Unify OpenScape Contact Center

Processing of Personal Data

Whitepaper

Version 2.0

Atos

Trusted partner for your **Digital Journey**

Purpose

The European Data Protection Regulation came into force on May 25th, 2018.

The GDPR not only applies to organisations located within the EU but also applies to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

The GDPR applies to 'personal data', meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

This document is intended to assist direct customers and partners in answering technical questions related to OpenScape Contact Center and compliance with EU-GDPR requirements with regards to their employees' personal data when using OpenScape Contact Center. It describes which customer personal data are being collected, processed and transferred by OpenScape Contact Center and for what purpose these data are accessed.

This document describes the main functions of OpenScape Contact Center. It makes no claim to completeness. For clarification of unaddressed topics or detailed questions, the user documentation of the used clients, the OpenScape Contact Center Manager Administration Manual, the OpenScape Contact Center System Management Guide and OpenScape Contact Center Security Checklist must be used. The documents can be downloaded within the Internet via the Unify Partner Portal.

https://www.unify.com/us/partners/partner-portal.aspx (Login is required)

Within the Unify Partner Portal the documents can be accessed using the path: Sell -> Products & Services A-Z -> OpenScape Contact Center Enterprise V10 -> Documents or Sell -> Products & Services A-Z -> OpenScape Contact Center Agile V10 -> Documents
The descriptions in this Whitepaper refer to OpenScape Contact Center V10 R4

In the course of technical development, changes to this document may arise at any time.

Disclaimer & Copyright

This Whitepaper is published for general information purposes only; it is of a general scope and is used for informational purposes only. It is not to be construed as providing legal, tax, financial or professional advice. The contents hereof are subject to change without prior notice. This document does not establish or affect legal rights or obligations and cannot be used to settle legal issues.

The information provided in this document contains general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change because of further development of the products. The detailed characteristics shall be provided in the contract. Availability and technical specifications are subject to change without notice.

Unify, OpenScape are registered trademarks of Unify Software and Solutions GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

Document History

Date	Version	Changes/Comments
2018-08-01	1.0	Draft
2018-08-03	1.1	Changes after review
2021-09-23	2.0	New features for OSCC V10

Table of Contents

1. Introduction 6
   1.1. Fulfilment of EU-GDPR requirements 6
   1.2. EU-GDPR Declaration of Conformity 6
   1.3. Legacy products notice 6
2. Processing of Personal Data in 7
3. Data Acquisition by the System 7
   3.1. Contact Center Manager 7
4. Data Collection during Operation 8
   4.1. Data Acquisition by the OpenScape Contact Center 8
      4.1.1. Caller Identification 8
      4.1.3. DTMF Collected Data 10
      4.1.4. Transcript of the Text Media Contacts 11
      4.1.5. Call Recording 12
      4.1.6. Data acquisition for diagnostic purposes 13
   4.2. Data Acquisition by the Agent 14
      4.2.1. Team List 14
      4.2.2. Speed List 15
5. Display of Personal Data on 16
   5.1. Agent Client Applications 16
   5.2. Manager Client Application 16
   5.2. Web Supervisor Application 16
6. Transmission of Personal Data 17
   6.1. Transmission between Clients and System 17
   6.2. Transmission between Communication Platforms and 17
   6.3. Transmission between System and E-mail Server 17
   6.4. Transmission between Clients and E-mail Server 17
   6.5. Transmission between System and Web Corporate Server 17
   6.6. Transmission between System and OpenMedia Connectors 18
   6.7. Transmission between Facebook Connector and Facebook 18
   6.8. Transmission between Twitter Connector and Twitter 18
   6.9. Transmission between WatsApp Connector and WatsApp 18
   6.10. Transmission between Life of Call and System 18
   6.11. Transmission between Custom Applications and System 18
   6.12. Transmission between CRS and System 18
   6.13. Transmission between Auxiliary and System 18
   6.14. Transmission between OS CMS and System 19
   6.15. Transmission between OS CMS and Communication 19
   6.16. Transmission between Browser and OS CMS for WebR 19
   6.17. Transmission between OS CMS and Google Cloud for Speechbot 19
7. Recovery of Personal Data 20
8. Personal Data Retention 20
   8.1. System in general 20
9. References and Sources 21

9.1. OpenScape Contact Center Service-/Administrator documentation 21
9.2. User Guides 21

1. Introduction

1.1. Fulfilment of EU-GDPR requirements

According to GDPR the operator (controller) determines which data are collected and where, how, by whom (processor) they are processed. Mirrored on OpenScape Contact Center this means:

The system administrator (processor) may only collect or release personal data and functions in the system configuration specified by the operator (controller). This applies in detail to subscriber telephone, address and contact data (telephone numbers, e-mail), contacts and directories.

