Security Guide

CUSTOMER

SAP CoPilot
Document Version: Q2 2018 – 2018-05-18

SAP CoPilot for S/4HANA Cloud and iOS Security Guide

Content

1 About

The following information is made available for your reference when taking security into consideration: SAP Community Network (SCN) information on security, fundamental SAP Security guides, and the SAP CoPilot user guides.

> **Note**
>
> This guide applies to SAP CoPilot for **SAP S/4HANA Cloud** and the **SAP CoPilot iOS** app only.

Important Links

Content	Link
SAP Community (SCN) Network Security Information	SAP SCN Info
SAP Security Guides	SAP Security Guides
SAP CoPilot User Guides	The SAP CoPilot Product Page

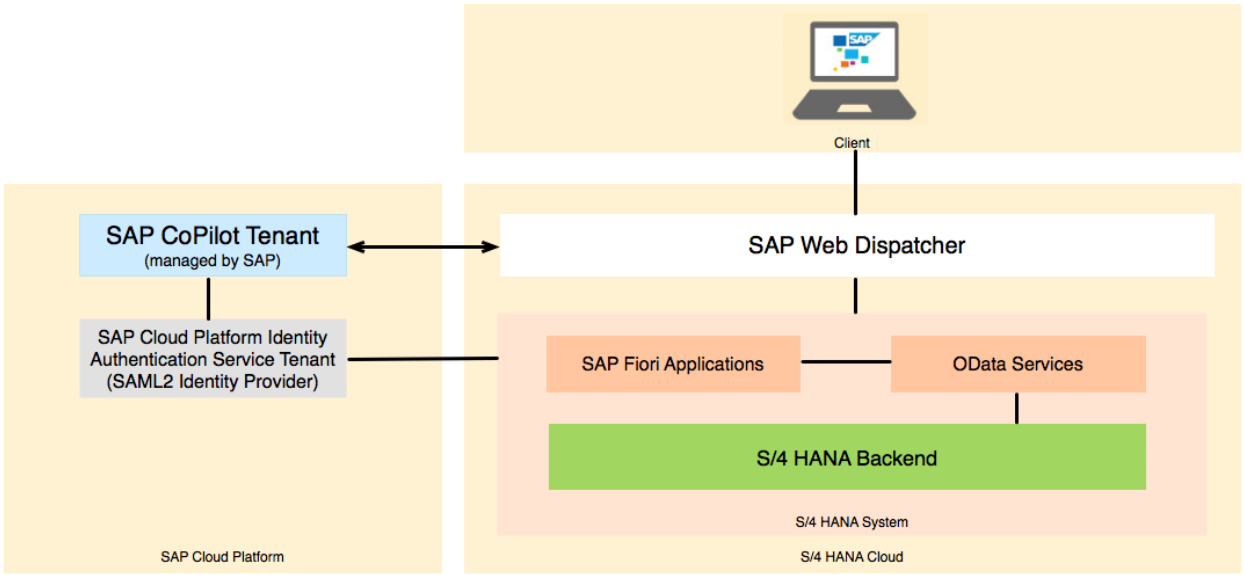
2 Technical System Landscape

SAP CoPilot for S/4HANA Cloud is a fully SAP-managed cloud application provided via the SAP Cloud Platform and is integrated into the rest of the S/4HANA Cloud landscape.

