MiCloud Management Portal – Important Product Information for Customer GDPR Compliance Initiatives

MiCloud Management Portal Release 6.1

Version 1.1

June 2018

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 document will be of interest to MiCloud Management Portal customers that are putting security processes and security controls in place to comply with GDPR.

This document is intended to assist MiCloud Management Portal customers with their GDPR compliance initiatives by:

- Identifying the types of personal data that are processed by MiCloud Management Portal
- Listing the MiCloud Management Portal security features that customers may require to achieve GDPR compliance
- Providing a description of the MiCloud Management Portal security features
- Providing information on where the MiCloud Management Portal 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 information' 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 MiCloud Management Portal system and highlights available security features to safeguard such data.

2 Personal Data Collected by MiCloud Management Portal

MiCloud Management Portal manages customers and their end users. Data relating to customers and end users are collected, stored, and distributed amongst the related systems that MiCloud Management Portal communicates with.

During installation, provisioning, operation, and/or maintenance, MiCloud Management Portal collects data related to several types of users, including:

- Resellers, VARs and Customers, including their company names, contact information, branding information, web site information, dialling plans, and phone number ranges.
- End users of MiCloud Management Portal who are given Mitel phone and UC services.
- 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 MiCloud Management Portal.

3 Personal Data Processed by MiCloud Management Portal

MiCloud Management Portal processes only personal data required for the provisioning of communication services, billing services, and technical support services.

MiCloud Management Portal processes the following types of data:

- **Provisioning Data:**
  - The user's name, business extension phone number, mobile phone number, location, department, and email address.
- **Maintenance, Administration, and Technical Support Activity Records:**
  - System Logs
  - Content Database backup
- **User Activity Records:**
  - Logs.

4 Personal Data Transferred by MiCloud Management Portal

Depending on configuration, and specific user requirements, the personal data collected is processed and/or transferred between MiCloud Management Portal and other related systems and applications (such as MiVoice Business, MiCollab, MiVoice Border Gateway, and customer authorized billing systems).

For example:

- User provisioning data such as the user's first name, last name, office phone number, and mobile phone number are shared between MiCloud Management Portal and clustered MiVoice Businesses, MiVoice Border Gateway, and MiCollab.
- An XML billing report containing users' names, email, extension, and phone device types are exported from MiCloud Management Portal and delivered to a third-party customer authorized application for further processing.
- System logs are exported for secondary (backup) storage or transferred to authorized technical support personnel.
- Provision to import users from LDAP Active Directory file and generate a bulk import spreadsheet of users to import into MiCloud Management Portal by authorized users.
- Provision to generate a bulk import spread sheet that a Service Provider uses to fill in customer user data and then import the user data into MiCloud Management Portal.

5 How MiCloud Management Portal Security Features Relate to GDPR

MiCloud Management Portal 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 may use/rely on when implementing and evaluating both customer policy and technical and organizational measures required to achieve customer GDPR compliance.

Table 1: MiCloud Management Portal Security Features that Customers May Require to Achieve GDPR Compliance

Security Feature	Feature Details	Where the Feature is Documented
System and Data Protection, and Identity and Authentication	Access to the system is limited by allowing only authorised access that is authenticated using username/password login combinations that use strong password mechanisms. Failed login attempts are logged. There is no maximum number of retries at the portal login.	Details on access controls are available in the document *MiCloud Management Portal Engineering Guidelines;* in the section *Security,* sub-section *Access and Authorization*. Details on identity and authentication are available in the document *MiCloud Management Portal Engineering Guidelines;* in

	Communications to the system are performed over authenticated, encrypted communications channels using HTTPS (TLS). 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.	the section *Security,* sub-section *Identity and Authentication.* Additionally, the server administrator account is described in the *Mitel Standard Linux Installation and Administration Guide;* in the section *Configure the Server*. • The *Administration > System users* form is used to configure administrative access controls. This form can be used to: ▪ Set/reset the password ▪ Provide feedback on password strengths
Communication Protection	Personal data are exchanged between MiCloud Management Portal and the following related systems: • MiVoice Business • MiCollab • MiVoice Business Express • MiVoice Border Gateway • Operators, Customers and End Users' PCs. • Customer's Email server All personal data transmissions use secure channels such as THRIFT, HTTPS, and SMTP. Communications protection is further provided with the following controls: • Only the LAN interface is enabled. All other network interfaces are disabled by default. • All unused ports are disabled by default. • Remote Access is disabled by default	Details on MiCloud Management Portal secure connections are available in the document *MiCloud Management Portal Engineering Guidelines;* in the sections *Port Usage* and *Security > Network Settings*.
Access and Authorization	MiCloud Management Portal ships with a root administrator, so that the root administrator can create additional administrators with access restriction based on defined profiles. A customer can further limit access over the network using standard network security	Details are available in the document *Service Providers Help;* in the section *Manage Users*. Of relevance also are details on administrators, which can be found in the document *MiCloud Management Portal Engineering Guidelines;* in the section *Administrators*.

	techniques such as VLANs, access control lists (ACLs), and firewalls. In all cases, physical access to systems should be restricted by the customer.	
Data Deletion	The system provides the administrator acting on behalf of the data subject, with the ability to delete a user and all the user's provisioned services. Certain types of user data cannot be deleted on a per user basis or by the administration tool. However, MiCloud Management Portal provides the administrator with the ability to delete the entire contents from all logs through the console interface.	Details are available in the document *Service Providers Help;* in the section *Manage Users* section.
Audit	Audit logs are available for data processing activities. The audit logs provide a historical record of changes made to the system. It does this by recording certain actions and storing this information in a log. The logs are used to help with troubleshooting and to determine in a multi-administrator system who is responsible for a particular change. For example, the action to modify a user is recorded in a log containing such information as the action taken, the user name, the user email address, and so on.	Details are available in the document *MiCloud Management Portal Engineering Guidelines;* in the section *Audits and Logs* of *Security*.
End Customer Guidelines	Security guidelines are available to assist with installation, upgrades, and maintenance.	Details are available in the document *MiCloud Management Portal Engineering Guidelines.* The *Security* section has information that can help the customer to achieve GDPR compliance. The *MiCloud Management Portal Engineering Guidelines* document is available at Mitel Online.

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