During operation, OpenScape Contact Center can generate and process further personal data. These include, but are not limited to: caller data (like phone number, e-mail address, social media identification), journal data, exchanged e-mails, chats and social media posts and other personal information. The OpenScape Contact Center agents can also individually process further personal data in their client applications. e.g. Speed dialing destinations and personal information.

The operator (controller) of OpenScape Contact Center must be informed by the system administrator (processor) so that he can take these functions into account in the data protection concept.

OpenScape Contact Center offers many options for blocking or restricting the collection and processing of personal data. The detail data that can be captured and processed, as well as the limitations, are to be described in further detailed documentation.

In principle, the operation of OpenScape Contact Center is also possible without the use of personal data. However, certain functions are only limited or no longer available. (e.g., caller identification in 360 degree view feature).

1.2. EU-GDPR Declaration of Conformity

Unify Commitment to the EU GDPR is available under the following link:

https://www.unify.com/us/Home/Internet/web/Container Site/Misc/Footer-content/privacy-policy/data-protection.aspx

An OpenScape Contact Center product-specific Declaration of Conformity is not provided for the reasons shown above.

1.3. Legacy products notice

Our products have a long tradition of design for security and certainly our recommendations for personal data handling apply to some extent to our past product versions or solutions too.

Nevertheless, enhancements addressing current market needs, GDPR included, are only provided on our latest solutions or product versions. Please consider upgrading your systems to assure up-to-date security and features to help you comply with GDPR requirements.

2. Processing of Personal Data in OpenScape Contact Center

OpenScape Contact Center is a family of communications solutions that offers a comprehensive contact center application. OpenScape Contact Center uses personal data in addition to pure telephone numbers in order to offer users the desired scope of service on the telephones and Contact Center Clients.

The use of personal data is optional but not mandatory for the overall function of OpenScape Contact Center. If no personal data is used, functions such as dialing from phonebook, caller identification and contact information are not possible.

Personal data is collected by various tools and processes in the OpenScape Contact Center System or in the connected clients and phone devices. Data is either stored in the system or in the client. The collected data is used for the OpenScape Contact Center functions.

OpenScape Contact Center differentiates between data processing during system setup and configuration and data processing during operation in general.

During system configuration, personal data can only be collected and stored by an authorized system administrator.

Consent

The company that uses the Contact Center system can request Consent from the users in a paper-form, electronic form etc. The company can maintain a record with the collected consents. Withdrawal of consent is equivalent to user deletion. Withdrawal can be requested from the admin of the system via a paper form, e-mail etc.

3. Data Acquisition by the System Administrator (Master Data)

3.1. Contact Center Manager

Personal data are collected in the system configuration when setting up:

- Agents and Supervisors

The data is acquired by the system administrator or by the supervisor via the OpenScape Contact Center Manager application with the Manager or Supervisor profile.

The First Name and Last Name of the Agent may be configured in the Manager but they are not mandatory for the configuration of the Agent user.

Currently no Customer data is collected for the configuration of the Contact Center. The Manager can configure the system to get access to the Directory of the company via LDAP or via UC Server.

Data Storage
The Agents and Supervisors data are stored in the Informix database which is integrated in the OpenScape Contact Center.

Data Access/Data Use
The Agents and Supervisors data can be accessed by the manager or by the supervisors in the same screen in which they are configured.

The Agents user identification and/or "<last name>, <first name> can be presented in reports which are related to the agents. The reports are only accessible by users who have permissions to access the reports.

The Agent Id is used by the Agents to log in to the Agent application.

Data Transmission
The communication between the Manager application and the OpenScape Contact Center main server can be configured to be established via TLS.

The communication between the Agent Portal/Client Desktop and the OpenScape Contact Center main server can be configured to be established via TLS.

The Agent Portal Web can only be accessed via HTTPS.

