regulations.**

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

| Security Feature | Relationship to Data Security Regulations | Where the Feature is Documented |
|---|---|---|
| | included in Call Detail Records can be masked or anonymized. | |
| **Communication Protection** | Encryption is highly recommended to be used for communications protection.<br><br>The following controls are available in MiVoice MX-ONE:<br>**Data protection**<br>MiVoice MX-ONE Service Node<br>• SSH version 2 is used to access MiVoice MX-ONE.<br>• HTTPS is used between MX-ONE and SIP phones to protect VDP (Visitor Desktop/hot-desking) data transmission.<br><br>MiVoice MX-ONE Service Node Manager and MiVoice Provisioning Manager<br>• HTTPS is used to protect data transmission in MiVoice MXONE Service Node Manager and MiVoice MX-ONE Provisioning Manager.<br>• HTTPS is used to protect data transmission between Provisioning Manager and Mitel applications as well as third-party applications.<br><br>**Voice Call Signaling**<br>Only authenticated devices may | Details can be found in the documents, *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.<br><br>**Data protection**<br>MiVoice MX-ONE Service Node<br>SSH version 2 is enabled by default in MiVoice MXONE. To enable HTTPS to protect VDP data, go to **mxone_maintenance > certificate management.**<br><br>**MiVoice MX-ONE Service Node Manager and MiVoice Provisioning Manager**<br>To enable HTTPS to protect management data, go to **mxone_maintenance > webmanagement.**<br>After that, enable HTTPS in the proper Provisioning Manager subsystem.<br><br>**Voice Call Signaling, Voice Streaming, and CSTA traffic**<br>To enable encryption in the MX-ONE Service Node, go to **mxone_maintenance > certificate management.**<br>After that, correctly configure the application that will use encryption; for example, SIP extensions, SIP trunks, or CSTA.<br><br>**Call Privacy (Restrict user identity)**<br>There are category parameters that are used to configure the following features in MX-ONE Service Node:<br>- Request A-number from the PSTN |

| Security Feature | Relationship to Data Security Regulations | Where the Feature is Documented |
|---|---|---|
| | connect to the MiVoice MX-ONE. Call signaling between the MiVoice MX-ONE and IP phones may be secured with TLS. Note that TLS 1.3 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.<br>**CSTA traffic**<br>MiVoice MX-ONE may be configured to encrypt all CSTA traffic with TLS 1.3.<br><br>**Call Privacy (restrict user identity)**<br>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.<br><br>**Other setups**<br>A customer can further limit access over the network using standard network security techniques such as VLANs, and firewalls. | - Use Number Presentation Restriction<br>- Number Presentation Restriction is Permitted per Call<br>- Calling Line Identification Presentation Restriction Override<br>- Never Display Number from PSTN<br>Configure the Common Service Profile or the category as needed.<br><br>To restrict name presentation (user identity) in calls in the MiVoice MX-ONE Service Node Manager, go to the **Telephony > Extension> Common Service Profiles** and select/edit a CSP Number Presentation. |
| **Access and Authorization** | Access to the MiVoice MX-ONE system is restricted by a login password.<br><br>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.<br><br>All system data processing and all | Details can be found in the documents, *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.<br>Linux accounts are managed in the MX-ONE Service Node (mxone_maintenance).<br><br>System administrators and technical support personnel can: |

| Security Feature | Relationship to Data Security Regulations | Where the Feature is Documented |
|---|---|---|
| | access to databases, files, and operating systems, are protected with role-based access and authorization controls.<br><br>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. | - Set/reset the password<br>- Enable/disable the Login banner<br><br>Provisioning Manager administrators and end-users can manage their account settings in the end-user information task. They can:<br>- Set/reset the password<br>- Set/reset PIN for extensions<br><br>In the MX-ONE Service Node, the following task is used to establish role-based access controls:<br>- mxone_maintenance, user task<br>In the MiVoice MX-ONE Provisioning Manager, the following task is used to establish role-based access controls:<br>- 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:<br>- Provisioning Manager, Administration Portal<br>- Service Node Manager |
| **Data Deletion** | 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.<br><br>**Deleting a User and Phone Services**<br>MiVoice MX-ONE allows the administrator to delete a user, the user and all of the user's associated phone services. | 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.<br><br>**Deleting a user in MX-ONE Service Node**<br>In the MiVoice MX-ONE Service Node, command line interface (CLI) is used to delete user data; basically, first name, last name, |

