Personal Data Protection features in SAP Contact Center for version 7.0.12.0

Contents

1. Security related terms 2
2. Privacy Statement and Data Protection Officer 3
Privacy Statement 3
Data Protection Officer (DPO) 3
3. Sensitive Personal Data 4
Call Recordings 4
4. Deletion of Personal Data 4
Data Deletion on Request 5
Blocking 5
5. Logging Changes to Personal Data 5
6. Customer Consents 5
Customer Consent for Saving Personal Data 6
Inbound Queue Calls and IVR Calls 6
Call Recording 6
Inbound Direct Calls 6
Inbound E-Mails 6
Inbound Web Chats 7
Inbound SMS Messages 7
Outbound Campaigns 7
7. Generating Personal Data Report 7
Prerequisites 7
Generating Personal Data Report 7
User interface 8
Personal Data 9
Personal Data in Diagnostic Logs 10

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. This SAP document describes the specific features and functions that SAP provides to support compliance with the relevant legal requirements and data privacy.

This document do not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to additional features that would be required in a particular environment; decisions related to data protection must be made on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

Note!

In the majority of cases, compliance with data privacy laws is not a product feature.

SAP software supports data privacy by providing security features and specific data-protection-relevant functions such as functions for the searching and deletion of personal data.

SAP does not provide legal advice in any form. The definitions and other terms used in this guide are not taken from any given legal source.

1. Security related terms

Glossary Term	**Definition**
Personal data	Information about an identified or identifiable natural person.
Business purpose	A legal, contractual, or in other form justified reason for the processing of personal data. The assumption is that any purpose has an end that is usually already defined when the purpose starts.
Blocking	A method of restricting access to data for which the primary business purpose has ended.
Deletion	Deletion of personal data so that the data is no longer usable.
Retention period	The time period during which data must be available.
End of purpose (EoP)	A method of identifying the point in time for a data set when the processing of personal data is no longer required for the primary business purpose. After the EoP has been reached, the data is deleted. If restricted part of the data is saved for longer period, hat is, blocked, it can only be accessed by users with special authorization.

Caution

The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

2. Privacy Statement and Data Protection Officer

We strongly recommend that you publish privacy statement on your web page and nominate a person or persons to be Data Protection Officers in your organization.

Privacy Statement

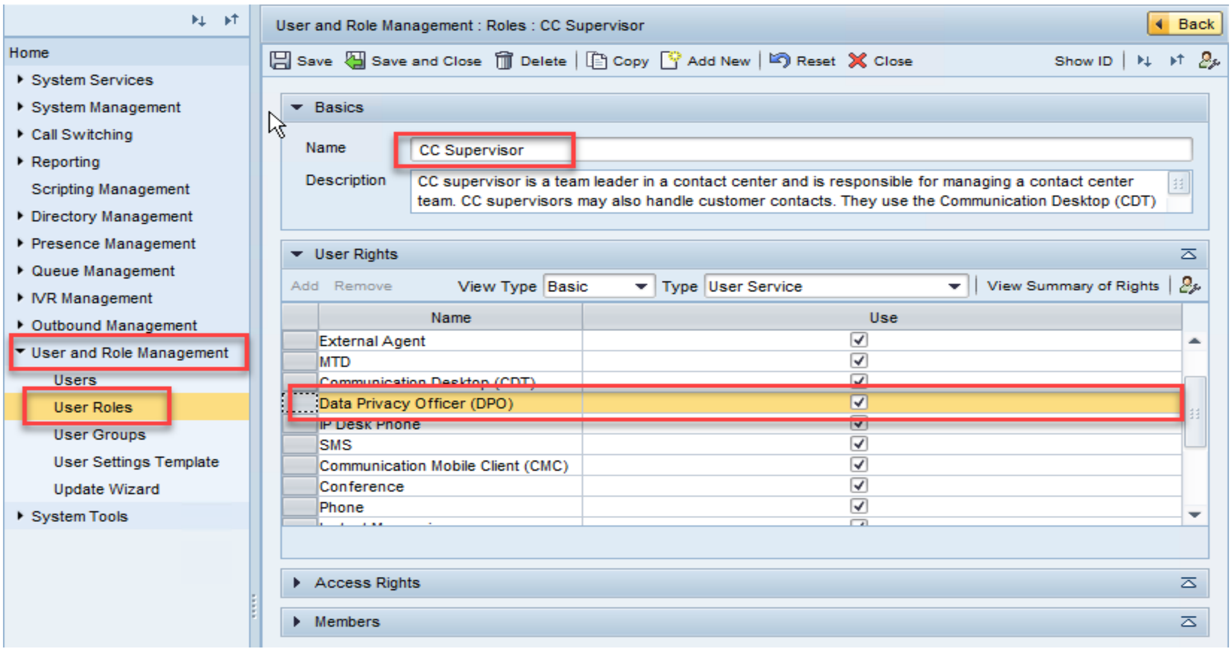
For communicating your security policy both to your customers and your employees, and other people involved, make sure that you have the privacy statement defined, and that it can be accessed by all concerned. Consider defining the following items in your policy:

