OpenScape UC

Whitepaper

Processing of Personal Data

Version 1.6

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 UC and compliance with EU-GDPR requirements with regards to their employees' personal data when using OpenScape UC. It describes which customer personal data are being collected, processed and transferred by OpenScape UC and for what purpose these data are accessed.

This document describes the main functions of OpenScape UC. It makes no claim to completeness. For clarification of unaddressed topics or detailed questions, the user documentation of the used devices/clients and the OpenScape UC Administration Manual must be used. The documents can 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 UC Applicaton V9 → Documents

The descriptions in this Whitepaper refer to OpenScape UC V9R3

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

Disclaimer & Copyright

This Whitepaper is published as a service to our partners and customers for general information 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 as a result 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
2018-06-01	1.0	Draft
2018-06-11	1.1	Initial Version with input for OpenScape UC, WebClient, Mobile Clients
2018-06-27	1.2	Fusion for Office and Fusion for Noites input and corrections
2018-06-29	1.3	Corrections and additions for conference recording/data available in clients
2018-07-09	1.4	Final wording correction
2018-07-23	1.5	Minor corrections and additions
2018-10-08	1.6	Small changes

Table of Content

1. Introduction

1.1. Fulfillment 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 UC 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 data of telephone and UC subscribers, address and contact data (telephone numbers, e-mail), contacts and directories.

During operation, OpenScape UC can generate and process further personal data. These include, but are not limited to: caller lists or journal data, presence status. The client applications and UC subscribers of OpenScape UC can also individually process further personal data in their client applications, e.g. Speed dialing destinations and personal directories/contacts.

The operator (controller) of OpenScape UC must be informed by the system administrator (processor) about such generating and processing of personal data so that he can take these functions into account in the data protection concept.

OpenScape UC 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 described in the following chapters of this document.

In principle, the operation of OpenScape UC is also possible without the use of personal data. However, certain functions are only limited or no longer available (e.g., caller identification).

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%20Site/Misc/Footer-content/privacy-policy/data-protection.aspx

An OpenScape UC 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 UC

OpenScape UC is a communications solution that offers a comprehensive unified communications (UC) application.

OpenScape UC uses personal data in addition to telephone numbers (E.164 or private ones) in order to offer users the desired scope of service on the telephones and Unified Communication Clients.

The use of personal data is optional but not mandatory for the overall function of OpenScape UC. If no personal data is used, functions such as dialling from phonebook or caller identification are not possible.

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

OpenScape UC 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.

During operation of OpenScape UC, personal data can be captured and stored either by the base system and by the embedded applications or by the subscribers in their telephone or the users of the UC clients.

Consent

The company that uses the UC 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. OpenScape UC

Storage

The data that are collected and stored by an authorized system administrator during system setup can be split into the following categories:

User related Configuration Data

They are used for provisioning of the offered telephony functions

- First/Last Name,
- User IDs,
- E-Mail Address,
- Telephone Numbers,
- Location/Address data,
- Contact Information,
- Gender,
- IM(Chat) Address

Authentication data:

Required for login to services and systems by users, administrators

User based credentials such as certificates, PWs, PINs for authentication on systems

- Account names for GUI access,
- passwords,
- PINs,
- user passwords/credentials,
- SIP digest password

Data Access/Data Use

The OpenScape Clients (Web Client, Fusion for Office, Fusion for Notes, Mobile Clients) use the above data for Login/Display purposes.

Data Export

Currently the above data can be available in a database export. The data are exported in .csv files and the information is collected for all users. The system administrator can retrieve from this file the information that is related to one user. Further processing from the system administrator is required in order the data are presented in a readable format before they are delivered to the user.

Data Transmission

During operation, the above data are transmitted between UC and Clients for the realization of the desired functions. Additionally, these data are exchanged between UC Clients and other products that are part of the OpenScape Solution (OSV, 4K, UC, Xpressions,

DLS, LDAP). For this purpose, different interfaces and protocols are used. A detailed list of the protocols and security guidelines can be found in the product Security Checklist (the link can be found in par. 9.2).

Backup/Restore

All the above mentioned data are part of the Backup/Restore Functionality.

JCE (Java Cryptography Extensions) is used to implement a cryptographic mechanism for the Backup/Restore using symmetric algorithms.

More specifically AES with 128 bit key in CBC mode with PKCS#5 padding is being used for the encryption of backup sets.