Backup/Restore
The Agent data can be exported and imported in the Design DB. The exported Design DB is protected by password.

Data Retention/Modification/Deletion
Agent data can be modified/deleted via the Manager Application by the Manager or by the Supervisor who has the corresponding permission.

4. Data Collection during Operation (Traffic Data)

4.1. Data Acquisition by the OpenScape Contact Center

4.1.1. Caller Identification

The Contact Center automatically collects caller identification which are provided with the contacts that are handled by the system via Voice, Chat, E-mail or Social Media and stored in the contact record data.

For voice calls, contact record data will only be collected for those calls that arrive over the designated contact center call numbers. Direct-dial calls to agents and internal calls are not subject to data collection. For voice calls which are established with the Integrated Softphone, the contact record data are not stored by the Integrated Softphone being presented to the agent only during the call.

For e-mails, only e-mail in the contact center that have been received or sent via the email account set up specifically for the
OpenScape Contact Center on an e-mail server are recorded.

The data collected by the OpenScape Contact Center can be evaluated by the Supervisor / Administrator in real time via the Mobile
Supervisor, Web Supervisor or Manager Application.

The data collected by the OpenScape Contact Center can be evaluated by the Supervisor / Administrator historically via the Manager
Application.

The Manager Application provides the contact center supervisor / administrator with the option of evaluating via predefined report templates and exporting contact center reports as files for processing in other applications.

Storage

The contact record data, chat transcripts and e-mails as well as the availability status of the agents in the contact center are stored in the Informix database which is integrated in OpenScape Contact Center. The storage duration in the database can be configured by the Manager (maximum configurable value is 10 years).

Data Access/Data Usage

The contact record data is used in the construction of historical reports.

During the handling of a contact, the Agent is able to see the previous contacts from the customer to the Contact Center. The contact record data is used to present the previous contacts.

The contact record data cannot be directly accessed.

If required, contact record data can be queried by means of a Stored Procedure which shall be used as described in the GDPR Stored Procedures Whitepaper.

Contact record data can also be accessed by means of the SDK which allows 3rd party to implement customized applications. The access to SDK is protected by user and password.

Data Transmission

The communication between the Manager application and the OpenScape Contact Center main server can be configured to be established via TLS.

The communication between the Agent Portal/Client Desktop and the OpenScape Contact Center main server can be configured to be established via TLS.

The Agent Portal Web can only be accessed via HTTPS.

Backup/Restore

The contact record data can be exported and imported by means of a specific tool. The resulting file cannot be read in clear text. Importing data back into the database can only be done with user and password.

Data Retention/Modification/Deletion

Retention time is configurable and can be configured (maximum configurable value is 10 years).

Contact record data cannot be modified because it corresponds to the data about the contact that is automatically collected.

If required, contact record data can be deleted by means of a Stored Procedure which shall be used as described in the GDPR Stored Procedures Whitepaper.

4.1.2. 360° Customer View Data

360º Customer View allows that the agent visualizes the previous contacts the customer has done to the contact center.

While handling a contact which was routed by the OpenScape Contact Center, the Agent is able to complement customer data by adding First Name, Last Name, Phone Numbers, Address, E-mail addresses, Customer Ids, Social Media ids.

Storage

The 360° Customer View data are stored in the Informix database which is integrated in OpenScape Contact Center.

Data Access/Data Usage

The 360° Customer View data can only be accessed by the Agent while handling a call from the customer.

If required, 360° Customer View data can be queried by means of a Stored Procedure which shall be used as described in the GDPR Stored Procedures Whitepaper.

Data Transmission

The communication between the Agent Portal/Client Desktop and the OpenScape Contact Center main server can be configured to be established via TLS.

The Agent Portal Web can only be accessed via HTTPS.

Backup/Restore

The contact record data can be exported and imported by means of a specific tool. The resulting file cannot be read in clear text. Importing data back into the database can only be done with user and password.

Data Retention/Modification/Deletion

The customer data will be kept in data while there is a contact record data for this customer. Retention time of contact record data is configurable and can be configured (maximum configurable value is 10 years).

Customer View Data can be modified by the agent while handling a contact from this customer.

If required, contact record data can be deleted by means of a Stored Procedure which shall be used as described in the GDPR Stored Procedures Whitepaper.

