OpenScape Voice Ecosystem

Whitepaper

Processing of Personal Data

Version 0.6

PURPOSE

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 whitepaper is intended to assist Partners in answering technical questions from customers related to the OpenScape Voice Ecosystem and compliance with EU-GDPR requirements. It describes which Client personal data are being collected, processed and transferred by the OpenScape Voice Ecosystem and for what purpose these data are accessed.

The OpenScape Voice Ecosystem consists of:

OpenScape Voice
OpenScape Branch
OpenScape SBC
OpenScape Media Server
OpenScape CMP
OpenScape DLS

This document describes the main functions of OpenScape Voice Ecosystem. 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 Voice Ecosystem Documentation must be used. The documents can be downloaded from 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->Portfolio Information->Solution Suites->OpenScape Voice Ecosystem Version 9

The descriptions in this Whitepaper refer to OpenScape Voice Ecosystem V9R3

During 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, OpenStage and HiPath 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	Author/Editor	Changes / Comments
2018-07-11	0.1	Jeff Engle	Initial creation
2018-07-16	0.2	Joseph Budziak	Added OS Voice information
2018-07-18	0.3	Rick Jezierny	Added OS-Branch and OS-SBC Information
2018-9-5	0.4	Jeff Engle	Converted from OSE to OS Voice Ecosystem and added DLS and CMP based on GDPR Product Assessments in Confluence.
2018-9-13	0.5	Panagiotis Botsaris	Updated CMP and DLS sections
2018-9-25	0.6	Jeff Engle	Consistency edits

1 Introduction

1.1 Fulfilment of EU-GDPR requirements

For the purpose of this document

Controller (Operator) is the customer departments that provide communication and collaboration for employees. Operators will sometimes make changes to the OpenScape Voice Ecosystem software and/or hardware

Processor is the system administrator that makes changes to the OpenScape Voice Ecosystem software and/or hardware

Within a data protection concept the operator (controller) determines which data are collected and where, how, by whom (processor) they are processed. Applying these concepts to OpenScape Voice Ecosystem V9 (or higher) this means:

The customer system administrator (processor) may only collect or release personal data and functions in the system configuration specified by the operator (typically customer departments that provide communications and collaboration to their employees; the Controller). This applies in detail to data of telephone, UC and Xpressions subscribers, as well as contact center and attendant console functions.

During operation, OpenScape Voice Ecosystem can generate and process further personal data. These include but are not limited to: call detail records (CDR), caller lists or journal data, presence status. The telephone and UC subscribers of OpenScape Voice Ecosystem can also individually process further personal data in their telephone devices and clients. e.g. Speed dialing destinations and personal directories / contacts.

The operator (controller) of OpenScape Voice Ecosystem must be informed by the system administrator (processor) so that they can take these functions into account : For example, the operator tells the administrator to setup collaboration between two employees: the system administrator must inform the Operator (controller) that this involves personal data that must be protected..

OpenScape Voice Ecosystem 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 Voice Ecosystem is also possible without the use of personal or pseudo-anonymized 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 Voice Ecosystem product-specific Declaration of Conformity is not provided for the reasons shown above.

2 Processing of Personal Data in OpenScape Voice Ecosystem

OpenScape Voice Ecosystem is a communications solution built around the high-performance OpenScape Voice (OSV) telephony application. No Sensitive personal data is used by the OpenScape Voice Ecosystem.

The OpenScape Voice Ecosystem uses personal data in addition to pure telephone numbers to offer users the desired scope of service on the telephones.

Only personal data necessary for OpenScape Voice Ecosystem operation in conducting normal business operation are used. No Sensitive personal data is used. The use of personal data is optional but not mandatory for the overall function of OpenScape Voice Ecosystem. If no personal data is used, functions such as dialing from phonebook or caller identification are not possible.

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

OpenScape Voice Ecosystem 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 and authenticated system administrator who may or may not use an Atos/Unify hosted WebCDC tool.

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

The organization for the product sections is described in the table below.

