MiContact Center Office – Important Product Information for Customer GDPR Compliance Initiatives

MiContact Center Office Release 6.2 SP1

Version 1

August 2018

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). 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.

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 MiContact Center Office customers that are putting security processes and security controls in place to comply with GDPR.

This document is intended to assist Mitel MiContact Center Office customers with their GDPR compliance initiatives by:

- Identifying the types of personal data that are processed by MiContact Center Office
- Listing the MiContact Center Office Security Features that customers may require to achieve GDPR compliance
- Providing a description of the MiContact Center Office Security Features
- Providing information on where the MiContact Center Office 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 MiContact Center Office and highlights available security features to safeguard such data.

2 Personal Data Collected by MiContact Center Office

MiContact Center Office only processes personal data that is required for the delivery of communication services, technical support services or other customer business interests. For example, call billing, and reporting services.

There is no end user opt-in consent mechanisms implemented in MiContact Center Office.

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

- End users of MiContact Center Office – 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 contain records of the activities of system administrators and technical support personnel.

3 Personal Data Processed by MiContact Center Office

MiContact Center Office 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 and logs.
- **End User Activity Records:**
  - Call history and call detail records.
- **End User Personal Content:**
  - Personal contact lists, and 'Media Blending', which can be configured to enable users to send SMS, Fax, and emails.

4 Personal Data Transferred by MiContact Center Office

Depending on the customer's configuration, and specific use requirements, the personal data collected may be processed and/or transferred between MiContact Center Office and other related systems and applications (such as, Customer Relationship Management (CRM) systems). For example:

- Provisioning data, such as name, phone number, location, and IP and MAC addresses.
- Maintenance, administration, and technical support activity records, such as system and content backups, logs.
- 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, and associated data), chat history.
- 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.
- "Media Blending" can be configured, which allows users to send SMS, Fax, and emails.

5 How MiContact Center Office Security Features Relate to GDPR

MiContact Center Office 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: MiContact Center Office Security Features that Customers May Require to Achieve GDPR Compliance

Security Feature	Feature Details	Where the Feature is Documented
System and Data Protection	System and data protection is achieved through secure installation and configuration of the Windows Operating System, along with role-based password protected access through the MiContact Center Office administration interface. Additional security techniques can be used, such as encrypting the hard drive with Bitlocker, applying	Refer to Windows OS Help. Online documentation is at: https://docs.microsoft.com/en-us/windows/

	regular Microsoft Windows Updates, and using anti-virus software. Access to the system is limited by allowing only authorised access that is authenticated using the Microsoft Windows name/password login combinations that use strong password mechanisms. 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.	Information about setting login thresholds can be found at: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold
Communications Protection	MiContact Center Office is an application that is installed on a Microsoft Windows operating system. The Windows computer can be configured to work in combination with Microsoft® Active Directory (AD) to leverage Active Directory user accounts for access to the local machine, making use of the AD security rules and existing domain policies, such as authentication using username/ password login combinations that use strong password mechanisms, account enable/disable policies, restriction on 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 limited by allowing only authorised access and that administration access and activities related to passwords are audited and failed login attempts are logged. SMTP communications between the email server and MiContact Center Office may be secured with TLS. Communications protection is achieved through maintaining a secure infrastructure, along with a robust monitoring and notification system.	See Technician Handbook > Overview > Security Guidelines. See Technician Handbook > Specifications > Firewall and Router Ports.

	A customer can further limit access over the network using standard network security techniques such as VLANs and firewalls. In all cases, physical access to systems should be restricted by the customer.	
Identity and Authentication	MiContact Center Office is an application that is installed on a Microsoft Windows operating system. The Windows computer can be configured to work in combination with Microsoft® Active Directory (AD) to leverage Active Directory user accounts for access to the local machine, making use of the AD security rules and existing domain policies, such as authentication using username/ password login combinations that use strong password mechanisms, account enable/disable policies, restriction on 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 limited by allowing only authorised access and that administration access and activities related to passwords are audited and failed login attempts are logged. To access the MiContact Center administration interface, you must go through the local Microsoft Windows user authentication process. Access to the MiContact Center Office administration interface is further protected by the application with a configurable username/password combination.	Refer to Windows OS Help. Online documentation is at: https://docs.microsoft.com/en-us/windows/
Access and Authorization	All system data processing and all access to databases, files, and operating systems, are protected with Windows password authorization controls. MiCC Office provides three levels of access: **Administrator**: This is the highest level of password. Anyone who has this password can configure the Server, and has full access to all	Refer to Windows OS Help. Online documentation is at: https://docs.microsoft.com/en-us/windows/

	features in all modules. **Supervisor**: This password level allows restricted access to software features. For example, it does not allow controlling what device the Client is associated with. **User**: At this password level, access to software features is restricted further. For example, it does not allow creating actions. A customer can further limit access over the network using standard network security techniques such as VLANs and firewalls. In all cases, physical access to systems should be restricted by the customer.	
Data Deletion	The system provides the administrator with the ability to delete a user, or to delete a user and all services associated with that user. The Data Manager is used to configure the system. It allows the administrator to add, change, or delete specific extensions, and agents. Certain types of logs cannot be deleted on a per user basis. However, MiContact Center Office provides the administrator the ability to delete the entire contents of logs. However, doing this may affect the capabilities of the application because certain logs are used for creation of contact center reports and they may no longer be available or be accurate if this data is deleted.	See Technician Handbook > Applications > Server User Interface Components > Data Manager. See also Data Manager Online Help.
Audit	MiContact Center Office supports several application logs including Call Viewer, RealViewer, Reporter, Reporter Real-Time, and Backup Utility logs, but these have no audit trails.	See Data Manager Online Help > Server Logging and Data Manager Online Help > Diagnostics.
End Customer Guidelines	MiContact Center Office documentation is available to assist with installation, security, upgrades, and maintenance.	See MiContact Center Office, General Information Guide > Introduction > About the MiCC Office Documentation.

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/security/mitel-product-security-policy

6.2 Mitel Product Security Publications

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

7 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 MiContact Center Office 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.