4.1.3. DTMF Collected Data

Depending on the IVR design, personal data like Credit Card Number or Social Security Number can be collected via DTMF dialing. These data can be stored as Contact Data in the database.

Storage

The Contact Data are stored as part of the Contact Record Data in the Informix database which is integrated in OpenScape Contact Center.

Data Access/Data Usage

These data can be seen by the Agent. They can also be used to open customer files in other system and to make decisions regarding to the routing of the contacts.

Data Transmission

The OpenScape Contact Media Service allows the configuration of SRTP for the media connection.

The DTMF dialed data are transmitted via a secure connection between the OpenScape Contact Media Service and the OpenScape Contact Center.

The communication between the Agent Portal/Client Desktop and the OpenScape Contact Center main server can be configured to be established via TLS.

The Agent Portal Web can only be accessed via HTTPS.

Backup/Restore

The Contact Data can be exported and imported by means of a specific tool. The resulting file cannot be read in clear text. Importing data back into the database can only be done with user and password.

Data Retention/Modification/Deletion

Retention time is configurable and can be configured (maximum configurable value is 10 years).

Contact Data cannot be modified because it corresponds to data which was provided by the customer.

If required, Contact Data can be deleted as part of contact record data by means of a Stored Procedure which shall be used as described in the GDPR Stored Procedures Whitepaper.

4.1.4. Transcript of the Text Media Contacts

The OpenScape Contact Center can handle contacts via text media like chat and social media. The content of the exchanged messages can be stored by the contact center.

These messages can contain any kind of information, including personal and sensitive personal data.

Storage

The transcripts of text media contacts are stored in the Informix database which is integrated in OpenScape Contact Center.

The content of the e-mails is only stored in the corporate e-mail server. References to the e-mail contacts are stored as part of the contact record data.

Data Access/Data Usage

The transcripts of text media can only be accessed by directly accessing the database. Notice that the direct access to the database is protected by user and password.

If required, transcripts of text media data can be queried by means of a Stored Procedure which shall be used as described in the GDPR Stored Procedures Whitepaper.

Agents and supervisors can search on historical e-mails and send post-responses to these e-mails.

Data Transmission

The protection of the connection to the database is under responsibility of the application.

The connection to the e-mail server can be configured to be established via TLS.

Backup/Restore

The transcripts of text media can be exported and imported by means of a specific database import export tool. The resulting file cannot be read in clear text. Importing data back into the database can only be done with user and password.

E-mails on the corporate e-mail server are submitted to the backup/restore policy of the corporate e-mail server.

Data Retention/Modification/Deletion

Retention time is configurable and can be configured (maximum configurable value is 10 years).

Transcripts of text media cannot be modified because it corresponds to the conversation between the customer and the agent.

If required, transcripts of text media can be deleted by means of a Stored Procedure which shall be used as described in the GDPR Stored Procedures Whitepaper.

E-mails on the corporate e-mail server are submitted to the retention policy of the corporate e-mail server. E-mails on the corporate e-mail server can only be modified and deleted by using tools of the corporate e-mail server.

4.1.5. Call Recording

The OpenScape Contact Center can record calls which are routed to the agents. Both the content of the call and the metadata of the call are recorded.

These stored calls can contain any kind of information, including personal and sensitive personal data.

Storage

The recorded call are stored in .wav or .ogg files in the hard disk of the OpenScape Contact Media Service. The recorded call files are encrypted with AES-256 and the keys are system wide and randomly generated and stored in a protected area of OpenScape Contact Media Service.

The metadata about the calls are stored in a PostgreSQL database which is located in the OpenScape Contact Media Service.

Data Access/Data Use

The recorded call files and metadata can be accessed via the Web Supervisor application, by supervisors which have the permission to monitor the involved agents.

The recorded call files are also accessed via a REST API interface which connects via HTTPS and is authenticated via OAuth. Softcom accesses the recording files via this REST API interface to collect recorded files to perform call analysis. More information about the GDPR compliance of Softcom must be provided by them directly.

Data Transmission
The recorded call files are always transported via TLS. All the interfaces are authenticated.

Backup/Restore
A backup mechanism allows creating external backups of the recorded call files. The files are encrypted SMB connection. The backup infrastructure is out of the scope of the OpenScape Contact Center solution.

Recorded call files can be restored from the backup via the Web Supervisor.