GDPR Area	**OpenScape Voice Ecosystem Overview (details provided for each product in addition to table)**
1-Data Access by System Administrator (Master Data)	The system administrator collects personal data using the OpenScape WebCDC tool. The system administrator can either manually populate the personal data from WebCDC or can import mass data from other sources into the directories. • The system administrator maintains the personal data in the OSE database through the CMP. The CMP provides role-based secure controller access to the OSE systems and OSE DB. • All CMP controller access is logged. • Attempts to bypass CMP access authentication or violate customer security policies are logged and alarmed.

2-Data Collected during Operation (Traffic Data)	For data collection during operation, a distinction is made between the collections during operation by:
	• OpenScape Voice Ecosystem Voice, SBC and Branch
	• Users of:
	  ○ telephone device
	  ○ client
	• Basic system and applications for diagnostic purposes

3-Display of Personal Data	The personal data collected in OpenScape Voice Ecosystem serves to support the user in his business processes. For this purpose, the data are displayed on the telephone devices / clients of the OpenScape Voice Ecosystem 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.
4-Transmission of Personal Data (Data on the Move)	Personal data are transmitted on the one hand between the OpenScape Voice Ecosystem 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 individual products (OSV, SBC, Branch, etc.) Security Checklist.
5-Recovery of Personal Data	OpenScape Voice Ecosystem offers an integrated backup / restore function that allows 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 the system database can be stored in backup files, saved and, if necessary, restored.

6-Personal Data Retention	The personal data acquired by the system administrator in OpenScape Voice Ecosystem 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, shortcuts, and personal directory can be deleted by users themselves. The deletion of personal data always refers to the current system configuration or to the current client / telephone device configuration as well as to the current personal directories. Personal data in system backups and archived files are not deleted. Personal data (e.g., surname, first name) associated with connection data (CDRs) and the call logs or journals of other users during OpenScape Voice Ecosystem operation are retained after deleting the user in the other users' journals and the connection data (CDR). 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 held directly in a telephone device or in a client. If necessary, these data must be deleted by direct access to the phone device or client.

3 OpenScape Voice

3.1 Data Access by the System Administrator (Master Data)

The OpenScape Voice (OSV) VoIP application is the primary processing entity of personal data within the internal OSV Database (DB).

- Authorized direct controller or processor access to the OSV DB requires the controller or processor be authenticated.
- Authentication utilizes dynamic authentication modules with stringent baseline password rules/policies which may be adapted to meet customer specific security policies.
- Optional Controlled Access Card (CAC) authorization is available.
- All OSV controller access is logged.
- Attempts to bypass or violate dynamic authentication module security policies are logged and alarmed.

Personal data are collected in the basic system configuration when setting up or administered throughout the life of the system.

Only personal data necessary for company normal business operation are used.

Personal data configured in the OpenScape Voice database include:

- Username,
- Telephony DN(s)
- Authorization Code (Administrator assigned for call restriction override)
  Password (Administrator assigned for a user logging in at a phone)

3.2 Data Collection during Operation (Traffic Data)

During operation, OpenScape Voice can collect connection-related data and link it with personal data. This link is made at:

- Collection of Call Data Records (CDR)
- Syslog (used for tracking Administrator Logging information)
- Transient diagnostic trace (RTT) data (used for Unify/Atos service diagnostics)

3.2.1 Call Data Records (CDR)

The call data records contain data about all calls. A Call Detail Record (CDR) is a collection of information for each call that is processed by OpenScape Voice. More complex call scenarios such as transfer, conference, networking, and other OpenScape Voice features may produce multiple CDRs.

OpenScape Voice generates CDRs that include information such as the following:

- Date and time
- Originating telephone number
- Originating telephone name
- Destination telephone number
- Duration of Call
- Carrier identifiers
- Global call identifier, which correlates and combines information from multiple CDRs that pertain to the same call - for example, when a call spans more than one node
- Thread identifier, which correlates separate calls that are part of a complex call scenario - for example, when a call is transferred
- IP address or FQDN (Fully-Qualified Domain Name) / location domain name
- Other related information (i.e. Account Codes, Authorization Codes, alerting time, etc.)