- What kind of data is saved in the system?
- What is the retention time of the data saved in your system?
- How is this data protected?
- Who is your Data Protection Officer to be contacted if any interest to data protection questions arise?
- How can the people interested in their personal data saved in the system request information about it?

Data Protection Officer (DPO)

Each organization should have a person or persons named to be Data Protection Officer (DPO). The tasks of a DPO include but are not limited to:

- DPO makes sure that should there be any changes in the privacy statement, the customers are informed about it in an appropriate way.
- DPO is a contact person for the customers that request information about the personal data saved about them in the system, and deletion of that data when requested.
- Only DPO can collect a person's personal data, or delete it, on request.
- DPO rights are not included in any default role but user administrators can grant DPO rights in the *|> System Configurator -> User and Role Management -> Users -> User Rights -> User Service -> Data Protection Officer (DPO) <|*. This right enables a user to search and delete personal data with the *Generate Personal Data Report* tool.



User and Role Management : Roles : CC Supervisor

Name: CC Supervisor

Description: CC supervisor is a team leader in a contact center and is responsible for managing a contact center team. CC supervisors may also handle customer contacts. They use the Communication Desktop (CDT)

View Type: Basic
Type: User Service

Name	Use
External Agent	☑
MTD	☑
Communication Desktop (CDT)	☑
Data Privacy Officer (DPO)	☑
IP Desk Phone	☑
SMS	☑
Communication Mobile Client (CMC)	☑
Conference	☑
Phone	☑

3. Sensitive Personal Data

Sensitive personal data is a category of personal data that needs special handling. The definition of what qualifies as sensitive personal data may differ for different legal areas or industries. Sensitive data may, for example, be information on racial or ethnic origin, political opinions, or bank and credit accounts. SAP Contact Center is not designed to store and process sensitive personal data.

This applies specifically for the following SAP Contact Center capabilities:

- Directory fields. Do not use directory fields for collecting or storing any sensitive personal data.
- Scripts. Do not use scripts for collecting any sensitive personal data.
- IVR. Do not use IVR for collecting any sensitive personal data.
- Outbound campaigns. Do not store or collect any sensitive personal data in outbound call list fields.
- Call recordings: Do not use or implement call recording if the calls in your line of business include sensitive topics unless there is a legal obligation to do that.

Call Recordings

Call recordings need to be treated in a special way because of their sensitive nature. SAP Contact Center provides logging of listening of call recordings. A user with rights to listen to a specific call recording leaves a log trace of the event, and additionally can provide an explanation for the listening.

As of earlier version of SAP Contact Center can be configured so that call recording is done only if a caller has given his consent for that (please see the chapter Customer Consents). For emergency or other legal or business cases, it is possible for agents to override this configuration and record a call without customer consent. These occasions can be audit logged.

4. Deletion of Personal Data

System administrator (Prominion employee) defines (according to the agreement with the customer) the data retention time for each contact channel and for handled/expired Outbound campaigns according to end of business purpose. After the retention time all data will be anonymized or deleted automatically. Alternatively, Data Protection Officer (DPO) can on a person's request erase data related to a person.

Anonymizing contact data means that the contact event data will be modified so that the event can no longer be linked with a person. Anonymizing, instead of deleting the contact event, is done to ensure that the contact statistics will show correct numbers.