Data Retention/Modification/Deletion
The retention time is configurable and can be configured (the possible values are 6 months, 1 year, 2 years, 3 years, 4 years and 5 years).

The recorded call files and metadata cannot be modified as they are collected during the call.

The recorded call files and metadata can be deleted via the Web Supervisor by users which have the permission to delete recorded files.

The retention time of the backup is under the responsibility of the customer.

4.1.6. Data acquisition for diagnostic purposes

OpenScape Contact Center and the integrated applications provide diagnostic mechanisms that store log and trace files in the system. These files may also contain personally identifiable information.

The acquisition of base trace and log data is active after factory commissioning.

The system administrator is able to use the OpenScape Contact Center System Monitor to change the detection depth of traces/logs as directed by the system development, as well as to activate or deactivate further traces/logs.

Data Storage
The collected data is stored in the server file system. The traces/logs are only accessible by the system administrator. OpenScape Contact Center – Whitepaper Processing of Personal Data

Data Access/Data Use
Access to traces and logs is only possible for the system administrator or the system development. Traces and logs are used for system diagnostics in the event of an error.

Data Export
The export of trace log files can only be done by the system administrator or by the system development via the administration access of the system.

Data Transmission
Traces/logs must be transferred via TLS encrypted SSH access to the operating system.

Backup/Restore
A backup/restore of the trace and log files is not provided.

Data Retention/Modification/Deletion
The trace/log files are subject to file rotation by time and by size.

The trace/log files can be modified and deleted by the system administrator.

4.2. Data Acquisition by the Agent

Currently, the Agent can use the Client Desktop, the Agent Portal or the Agent Portal Web to handle customer contacts.

4.2.1. Team List

The Agent can access a Team List with information about other agents either on the Client Desktop, the Agent Portal or the Agent Portal Web. The Team List can be accessed by means of the Agent client application. The Team List present the following information: first and last name, agent id, presence state, routing state, handling state, extension number, group, department, contact type, active contacts, contacts waiting and description.

The System Manager can configure the agents which can be viewed by an agent.

Storage
The identification of the agents is stored in the Informix database in the OpenScape Contact Center main server. The other data are dynamically updated.

Data Access/Data Usage
The data are accessed by the agent during regular contact center operation in order to identify other agents which may be available to provide support.

Data Transmission
The communication between the Agent Portal/Client Desktop and the OpenScape Contact Center main server can be configured to be established via TLS.

The Agent Portal Web can only be accessed via HTTPS.

Backup/Restore
Not applicable.

Data Retention/Modification/Deletion
Not applicable.

4.2.2. Speed List

The agent can build a Speed List with a list of contact persons on the Client Desktop, the Agent Portal or the Agent Portal Web. The Speed List can be accessed by means of the Agent client application.

The agent can feed the Speed List manually or by importing contacts from a Directory Server via LDAP(S).

The Speed List present the following information: first and last name, phone number, home phone number, mobile phone number, office email and home email.

Storage
The identification of the agents is stored in the Informix database in the OpenScape Contact Center main server. The other data are dynamically updated.

Data Access/Data Usage
The data are accessed by the agent during regular contact center operation by means of the client applications Client Desktop, Agent Portal or Agent Portal Web.

The agent can use the Speed List to speed dial to customers, partners or any other contacts. The Speed List can also be used to provide further information about the incoming contacts.

Data Transmission
The communication between the Agent Portal/Client Desktop and the OpenScape Contact Center main server can be configured to be established via TLS.

The Agent Portal Web can only be accessed via HTTPS.

The connection between the client application and the Directory Server can be encrypted via LDAPS.

Backup/Restore
The communication between the Agent Portal/Client Desktop and the OpenScape Contact Center main server can be configured to be established via TLS.

The Agent Portal Web can only be accessed via HTTPS.

Data Retention/Modification/Deletion
The Speed List is managed by the Agent. The Agent is responsible for adding, modifying and deleting entries in the Speed List.

5. Display of Personal Data on Software Clients

The personal data collected in OpenScape Contact Center serves to support the agent and supervisor in his business processes. For this purpose, the data is displayed on the Agent application of the OpenScape Contact Center System for the realization of certain functions. Depending on the data and the functions, the visibility of the data can either be limited or completely prevented by the system administrator or by the user itself.