In the call data records, no sensitive personal data is recorded, apart from the internal subscriber name and number.

3.2.1.1 Storage

The collected call data records are stored in the OpenScape Voice System Hard Disk.

3.2.1.2 Data Access / Data Use

Passwords for the OpenScape Voice CLI (Command Line Interface) login are stored encrypted within the Linux OS.

Application-level passwords for transferring CDRs (Call Detail Records) from the OpenScape Voice server to the billing mediation server are stored via two-way encryption within the OpenScape Voice database.

3.2.1.3 Data Export

The CDRs (Call Detail Records) are first stored on the local hard drive and are then pushed to or pulled from a billing server (for example, OpenScape Voice Accounting Management or a third-party billing application) which post-processes the CDRs.

3.2.1.4 Data Transmission:

The type of file transfer protocol depends on the entity that initiates the CDR transfer:

- If OpenScape Voice initiates CDR transfer (also known as file transfer by push), FTP is used.
- If the billing server initiates the transfer (also known as file transfer by pull), either FTP or, if the billing server supports it, SFTP (Secure FTP) can be used.

FTP connections can be protected with IPsec if the billing server supports it.

3.2.1.5 Backup / Restore

The call data records are not part of the OpenScape Voice Ecosystem backup.

Call Data Records may be backed up if the billing server supports the function.

3.2.1.6 Data Retention / Modification / Deletion

After they are pushed to the billing server, the files can be:

- Deleted immediately
- Saved, then automatically deleted after a specified retention period
- Saved until the system administrator manually deletes them.

Operator (Controller) defines the retention period, The System Administrator (Processor) makes the needed changes to configure the retention period as instructed by the Operator.

The system administrator cannot use its system administration tools to selectively delete or delete call data records.

3.3 Display of Personal Data

For OpenScape Voice, personal data are displayed on the telephone devices. These are covered in their own section in this document.

3.4 Transmission of Personal Data (Data on the Move)

3.4.1 Transmission between Telephone Device / Client and System

Personal data can be transferred to implement the OpenScape Voice functions between telephone devices and application clients. Here, personal information such as 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 are used.

The transmission of all data between the devices and system can be encrypted (SRTP/TLS) depending on the device / client used.

3.4.2 Transmission to external Applications

Personal data can also be transferred to an external application for further processing.

The transmission of all data between the system and the application can be encrypted application used.

- SIP (TLS) - Signaling to subscribers, network interfaces and applications
- RTP /SRTP – Media to subscribers and network interfaces
- CSTA monitoring (TLS) – Signaling to applications (i.e. user presence)
- Billing (CDR) (SFTP)
- MGCP (IPSec) – Signaling to the Media server
- Inter-node X-Channel (secured via IPsec) – n/a
- Inter-node Database transfer (FTP)
- SOAP-XML (TLS)
- SSH-CLI (opt. CAC)
- Remote Admin (SFTP)
- Trace Data files (RTT) (SFTP)
- SNMP traps – n/a
- DNS C/S – n/a
- NTP – n/a

* n/a - personal data does not apply, otherwise secured as noted

3.4.3 Data acquisition for diagnostic purposes (Syslog and Call Trace)

OpenScape Voice and the integrated applications provide diagnostic mechanisms that store log and trace files in the system. These files may also contain personal information.

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

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

3.4.3.1 Data Storage

The collected data is stored on the OpenScape Voice System Hard Disk.

3.4.3.2 Data Access / Data Use

Access to traces and logs is only possible for the system administrator or if allowed by Unify Service and development. Traces and logs are used for system diagnostics in the event of an error.

3.4.3.3 Data Export

The export of trace log files can only be done by the system administrator or if allowed by Unify Service and development via the administration access of the system.

3.4.3.4 Data Transmission

Traces / logs are transferred via SFTP.

3.4.3.5 Backup / Restore

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

3.5 Recovery of Personal Data

Refer to the OpenScape Voice Ecosystem Overview table.