- Calls: call events are anonymized and the possible call recording is deleted.
- Handled e-mails: e-mail events are anonymized, and the e-mail subject and body are replaced with a `{Anonymized by DPO}` text. Possible attachments are deleted. This applies also for other e-mail type items, such as tasks, and XRI items.
- Chats: chat events are anonymized and the chat transcript is deleted. This applies also for other chat-type sub channels, such as SMS, and Facebook Messenger.
- If there is a script linked with a contact item, the script freetext contents are deleted.
- Completed or expired outbound campaigns:
  - When a retention time expires: the campaign and the corresponding call events are deleted.
  - When deleting data on request: the customer data and call events are deleted in the campaign.
- Directory data and consent information: These items are not removed after retention times but only on request.

Data Deletion on Request

Data Protection Officer (DPO) can create the Personal Data Report and remove all personal data on request. For more information, see Generating Personal Data Report.

Blocking

Blocking means the identification of recorded stored personal data so as to restrict their further processing or use. In the contact center context blocking can be used, for example, in cases where the organization needs to keep contact related data and contents for longer time than otherwise defined in their data privacy policy. Whilst the blocked data shall not be erased, it can be, that it should not appear in any regular data searches.

In this case the DPO will use the Generate Personal Data Report tool to find the relevant personal data, and then collect and store the verified event data, event contents, including possible attachments and call recordings to a Contact Center external storage from where it will be deleted.

To block the data from operative usage (for example to appear in historical search), DPO needs to erase the corresponding data from Contact Center.

5. Logging Changes to Personal Data

SAP Contact Center Audit Logging capability logs changes made to personal data. This applies to changes done via user interfaces like CDT or System Configurator, and as of earlier version of SAP CCtr, also changes done via Import/Export functionality, integration interfaces, or the *Generate Personal Data Report* application.

The audit log contains information of the attribute that was changed, who changed the data, when the data was changed, and what was the new value after change.

6. Customer Consents

It is recommended to capture user content before collecting any personal data. The methods what SAP Contact Center supports, vary in different channels.

A couple of new functions are added to support capturing customer consents:

- When a customer calls a system, it is possible to use a consent IVR to ask permission for recording the call. The consent value (given or denied) can be saved in database for later use. Consents are included in Personal Data Report.
- Customer consents can be imported/exported from an external system. They can also be imported and exported automatically as any configuration item.
- Data Protection Officers can delete a customer's consent information on request with the *Generate Personal Data Report* tool.

Note that:

- If customer consents for call recordings are used in the system, and a customer has not given his consent for recording, the call is reported to *Quality Monitoring Server* but no stream is provided. In that case the call also bypasses SAP system resource reservation for such calls, so media stream will not be routed through system for these calls.
- In CDT, agents may be able to record the call even if the customer has not given permission for the recording if there is an emergency or a threatening situation.

Customer Consent for Saving Personal Data

The capture of the customer consent for saving personal data varies depending on the contact channel.

Generally, when actively contacting an organization by calling in to a specific phone number, sending e-mail to a specific e-mail address, sending SMS to a specific number, or initiating a web chat from an organization's web pages, a customer understands, and thus provides his consent, that his contact data and content will be handled and stored in the system, in this case SAP Contact Center.

It is recommended, that organization informs the customer about collecting personal data in such an occasion. The methods what SAP Contact Center supports, are described below.

Data Protection Officer (DPO) can reset the consent database in case the organization renews its data privacy policy. In such occasion, it is recommended that the DPO exports the consent database and stores it per organization's data protection and privacy policy.

Inbound Queue Calls and IVR Calls

SAP Contact Center enables organizations to define and record the *Welcome* prompt for each phone queue. In the *Welcome* prompt the organization can inform customers about the service to which he has called and also about how organization handles the personal data.

Call Recording

Organization should determine their policy for recording calls. In some industries, there is a legal obligation to record calls, whereas in other organizations the call recordings are needed to fulfill a contract. In these cases using call recording may happen without consent.

In other cases, it is recommended to get a customer's consent prior recording. It is possible to define and activate a consent IVR, where the customer can give a consent for call recording, or deny it.

This consent or non-consent information of a customer can be stored in database, and that information can later on be used for consent reporting as well as for fine-tuning the call handling flow in future calls. Data Protection Officer can reset the consent information in case the organization renews its Data Privacy Policy, or in case customer wants to withdraw his/her consent.