Data displayed on the telephone devices is under the responsibility of the communication platforms. For the handling of GDPR requirements on the communication platforms, please refer to the corresponding documentation for OpenScape Voice, OpenScape 4000 and OpenScape Business.

Personal data can generally be displayed in the subsequent functions of the software clients.

- Caller Identification
- 360º Customer View
- Team list
- Speed list
- IVR collected digits
- Contact Center agent assignment
- Contact Center reports

5.1. Agent Client Applications

The Agent Client Applications, namely Agent Portal Web, can present the following personal data:

- Caller Identification
- 360º Customer View
- Team list
- Speed list
- IVR collected digits

5.2. Manager Client Application

The Agent Client Application, namely Agent Portal Web, can present the following personal data:

- Team list
- Contact Center agent assignment
- Contact Center reports

5.2. Web Supervisor Application

The Web Supervisor Application can present the following personal data:

- Recorded calls files and metadata

6. Transmission of Personal Data (Data on Move)

Person-related data is transmitted on the one hand between the OpenScape Contact Center System and the connected telephone devices and clients and on the other hand as an option to external applications.

The communication between the telephone devices and the communication platforms is out of the scope of the OpenScape Contact Center. Please refer to the communication platforms documentation for OpenScape Voice, OpenScape 4000 and OpenScape Business.

Further information on securing the transmission paths and the transmission protocols used etc. can be found in the OpenScape Contact Center Security Checklist.

6.1. Transmission between Clients and System

Personal data can be transferred to implement the OpenScape Contact Center functions between client applications and OpenScape Contact Center main server. Here, the caller identification, the search in the telephone book or data directories of the system as well as the telephone status or presence status of a user is to be seen as a priority.

The following client applications can currently connect to the OpenScape Contact Center main server: Client Desktop, Agent Portal, Agent Portal Web, Manager, Mobile Supervisor, Web Supervisor.

The communication between the client applications and the system can be encrypted.

6.2. Transmission between Communication Platforms and System

The transmission of data between the Communication Platforms and the OpenScape Contact Center is performed via CSTA protocol. The CSTA protocol carries customer data like phone numbers. The communication between contact center and communication platform can be encrypted via a VPN.

6.3. Transmission between System and E-mail Server

The transmission of data between the OpenScape Contact Center and the E-mail Server is performed via IMAP/SMTP protocols. The communication between the OpenScape Contact Center and the E-mail Server can be encrypted.

6.4. Transmission between Clients and E-mail Server

The transmission of data between the Agent client applications, namely Client Desktop, Agent Portal, Agent Portal Web and the E-mail Server is performed via IMAP/SMTP protocols. The communication between the Agent client applications and the E-mail Server can be encrypted.

6.5. Transmission between System and Web Corporate Server

The transmission of data between the OpenScape Contact Center and the Corporate Web Server for chat media is performed via proprietary protocol. The communication between the OpenScape Contact Center and the Corporate Web Server can be encrypted.

6.6. Transmission between System and OpenMedia Connectors

The transmission of data between the OpenScape Contact Center and the OpenMedia Connectors for text media and social media is performed via REST interface. The communication between the OpenScape Contact Center and the OpenMedia Connectors can be encrypted.

6.7. Transmission between Facebook Connector and Facebook

The transmission of data between the OpenScape Contact Center Facebook Connector and the Facebook Web Server is performed via the Facebook Graph API. The communication between the OpenScape Contact Center Facebook Connector and the Facebook Web Server is encrypted.

6.8. Transmission between Twitter Connector and Twitter

The transmission of data between the OpenScape Contact Center Twitter Connector and the Twitter Web Server is performed via the Twitter Graph API. The communication between the OpenScape Contact Center Twitter Connector and the Twitter Web Server is encrypted.

6.9. Transmission between WatsApp Connector and WatsApp

The transmission of data between the OpenScape Contact Center WhatsApp Connector and the WhatsApp Web Server is performed via a broker which is homologated by WhatsApp. Currently Novomind is the only supported broker. The communication between the OpenScape Contact Center Facebook Connector and the Novomind Web Server is encrypted.

6.10. Transmission between Life of Call and System

The transmission of data between the Life of Call and the OpenScape Contact Center is performed via the ODBC. Contact data are transferred from OpenScape Contact Center and Life of Call. The communication between contact center and Life of Call can be secured through a segregated network or via VPN.

