MiVoice 5000 – Personal Data Protection and Privacy Controls

MiVoice 5000 Release 6.5, 7.0 and 7.1

MiVoice 5000 Manager Release 3.5, 7.0 and 7.1

Version 2.0

July 2020

NOTICE

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 particular document will be of interest to Mitel MiVoice 5000 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 5000 customers with their data security regulations compliance initiatives by:

- Identifying the types of personal data that are processed by MiVoice 5000
- Listing the MiVoice 5000 Security Features that customers may require to achieve compliance with security regulations
- Providing a description of the MiVoice 5000 Security Features
- Providing information on where the MiVoice 5000 Security Features are documented

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

1.2 What is New in this Release

- The document is renamed from “MiVoice 5000 - Important Product Information for Customer GDPR Compliance Initiatives” to “MiVoice 5000 – Personal Data Protection and Privacy Controls” and uses a modified template.
- This release takes into account changes made in MiVoice 5000 releases 7.0 and 7.1, and in corresponding releases of MiVoice 5000 Manager: SRTP encryption over SIP trunks, implementation of LDAPS, SSO for users and administrators, log of all administrator’s operations.
-

2 Personal Data Collected by MiVoice 5000

MiVoice 5000 is made available as both on-premises and hosted offerings. Both offerings collect 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 5000.

During the course of installation, provisioning, operation and maintenance, the MiVoice 5000 **collects** data related to several types of users, including:

- End users of MiVoice 5000 – typically Mitel customer employees using Mitel phones.

- Customers of Mitel customers – for example, voice mail recordings may contain personal content of both parties in the call; the end user's personal contact lists may 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.

Table 1: Personal Data Collected by MiVoice 5000

Types of Users	Personal Information Collected	Activity Information Collected
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 • Voicemail PIN
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.

3 Personal Data Processed by MiVoice 5000

The MiVoice 5000 **processes** the following types of data:

- **Provisioning Data:**
  - The end user's name, end user's title (for example, Mr. Mrs. and Ms.) business extension phone number, mobile phone number, location, function, department, and login and email addresses; in addition to 10 configurable attributes (under client definition).
- **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 and personal contact lists.

Personal data processed by the MiVoice 5000 is required for the delivery of communication services, technical support services or other customer business interests. For example, call billing and reporting services.

There are no end user opt-in consent mechanisms implemented in the application.

4 Personal Data Transferred by MiVoice 5000

The types of **personal data transferred** among the MiVoice 5000 and various applications and services will depend on the specific use requirements of those applications or services, 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 MiVoice 5000 components and management systems (for example, MiVoice 5000 Manager).
- Maintenance, administration, and technical support activity records, such as system and content backups, logs, and audit trails.
- User activity records such as call history and call detail records.
- Personal content such as contact information (name, number, email address, and associated data) and voice mail.
- Voice quality logs, phone inventory, username, and phone number may be configured to be read by 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 customer authorized third-party call accounting systems

- Call Detail Records may be configured to be transferred to customer authorized third-party Property Management Systems (PMS).
- Backups of the MiVoice 5000 containing collected personal data, may be retrieved by an authorized system administrator
-

5 How the Security Features Relate to Data Security Regulations

MiVoice 5000 provides security-related features which allow customers to secure user data and telecommunications data and to prevent unauthorized access to the user's data.

Table 2 summaries the security features Mitel customers can use when implementing both customer policy and technical and organizational measures which the customer may require to achieve compliance with data security regulations.

Table 2: MiVoice 5000 Security Features that Customers May Require to achieve Compliance with Data Security Regulations.

Security Feature	Feature Details	Where the Feature is Documented
System and Data Protection	Access to personal data is limited with administrative controls on accounts for both personnel and Application Programming Interfaces. Access to the system is limited by allowing only authorized access that is authenticated using username/password login combinations that use strong password mechanisms. Communications to the system are performed over authenticated, encrypted communications channels using HTTPS (TLS 1.2). A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs) and firewalls. In all cases, physical access to systems should be restricted by the customer.	MiVoice 5000 Operating Manual, MiVoice 5000 Manager Operating Manual. MiVoice 5000 Product Guide – Chapter 14 – *Security.*
Communications Protection	Most personal data transmissions use secure channels. Channels that are not secured can be disabled by the administrator.	MiVoice 5000 Operating Manual, MiVoice 5000 Manager Operating Manual.

