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

MiContact Center Business Release 9.2

Version 1.0

October 2019

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.

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 Mitel MiContact Center Business customers who are putting security processes and security controls in place to comply with GDPR.

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

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

NOTE: MiContact Center Business refers to the onsite or private cloud implementation of MiContact Center Business on the MiVoice Business, MiVoice Connect, MiVoice Office 400, or MiVoice 5000 platforms. MiCloud Flex Contact Center refers to Mitel's retail cloud contact center, powered by the same MiContact Center Business platform used onsite. For purposes of simplifying the naming in this document, the term *MiContact Center Business* is assumed to include Mitel's retail cloud MiCloud Flex Contact Center as well.

2 Personal Data Collected by MiContact Center Business

MiContact Center Business provides omnichannel (voice, email, chat, SMS, and open media) capabilities that can be applied in a number of verticals to address customer experience requirements.

The usage of personal data is required for the delivery of customer experience services. For example, sales and technical support services and billing services. A user's personal data, such as phone number and email address, is required for certain capabilities of the software to operate properly. In addition, the system can capture custom information in workflows (known as variables) that use customer-specific information (such as account numbers and credit card numbers) based on specific use cases. There are no end user opt-in consent mechanisms implemented in MiContact Center Business. Mitel recommends customers add statements about data collection upfront in workflows as a best practice so that they can ensure that their customers are aware of what information is captured by the systems.

During the course of installation, provisioning, operation, and maintenance, MiContact Center Business collects data related to several types of users. The data collected may be related to user provisioning, user activity monitoring and analytics, the user's personal content, and system management activity such as audit trails and logs.

The Mitel MiContact Center Business collects data related to several types of natural persons, including:

- End users of Mitel products and services—typically employees using Mitel phones and contact center tools.
- Customers of Mitel customers—personal information collected in workflows, voice and multimedia activity records, call recordings, and multimedia transcripts (including email address) contain personal content of both (or all) parties involved in interactions. The MiContact Center Business contact lists also contain personal information (such as the name, phone numbers, and email address) of end customers.
- System administrators and technical support personnel—logs and audit trails contain records of the activities of system administrators and technical support personnel, which may include employees of Mitel customers, Mitel sales channel partners, Mitel, and third-party suppliers.

- Agent information— capturing agent performance data is a core capability of the MiContact Center Business application. In addition, personal information pertaining to payroll and scheduling preferences may be optionally stored if Mitel's Workforce Scheduling, Scheduling Adherence, and Employee Portal applications are used.
- In some Mitel customer instances, workforce scheduling and adherence may be through a third party such as Teleopti.
- As of MiContact Center Business version 9.2.0.0, if a customer chooses to configure and use the web chat Contact Center Messenger feature, they will be using Mitel's CloudLink Cloud services. hosted in Amazon Web Services (AWS).
    - When using the Contact Center Messenger feature, if an employee was provisioned with a supervisor license or with a chat agent, then the user's first name, last name, email address, and nick name are stored in the CloudLink data center as part of provisioning a CloudLink user. This is required for the Contact Center Messenger feature to function properly.
- Customers making use of MiContact Center Business' Artificial Intelligence (AI) capabilities such as Agent Assist will be utilizing Google Cloud infrastructure if the Google AI feature is enabled. In this configuration the customer can turn off history in DialogFlow if they do not want to have a chat history within DialogFlow shown. Further information on Google's data deletion policy and procedures can be found here: https://cloud.google.com/security/deletion/ .
  Cloud services are hosted regionally based upon the customer's location.

3 Personal Data Processed by MiContact Center Business

The personal data processed by the MiContact Center Business has been classified as follows:

- **Provisioning Data**
    - Internal user (employee/supervisor/agent) 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.
- **Activity Records**
    - Internal/external user call history, chat or SMS transcripts, case subject and notes, email message files, call detail records, and system or user-defined variables that can be used to capture customer-specific information based on specific use cases.
    - As of MiContact Center Business version 9.2.0.0, if a customer chooses to configure and use the web chat Contact Center Messenger feature, they will be using Mitel's CloudLink Cloud services. hosted in Amazon Web Services (AWS).