Data Deletion

Personal Data can be deleted from the Admin of the UC system with manual actions: In more detail:

Master data: Any data may be deleted via Administrator's actions using the UI or API (SPML).

Trace data: Any data may be deleted via Administrator's actions using the UI or access to the file system.

Authentication data: Any data may be deleted via Administrator's actions using the UI or API (SPML).

Backup data: Backup data can be deleted via Administrator's actions using the UI or access to the file system. Also a max number of backups can be configured after which old backups are deleted.

The deletion of personal data from backups can be done via the following sequence of actions:

- Restore the backup, perform the delete action and then perform the backup again.

- Perform the delete action, create a new backup and delete any old backups.

Data Modification

Adding, modifying and deleting personal data, considered as master data, can be performed in the following ways: Admin actions through the UI, API (SPML) requests, by syncing with other Element Managers

Data Retention

For master data, there is no pre-configured data retention period, simply because any deletion of data will immediately mean that the user/device/endpoint will be out of service. Deletion of data may be performed via Administrator's actions using the UI or API (SPML).

3.2. OpenScape Web Collaboration

An OpenScape UC installation can be configured with a Web Collaboration solution. This is a sub-system that is also available on standalone mode. Please refer to 9.3 “Technical and Organizational measures” document provided by FastViewer GmbH.

4. Data Collection during Operation (Traffic Data)

4.1. OpenScape UC Clients

The client applications and UC subscribers of OpenScape UC can also individually process further personal data in their client applications.

User Related Data

- Caller Lists
- Journal Data
- Presence Status
- Contacts, Groups of Contacts
- Preferred Devices, Device Groups (phone numbers in E.164 or private format)
- Call Forward Destinations
- Rules
- Conference Data
- Chat Data

Traffic data (Call/Communication/Collaboration Detail Recording)

Data that is transmitted and recorded during the communication/collaboration session like:

- Journal Data
- Call Data
- Chat Data

Trace Data

Data that is used for troubleshooting purposes or evaluation of the service quality.

- Trace data that is collected within the systems and be made available on request

- Trace data that is collected centrally (e.g. via the Trace Manager)

- Trace data that is collected by separate tools (e.g. wireshark) for troubleshooting

- Trace data that is collected by OSMO application (iOS/Android)

Log Data

Log data to prove the activities carried out, for example logging of login accesses and login access attempts, logging of changed adding, changing and deleting personal Master Data, etc.

Data to detect attacks and irregularities

Data Transmission

User Related Data/Traffic Data

During operation, the above data are transmitted between UC and Clients for the realization of the desired functions. Additionally, these data are exchanged between UC Clients and other products that are part of the OpenScape Solution (OSV, 4K, UC, Xpressions, LDAP). For this purpose, different interfaces and protocols are used. A detailed list of the protocols and security guidelines can be found in the product Security Checklist (the link can be found in par. 9.2).

Trace data category

Trace Data files sent to SESAP using SFTP - includes personal data in the form of Telephony DN(s), Calling Name for problem analysis. Personal data may be under go pseudonymization by obfuscation utilities. Data transmitted over encrypted connection using SFTP.

Data Deletion

Personal Data can be deleted from the Admin of the UC system with manual actions: In more detail:

Log data: Audit logs cannot be deleted from the UI. Audit logs functionality offers the ability to configure a specific period of time after which the audit logs will be deleted/overwritten.

Backup data: Backup data can be deleted via Administrator's actions using the UI or access to the file system. Also a max number of backups can be configured after which old backups are deleted.

Chat Data: If Chat History and Archiving is not activated the data are not saved. When Chat History and/or Archiving is activated, the deletion of the chat data is a subject of another legislation and should not be deleted. For example, the messages of a user that has participated in a conversation and has requested the erasure of his personal data will not be deleted for the archiving period. If another user retrieves chats that had the deleted user as participant, the IM address of the deleted user is shown.

Conference Recording data: In case a conference recording is activated the recording in stored in the system and may be deleted ad hoc or after a specified amount of days by the system administrator.

Backup data: Backup data can be deleted via Administrator's actions using the UI or access to the file system. Also a max number of backups can be configured after which old backups are deleted.

There is no easy procedure to easily delete personal data from backups. Possible workarounds:

- Restore the backup, perform the delete action and then perform the backup again.

- Perform the delete action, create a new backup and delete any old backups.