| Security Feature | Relationship to Data Security Regulations | Where the Feature is Documented |
|---|---|---|
| | **Deleting Logs**<br>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.<br><br>**Note:** Logs that are transferred to external or third-party systems are not deleted by this step. For information about how to delete logs from these systems, refer to the vendor's documentation. | extension number, function keys, and VDP (visitor desktop/ hot desking) data.<br><br>**Deleting a user in MX-ONE Provisioning Manager**<br>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.<br><br>**Deleting Logs**<br>The System Administrator can delete system logs from the MiVoice MX-ONE using the root account or mxone_admin account. However,<br>Linux audit logs cannot, for other security reasons, be deleted. |
| **Audit of logs** | 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.<br><br>**Deleting a User and Phone Services**<br>MiVoice MX-ONE allows the administrator to delete a user, the user and all of the user's associated phone services.<br><br>**Deleting Logs**<br>Certain types of logs cannot be deleted on a per user basis such as Call Detail Record logs. However, MiVoice MXONE | Details can be found in the document *Security Description* and *Security Guidelines, Provisioning Manager Description*, *Service Node Manager Description* and in the MiVoice MX-ONE Provisioning Manager Help files.<br><br>**Audit logs**<br>In the MX-ONE Service Node, the audit logs are enabled by default and these logs can be accessed only by the root account.<br>In the MiVoice MX-ONE Provisioning Manager and Service Node Manager, the Audit Trails Logs task provides a historical record of changes |

| Security Feature | Relationship to Data Security Regulations | Where the Feature is Documented |
|---|---|---|
| | provides the administrator with the ability to delete the entire contents from almost all logs, except the audit log in Service Node.<br><br>**Note:** Logs that are transferred to external or third-party systems are not deleted by this step.<br>For information about how to delete logs from these systems, refer to the vendor's documentation. | made to the system from the MX-ONE Management tools.<br><br>**CIL logs**<br>In the MX-ONE Service Node, the Call Information Logging is configured via the command-line interface (CLI). |
| **End Customer Guidelines** | MiVoice MX-ONE Security Guidelines are available to assist with installation, upgrades, and maintenance. | 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.<br>The *MiVoice MX-ONE Security Guidelines* can be found in the MiVoice MX-ONE CPI documentation. |
| **Communications Protection** | Encryption is highly recommended to be used for communications protection.<br><br>The following controls are available in MiVoice MX-ONE:<br><br>**Data protection**<br>MiVoice MX-ONE Service Node<br><br>• SSH version 2 is used to access MiVoice MX-ONE.<br><br>• HTTPS is used between MX-ONE and SIP phones to protect VDP (Visitor | Details can be found in the *MiVoice MXONE Security Description* and *Security Guidelines, Provisioning Manager Description and Service Node Manager Description,* and in the MiVoice MX-ONE Provisioning Manager Help files.<br><br>**Data protection**<br>MiVoice MX-ONE Service Node<br>SSH version 2 is enabled by default in MiVoice MXONE. To enable HTTPS to protect VDP data, go to **mxone_maintenance > certificate management** |

| Security Feature | Relationship to Data Security Regulations | Where the Feature is Documented |
|---|---|---|
| | Desktop/hot-desking) data transmission.<br><br>MiVoice MX-ONE Service Node Manager and MiVoice Provisioning Manager<br><br>• HTTPS is used to protect data transmission in MiVoice MXONE Service Node Manager and MiVoice MX-ONE Provisioning Manager.<br><br>• HTTPS is used to protect data transmission between Provisioning Manager and Mitel applications as well as third-party applications.<br>**Voice Call Signaling**<br><br>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 1.3 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.<br><br>**CSTA traffic**<br>MiVoice MX-ONE may be configured to encrypt all CSTA traffic with TLS 1.3.<br><br>**Call Privacy (restrict user** | **MiVoice MX-ONE Service Node Manager and MiVoice Provisioning Manager**<br>To enable HTTPS to protect management data, go to **mxone_maintenance > webmanagement**<br>After that, enable HTTPS in the proper Provisioning Manager subsystem.<br><br>**Voice Call Signaling, Voice Streaming, and CSTA traffic**<br>To enable encryption in the MX-ONE Service Node, go to **mxone_maintenance > certificate management.**<br>After that, correctly configure the application that will use encryption; for example, SIP extensions, SIP trunks, or CSTA.<br><br>**Call Privacy (Restrict user identity)**<br>There are category parameters that are used to configure the following features in MX-ONE Service Node:<br><br>- Request A-number from the PSTN<br>- Use Number Presentation Restriction<br>- Number Presentation Restriction is Permitted per Call<br>- Calling Line Identification Presentation Restriction Override<br>- Never Display Number from PSTN<br><br>Configure the Common Service Profile or the category as needed. |