3.6 Personal Data Retention

After they are pushed to the billing server, the files can be:

- Deleted immediately
- Saved, then automatically deleted after a specified retention period
- Saved until the administrator manually deletes them.

Operator (Controller) defines the retention period, The system Administrator (Processor) makes the needed changes to configure the retention period as instructed by the Operator.

The system administrator cannot use their system administration tools to selectively delete or delete call data records.

4 OpenScape Desk Phones and Software Phones

4.1 Data Access by the System Administrator (Master Data)

The system administrator records personal data using the OpenScape Deployment Service (DLS) or OpenScape Common Management Platform (CMP) administration tools. The configuration distinguishes between:

- Basic system configuration
- Configuration of other OpenScape products (optional)

Furthermore, the system administrator can either populate manually the Speed Dials Lists or the Global Directory with personal data or can import mass data from other sources into the directories.

4.2 Data Collection during Operation (Traffic Data)

4.2.1 Caller Lists

Depending on the telephone device used, call lists, journals or conversations are stored directly in the telephone device. These may include personal information.

Person related data	System devices TDM								System devices HFA												Unify SIP devices											
Recording in operation	OpenStage T								OpenStage HFA					OpenScape			OpenScape				OpenStage SIP						OpenScape			OpenScape			
Call lists / Journals / Conversations	10	15	20	30	40	60	80		15	20	40	60	80	35G	55G		200 205	400	600		5	15	20	40	60	80		35G	55G		200 205	400	600	
In device																																	
Last name												■	■		■			■	■					■	■	■		■	■		■	■	■	
First name												■	■		■			■	■					■	■	■		■	■		■	■	■	
Caller number												■	■		■			■	■					■	■	■		■	■		■	■	■	
# of Calls												■	■		■			■	■					■	■	■		■	■		■	■	■	
Date / Time												■	■		■			■	■					■	■	■		■	■		■	■	■	

FIGURE 1 - PERSONAL DATA IN CALLER LISTS OF TELEPHONE DEVICES

The call logs stored in the Unify telephone devices of the current product portfolio are shown in the figure above. For unlisted Unify telephone device or for phone devices of other manufacturers, it is to be seen from the respective operating administration manuals whether and what data is stored in the device.

4.2.1.1 Data Access / Data Use

Access to and management of the caller lists stored in the devices are made by subscribers from their telephone or via the phone manager or via a web server if the terminals support it.

4.2.1.2 Data Export

Whether and how the entries stored in the telephone can be exported can be found in the respective operating instructions.

4.2.1.3 Data Retention / Modification / Deletion

The system administrator cannot delete or change specific lists or entries in the caller lists with its administration tools. The caller lists of a subscriber remain in the telephones even if the system administrator deletes the subscribers in the basic system configuration of OpenScape Voice Ecosystem.

Whether and how data in the subscriber-specific caller list can be changed or deleted by an operating procedure on the telephone or by a corresponding tool depends on the telephone used. For details, refer to the respective operating instructions of the telephone.

4.2.1.4 Data Transmission:

There is no transmission of the stored entries in the caller list between the system and the telephone.

4.2.1.5 Backup / Restore

The telephone book entries individually stored in the terminals are not part of the system backup. Whether the entries can be saved in telephone specific backups can be found in the respective operating instructions.

4.2.1.6 Data Storage

The caller lists are stored in the devices

4.2.2 Telephone user

A telephone subscriber can store individual telephone numbers from his telephone device. Depending on the device, these are stored either in the OpenScape Voice Ecosystem System or directly in the device.

4.2.2.1 Call number storage in the system

The system can store up to 10 call number entries per subscriber with up to max. 25 digits plus directional code.

A link to personal data in the system takes place only if a speed dial destination of the system for which a name entry exists is programmed as destination. In this case, the name of the destination is displayed on system devices with "Self-Labeling Keys".

4.2.2.2 Destination call number storage in the telephone device

The telephone devices connected to OpenScape Voice Ecosystem allow the subscriber to store individual speed dial destinations in the device. This option depends on the device used. The data stored in the terminals is not stored in OpenScape Voice Ecosystem.