Data Modification

Adding, modifying and deleting personal data, considered as master data, can be performed in the following ways: Admin actions through the UI, API (SPML) requests, by syncing with other Element Managers

Data Retention

- Data regarding IM messages (chats): By default, Chat History and Archiving in Openfire are not activated. Customers can activate on their wish with the required retention period. By default the chat history is kept for 365 days and users can retrieve their chat messages for the last 14 days.
- User related data (Traffic data) can be deleted also from the user themselves (apart from chat data) from the Clients' UI.
- Conference Recording data: In case a conference recording is activated the recording in stored in the system and may be retained for specified amount of days by the system administrator.

4.2. OpenScape Web Collaboration

An OpenScape UC installation can be configured with a Web Collaboration solution. This is a sub-system that is also available on standalone mode. Please refer to 9.3 “Technical and Organizational measures” document provided by FastViewer GmbH.

5. Display of Personal Data on Clients

The personal data collected in OpenScape UC serves to support the user in his business processes. For this purpose, the data is displayed on the telephone devices/clients of the OpenScape UC 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 himself.

Personal data can generally be displayed in the subsequent functions of the telephone devices or the UC clients.

- Call History
- Conference list
- Contacts/Directory
- Chat history
- Voicemail
- Devices
- User profile

5.1. OpenScape UC Clients

All OpenScape UC clients (including OpenScape UC web client, OpenScape Mobile and OpenScape Fusion for Office and OpenScape Fusion for Notes) display the following data categories and fields as available on the OpenScape UC system.

- Call History
  - Called/calling party First Name, Last Name
  - Contact picture
  - Phone number
  - Date/Time call started
  - Call duration
  - User Presence State

- Contacts
  - First Name, Last Name
  - Company
  - Department
  - Location
  - Work Phone
  - Mobile Phone
  - Home Phone
  - Video
  - Work e-mail
  - Chat (IM address)
  - Time zone
  - User Presence State
  - Phone media State

These are the standard attributes of the Contact Data that are shown to the user. Additional data can be shown after retrieval from external servers (like Domino, Microsoft Exchange, LDAP)

- Conferences
  - Conference Bridge Number
  - Conference PIN
  - Participant list

    - Devices
    - Contact Name
    - Address (the phone number of the contact)

- Chat History
    - Participants' names
    - Text Message
    - Date/Time

- Voice mail (not available in OpenScape Mobile)
    - Participant's name
    - Voice Message
    - Date/Time

- User profile
    - User picture
    - First name,
    - Last name
    - Work phone number
    - Mobile Phone
    - Personal email
    - Work email
    - Location,
    - Presence status text and state

- Other Devices
    - Device name
    - Phone number

5.2. OpenScape Fusion for Office and for Notes clients

Beyond the common data displayed in all OpenScape UC clients Fusion clients contain additional settings:

- System User name
- User Password

5.3. OpenScape Mobile Clients (Android, iOS)

Beyond the common data displayed in all OpenScape UC clients OpenScape mobile clients contain additional settings:

- System User name or Phone number
- User Password

5.4. OpenScape Web Collaboration client

An OpenScape UC installation can be configured with a Web Collaboration solution. This is a sub-system that is also available on standalone mode. Please refer to 9.3 “Technical and Organizational measures” document provided by FastViewer GmbH.

6. Transmission of Personal Data (Data on Move)

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

Further information on securing the transmission paths and the transmission protocols used etc. can be found in the OpenScape UC Security Checklist. (see chapter 9.1)

6.1. Transmission between Clients/Telephone Devices and System

Personal data can be transferred to implement the OpenScape UC functions between telephone devices and application clients. 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 transmission of personal data between the devices and system can be encrypted depending on the device/client/settings used.

6.2. Transmission to external Applications

Personal data can also be transferred to an external application for further processing. The data is transmitted either online via a system interface or offline via a file interface.

6.2.1. Online transmission

Data that can be transferred online are:

- Personal data displayed in OpenScape UC clients (Mobile, web and desktop), as described in paragraph 5.1.
- Master data, authentication and presence and user related data can be exchanged between UC Clients and other Products V, H4K, SBC, Xpressions etc)
- UC account and OSV subscriber details if Fusion client settings are managed via DLS (OpenScape Deployment Service)

6.2.2. Offline transmission

The data that can be transferred offline are

- Depending on the system configuration and customer needs, logs can be sent to an external application like OpenScape Voice Trace Manager -OSVTM using secure protocols like SFTP or SNMPv3.. All other trace/log data contains personal data and are stored unencrypted on the server on an operational system folder. The access will be controlled by the operating system
- Audit/security logs can be sent to external syslog server

7. Recovery of Personal Data

OpenScape UC offers an integrated backup/restore function that allows system Administrators 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.