The consent information follows customer's call for the lifetime of the call, either enabling or disabling the call recording accordingly. This means that if the call is transferred to another queue with different consent behavior settings, the settings of the first queue are applied.

Consent configurations affect server-side call recordings, and for emergency, or other legal or business cases, it is possible for agents to override this configuration and record a call without customer consent.

If consents are used, CDT-controlled local call recordings should not be enabled.

Inbound Direct Calls

As there is a policy described for IVR and queue calls, it is not recommended to publish direct extension numbers for inbound customer service but manage all customer calls via queues and IVRs.

Technically, customer consent can be captured with direct inbound calls as well.

Inbound E-Mails

SAP Contact Center enables organizations to define an automatic receipt message for each e-mail queue.

In the receipt message the organization can inform customers about the service to which he has sent the e-mail, and also about how does the organization handle personal data. A good practice is to provide a link to organization's web page where the organization's data privacy statement is published.

Inbound Web Chats

SAP Contact Center enables organizations to define an automatic *Welcome* prompt for each chat queue.

In the *Welcome* prompt the organization can inform customers about the service to which he has initiated the chat and also about how organization handles the personal data. A good practice is to use a link to web page where the organization's data privacy statement is published.

Inbound SMS Messages

SMS message is a subtype of chat. SAP Contact Center enables organizations to define an automatic *Welcome* prompt for each SMS (chat) queue.

In the *Welcome* prompt the organization can inform customers about the service to which he has sent the SMS and also about how organization handles the personal data. A good practice is to use a link to web page where the organization's data privacy statement is published.

Outbound Campaigns

We recommend that organization ensures customer's consent for telemarketing activities prior importing customer data to SAP Contact Center.

7. Generating Personal Data Report

Data Protection Officers (DPOs) can create Personal Data Reports and delete selected data on request with the Generate Personal Data Report tool.

Prerequisites

DPO must have the *Use* rights for the *Data Protection Officer (DPO)* user service.

Generating Personal Data Report

1. **Go to the web page <ECF Web Server address and port>/ecf/<version>/dporeport/index.html.**
2. Log on.
3. Enter customer information into the *Search Criteria* fields. Search uses OR operator.
   - *E-Mail Address*: Enter one e-mail address.
   - *Phone Number*: Enter one phone number.
     The search criterion must be a numeric value and have at least 3 digits.
   - *First Name, Last Name*: To search with the name criteria, define both name fields.
   - *Start Date, End Date*: Define the time span that is used in the search.
   - *Digits Used in Search*: Define how many digits from the end of the phone number are used in the search. The minimum value to be used in search is 3 digits. Before search, spaces and other separating characters are removed from the numbers.
4. Click *Search*.
   If there are more than 1000 items found, the search suggests that you should define criteria more specifically, otherwise handling search results may be difficult and time consuming. You can ignore this suggestion, or return to the criteria page and, for example, produce the report in shorter time spans.
5. The search results appear. To see detailed information of each item, click the > arrow at the right end of the row. To return to the result list, click the < arrow at the upper left corner of the *Search Result Details* view.

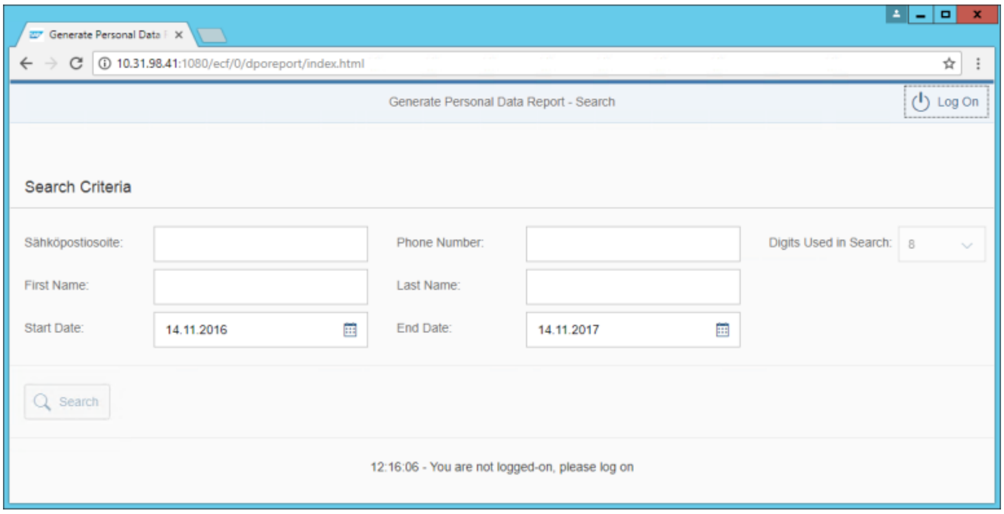
The results include the following groups:

- *Contacts*: All contact events that are linked to the searched e-mail address or phone number are listed. This means that you must search with the phone number or e-mail address; the name search can only give results for *Directory Entries* or *Outbound Campaign Customers*.
- In details view you can find contact details, for example: agent name, e-mail body, possible attachment name and size, possible call recording file name. If a call recording, voicemail or an other attachment is available, a download button (Listen/Show) is displayed in the details view.
- *Directory Entries*: All directory entries where the search criteria is found are listed.
  In details view you can find all entries made to directory, and a download button for possible files, such as photo.
- *Outbound Campaign Customers*: All Outbound campaigns where the given search criteria is found in the customer information are listed.
  In details view you can find the campaign name and status, and all customer information available.
- *Customer Consents*: Date and time information and the value (1 = yes, 0 = no) of the customer consent linked to the searched phone number are listed.

6. By default all search results are selected. To remove the selection from any of the results, click the selected checkbox in the beginning of the search result row. To remove all results of a result group, click the selected checkbox in the beginning of the group title row.
   Do one of the following:
   - To return to the search view, click the < arrow at the upper left corner of the *Search Results* window.
   - To create a report, click the *Create Report* button.
   - A CSV file is created that includes all information of selected items, also detailed information. To include attachments, such as call recordings or e-mail attachments, download them in your local computer and zip. Downloading can be audit logged.
   - To delete personal data, click the *Delete* button.
   - All information of selected items, also detailed information, is deleted or anonymized, and the report is removed, also from all Monitoring Databases. The removed information may be replaced with the text {Anonymized by DPO}. For more information about deleting and anonymizing, see Deletion of Personal Data.

User interface

User interface looks like this, user must log on to be able to make searches and delete the data:


Generate Personal Data
10.31.98.41:1080/ecf/0/dporeport/index.html
Generate Personal Data Report - Search
Log On
Search Criteria

Sähköpostiosoite:

Phone Number:

Digits Used in Search: 8

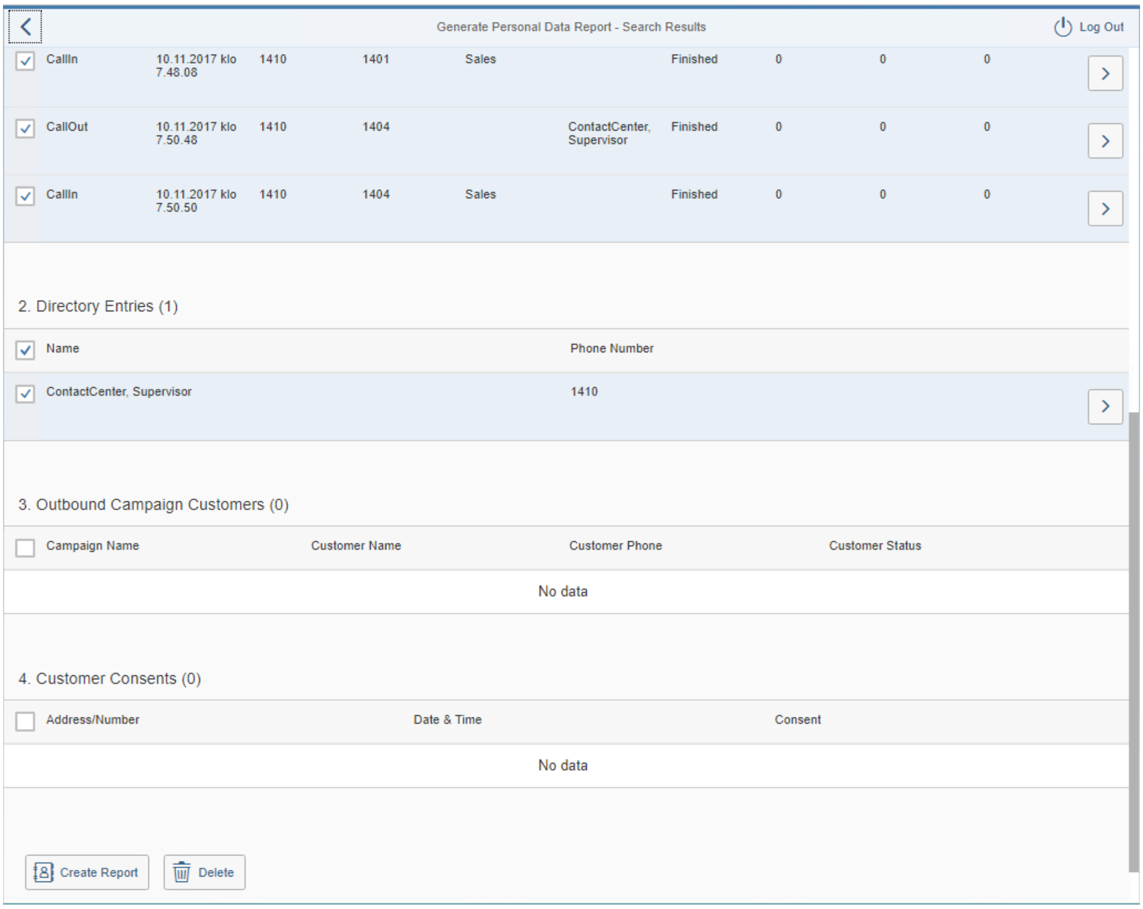
First Name:

Last Name:

Start Date: 14.11.2016

End Date: 14.11.2017

12:16:06 - You are not logged-on, please log on



Generate Personal Data Report - Search Results

Log Out

☑	CallIn	10.11.2017 klo 7.48.08	1410	1401	Sales		Finished	0	0	0	>
☑	CallOut	10.11.2017 klo 7.50.48	1410	1404		ContactCenter, Supervisor	Finished	0	0	0	>
☑	CallIn	10.11.2017 klo 7.50.50	1410	1404	Sales		Finished	0	0	0	>

2. Directory Entries (1)

☑	Name	Phone Number	
☑	ContactCenter, Supervisor	1410	>

3. Outbound Campaign Customers (0)

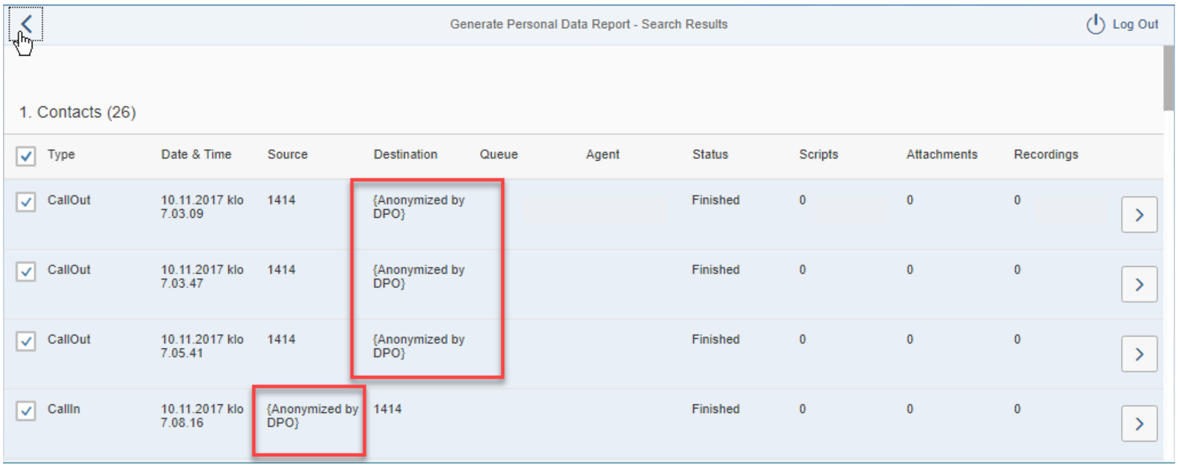
☐	Campaign Name	Customer Name	Customer Phone	Customer Status
	No data			