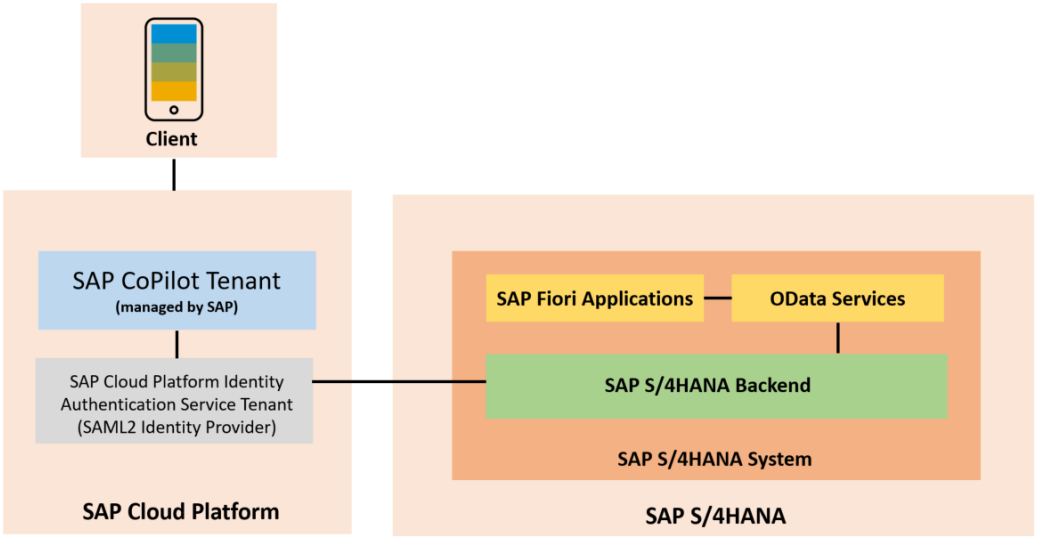
Since SAP manages both SAP CoPilot as well as the S/4HANA Cloud landscape, SAP is also responsible for managing all security related aspects. This following diagram shows a high-level overview of the S/4HANA Cloud and SAP CoPilot system landscape and how the components communicate.

The following diagrams shows a high-level overview of the S/4HANA Cloud and SAP CoPilot system landscape and how the components communicate in both S/4HAHA Cloud and SAP CoPilot for iOS.

S/4HANA Cloud:



SAP CoPilot for iOS:



3 Communication Channel Security

Learn about the communication channel security set up for both SAP CoPilot for S/4HANA Cloud and iOS.

In **SAP CoPilot for S/4HANA Cloud**, all communication from the frontend (browser) to the SAP CoPilot backend happens through the SAP Web Dispatcher using HTTPS and WSS (secure web sockets) protocols.

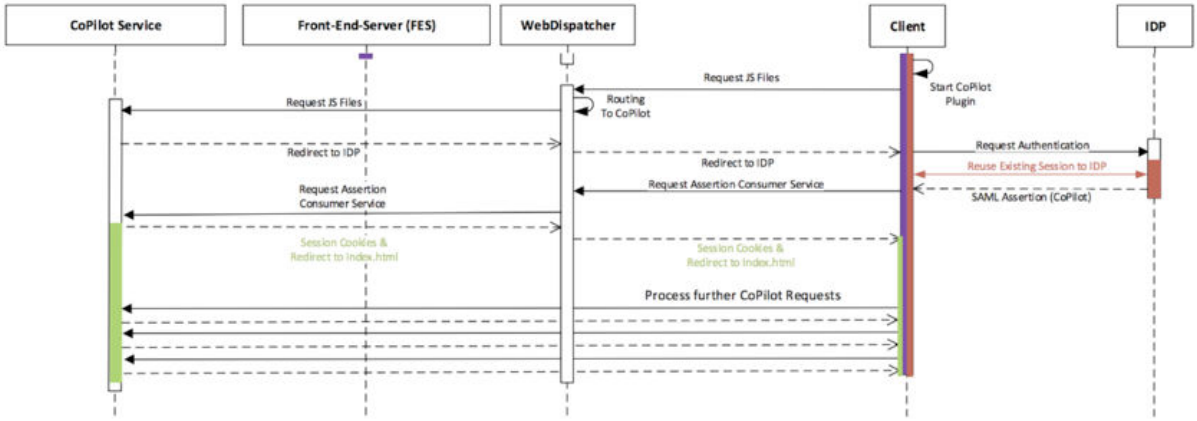
In **SAP CoPilot for iOS**, all communication to the SAP CoPilot backend happens through the SAP Cloud Platform mobile services using HTTPS and WSS protocols.

4 User Administration, Identity Management, and Authentication

The authentication for SAP CoPilot is done via single-sign-on from the SAP Fiori launchpad in SAP S/4HANA Cloud. The same authentication flow applies for SAP CoPilot for iOS.

SAP CoPilot connects to the same SAML2 Identity provider that is used by the S/4HANA Cloud system. In both cases, the SAML2 Identity provider is an SAP Cloud Platform Identity Authentication service tenant on the SAP Cloud Platform.