4.2.2.3 Subscriber-specific phonebook / directory in the telephone device

Depending on the device used, an OpenScape Voice Ecosystem subscriber can also manage a personal directory in his device.

Person related data Acquisition by subscriber: Personal phone book	System devices TDM								System devices HFA													Unify SIP devices													
	OpenStage T								OpenStage HFA					OpenScape Desk Phone IP			OpenScape Desk Phone CP				OpenStage SIP							OpenScape Desk Phone IP				OpenScape Desk Phone CP			
	10	15	20	30	40	60	80		15	20	40	60	80	35G	55G		200 205	400	600		5	15	20	40	60	80		35G	55G			200 205	400	600	
In device																																			
Last name		■	■	■	■	■	■			■	■	■	■	■	■		■	■	■			■	■	■	■	■		■	■			■	■	■	
First name		■	■	■	■	■	■			■	■	■	■	■	■		■	■	■			■	■	■	■	■		■	■			■	■	■	
Business 1		■	■	■	■	■	■			■	■	■	■	■	■		■	■	■			■	■	■	■	■		■	■			■	■	■	
Business 2						■	■					■	■		■			■	■						■	■			■				■	■	
Mobil						■	■					■	■		■			■	■						■	■			■				■	■	
Privat						■	■					■	■		■			■	■						■	■			■				■	■	
Company																		■	■														■	■	
Picture						■	■					■	■		■			■	■						■	■			■				■	■	
Address 1						■	■					■	■		■			■	■						■	■			■				■	■	
Address 2																		■	■														■	■	
Function						■	■					■	■		■			■	■						■	■			■				■	■	
E-Mail																		■	■														■	■	

FIGURE 2 TELEPHONE DEVICE – PERSONAL DIRECTORY

Data Storage

The data recorded in the telephone devices is not stored in OpenScape Voice Ecosystem.

Data Access / Data Use

The user manual of the device must be consulted to determine if and how the access to the data stored in the telephone device is possible.

Data Export

Whether a data export is supported by the device can be found in the operating instructions of the device.

Data Transmission:

The user manual of the device must be consulted to determine if and how a data transfer of personal data is supported by the device.

Backup / Restore

Whether and how data backup can be performed by the device and how data can be restored can be found in the operating instructions of the device.

4.3 Display of Personal Data

At the telephone devices with display personal data are displayed depending on the equipment of the devices:

- Caller Identification
  - Telephone number, name first name from internal / external directories
- Caller list
- Phone book
- Speed dial key with labeling field
- Key module / busy lamp field with labeling field

4.4 Transmission of Personal Data (Data on Move)

Person-related data is transmitted on the one hand between the OpenScape Voice Ecosystem 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 Voice Security Checklist.

4.4.1 Transmission between Telephone Device / Client and System

Personal data can be transferred to implement the OpenScape Voice Ecosystem 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 are a priority.

The transmission of personal data between the devices and system can be encrypted depending on the device / client used.

4.5 Recovery of Personal Data

OpenScape Voice Ecosystem offers an integrated backup / restore function using the CMP that allows 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.

4.6 Personal Data Retention

Personal data that has been recorded in directories, journals and conversations of a telephone device can be deleted by the user via the user interface of the telephone device.

Before exchanging a telephone device, the personal data possibly stored in the telephone device may have to be deleted by re-initializing (reset) the telephone. This can be done by the system administrator or by the user himself depending on the telephone device. Information on this can be found in the respective operating instructions.

4.6.1 Caller lists

When deleting or changing caller lists that are displayed in terminals, a distinction is made in:

- System led caller lists
- Telephone led caller lists

4.6.1.1 System led caller lists

The caller lists can be deleted by the via the telephone user interface. The system administrator cannot delete or change specific lists or entries in the lists.

System-controlled caller lists of subscribers are completely deleted if the subscribers are deleted by the system administrator in the basic system configuration.

