InAttend and CMG – Personal Data Protection and Privacy Controls

InAttend Release 2.6 SP2 and CMG Release 8.5 SP2

Version 1

January 2021

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

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 InAttend and CMG customers that are putting security processes and security controls in place to comply with GDPR.

This document is intended to assist Mitel InAttend and CMG customers with their GDPR compliance initiatives by:

- Identifying the types of personal data that are processed by InAttend and CMG
- Listing the InAttend and CMG Security Features that customers may require to achieve GDPR compliance
- Providing a description of the InAttend and CMG Security Features
- Providing information on where the InAttend and CMG 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.

2   Personal Data Collected by InAttend and CMG

During installation, provisioning, operation, and maintenance, InAttend and CMG collects data related to several types of users, including:

- End users of InAttend and CMG – 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.

3   Personal Data Processed by InAttend and CMG

InAttend and CMG processes the following types of data:

- **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:**

- o   System and content backups, logs, and audit trails.
- **User Activity Records:**
  - o   Call history and call detail records.
- **User Personal Content:**
  - o   Voice-mail, call recordings, and personal contact lists.

Personal data processed by InAttend and CMG is required for the delivery of communication services, technical support services, or other customer business interests. Data is stored in the CMG Directory SQL DB and administered via the Directory Manager (DM) Web application. This data is used when calls are made to the attendant and the caller is identified. Only the administrator has ability to change or delete this data upon request.

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

4   Personal Data Transferred by InAttend and CMG

The types of personal data transferred among InAttend and CMG and various applications and services will depend on the customer's specific configuration and use requirements of those applications or services. For example:

- User provisioning data such as user's name, business extension phone numbers, business mobile phone number, location, department, user photo, email address, organisation, and title may be configured to be shared between clustered InAttend, CMG, and management systems such as the Mitel Performance Analytics system.
- Maintenance, administration, and technical support activity records, such as system and content backups, logs, and audit trails.
- System logs such as login and logout audit logs for the desktop tools, customer databases, and call detail records 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.
- Quality Manager might access historical call details for purposes of post activity call statistics to measure call volume and traffic patterns for the inbound attendant traffic. However, only telephone numbers with timestamps for call duration are stored. Data stored for statistics purposes can be deleted automatically at predefined periods based on configuration by an authorized administrator.

5   How the Security Features Relate to Data Security Regulations

InAttend and CMG provide 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 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: InAttend and CMG 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, and Identity and Authentication	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). The call recordings of the calls handled by the attendant are stored in the media server in encrypted format and each call can be identified, retrieved, and if required, deleted by an authorized system administrator using standard Windows file manager processes. 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. Access to InAttend and CMG is restricted by a login password. The system validates certificates on all TLS connections. Access to the system is limited by allowing only authorised access	• Details on securing log locations, CDRs, and recordings are available in the *InAttend Install and Configuration Guide > Configuring EFS* section. • Details on data backup and restoration, configuring database backups/restores, scheduled software downloads, and file transfers are available in the *InAttend Administration and Maintenance Guide > Backup and Restore* section. • Details on verification of administrators and InAttend attendant's authorization to use certain services are in the InAttend Installation and Configuration Guide > Configuring the Authentication and Authorization (AnA) W*eb Service* section. • Details on Password Management are in the *CMG CM Online Help > Security Parameters* section and in the *InAttend Installation and Configuration Guide > Configuring InAttend Users* section.