The diagram below shows the components and data flow involved in the login and initial data loading process:



For more information, refer to SAP Cloud Platform - Identity and Access Management.

5 Frontend Security

The SAP CoPilot frontend is a regular SAPUI5 application loaded as as an SAP Fiori Launchpad plugin, therefore no special security conditions apply. SAP CoPilot for iOS is a regular Swift application available in the app store.

For general guidelines on securing SAPUI5 applications, refer to Securing SAPUI5 Applications .

For guidelines on following Apple's recommended security framework, refer to Apple Documentation - Security .

6 Storage and Network Security

SAP CoPilot is a service that runs on the SAP Cloud Platform.

The physical storage, include servers and databases, are provided and secured by the SAP Cloud Platform and is not operated by the customer. Communication for all channels is encrypted via HTTPS and SSL.

7 Data Storage Security

Learn about how SAP CoPilot stores and manages user data and multi-tenancy on the SAP Cloud Platform.

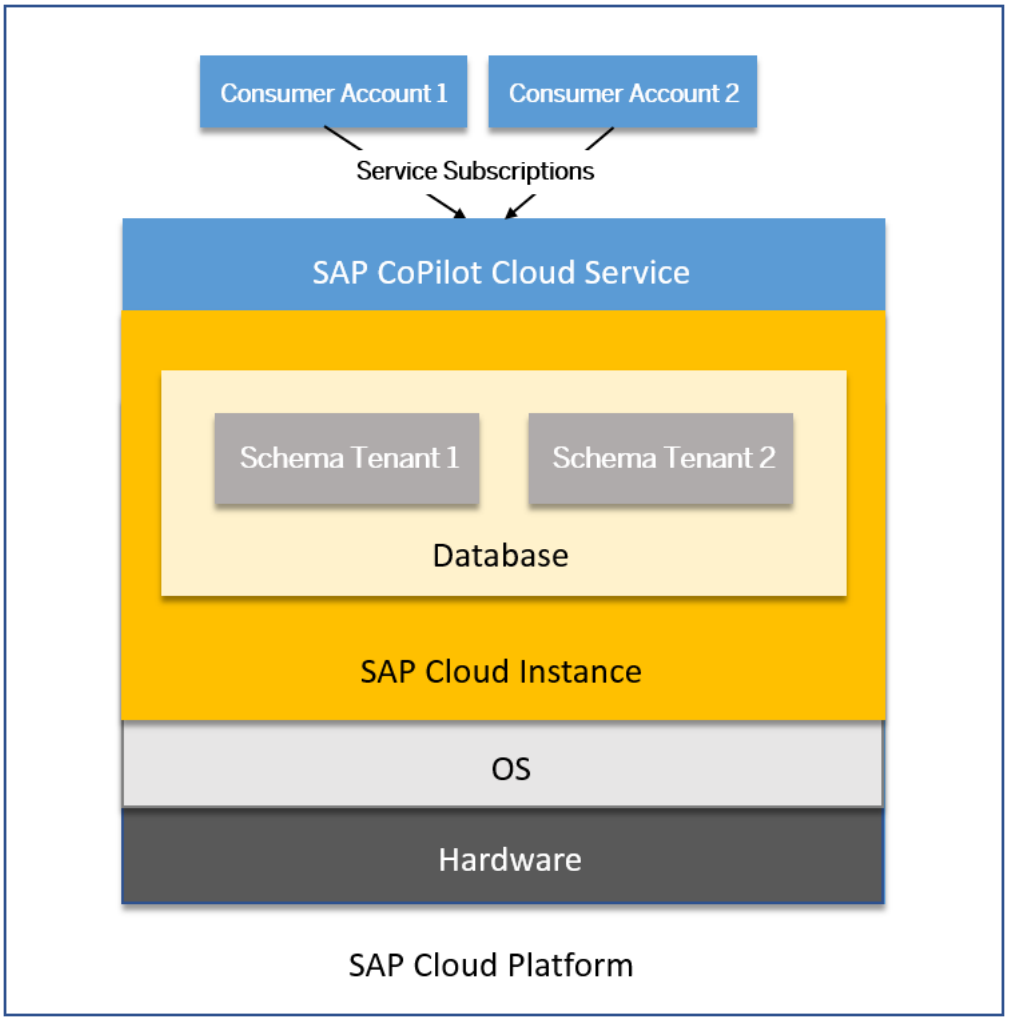
Data Storage and Databases

SAP CoPilot stores all data in the SAP Cloud Platform Persistence Service within a designated SAP HANA database instance.

