Sinch Contact Pro Security Guide

Version 22Q4 – December 2022

Revision History

Version	Date	Description
1.0	24.09.2021	Document for version 21Q3
2.0	14.01.2022	Document for version 21Q4
3.0	25.03.2022	Document for version 22Q1
4.0	17.06.2022	Document for version 22Q2
5.0	08.09.2022	Document for version 22Q3

Table of Contents

1 Introduction

1.1 About this Document

The Security Guide provides an overview of security and data privacy of Sinch Contact Pro.

1.2 Target Audience

- CIO:s
- DPO:s
- Security Experts and Consultants

2 Personal Data Protection

This section provides information about handling of personal data in Sinch Contact Pro and describes the specific features and functions Sinch Contact Pro provides to support compliance with the relevant legal requirements and data privacy.

- Privacy Statement and Data Protection Officer
- Deletion of Personal Data
- Sensitive Personal Data
- Logging Changes to Personal Data
- Customer Consent for Saving Personal Data
- Generating Personal Data Report

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.

Please note that this document does not constitute a legal advice; instead, all information, content, and materials available in this document are for general informational purposes only. No claim or representation is made or warranty given, express or implied, in relation to any of the information. If Customer would like to receive legal advice, Sinch recommends that it contacts its own internal or external lawyers. 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.

- In most cases, compliance with data privacy laws is not a product feature.
- Sinch 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.
- Sinch 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.

Title	Title
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.

Table 1: Terminology

The following topics are related to data protection and require appropriate technical and organizational measures:

- Access control: Authentication features as described in section User Administration and Authentication.
- Separation by purpose is subject to the organizational model implemented and must be applied as part of the authorization concept. Sinch Contact Pro uses role-based user management that enables defining user authorizations on individual, group, or role level.

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.

2.1 Privacy Statement and Data Protection Officer

We strongly recommend that you publish a 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, as well as 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 in data protection questions arises?
- How can 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 as Data Protection Officer (DPO). The tasks of a DPO include but are not limited to the following:

- 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 *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.

2.2 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. Sinch Contact Pro is not designed to store and process sensitive personal data.

This applies specifically for the following 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.
- Attached Data (CAD) for chat and phone. Do not use attached data for collecting and storing any sensitive personal data.
- Internal notes. Do not use internal notes for storing any sensitive personal data.

Call Recordings

Call recordings need to be treated in a special way because of their sensitive nature. The system provides logging for listening of call recordings. A user with rights to listen to a specific call recording leaves a log trace of the event and provides an explanation for listening. Listening logs are saved in the Configuration database’s

CallRecordingListenLog table, and agents can see their own logs in Communication Panel. With the Listen to Recording rights it is possible to view all listening logs via Restful Contact Management (CMI) integration interface. The logs can be removed with SQL tools only.

Customer Consent for Call Recordings

Sinch Contact Pro can be configured so that call recording is done only if a caller has given their consent for that. In 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. For more information about customer consents, see Customer Consent for Saving Personal Data.

2.3 Deletion of Personal Data

System administrator can define the data retention time for all conversation channels and for handled/expired Outbound campaigns on both system and queue level. System level setting is the default setting for all queues, and queue level setting overrides it for specific queue. After the retention time, all data will be anonymized or deleted automatically. Alternatively, Data Protection Officer (DPO) can, on the person's request, destroy data related to a person.

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

The following list explains which data is anonymized and which deleted:

- Call events are anonymized and the possible call recording is deleted.
- Handled e-mail conversations are anonymized, and the e-mail subject and body are replaced with text {Anonymized by DPO}. Possible attachments are deleted. This applies also for other e-mail type items, such as tasks, and XRI items.

- Chat events and chat subject are anonymized and the chat transcript is deleted. This applies also for other chat-type sub channels, such as SMS, and Facebook Messenger. Possible attachments are deleted.
- If there is a script linked with a conversation item, the script freetext contents are deleted.
- If internal notes have been added to a conversation, the notes are replaced with text {Anonymized by DPO}.
- If attached data (CAD) has been added to a conversation, the data is replaced with text {Anonymized by DPO}.
- 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 are not removed after retention times but only on request.

Retention Times

- Retention times of personal data are defined in *System Configurator > System Management > Personal Data Retention Times*.
- Call recordings are deleted when the *Retention Time for Calls* expires, but they can also be deleted by defining the time in *System Configurator> System Services > Recording Settings > Automatic File Removal*. Recordings are deleted based on the time that expires earlier.
- All conversation-related reporting data can be deleted (in addition to the anonymization done after the retention time) by defining the Reporting Database Server variable *Reporting Data Retention Time in Years* in Infrastructure Administrator.