6.11. Transmission between Custom Applications and System

The transmission of data between the Custom Applications and the OpenScape Contact Center is performed via legacy SDK or via REST SDK (beginning on V9R2 FP2). The communication between the Custom Applications and the OpenScape Contact Center can be encrypted.

6.12. Transmission between CRS and System

The transmission of data between the OpenScape Contact Center Central Reporting Server (CRS) and the OpenScape Contact Center main server is performed via the ODBC. The communication between contact center and CRS can be secured through a segregated network or via VPN.

6.13. Transmission between Auxiliary and System

The transmission of data between the OpenScape Contact Center Auxiliary Server and the OpenScape Contact Center main server is performed via the ODBC. The communication between contact center and auxiliary server can be secured through a segregated network or via VPN.

6.14. Transmission between OS CMS and System

The transmission of data between the OpenScape Contact Media Service and the OpenScape Contact Center is performed via proprietary protocol. The communication between the OpenScape Contact Media Service and the OpenScape Contact Center is encrypted.

6.15. Transmission between OS CMS and Communication Platform

The transmission of data between the OpenScape Contact Media Service and the Communication Platforms is performed via SIP (over TLS) and (S)RTP. The communication between the OpenScape Contact Media Service and the Communication Platforms can be configured to be encrypted via SIP over TLS and SRTP.

6.16. Transmission between Browser and OS CMS for WebR

The registration of the WebRTC client, the call signalling and media the browser, the Application Server and the OpenScape Contact Media Service are performed via proprietary protocols and (S)RTP or (S)RTP over TURN. The communication between the browser and the OpenScape Contact Media Service are encrypted over HTTPS and SRTP.

6.17. Transmission between OS CMS and Google Cloud for Speechbot

The access to the Speech API, DialogFlow API and Text-to-Speech API, from the OpenScape Contact Media Service to Google Cloud are performed via HTTPS.

7. Recovery of Personal Data

OpenScape Contact Center offers an integrated backup/restore function that allows customer to quickly restore the system configuration and the personal data contained in the event of an error. For this purpose, the personal data stored in the system configuration as well as a deduction of the system database can be stored in special backup files, saved and, if necessary, restored from these.

8. Personal Data Retention

8.1. System in general

The personal data acquired by the system administrator in OpenScape Contact Center can also be deleted by the system administrator.

Personal data acquired by the user himself in the clients, e.g. user picture, shortcuts, personal directory and e-mails can be deleted by users themselves.

The deletion of personal data always refers to the current system configuration or to the current client configuration as well as to the current personal directories and journals. Personal data in system backups and archived files are not deleted.

Personal data (e.g., surname, first name) associated with Caller Identification, Chat Transcript, OpenMedia Transcript will be retained for the configured Retention Period which can be configured (maximum configurable value is 10 years).

Personal Data associated to 360º Customer View will be retained while there is a Caller Identification registry associated to it. When the last Caller Identification registry associated to a 360º Customer View data is deleted due to Retention Period expiration, the corresponding 360º Customer View data is also deleted.

The system administrator can use the database scripts to delete the data collected by the system during operation, like Caller Identification, 360° Customer View Data, Chat Transcript and OpenMedia Transcript.

9. References and Sources

The documents can be downloaded within the Internet via the Unify Partner Portal.

https://www.unify.com/us/partners/partner-portal.aspx (Login is required)

Within the Unify Partner Portal the documents can be accessed using the path: Sell -> Products & Services A-Z -> OpenScape Contact Center Enterprise V10 -> Documents or Sell -> Products & Services A-Z -> OpenScape Contact Center Agile V10 -> Documents

9.1. OpenScape Contact Center Service-/Administrator documentation

OpenScape Contact Center V10 R4, Manager Administrator Documentation

OpenScape Contact Center V10 R4, System Management Guide

OpenScape Contact Center V10 R4 Security Checklist

OpenScape Contact Center – GDPR Stored Procedures

9.2. User Guides

OpenScape Contact Center Client Desktop

OpenScape Contact Center Agent Portal

OpenScape Contact Center Agent Portal Web

OpenScape Contact Center Mobile Supervisor

OpenScape Contact Center Manager Administration

About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about
us atos.net
atos.net/career

Let’s start a discussion together

For more information: XXXX@atos.net