	that is authenticated using username/password login combinations that use strong password mechanisms.	
Communications Protection	Most personal data transmissions use secure channels. Channels that are not secured can be disabled by the administrator. **Voice Streaming** May be configured to encrypt all IP voice call media streams with SRT using AES 128 encryption. **Note**: Not all SIP trunks service providers and third-party SIP devices support encryption. In cases where permitted, the communications will negotiate to no encryption. **Voice Call Signaling** Call signaling between InAttend and IP phones may be secured with TLS. **Call Privacy** All IP communications are encrypted by Mitel. Caller privacy is controlled by a few optional settings.	• Details on security control of different call managers supported by InAttend and CMG are in the *InAttend Installation and configuration Guide > Call Manager Configuration* section. • Details on certifications are in the *InAttend Installation and configuration Guide > TLS Certificates Installation* section. • Details on Network Telephony System are in the *InAttend Installation and configuration Guide > Configure the NeTS* section. • Details on SRTP are in the *InAttend Installation and configuration Guide > Configuring the Media Server* section. • Details on administration of the InAttend server using the BluStar Server Administration tool (WebAdmin) are in the *InAttend Administration and Maintenance Guide > Administration* section. • Details on HTTPS are in the *CMG Configuration Guide > IIS Configuration to access CMG CM, DM, and Web applications over HTTPS* section.
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 machine APIs. Information that resides in InAttend and CMG is password protected. The data backups can be stored as encrypted files to protect against unauthorized data access and as protection of stored user data at rest. If data is not used, then it is manually removed from the database.	• Details on User Management; adding, editing, and deleting Users and User Groups, are in the *QM User Guide > Administration* section**.** • Details on Profiles, Users, and Calls Management are in the *InAttend Installation and Configuration Guide > Configuring InAttend Profiles and Users*, and the *Working with Profile Groups* sections and in the *Configuring InAttend Users* section. • Details on defining roles and providing access based on the roles to different users are in the *CMG CM Online Help > All Users* section. • Details on setting basic and advanced security restrictions for the CMG User are in the *CMG Configuration Guide > Configuring Advanced Security* section.

	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.	• Details on configuring Default Voice mail Pin for new users are in *CMG Speech System settings Maintenance guide.* • Details on unlocking Voicemail after max faulty attempts tries are in *Directory Manager user guide.*
Data Deletion	The system provides an end user or an administrator with the ability to erase the end user's personal data. Only authorized administrators can use Directory Manager to modify or delete records. Any data stored for the purpose of statistics can be deleted automatically at predefined periods based on the configuration set by an authorized administrator. Erasing personal data implies that the data is deleted from the media, not simply de-referenced. The users themselves, through a web-based self-service GUI, can request that any stored personal data be modified or even deleted in certain cases, by the administrator.	• Details on how user records are managed and deleted are in *Directory Manager User Guide > Managing User Records* section. If a user record is deleted, IVR, Voicemail, Greetings, Menus, and all the personal data of the user will be deleted.
Audit	Audit trails are supported to maintain records of data processing activities. All components in InAttend have log files for troubleshooting and audit purpose. This includes security logs, end-user activity records, and administration activity audits.	• Details on Logs and Log's Management are in the *InAttend Administration and Maintenance Guide > Logging* section.
End Customer Guidelines	InAttend and CMG documentation is available to assist with installation, upgrades, and maintenance.	• Details are covered under *InAttend Installation and Configuration Guide*, *CMG Configuration Guide,* and *InAttend Administration Guide*.

Detailed logging for user data management in CMG	When a user record added, modified, or deleted in CMG DM, there will be detailed log information of admin ID or email who added, modified, or deleted the user record. There will be detailed log information of what information was changed – name, phone number, phonetics, organisation, keyword, activity along with the timestamp.	• Detailed logging features are in the *CMG DM Records>New Records* and in the *CMG DM Records>New Records* section. • Log details on Main Form Tab; User is modifying the first name, last name, extension, misc. fields and so on to the corresponding record id with date stamp. • Log details on Phonetic Tab; User is modifying the phonetic information to the corresponding record id with date stamp. • Log details on Organization Tab; User is modifying the Organization to the corresponding record id with date stamp. • Log details on Keywords Tab; User is adding, editing, and deleting the keywords to the corresponding record id with date stamp. • Log details on Recurring Activity Tab; User is adding, editing, and deleting the recurring activity to the corresponding record id with date stamp. • Log details when delete an existing Record; User is deleting an existing record with first name, last name, Telno and date stamp • Log details when create a new Record; User is adding a new record with first name, last name, Telno and date stamp.

6   Data Security Regulations

This section provides an overview of the security regulations that InAttend and CMG 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 organizational measures are used to adequately safeguard such data. Section 3 of this document explains what personal data is processed by InAttend and CMG and 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 Security Advisories

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

7.3 Mitel Security Documentation

Mitel security documentation includes product specific; Security Guidelines, 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

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 InAttend and CMG 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.