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 the 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 conversation-related data and contents for a longer time than otherwise defined in their data privacy policy. Whilst this data shall not be erased, it may be necessary to block it from appearing 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, that is event contents including possible attachments and call recordings, to a Sinch Contact Pro external storage from where it will be deleted.

To block the data from operative usage (for example appearing in historical searches), DPO needs to erase the corresponding data from Sinch Contact Pro.

2.4 Logging Changes to Personal Data

The Audit Logging capability logs changes made to personal data. This applies to changes done via user interfaces like Communication Panel or System Configurator, and 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

- what was the new value after change.

Audit logs are managed with the Logging Wizard that is currently managed by Sinch Operations team only. To enable audit logging, create a support ticket and tell which type of event you want to be logged:

- `presence`: Events related to presence of a user or device.
- `config`: Events related to configuration data or process.
- `rights`: Events related to user rights and access control.
- `modify`: Events related to modifying information. Use this value to log changes made to any data or configuration.
- `read`: Events related to reading information.
- `failure`: Events related to situations when something has failed, for example unsuccessful logon attempts, or unsuccessful attempts to change user information or access rights.
- `system`: Events related to server system state, such as starting and stopping of a module.

2.5 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 their consent, that their contact data and content will be handled and stored in the system.

It is recommended that the organization informs the customer about collecting personal data in these occasions. The methods for doing this in Sinch Contact Pro are described below.

Data Protection Officer (DPO) can reset the consent database in case the organization renews its data privacy policy. In such an occasion, it is recommended that the DPO exports the consent database and stores it according to the organization's data protection and privacy policy. For more information about how to manage consents, see the System Configurator document: *System Tools > Managing Customer Consents*.

Inbound Queue Calls and IVR Calls

It is possible to record the *Welcome* prompt for each phone queue. In the *Welcome* prompt, the organization can inform customers about the service to which they have called and about how the organization handles personal data.

To define such a prompt, create an audio prompt with type *Welcome* in *System Configurator > Queue Management > Prompt Management*.

Call Recording

The 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, calls may be recorded without consent.

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

This information on customer consent or non-consent can be stored in the database, and the information can later 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 the customer wants to withdraw their consent.

The consent information follows the customer's call for the lifetime of the call, either enabling or disabling 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.

To use IVR for asking consent for recording a call, add the Consent IVR in *System Configurator > IVR Management* and configure it in *System Configurator > System Services > Recording*. For more information, see corresponding sections in System Configurator documentation.

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

It is possible 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 they have sent the e-mail, and also about how the organization handles personal data. A good practice is to provide a link to the organization's web page where the organization's data privacy statement is published.

To define an automatic receipt message, define an e-mail prompt with type E-Mail Received Message in *System Configurator > Queue Management > Prompt Management*.

Inbound Web Chats

It is possible to define an automatic *Welcome* prompt for each chat queue.

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

To define such a prompt, create a chat prompt with type *Welcome* in *System Configurator > Queue Management > Prompt Management*.

Inbound SMS Messages

SMS message is a subtype of chat. It is possible 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 they have sent the SMS and about how the organization handles personal data. A good practice is to provide a link to a web page where the organization's data privacy statement is published.

To define such a prompt, create a chat prompt with type *Welcome* in *System Configurator > Queue Management > Prompt Management*.

Outbound Campaigns

We recommend that the organization ensures the customer’s consent for telemarketing activities prior to importing customer data to the system.

Inbound and outbound WhatsApp messages

The rules for WhatsApp opt-in are set by Facebook and we recommend you get familiar with the guidance.
Contact Pro can store WhatsApp opt-in and Communication Panel works according to rules defined by Facebook.

2.6 Generating the 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 *Use* rights for the Data Protection Officer (DPO) user service. User administrators can define the rights in the System Configurator application.

Generating the Personal Data Report

1. Go to the web page https://login-<region>.cc.sinch.com/<tenant id>/ecf/latest/dporeport/index.html.
2. Log on using your Sinch Contact Pro username and password.
3. Enter customer information into the Search Criteria fields. Search uses the OR operator.

- E-Mail Address: Enter one e-mail address.
- Phone Number: Enter one phone number. The search term must be a numeric value and have at least 3 digits.
- First Name, Last Name: To search for a customer by name, define both name fields.
  Note: Searching by name only gives results for Directory Entries and Outbound Campaign Customers. To find conversations, use an e-mail address or phone number in the search.
- 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 is 3. Before the search, the system removes spaces and other separating characters from the numbers.
- Display Name: Enter the exact name a customer has used in a chat conversation.