  - Customers making use of MiContact Center Business' Artificial Intelligence (AI) capabilities such as Agent Assist will be utilizing Google Cloud infrastructure if the Google AI feature is enabled and data will be processed by the Google AI engine.

- **User Personal Content**
  - Call recordings, personal contact lists and phone information, and so on.

    Note: User activity records and user personal content may not be limited to the above-listed information. There may be instances where records contain personal data stored in the system. For example, email subjects, email body text, or attachments, and system or user-defined variables may contain information such as account numbers, credit card numbers, and so on. Note that a manual process may be required to determine whether a user activity record contains personal information, for example, within email body text.

- **Data in Elasticsearch**
  - Elasticsearch Contact records: Information that you can view in Web Ignite, Elasticsearch Manager, the Elasticsearch plugin or in the MiContact Center Software Development Kit (MiCCSDK) API.
  - Contact info in Elasticsearch Interaction records (Message and Voice indices): You can view this information only in Elasticsearch Manager or the plugin. It is used when searching in the History section of Ignite (Desktop or Web version).
  - Contact info in Elasticsearch Case records: You can view this information only in Elasticsearch Manager or the Head plugin. It is used when searching in the Cases section of Web Ignite.
  - Contact info in Active Directory Contacts: You can view this information only in Web Ignite, Elasticsearch Manager, and the plugin or in the MiCCSDK API.

- **Contact Information in SQL Server Table Records**
  - CDR contact information: If the "Conversation Detail Reporting" option is selected for a particular media server (multimedia or SIP), CDR contact information is written to the CCMStatisticalData database (*ConversationSummary* table) for that media server. This data can be viewed later in the CDR reports generated from the CCMWeb tool.
  - Life cycle contact information: If the "Enable Life Cycle Reports" option is selected on the Enterprise tab of the management tool, Your Site Explorer (YSE), MiVoice Business Contact Life Cycle data is written to various tables in the CCMStatisticalData database (*tblData_LC_CallRecording*, *tblData_LC_Note*, and *tblData_LC_Trace* tables). The *tblData_LC_Trace* table is the one that contains contact information. This data can be viewed later in the life cycle reports generated from the CCMWeb tool.
  - Trace contact information: MiVoice Business Trace data is written to various tables in the CCMData database (*tblData_CA_Trace, tblData_InboundTrace*, and *tblData_OutboundTrace* tables). This data can be viewed later in Trace reports generated from the CCMWeb tool.

- Incoming contact information: The Condition and Branch workflow data is stored in *tblData_VWM_ConditionTrace* tables.
- Call Accounting /Subscriber information: The call accounting and subscriber services details are stored in *CCMData.dbo.tblData_CA_Trace* tables.

When connected to MiVoice Business, ACD/SMDR/MiTai Events are collected in real-time, stored, and are used for writing data to the SQL tables.

Cloud services are hosted regionally based upon the customer's location.

4 Personal Data Transferred by MiContact Center Business

Depending on configuration and specific use requirements, the personal data collected may be processed and/or transferred between MiContact Center Business and other related systems and applications including Mitel cloud hosted applications. For example, Customer Relationship Management (CRM) or Enterprise Resource Planning (ERP) systems, directory systems, voice mail systems, and billing systems. Examples include:

- Internal user provisioning data such as the user's first name, last name, office phone number, mobile phone number, and email address may be shared between MiContact Center Business, MiVoice Business, MiCollab, and other systems such as MiVoice Call Recording.

- End user personal data such as user's first name, last name, phone number, email address, and mobile number might be required for the software to function properly or for a contact center agent to link cases and conversations for a customer.

- Data is collected for the delivery of improved customer experience services and providing technical support. Personal data is not used for combining or profiling by Mitel.