4.6.1.2 Telephone led caller lists

Whether and how data in terminal lists managed by telephone devices can be changed or deleted by an operating procedure on the telephone or by a corresponding tool depends on the telephone used. For details, refer to the respective operating instructions of the telephone.

The system administrator cannot delete or change specific lists or entries in the caller lists with his administration tools. The caller lists of a subscriber remain in the telephones even if the system administrator deletes the subscribers in the basic system configuration of OpenScape Voice Ecosystem.

5 OpenScape Branch

5.1 Data Access by the System Administrator (Master Data)

The OpenScape Branch (OSB) VoIP application provides survivability functions at the remote branch-office level. During normal operation, the OpenScape Voice provides all call handling functions for users connected to the OpenScape Branch; the OSB only contains non-sensitive personal information such as user names, directory numbers and IP addresses necessary to support call handling when the link to the OpenScape Voice is out of operation.

- Authorized direct controller or processor access to the OSB DB requires the controller or processor be authenticated.
- All OSB controller access is logged.
- Attempts to bypass or violate dynamic authentication module security policies are logged and alarmed.

Personal data is collected in the basic system configuration when setting up or administered throughout the life of the system.

Only personal data necessary for company normal business operation is used.

Personal data configured in the OpenScape Branch database includes:

- Username,
- Telephony DN(s)

5.2 Data Collection during Operation (Traffic Data)

During normal operation, the OpenScape Branch does not generate Call Data Records (CDRs) but relies on the OpenScape Voice to do this. When in stand-alone/survivability mode, the OSB does generate CDRs, but containing only a subset of the fields that are contained in OSV CDRs. The OSB generated CDRs can be delivered via sFTP to an external recording node.

The OpenScape Branch also collects and stores data for diagnostic purposes, similarly to what is done for the OpenScape Voice as described in section 4.1.2 above.

5.3 Display of Personal Data

For OpenScape Branch, personal data are displayed on the telephone devices. These are covered in their own section in this document.

5.4 Transmission of Personal Data (Data on the Move)

Transmission of data from the telephone/client to the OpenScape Branch takes places in a manner like what is described above for the OpenScape Voice. In normal mode, the OSB is in the path between the telephone device/client and the OpenScape Voice. This data is transmitted only in support of setting up, configuring and releasing telephone calls. Here, also, the transmission of this data can be encrypted.

Transmission of data to external applications for the OpenScape Branch is also like that described above for the OpenScape Voice, with the exception that there are no CSTA or inter-node connections. Data on these interfaces can be encrypted as well.

5.5 Recovery of Personal Data

Refer to the OpenScape Voice Ecosystem Overview table.

5.6 Personal Data Retention

Refer to the OpenScape Voice Ecosystem Overview table.

6 OpenScape SBC

6.1 Data Access by the System Administrator (Master Data)

The OpenScape SBC performs firewall and proxy functionalities and does not contain any personal information in its configuration data. No user names or single directory numbers are stored.

6.2 Data Collection during Operation (Traffic Data)

The only data collected by the SBC during operation is trace data to be used for performance analysis and problem resolution purposes. This data is stored in local text and log files and is also transferred in some cases to the Trace Manager.

6.3 Display of Personal Data

For OpenScape SBC, personal data is displayed on the telephone devices. These are covered in their own section in this document.

6.4 Transmission of Personal Data (Data on the Move)

As the OpenScape SBC performs only firewall and proxy functions, any transmission of personal data by the SBC is under the control of another node, such as the OpenScape Voice or a phone device.

6.5 Recovery of Personal Data

6.6 Personal Data Retention

The only personal data retained in the SBC would be in the form of call trace data taken by the SBC for debugging or problem resolution purposes. This data potentially contains user names, directory numbers and IP addresses that were contained in signaling messages handled by the SBC (but originating at other nodes, such as IP telephones or the OpenScape Voice). These data files are retained on the OpenScape SBC until deleted by the system administrator or over-written by newer data files.

7 OpenScape CMP

7.1 Data Access by the System Administrator (Master Data)

Common Management Platform (CMP) and CMP User Management application is the main administration tool of the OSV ecosystem and is the main processing entity of user personal data within its DB.