4. Click Search.

   If there are under 1000 search results, the search results appear.
   If there are over 1000 results, the search suggests you to 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. 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:

- Conversations: All events that are linked to the searched e-mail address or phone number are listed. . In the details view you can find conversation details, for example: agent name, e-mail body, possible attachment name and size, possible call recording file name. If a call recording, voicemail or another attachment is available, a download button (Listen/Show) is displayed in the details view.
- Directory Entries: All directory entries where the search criteria are found are listed. In the details view you can find all entries made to directory and a download button for possible files, such as photos.
- Outbound Campaign Customers: All Outbound campaigns where the given search criteria are found in the customer information are listed. In the details view you can find the campaign name and status, as well as 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 to your local computer and zip them. 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.

.

3 User Administration and Authentication

3.1 User Administration

User accounts, their rights and roles are managed with System Configurator.

3.2 User Authentication

Users are authenticated either with basic authentication (username and password) or Single Sign-On (SSO). Basic authentication is used by default.

By default, the initial password must be changed, and it must be longer than 8 characters. Authentication policies, such as minimum password length, password expiration, maximum number of failed logon attempts, and how long the password is locked after too many attempts, can be defined in the System Configurator.

As an alternative to basic authentication, Sinch Contact Pro can be integrated into your identity provider with SAML federation. SSO is available for all Sinch Contact Pro user interfaces, except Business Objects reporting. SSO is implemented with Amazon Cognito and it uses common identity management standards, including OpenID Connect, OAuth 2.0, and SAML 2.0.

4 Authorizations

Sinch Contact Pro uses role-based user management that enables defining user authorizations on individual, group, or role level. Roles are managed in the *System Configurator > User and Role Management.*

4.1 Authorization Types

User rights are defined for roles. The customer or implementation partner is granted one superuser account that is used for creating users and assigning them to roles. The superuser account is the only account that can create new roles and grant rights to roles. Each role has rights to modify its own settings (*User > Self > User Setting*).

The roles are as follows:

Contact center supervisor

This role includes rights to act as a contact center team leader, to manage teams, and to handle customer conversations.

Contact center agent

This role includes rights to handle customer conversations.

Reporting administrator

This role includes rights to manage settings related to monitoring and reporting applications.

Queue administrator

This role includes rights to manage inbound contact center operations related to queues. This includes, for example, schedules, prompts, and scripts.

Outbound administrator

This role includes rights to creating and manage outbound campaigns. This includes, for example, defining campaign settings and assigning agents to campaigns.

IVR administrator

This role includes rights for creating and managing custom-made IVRs.

Advanced Monitoring User

This role has rights to all users and queues. It is recommended to limit the role rights according to business and data privacy needs.

Note 1 Do not modify these roles. If you want to change the default roles, copy them and make your modifications to the copied versions.

Note 2 The object types *Customer Consent* and *Data Protection Officer (DPO)* are not included in any default roles. Superuser can grant these rights only to a user separately.

5 Security of Data Storage and Data Centers

The data centers that support Sinch Contact Pro incorporate multiple safeguards for physical data security and integrity. They also provide high availability of your business data, using redundant networks and power systems.

Asset Protection and Data Integrity

Best practices for operating data centers are followed by deploying computation and storage parts of the solution over separated fire-safe areas to support disaster recovery in the event of a fire.

For data backup and recovery purposes, a redundant hardware storage system performs regular backups. To provide enhanced data integrity, Sinch Contact Pro uses an advanced database management solution to store customer data and securely isolate each customer's business information in its own database instance.

Power Backup and Redundancy

Data centers maintain multiple connections to several power companies, making a complete power outage highly unlikely. Even if the local power grid were to fail, the data centers supporting your cloud solution have an uninterruptible power supply for short-term outages, and a diesel generator backup power supply for longer-term outages. Therefore, power interruptions or outages are unlikely to affect customer data or solution access.

6 Product Security

6.1 Security Vulnerabilities

Modern times challenge security in all software products. Sinch takes security seriously: products go through penetration testing and security validation, and we are committed to fixing security vulnerabilities classified as *high* with a patch or, at the latest, in the next release. Vulnerabilities classified as *medium* or *low* are analysed by the product development team and fixed in the next release if not decided otherwise.

We ask you to report possible security findings via Sinch Contact Pro customer support.