| Security Feature | Relationship to Data Security Regulations | Where the Feature is Documented |
|---|---|---|
| | **identity)**<br>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.<br><br>**Other setups**<br>A customer can further limit access over the network using standard network security techniques such as VLANs, and firewalls.<br>**Remote Access Security**<br>The firewall can also be programmed to allow Virtual Private Network (VPN) tunnels with PPTP and IPSec pass-through and inbound connections with IP Port Forwarding.<br><br>**IMAP Server**<br>Transmission of user names and passwords between the MiVoice MX-ONE and an IMAP server may be secured with TLS.<br><br>A customer can further limit access over the network using standard network security techniques such as VLANs, and firewalls.<br><br>In all cases, physical access to systems should be restricted by the customer. | To restrict name presentation (user identity) in calls in the MiVoice MX-ONE Service Node Manager, go to the **Telephony > Extension> Common Service Profiles** and select/edit a CSP Number Presentation and fill in the following forms.<br><br>• *Port Forward Table Form* to configure the MiVoice MX-ONE's integral router.<br>• *IP Routing Form* to configure routing capabilities.<br>• *Firewall Control Form* to configure the integral Internet gateway.<br>*Embedded UM (Unified Messaging) Settings Form* to configure the IMAP Server connection. |
| **Access and Authorization** | **Role-Based Access**<br>MiVoice MX-ONE supports up to 5 System Administration Tool users, 5 Group | Details can be found in the *MiVoice MX-ONE Security Guidelines* and in the *MiVoice MX-ONE System Administration Tool* Help files. |

| Security Feature | Relationship to Data Security Regulations | Where the Feature is Documented |
|---|---|---|
| | Administration Tool users, and 10 Desktop Tool users at a time.<br><br>Only the root administrator can program access to the System Administration Tool and use the Import and Export functions in this form. Other administrators can manage only user profiles that do not have System Administrator Tool access rights.<br><br>A customer can further limit access over the network using standard network security techniques such as VLANs and firewalls.<br><br>In all cases, physical access to systems should be restricted by the customer. | In the MiVoice MX-ONE System Administration Tool, the following forms are used to establish role-based access controls:<br><br>• *User Authorization Profiles Form*. This form is to create, modify, and delete user profiles that are required to access the following MiVoice MX-ONE management interfaces:<br>  ○ System Administration Tool<br>  ○ Group Administration Tool<br>  ○ Desktop Tool<br><br>• The *Admin Policies Form.* This form is used to add, modify, and delete policies that are used to establish permissions for various user profiles. These permission policies dictate which System Administration Tool forms a user is allowed to access or modify. |
| **Data Deletion** | **Deleting a User's Embedded Voice Mail Box**<br>The MiVoice MX-ONE allows the administrator to delete a user's embedded voice mail box.<br><br>**Deleting a User from the Telephone Directory**<br>The MiVoice MX-ONE allows the administrator to delete a | Details can be found in the, *MiVoice MX-ONE Security Guidelines* and in the *MiVoice MX-ONE System Administration* Help files.<br><br>In the MiVoice MX-ONE System Administration Tool, the following forms and procedures are used to erase a personal data: |

| Security Feature | Relationship to Data Security Regulations | Where the Feature is Documented |
|---|---|---|
| | user from the telephone directory.<br><br>**Deleting Logs**<br>Certain types of logs cannot be deleted on a per user basis such as Call Detail Record logs, CESID logs, and HotDesking Logs. However, MiVoice MX-ONE provides the administrator with the ability to delete the entire contents from all logs.<br><br>**Note**: Logs that are transferred to external or third-party systems are not deleted by this method.<br>For information about how to delete logs from these systems, refer to the vendor's documentation.<br><br>**Deleting Voicemail Messages**<br>The system provides the administrator with the ability to erase a voicemail message that was left in the end-user's voicemail box by a customer.<br><br>The system administrator can, once authenticated, log in to the shell and locate and delete the file that contains the voicemail message based on the user's extension number and the time that the recording was left in the user's voicemail box. | • The *User and Services Configuration Form.* This form is used to delete a user or to delete a user and all associated phone services.<br><br>• The *User and Services Configuration Form* is also used to delete a user's embedded voice mailbox. Alternately, the administrator's mailbox can be used to delete a user's mailbox.<br><br>• The *Telephone Directory Form.* This form is used to delete a user from the telephone directory.<br><br>• MiVoice MX-ONE supports several logs. For a complete list of logs and the forms that are used to manage the logs, refer to the *MiVoice MX-ONE System Administration Tool Help* files.<br><br>• The System Administrator can delete Property Management System occupancy logs from the MiVoice MX-ONE, for details refer to the *MiVoice MX-ONE Security Guidelines,* in the section *Audits and Logs.*<br>In the *MiVoice MX-ONE System Administration Tool* Help files, look under *Property management System (PMS)* for additional information about PMS logs. |

