MiVoice Office Application Suite – Important Product Information for Customer GDPR Compliance Initiatives

MiVoice Office Application Suite Release 5.1 SP1

Version 1

July 2018

Mitel

NOTICE

Trademarks

Contents

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 MiVoice Office Application Suite customers that are putting security processes and security controls in place to comply with GDPR.

This document is intended to assist Mitel MiVoice Office Application Suite customers with their GDPR compliance initiatives by:

- Identifying the types of personal data that are processed by MiVoice Office Application Suite
- Listing the MiVoice Office Application Suite Security Features that customers may require to achieve GDPR compliance
- Providing a description of the MiVoice Office Application Suite Security Features
- Providing information on where the MiVoice Office Application Suite 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 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, 'processing personal data' means any operation performed on personal data, such as collecting, recording, erasing, usage, transmitting, and disseminating.

1.2.1 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 adequately safeguard such data. This document explains what personal data is collected, processed and transferred by Mitel's MiVoice Office Application Suite and highlights available security features to safeguard such data.

2 Personal Data Collected by MiVoice Office Application Suite

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

- End users of MiVoice Office Application Suite – typically Mitel customer employees using Mitel phones and collaboration tools.
- Customers of Mitel customers – for example, call recordings 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.
- There are no end user opt-in consent mechanisms implemented in the MiVoice Office Application Suite.

3 Personal Data Processed by MiVoice Office Application Suite

The MiVoice Office Application Suite processes the following types of data:

- **Provisioning Data:**
  - The end user's first name, last name, business extension phone number, mobile phone number, 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:**
  - Call recordings, personal contact lists, and chat communications.
  - Personal data processed by the MiVoice Office Application Suite is required for the delivery of communication services, technical support services, or other customer business interests—for example, call billing and reporting services.

4 Personal Data Transferred by MiVoice Office Application Suite

Depending on the customer's configuration, and specific use requirements, the personal data collected may be processed and/or transferred between the MiVoice Office Application Suite and

other related systems and applications such as Customer Relationship Management (CRM) 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 MiVoice Office 250 and MiVoice Office Application Suite.
- Maintenance, administration, and technical support activity records, such as system and content backups, logs, and audit trails.
- System logs, audit logs, customer databases and call detail records (also known as CDR or SMDR) may be configured to be transferred to Mitel product support or transferred to customer authorized log collecting systems.
- User activity records such as call history, call detail records, and contact center statistics.
- Personal content such as contacts (name, number, email address, associated data), and call recordings.
- Personal data such as the user's first name, last name, office phone number, and mobile phone may be configured to be shared between MiVoice Office Application Suite and a customer authorized CRM system.

5 How MiVoice Office Application Suite Security Features Relate to GDPR

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

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

Table 1: MiVoice Office Application Suite Security Features that Customers May Require to Achieve GDPR Compliance

Security Feature	Feature Details	Where the Feature is Documented
System and Data Protection	Access to personal data is limited with the following controls. The MiVoice Office Application Suite system is pre-configured with two default user accounts for engineer access and supervisor access. The engineer account has full access to the website to configure the system and create users. The	Mitel Communication Service – Technical Manual User Management and Security (see 2.5) Best Security Practice (see 2.7) Users and Business Units (see 9.2.7)

	supervisor account has limited rights, but allows performing basic management functions. Access to the system is limited by allowing only authorised access that is authenticated using user name/password login combinations that use strong password mechanisms. Failed logins are logged and restricted to a configurable maximum number of login attempts. MiVoice Office Application Suite can be configured to work in combination with Microsoft® Active Directory (AD) to leverage the AD security access rules for user accounts; for example, authenticated using user name / password login combinations that use strong password mechanisms, account enable / disable, login attempts, and so on. Mitel recommends using Microsoft Active Directory Authentication for added security measures. Doing so means that access to the system is restricted to authorised accounts and that administration access and activities related to passwords are audited and failed login attempts are logged. The website is hosted by IIS server, which is part of the host operating system. To enhance security, it is recommended to switch access to the MiVoice Office Application Suite website from HTTP (default) to HTTPS so that communications to the system are performed over authenticated, encrypted communications channels using HTTPS (TLS). User Roles are used to enforce security and access permissions for all Users that interact with the MCS and are used whenever a user logs into the website in order to determine what rights they have within the user interface. Any user accounts created on the system use the 'principle of least privilege', using the Roles and Profiles provided to limit user access to only the features they require. A customer can further limit access over the network using standard network security techniques such as VLANs, access control lists (ACLs), and firewalls.	http://edocs.mitel.com

	In all cases, physical access to systems should be restricted by the customer.	
Communications Protection	Web access and inter-service communications can be secured through the use of HTTPS / TLS connections. Communication between Phone Manager and the server's webservice is secured through the use of TLS by default. Communication between Phone Manager and the customer's CRM provider vary depending upon the CRM API capabilities. The Phone Manager softphone RTP stream is not encrypted. Call recordings are stored in an encrypted format using AES-256 block cypher and are digitally signed. The Open Application Interface (OAI) connection between the MiVoice Office 250 and the MiVoice Office Application Suite is not encrypted. To further protect communications a customer can limit access over the network using standard network security techniques such as VLANs, access control lists, and firewalls. In all cases, physical access to systems should be restricted by the customer. As a Windows Operating System application, security updates for the OS are provided by Microsoft.	Mitel Communication Service – Technical Manual Best Security Practice (see 2.7) Enabling HTTPS (see 11.6)
Identity and Authentication	Access to the MiVoice Office Application Suite is restricted by a strong login password. Failed login attempts are logged, after five failed login attempts (default setting), access to the account will be locked for an administrator-defined lockout period. Access to the product is restricted with Roles and Profiles, thereby limiting the access to just the features required.	Mitel Communication Service – Technical Manual User Management and Security (see 2.5) Users and Business Units (see 9.2.7)

	Access to configuration areas of the application is restricted to administrator accounts. By default, user accounts are created with access limited to their own data.	
Access and Authorization	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 MiVoice Office Application APIs. All system data processing and all access to databases, files, and operating systems, are protected with role-based access and authorization controls (Windows/Active Directory User Accounts). The system has 9 default security roles and these can be extended to over 40 individual additional granular access items. See the MiVoice Office Application Suite online manual for details of each specific item and the default role they apply to.	Mitel Communication Service – Technical Manual User Management and Security (see 2.5) Users and Business Units (see 9.2.7)
Data Deletion	The system provides an end user or an administrator the ability to erase the end user's personal data within contact directories and data that may have been tagged to call logs. Call recording data may be manually deleted from the host server's storage by an authorized user who has explicitly been granted permission.	Mitel Communication Service – Technical Manual Managing Directories (see 9.1.1.1)
Audit	Audit trails of user activity are supported to maintain records of data processing activities. Audit trails are stored within the system database and are accessible only by users with the required permissions. Logs can be enabled for tracking of faults.	Mitel Communication Service – Technical Manual Diagnostic Logging (see 9.3.1.2)
End Customer Guidelines	MiVoice Office Application Suite documentation is available to assist with installation, upgrades, security, and maintenance.	Mitel Communication Service – Technical Manual Best Security Practice (see 2.7)

6 Product Security Information

6.1 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:
www.mitel.com/support/security-advisories/mitel-product-security-policy

6.2 Mitel Product Security Publications

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

7 Disclaimer