- Authorized direct controller or processor access to the CMP DB requires the controller or processor be authenticated.
- CMP offers customizable password policy for its users. Authentication utilizes dynamic authentication modules with stringent baseline password rules/policies which may be adapted to meet customer specific security policies.
- CMP provides role-based secure controller access to the OSV eco-system. Roles can be configured to have add/modify/delete/search/view rights to different CMP configuration pages in the UI.
- Two-factor, Controlled Access Card (CAC) authorization is available.
- All CMP controller access is logged.
- Attempts to bypass or violate dynamic authentication module security policies are logged.
- Any audit/security logs and alarms can be reported to an external syslog server.

Only personal data necessary for System administration, User Management and normal business operation is used. Master Data are used for OpenScape users' configuration management

User related Configuration Data - Provision of the offered telephony functions are stored in the Communication & Collaboration system environment, these include:

- First/Last Name, User IDs, E-Mail Address, Telephone Numbers, Location/Address data, Contact Information, Gender
- Trace Data: Most of the Master Data are included in the system traces
- Authentication Data: Account names for GUI access, passwords, PINs, user passwords/credentials, SIP digest password
- Log Data: Audit logs contain: Username, IP Address, Timestamp, Action
- Backup data: All previously mentioned system/user data

7.2 Data Collection during Operation (Traffic Data)

No Traffic Data are collected or processed in CMP

7.3 Display of Personal Data

The personal data stored in the CMP (see 7.1 above) are displayed in the CMP User Interface, only to those individuals/controllers that are authorized for this access (see 7.1 above for more details).

7.4 Transmission of Personal Data (Data on the Move)

Categories of Data "On Move": Master data, Authentication data, Log data.

All data on the move is secured when signaled or sent to other platforms to prevent eavesdropping, masquerading attacks, unlawful destruction or modification.

Any personal data “On Move” is protected by using secure encryption in all interfaces (HTTPS, TLS V1.2, LDAPS).

7.5 Recovery of Personal Data

CMP offers complete Backup/Restore functionality through the UI.

In the event of an error, the CMP system configuration and the personal data can be restored from a CMP DB backup.

Please refer also to the OpenScape Voice Ecosystem Overview table.

7.6 Personal Data Retention

There is no pre-configured personal 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).

No automatic procedure to delete personal data from data subjects from the system is implemented. Only manual actions can be performed.

- 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).
- Log data: Audit logs cannot be deleted from the UI. Audit logs functionality offers the ability to configure a specific period 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 maximum number of backups can be configured after which old backups are deleted.

Please refer also to the OpenScape Voice Ecosystem Overview table.

8 OpenScape DLS

8.1 Data Access by the System Administrator (Master Data)

The Deployment Service (DLS) application is the management application of the Desk Phones and Soft Clients of the OS Voice Ecosystem and the only processing entity of user personal data within its database (DB).

- Authorized direct controller or processor access to the DLS DB requires the controller or processor be authenticated.
- DLS offers customizable password policy for its users. Authentication utilizes dynamic authentication modules with stringent baseline password rules/policies which may be adapted to meet customer specific security policies.
- DLS provides role-based secure controller access to all the configuration parameters and therefore to any personal data that are stored in the system. Roles can be configured to have add/modify/delete/search/view rights to different DLS configuration pages in the UI.
- Two-factor, Controlled Access Card (CAC) authorization is available.
- All DLS controller access is logged.
- Attempts to bypass or violate dynamic authentication module security policies are logged.
- Any audit/security logs and alarms can be reported to an external syslog server.