| Security Feature | Relationship to Data Security Regulations | Where the Feature is Documented |
|---|---|---|
| **Audit** | Audit trails are supported to maintain records of data processing activities.<br><br>**Audit Trail Logs**<br>Audit Trail Logs provide a historical record of changes made to the system from the System Administration Tool and various other user interfaces and applications. It does this by recording certain actions (such as who logged in and when) and storing this information in a log. Use the logs to help with troubleshooting when problems arise and to determine who in a multi-administrator system is responsible for a particular change.<br><br>**SMDR Logs**<br>Station Message Detail Recording (SMDR) is the Mitel name for Call Detail Recording (CDR) logs on the MiVoice MX-ONE platform. The system allows the administrator to configure the details that will be recorded for internal calls, external calls and details related to location-based accounting. | Details can be found in the document *MiVoice MX-ONE Security Guidelines* and in the *MiVoice MX-ONE System Administration Tool* Help files.<br><br>In the *MiVoice MX-ONE System Administration Tool,* go to the*:*<br><br>• *Audit Trails Logs Form.* This form provides a historical record of changes made to the system from the System Administration Tool and various other user interfaces and applications.<br>*SMDR Options Form* (Station Management Detail Recording). This form is used to configure SMDR options. |
| **End Customer Guidelines** | MiVoice MX-ONE Security Guidelines are available to assist with installation, upgrades, and maintenance. | 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.<br><br>The *MiVoice MX-ONE Security Guidelines* are available at Mitel online. |

# 6 Query/Printing of Personal Data

## 6.1 Query/Printing of End-User's Data

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, and so on. See applicable Operational Directions and MX-ONE Provisioning Manager online help text. See also third-party documentation if applicable (for example, for Voice Mail systems).

## 6.2 Query/Printing of Customer's Data

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. The related end-user data for that customer can also be printed. See applicable Operational Directions and MX-ONE Provisioning Manager on-line help text.

## 6.3 Query/Printing of System Administrators or Technical Support Personnel

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.

# 7 Removal of Personal Data

## 7.1 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, and so on.

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

## 7.2 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 must have been removed before. See applicable Operational Directions and MX-ONE Provisioning Manager on-line help text.

## 7.3 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.

# 8 Data Security Regulations

This section provides an overview of the security regulations that MiVoice MX-ONE customers may need to be compliant with.

## 8.1 The European Union General Data Protection Regulation (GDPR)

The European Union (EU) General Data Protection Regulation (GDPR) effective on 25 May 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 the EU must ensure that they comply with GDPR. Under GDPR, 'processes personal information' means any operation performed on personal data, such as collecting, recording, erasing, usage, transmitting, and disseminating.

### 8.1.1 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 organizational measures are used to appropriately safeguard such data. Table 1 explains what personal data is processed by Mitel’s MiVoice MX-ONE and highlights available security features to safeguard such data.

# 9 Product Security Information

## 9.1 Mitel Product Security Vulnerabilities

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:
https://www.mitel.com/support/security-advisories/mitel-product-security-policy

## 9.2 Mitel Product Security Advisories

Mitel Product Security Advisories are available at:
https://www.mitel.com/support/security-advisories

## 9.3 Mitel Security Documentation

Mitel security documentation includes product-specific; Security Guidelines, and Important Information for Customer GDPR Compliance Initiatives and Data Protection and Privacy Controls. Mitel also has Technical Papers and White papers that discuss network security and data centre security.

Mitel Product Security Documentation is available at:
https://www.mitel.com/en-ca/document-center

# 10 Disclaimer

THIS SOLUTIONS ENGINEERING DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY. IN NO EVENT WILL MITEL NETWORKS CORPORATION OR ITS AFFILIATES HAVE ANY LIABILITY WHATSOEVER ARISING FROM IN CONNECTION WITH THIS DOCUMENT. You acknowledge and agree that you are solely responsible to comply with any and all laws and regulations in association with your use of MiVoice MX-ONE and/or other Mitel products and solutions including without limitation, laws and regulations related to call recording and data privacy. The information contained in this document is not, and should not be construed as, legal advice. Should further analysis or explanation of the subject matter be required, please contact an attorney.