For more information, refer to the SAP Cloud Platform Persistence Service.

Multi-Tenancy

The SAP CoPilot service supports multi-tenancy by creating separate database schemas for each tenant. This way, from a security perspective, it is ensured that data of different customers is completely isolated from each other:


Consumer Account 1
Consumer Account 2
Service Subscriptions
SAP CoPilot Cloud Service
Schema Tenant 1
Schema Tenant 2
Database
SAP Cloud Instance
OS
Hardware
SAP Cloud Platform

8 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy regulation, it is necessary to consider compliance with industry-specific legislation in different countries.

SAP provides specific features and functions to support compliance with regards to relevant legal requirements, including data protection. SAP does not give any advice on whether these features andfunctions are the best method to support company, industry, regional, or country-specific requirements. Furthermore, this information should not be taken as advice or a recommendation in regard to additional features that would be required in specific IT environments; decisions related to data protection must be made on a case-by-case basis, taken into consideration the given system landscape and the applicable legal requirements.

> **Note**
>
> SAP does not provide legal advice in any form. SAP software supports data protection compliance by providing security features and specific data protection relevant functions, such as simplified blocking and deletion of personal data. In many cases, compliance with applicable data protection and privacy laws will not be covered by a product feature. Definitions and other terms used in this document are not taken from a particular legal source.

8.1 About Personal Data

SAP CoPilot builds up a user cache at runtime, with the exceptions of passwords not being stored.

SAP defines personal data as any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

SAP CoPilot stores the following user properties in the cache:

- User ID
- First Name
- Last Name
- Email Address
- Last Accessed Timestamp
- Created On Timestamp

The user cache is needed so that SAP CoPilot can search for users and so that a user can invite participants to chats.

Apart from the user cache, SAP CoPilot only stores data in the SAP CoPilot chats. Only users who are invited to a chat can see and modify that data. This is ensured by the SAP CoPilot service.

Personal Data in the SAP CoPilot iOS App

The SAP CoPilot iOS app tracks SAP CoPilot-related activity in the device for support purposes only. Users have the option to delete or save logs (containing data managed in the SAP CoPilot app). These logs are never transmitted anywhere, unless the user actively uploads or deletes them.

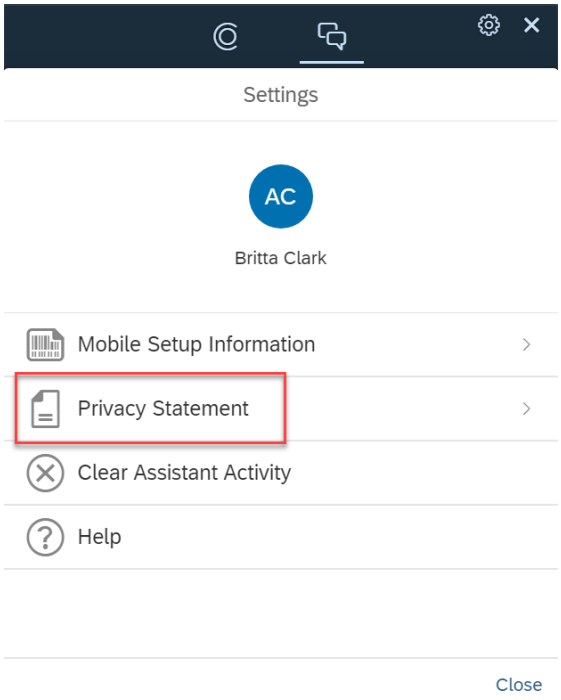
8.1.1 User Consent

SAP CoPilot provides a privacy statement that can be found in the *User Settings* in SAP CoPilot. The same applies in the SAP CoPilot iOS app.