- Technical Support Packages, which are used for troubleshooting, might involve transferring data to third-parties outside the EU for processing.

- As of MiContact Center Business version 9.2.0.0, if a customer chooses to configure and use the web chat Contact Center Messenger feature, they will be using Mitel's regionally based CloudLink cloud services hosted in regionally based Amazon Web Services (AWS) data centers.

- When using the Contact Center Messenger feature, if an employee was provisioned with a supervisor license or provisioned with a chat agent then the user's first name, last name, email address and nick name are stored in the CloudLink data center as part of provisioning a CloudLink user. This is required for the Contact Center Messenger feature to function properly.

- Customers making use of MiContact Center Business' Artificial Intelligence (AI) capabilities such as Agent Assist will be utilizing Google Cloud infrastructure if the Google AI feature is enabled. When using Google AI bot and the Agent Assist features, the chat messages that the customer types into the chat are captured by Google for the bot to make decisions on how to respond, take action, or offer suggestions based on what was entered into the chat. The customer is able to turn off history in DialogFlow if they don't want the chat messages history visible in DialogFlow history UI.

- A customer can choose to collect personal data from the customer through the "bot" capability of Contact Center Messenger chat overlay and it will pass through CloudLink AWS cloud services and (if configured) Google Cloud services. Chat transcripts are temporarily stored in CloudLink cloud services while the chat is active. Once the chat conversation is completed it is deleted from CloudLink (in AWS) and it is stored locally on the MiContact Center Business server.

Cloud services are hosted regionally based upon the customer's location.

5 How MiContact Center Business Security Features Relate to GDPR

MiContact Center Business 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 summarizes the security features Mitel customers may use/rely on when implementing and evaluating both customer policy and technical and organizational measures required to achieve customer GDPR compliance.

Table 1: MiContact Center Business 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: Access to the system is limited by allowing only authorised access; authenticated using username/password login combinations that use strong password mechanisms. Administration access and activities related to passwords are audited and failed login attempts are logged. Mitel recommends using Microsoft Windows Authentication for added security measures. MiContact Center Business supports Single Sign On (SSO) with Active Directory authentication. Communications to the system, including all connections to cloud services, are performed over authenticated, encrypted communications channels using HTTPS (TLS 1.2). Additional security techniques can be used, such as encrypting the local hard drive with Bitlocker, applying regular Microsoft Windows Updates, and using anti-virus software. Cloud services are encrypted at rest by using the native capabilities of GCP and AWS. A customer can further limit access over their network using standard network security	Details are available in the "Configuring Security Settings" section of the MiContact Center Business Installation and Administration Guide. The latest version of the document is available at: https://www.mitel.com/document-center/applications/contact-center/micontact-center-business Additional information can be found in the white paper, MICONTACT CENTER BUISNESS SECURING CONNECTIONS. The latest version of the document is available at: https://www.mitel.com/en-ca/document-center

	techniques such as VLANs, access control lists (ACLs) and firewalls. In all cases, physical access to systems should be restricted by the customer.	
Communication Protection	Personal data transmissions may use any of the following channels with MiContact Center Business. Voice – when deployed with MiVoice Business, voice media is handled by the MiVoice Business and is encrypted by default. When deployed with the MiVoice Office 400 or MiVoice 5000, the only the internal SIP connection between the PBX and MiContact Center Business voice media routing engine is unencrypted. Email – the email channel may be secured and authenticated using TLS encrypted SMTP or IMAP connection. Web Chat is secured through HTTPS (TLS 1.2) and WSS between the client and MiContact Center Business. Contact Center Messenger chat is secured through HTTPS (TLS 1.2) and WSS between the client machine (agent's browser or customer's desktop) and CloudLink AWS cloud as well as between MiContact Center Business and the CloudLink AWS cloud. Communications between Goggle AI cloud and CloudLink AWS cloud are also encrypted using certificates generated per Google service account and communication over HTTPS (TLS 1.2) SMS is secured via HTTPS (TLS) between the Twillio SMS service and the MiContact Center Business. Open Media – allows a customer to connect to a REST API to route just about any media type. The REST API can be secured via HTTPS (TLS).	Details are available in the following KB article: http://micc.mitel.com/kb/KnowledgebaseArticle51887.aspx?Keywords=firewall Additional information may be found in the white paper, MICONTACT CENTER BUISNESS SECURING CONNECTIONS, the latest version of the document is available at: https://www.mitel.com/en-ca/document-center