	Call Privacy Caller privacy is controlled with a few option settings, like hiding the caller ID or managing a red list of directory cards that are not displayed. **Voice Streaming** MiVoice 5000 may be configured to encrypt all IP voice call media streams with standards based SRTP including AES128 encryption, except over SIP trunks in releases prior to 7.1. Legacy technologies such as analog and digital trunks and devices do not support encryption. **Voice Call Signaling** Only authenticated users may connect to the MiVoice 5000 application. Call signaling between the MiVoice 5000 and IP phones may be secured with TLS 1.2. Legacy analog and digital trunks and devices do not support encryption. For system integrity and reliability, all provisioning interfaces use secure channels (TLS 1.2). Exchanges with external directories use the secure protocol LDAPS from release 7.0 onwards. A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs) and firewalls. In all cases, physical access to systems should be restricted by the customer.	MiVoice 5000 Product Guide – Chapter 14, *Security.*
Identity and Authentication	Access to the system is limited by allowing only authorized access that is authenticated using username/password login combinations that use strong password mechanisms. Access is restricted with five role-based access levels that require a username and login password. Transmission of this information is secured with TLS 1.2. Users have access to a user portal for simple self-administration, and a Single Sign-On mechanism with Microsoft Active Directory is available.	MiVoice 5000 Operating Manual, MiVoice 5000 Manager Operating Manual. MiVoice 5000 Product Guide – Chapter 14 – *Security.*

	A Single Sign-On mechanism, with either Microsoft Active Directory or a Kerberos server, is also available for administrators of the MiVoice 5000 Manager from release 7.0 onwards. On MiVoice 5000 Server and MiVoice 5000 Manager, the Linux 'root user' has full access to the operating system and is secured with TLS 1.2.	
Access and Authorization	**Role-Based Access** All personal data processing is protected with role-based access and authorization controls. This includes personal data processing by data subjects, administrators, technical support, and machine APIs. All system data processing and all access to databases, files, and operating systems, are protected with role-based access and authorization controls. Access to the product is restricted with five role-based access levels that require a username and login password. Transmission of this information is secured with TLS 1.2. On MiVoice 5000 Server and MiVoice 5000 Manager, the Linux 'root user' has full 'console' access to the operating system and the communications path is secured with TLS 1.2. 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.	MiVoice 5000 Operating Manual, MiVoice 5000 Manager Operating Manual. MiVoice 5000 Product Guide – Chapter 14 – *Security.*
Data Deletion	The system provides an authorized end user or administrator with the ability to erase the end user's personal data. End users can erase some of their usage and customizable data (such as personal call logs, voice mail, personal contacts, and programmable keys) by using the phones or the User Portal. The system provides the administrator with the ability to erase the end customer's personal data that may have been left in an end user's voicemail box.	MiVoice 5000 Operating Manual, MiVoice 5000 Manager Operating Manual. MiVoice 5000 Product Guide – Chapter 14 – *Security.*

	Personal information stored in system logs, call data records, backups cannot be erased from an individual user base. The end user's voicemail records may be deleted by the end user. Voicemail records are also deleted when the end user is deleted. If user information in backup files is not removed when deleting a user, then administrators should purge old backups and make a new backup without the end user's personal data. Any recordings made of the user's calls must be deleted from the call recording application.	
Audit	Audit trails are supported to maintain records of data processing activities. Call Data Records are stored in the MiVoice 5000 system and can be accessed only by the administrator or by trusted applications. The last four digits of external call numbers can be masked (with '*') automatically from CDR data by the system if required. All connections and operations made by administrators in the MiVoice 5000 Manager are logged. All connections and operations made by administrators in the MiVoice 5000 are logged from release 7.0 onwards. Most of the system logs can be erased by the administrator whereas some cannot be, unless the system is re-installed. Note that logs shared with external systems (Syslog interface) cannot be erased remotely.	MiVoice 5000 Operating Manual, MiVoice 5000 Manager Operating Manual. MiVoice 5000 Product Guide – Chapter 14 – *Security.*
End Customer Guidelines	The MiVoice 5000 *Product Documentation* is available to assist with installation, upgrades and maintenance.	MiVoice 5000 Operating Manual, MiVoice 5000 Manager Operating Manual. MiVoice 5000 Product Guide – Chapter 14 – *Security.* MiVoice 5300 IP/Digital Phones Mitel 6700 and 6800 SIP Phones, MiVoice 6900 IP Phones – Installation Manuals.

6 Data Security Regulations

This section provides an overview of the security regulations that MiVoice 5000 customers may need to be compliant with.

6.1 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.

6.1.1 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. Section 3 of this document explains what personal data is processed by Mitel's MiVoice 5000 and Section 5 highlights available security features to safeguard such data.

7 Product Security Information

7.1 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

7.2 Mitel Product Security Publications

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

8 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 5000 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.