4. Customer Consents (0)

☐	Address/Number	Date & Time	Consent
	No data		

Create Report Delete

Anonymized data:



Generate Personal Data Report - Search Results

Log Out

1. Contacts (26)

☑	Type	Date & Time	Source	Destination	Queue	Agent	Status	Scripts	Attachments	Recordings	
☑	CallOut	10.11.2017 klo 7.03.09	1414	{Anonymized by DPO}			Finished	0	0	0	>
☑	CallOut	10.11.2017 klo 7.03.47	1414	{Anonymized by DPO}			Finished	0	0	0	>
☑	CallOut	10.11.2017 klo 7.05.41	1414	{Anonymized by DPO}			Finished	0	0	0	>
☑	CallIn	10.11.2017 klo 7.08.16	{Anonymized by DPO}	1414			Finished	0	0	0	>

Personal Data

Person-related data in SAP Contact Center can be divided into the categories: **User Master Data, Directory Information, Reporting Data, Recordings**, and **Contact Data Records**. All these categories may be controlled separately and optional data can be switched off based on individual customer needs. See the list below.

- **User Master Data:** It is mandatory to save user data into the system. User can be identified based on the first name, last name, login id, and with different addresses.

Data retention: All user master data relations are removed at the same time when a user account is deleted. User with the name attribute is saved separately so that user can be linked until all other (optional) user-related data is removed from the system.

- **Directory Information:** Typically name and phone number information as well as job title and job responsibilities may be recorded into directory. Directory Information is optional, and directory data collection can be switched on/off based on customer needs. Typically Directory Information is used for finding the right person within an organization. Saving data into a directory can be switched off also on individual user level. Note that directory is not designed to hold sensitive data about a person like (social security id, sex or race) and it should not be used for such purposes.
  Data retention: The directory information is a separate record from user master data but it is possible to configure the system to remove directory information after the user record is removed. Customer directory data can be removed by Data Protection Officers (DPO) with a specific tool.

- **Reporting Data:** Reporting data may contain a person's phone number, name or persons login identifier. For users' performance reporting purposes the reporting contains also personal level statistics of work time distribution. The data may be used as a basis for persons (contact center agent) salary or bonus calculations.
  Data retention: As of earlier version of SAP, it is possible to set a retention time after which all reporting data is deleted.

- **Recordings:** Voice logging/voice recording is an optional feature in SAP Contact Center. Recording may be switched off/on on system and personal level. Persons voice may be recorded for different kind of purposes. Personal recordings are accessible only by authorized users (access to the recordings can be controlled with user rights). By default, user has right to access to his/her own recordings. It is also possible to give the user an ability to stop or start the recording and thus user is able turn off the recording whenever the nature of call is personal. All personal recordings contain only the part of the telephone conversation which was audible for the user during the call. Exceptionally it is also possible to setup the system to record calls for quality management purposes. In this case one recording may contain multiple users conversation. The access to these recordings are enabled for the user(s) who have listening rights for the service (queue, outbound campaign) i.e. it is possible to record sales service calls (calls that are accepted from sales service queue). In this kind of recordings the whole customer interaction will be recorded in single recording file. We recommend that companies using recording for quality management shall inform their users and customers if the calls may be recorded, and in some countries informing customer about recording functionality is mandatory by legislation. Refer to the local legislation about voice logging capability. System can be configured so that calls are recorded only with a customer consent.
  Data Retention: Data retention times defined for calls apply to call recordings is possible as well.

- **Contact Data Records:** Contact data records hold information about persons' addresses (phone number, e-mail address, IP address) that can be used to identify a person.

  Data Retention: Contact data retention times can be defined.

Personal Data in Diagnostic Logs

In the basic setup, diagnostics logs do not contain any personal identification data. The logging of individual communication events into the diagnostic logs is switched off in installation. This setting can be switched on for technical problem solving purposes, only.

Any changes to personal data can be audit logged.