	No media channels are open by default and must be configured to accept connections. For system integrity and reliability, all provisioning interfaces use secure channels over 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.	
Identity and Authentication	Access to the MiContact Center Business is restricted by an encrypted login username/password combination. MiContact Center Business supports Single Sign On (SSO) with Active Directory authentication. This is the recommended authentication method. Internal user access mechanisms support the principle of least privilege. The access control mechanism ensures there is no anonymous or shared logging in. Role Based Access Control is used. Customer-defined roles with edit permissions are supported. Predefined default roles are also used. Default roles support the principle of least privileges. Certain permissions are enabled only with the applicable licensing; for example, supervisor or administrator. 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.	Details are available in the “Changing the Default Administrative Password” section of the MiContact Center Business Installation and Administration Guide. The latest version of the document is available at: https://www.mitel.com/document-center/applications/contact-center/micontact-center-business

Access and Authorization	All personal data processing is protected with access and authorization controls. This includes personal data processing by data subjects, administrators, technical support, and machine APIs locally and in the cloud. All system data processing and all access to databases, files, and operating systems is protected with access and authorization controls locally and in the cloud.	Details are available in the "Configuring Security Settings" section of the MiContact Center Business Installation and Administration Guide. The document can be found at https://www.mitel.com/en-ca/document-center The latest version of the document is available at: *https://www.mitel.com/document-center/applications/contact-center/micontact-center-business*
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. Certain types of logs cannot be deleted on a per user basis. However, MiContact Center Business provides the administrator the ability to delete the entire content of logs. But doing so may affect the capabilities of the application. Call Detail Records and ACD Real Time Event logs are used for creation of contact center reports; and these may no longer be available/accurate if this data is deleted. Data stored off board such as on an external log server or SQL database is not deleted by this step, but further summarisation of data will not be possible. When using Contact Center Messenger chat *without* Google AI, the whole chat conversation is deleted from the CloudLink cloud once the conversation has completed. When using Contact Center Messenger chat *with* Google AI enabled, the whole chat conversation is deleted from the CloudLink cloud once the conversation has completed. However, data collected by Google (such as logs and phrases analyzed for Agent Assist) during interactions with Google Virtual Agent and when using Google Agent Assist is retained according to Google's data deletion policy.	See the Mitel Knowledgebase for more information. https://mitel.custhelp.com/app/answers/answer_view/a_id/1010053/loc/en_US See Google's data access policy for more information. https://cloud.google.com/security/overview/whitepaper#data_usage See Google's data deletion policy for more information. https://cloud.google.com/security/deletion/

Audit	Audit trails are supported to maintain records of data processing activities. The following log files are used to track customer data: • MiContact Center Business Server/Client log files—these log files show contact information, user authentication details, configuration changes, and so on. • IIS log files—log every request. • Search log files—search-related logs for multimedia contacts and transcripts. Automatic Call Distribution (ACD) and Station Message Detail Recording (SMDR) records are stored locally on the MiContact Center Business server. These records are required for MiContact Center Business to function properly.	
End Customer Guidelines	MiContact Center Business Guidelines are available to assist with installation, upgrades, and maintenance.	Details are available in various sections of the MiContact Center Business Installation and Administration Guide and the MiContact Center Business and MiVoice Analytics System Engineering Guide. The latest versions of these documents are available at: https://www.mitel.com/document-center/applications/contact-center/micontact-center-business

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

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 MiContact Center Business 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.