Only personal data necessary for company's IP Device/Soft Clients management in conducting their normal business operation is used. These include:

- Phone numbers, IP address, MAC address, Windows Username, Computer name, Email address, Windows Account – E.164 mapping, Terminal Name, Display ID, Terminal Host Name/WEB Name, Reg Subscriber Number and password, UserID, password, LDAP Data (39 in count, First Name, Surname, Postal Code, Room, Country, Mail 2, Private Phone 2…,), Name and Address of internet page, Dep, Accounting, Retailer, Billing ID
- Trace Data: All attributes are included in the DLS traces. Traces and logs of the phones are uploaded to DLS
- Authentication Data: Account names for GUI access, DLS user names, passwords, User/client Certificates, Phone's Admin and User password, Mobile User PIN, Security PIN, Cloud PIN, EAP-TLS, PEAP, EAP-FAST, LEAP credentials, SIP digest UserID, realm and password, Connection credentials (Windows SSO or WIN authentication), Instant messaging credentials
- Log Data: All audit/security/activity/error logs contain: Username, IP Address, Timestamp, Action, Detail/Content of Action, Result
- Content Data: Mobile User Unmanaged Data (Call Log, Phone Book, Screen savers, Ringtones)
- Backup data: All previously mentioned system/user data, Archive of Devices / Mobile users

8.2 Data Collection during Operation (Traffic Data)

No Traffic Data are collected or processed in DLS

8.3 Display of Personal Data

The personal data stored in the DLS (see 8.1 above) are displayed in the DLS User Interface, only to those individuals/controllers that are authorized for this access (see 8.1 above for more details).

8.4 Transmission of Personal Data (Data on the Move)

Categories of Data "On Move": Master data, Trace Data, Authentication data, Log data, Content Data

All data on the move is secured when signaled or sent to other platforms to prevent eavesdropping, masquerading attacks, unlawful destruction or modification.

Any personal data “On Move” is protected by using secure encryption in all interfaces (HTTPS, TLS V1.2, LDAPS).

8.5 Recovery of Personal Data

The DLS application is fully redundant supporting high availability access to personal data stored in the DLS DB. In the event of DLS system unavailability, the DLS system can be restored from a DLS DB backup to gain access to personal data.

Please refer also to the OpenScape Voice Ecosystem Overview table.

8.6 Personal Data Retention

There is no pre-configured personal 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, API or CLI (local).

No automatic procedure to delete personal data from data subjects from the system is implemented. Only manual actions can be performed.

- Master data: Any data may be deleted via Administrator's actions using the UI, API or CLI (local).
- 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, API or CLI (local).
- Log data: Audit logs cannot be deleted from the UI. Audit logs functionality offers the ability to configure a specific period after which the audit logs will be deleted/overwritten.
- Content data: Any data may be deleted via Administrator's actions using the UI, API or CLI (local).
- 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.

Please refer also to the OpenScape Voice Ecosystem Overview table.

9 References and Sources

9.1 OpenScape Voice Ecosystem Service- / Administrator Documentation

OpenScape Voice Ecosystem V2, Administrator Documentation

OpenScape Voice Ecosystem Security Checklist

9.1.1 Telephone Devices

OpenScape Desk Phone CP600 HFA (OpenScape Voice Ecosystem), User Guide

OpenScape Desk Phone IP 55G HFA V3 (OpenScape Voice Ecosystem), User Guide

OpenScape Desk Phone IP 55G SIP V3 (OpenScape Voice Ecosystem), User Guide

OpenStage 10 T (OpenScape Voice Ecosystem/HiPath 3000), User Guide

OpenStage 15 HFA (OpenScape Office/OpenScape Voice Ecosystem/HiPath 3000), User Guide

OpenStage 15 T (OpenScape Voice Ecosystem/HiPath 3000), User Guide

OpenStage 20 T (OpenScape Voice Ecosystem/HiPath 3000), User Guide

OpenStage 30 T (OpenScape Voice Ecosystem/HiPath 3000), User Guide

OpenStage 40 T (HiPath 3000/OpenScape Voice Ecosystem), User Guide

OpenStage 60/80 T (OpenScape Voice Ecosystem/HiPath 3000), User Guide

9.1.2 Other Clients

OpenScape Voice Ecosystem, OpenScape Voice Ecosystem Attendant, User Guide

OpenScape Voice Ecosystem, Application Launcher, User Guide

OpenScape Voice Ecosystem, myPortal for OpenStage, User Guide

unify
atos collaboration solutions