The SAP CoPilot privacy statement contains:

- A Preamble (Introduction)
- General Information
- Description of Personal Data
- Description of the Purposes for Processing Personal Data
- Potential Data Transfers within the SAP Group
- Data Retention and Deletion Principles
- Data Subject Rights

In SAP CoPilot for S/4HANA Cloud, the privacy statement can be found in the *User Settings*:



8.1.2 User Data Reporting

Users can access to a report containing personal data stored by SAP CoPilot.

Accessing the Report

Procedure

In the URL, paste `/copilot/userdata` after the customer or tenant URL.

The following information regarding the user's profile is displayed:

- User ID
- Email
- First Name
- Last Name
- Display Name
- Login Time
- Additional User IDs

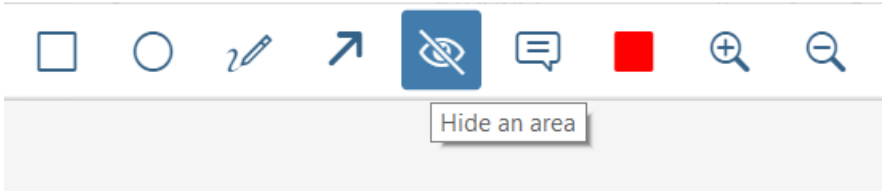
8.1.3 Data Privacy

SAP CoPilot allows users to create notes and share information with other users through the creation of chats.

A chat by default is only visible to the user who created it. When the chat owner (the creator) starts adding participants to the chat, these participants can see all historical info in the chat, prior to being added. Participants can also add comments using the text input field.

Because of these features, users are able to enter free text in the input fields to create notes and comments. SAP CoPilot does not control or filter sensitive information out of these messages. Users must be aware of the information that they share with other users, particularly if the information that they share is something other users should not have access to.

When it comes to sharing screenshots using the screenshot tool in SAP CoPilot, users can utilize the *Hide an area* feature so conceal or hide any confidential information on the screenshot before adding it to the chat:



8.1.4 Offboarding Users

SAP CoPilot comes preconfigured for users who have it enabled in their launchpad.

To offboard a user, you must file a ticket with SAP to have the user deleted from the user cache which is currently managed by SAP.

8.1.5 Data Retention Period

The data retention periods are managed by SAP, therefore requests to update the retention period must be filed via a customer ticket.

By default, the data retention period for all content in chats is set to 5 years. This can be changed to a period from 3 to 10 years (full years only). However, this configuration is managed by SAP and the customer will need to file a ticket with SAP to request this change. When the retention period ends, all chats and their respective objects older than the retention period will be deleted.

For SAP CoPilot on iOS, deleting the app will also delete the temporary stored data from the local device storage.

8.2 Glossary

This is a partial list of terms used with regard to Data Protection and Privacy at SAP.

Term	Definition
Blocking	A method of restricting access to data for which the primary **business purpose** has ended.
Consent	The action of the data subject confirming that the usage of his or her personal data shall be allowed for a given purpose. A consent functionality allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.
Deletion	The irreversible destruction of **personal data**.
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 **blocked** and can only be accessed by users with special authorization, for example, tax auditors.

Term	Definition
Personal data	Any information relating to an identified or identifiable natural person *data subject*. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
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.
Residence period	The period of time after the end of purpose (EoP) for a data set during which the data remains in the database and can be used in case of subsequent processes related to the original purpose. At the end of the longest configured residence period, the data is blocked or deleted. The residence period is part of the overall retention period.
Retention period	The period of time between the end of purpose (EoP) for a data set and when this data set is deleted subject to applicable laws. It is a combination of the residence period and the blocking period.
Sensitive personal data	A category of personal data that usually includes the following type of information: • Special categories of personal data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data, data concerning health or sex life or sexual orientation • Personal data subject to professional secrecy • Personal data relating to criminal or administrative offenses • Personal data concerning insurances and bank or credit card accounts
Where-used check (WUC)	A process designed to ensure data integrity in the case of potential blocking of business partner data. An application's where-used check (WUC) determines if there is any dependent data for a certain business partner in the database. If dependent data exists, this means the data is still required for business activities. Therefore, the blocking of business partners referenced in the data is prevented.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

go.sap.com/registration/contact.html