JCE (Java Cryptography Extensions) is used to implement a cryptographic mechanism for the Backup/Restore using symmetric algorithms.

More specifically AES with 128 bit key in CBC mode with PKCS#5 padding is being used for the encryption of backup sets.

8. Personal Data Retention

8.1. OpenScape UC clients & servers

The personal data acquired by the system administrator in OpenScape UC can also be deleted by the system administrator. Personal data acquired by the user himself in the clients and telephone devices, e.g. user picture, presence status text, personal directory, devices and voicemails can be deleted by users themselves. Exception is the user Master data, IM messages, conference recordings and user trace/log data generated on the OpenScape UC server.

For master data, there is no pre-configured data retention period, simply because any deletion of data will immediately mean that the user/device/endpoint will be out of service. Deletion of data may be performed via Administrator's actions using the UI or API (SPML).

Data regarding IM messages (chats): By default, Chat History and Archiving in Openfire are not activated. Customers can activate on their wish with the required retention period. By default the chat history is kept for 365 days and users can retrieve their chat messages for the last 14 days. The relevant data are stored in the Openfire Database.

User related data (Traffic data) can be deleted also from the user themselves (apart from chat data) from the Clients' UI.
Chat message are not retained on the system by default, when they are retained the retention period is defined by the administrator. By default, it is 12 months. Conference recordings are also retained for a period of time and then deleted automatically or can be deleted by the administrator.

The deletion of personal data always refers to the current system configuration or to the current user configuration. Personal data in system backups and archived files are not deleted.

The system administrator can use the administration tool to delete the data entered by the user/user himself in the system and the data collected by the system during operation for the participant. Excluded from this is personal data OpenScape Xpressions Voicemail

The Xpressions Voicemail subscriber can selectively or completely delete his voicemails via the UC client user interface.

The calls recorded by Xpressions Voicemail application can be deleted by the System Administrator by removing the subscriber's Voicemail Box from the system configuration.

8.2. OpenScape Fusion for Office/OpenScape Fusion for Notes and OpenScape Mobile

In addition to the data retention above, Fusion and Mobile clients maintain UC user account and OSV subscriber details and passwords stored and encrypted.

Fusion user settings are not removed upon client uninstallation. The relevant folders must be manually deleted if the user does not plan to install the client again in the future. (folders:"%AppData%\Siemens\OpenScape" or "%AppData%\Siemens\OpenScape\dlc if settings are retrieved by a DLS server".)

User settings for Mobile applications are deleted however at uninstallation.

The Fusion clients also provide a "voice recording" feature that enables users to record calls on their station OS filesystem. It generates WAV files under "Music\VoiceRecordings". Generated files have the format "VR_yyyyMMdd.HHmmss.wav" and are not encrypted. Once a voice recording file is generated, the user is responsible to handle it.

9. References and Sources

9.1. OpenScape UC Service-/Administrator documentation

OpenScape UC V9, Administrator Documentation
https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/7683ce92-f11e-472b-aa75-88dd2142aa16

OpenScape UC V9 Security Checklist
https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/a4ad53cc-2252-405b-a410-dc6521f2dee3

9.2. User Guides

OpenScape UC WebClient
https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/8ce70579-b44d-48b9-bb16-de299564fe97

OpenScape Fusion for Office
https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/27aa9e57-ed42-49f5-8765-b012e4bbf170

OpenScape Fusion for Notes
https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/70da04a9-255d-47ae-afec-c9bc62e84428

OpenScape Web Collaboration client
https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/996a293f-3270-462d-9516-053b587bece3

OpenScape Mobile V9 iOS
https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/56a9f01b-e68a-417b-9823-c6771f40f96d

OpenScape Mobile V9 Android
https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/pdf/e15eb523-2b9c-4c7c-9ea7-b414bdf7a927

9.3. OpenScape WebCollaboration

EN_General Technical and Organizational Measures_FastViewer GmbH.pdf

unify
atos collaboration solutions