Data Protection and Privacy Overview

Last Modified on 01/28/2022 8:41 am EST

Governments place legal requirements on industries to protect data and privacy. We provide features and functions to help you meet these requirements.

> **Caution**
>
> SAP does not provide legal advice in any form. SAP software supports data protection compliance by providing security features and data protection-relevant functions, such as blocking and the deletion of personal data. In many cases, compliance with applicable data protection and privacy laws is not covered by a product feature. Furthermore, this document should not be taken as advice or recommendation regarding additional features that would be required in specific IT environments. Decisions related to data protection must be made on a case-by-case basis, taking into consideration the given system landscapes and the applicable legal requirements. Definitions and other terms used in this documentation are not taken from a specific legal source.

> **Caution**
>
> We assume that you have not maintained any data related to an individual in the tools provided by SAP Open Connectors, exempt for the members of the account (for example, when designing integration content).
>
> We expect that sensitive personal data can only be included in message payloads. This responsibility lies exclusively with you as the operator of an integration scenario using SAP Open Connectors and remains your responsibility. If you include sensitive personal data within payloads or message attachments, SAP Open Connectors may store this information on your behalf. This applies also for data maintained in the tools provided by SAP Open Connectors. However, data within payloads can be protected by enabling encrypted storage. For more details on SAP Open Connectors' use of personal data, see Information Report.

User Consent

Various types of customer data are processed by and stored on SAP Open Connectors at different times. This data gets the highest level of protection, and SAP takes dedicated measures to guarantee this security level.

To comply with user consent, SAP customers should customize the SAP Open Connectors to use their own identity provider. SAP customers using the custom identity provider should ensure that the necessary mechanism for user consent is available to allow personal data (of a natural person such as a customer, contact, or account) to be collected as well as transferred to the solution.

Read Access Logging

Read Access Logging (RAL) is used to monitor and log read access to sensitive data. Data may be categorized as sensitive by law, by external company policy, or by internal company policy.

SAP Open Connectors does not store any sensitive personal data.

For more information about audit logs, see User Management via API in the Roles tab.

Information Report

An information report is a collection of data relating to a data subject. A data privacy specialist may be required to provide such a report, or an application may offer a self-service.

The only personal data of data subjects stored in the SAP Open Connectors is the user ID, the e-mail ID, as well as the first and last name of a member in the account. This user ID is stored whenever a user creates an artifact on SAP Open Connectors, for example a Connector Instance or a Formula, and this user ID can be obtained (read) only from that artifact or the corresponding member of the account.

To enable data subjects to obtain information about their personal data in the SAP Open Connectors, a retrieval service for their personal data is provided. For more information, see Retrieve Personal Data in the Roles tab.

Erasure

When handling personal data, consider the legislation in the different countries where your organization operates. After the data has passed its end of purpose, regulations may require you to delete the data. However, additional regulations may require you to keep the data longer. During this period, you must block access to the data by unauthorized persons until the end of the retention period, when the data is finally deleted.

Personal data can also include referenced data. The challenge for deletion and blocking is to first handle referenced data and then other data, such as business partner data.

SAP Open Connectors stores the user IDs of members of the account. Storing the user ID is a business requirement and the user ID is deleted when the related member is deleted in the account or when capability is deactivated.

All the personal data stored in the application is deleted once the access for the corresponding user is revoked by removing the user from the member list of the account.

In SAP Open Connectors, integration developers can contact their SAP Open Connectors administrators to have their personal data erased and their access revoked. For more information, see the User Delete section in the Roles tab.

Change Log

For auditing purposes or for legal requirements, changes made to personal data should be logged, making it possible to monitor who made which changes and when. Changes made in the identity provider should be logged by the identity provider.

SAP Open Connectors does not allow users to make any changes to their personal data, except adding members to the account, deleting members from the account, and assigning authorization roles. These changes are logged by SAP Open Connectors and can be displayed. For more information, see Read Personal Data Change Logs.

Glossary

Term	Definition
Blocking	A method of restricting access to data for which the primary business purpose has ended.
Business purpose	A legal, contractual, or otherwise 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.
Consent	The action of the data subject confirming that the usage of their personal data shall be given 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	Deletion of personal data so that the data is no longer available.
End of business	Date where the business with a data subject ends, for example the order has been completed, the subscription is canceled, or the last bill is settled.
	End of purpose and start of blocking period. The point in time, when the primary

Term	Definition
End of purpose	processing purpose ends (e.g. a contract is fulfilled).
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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. Any information relating to the integration developer using SAP Open Connectors.
Residence period	The period of time between the end of business and 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 the last business activity involving a specific object (for example, a business partner) and the deletion of the corresponding data, subject to applicable laws. The retention period is a combination of the residence period and the blocking period. SAP Open Connectors has a retention period of 90 days and all the data is automatically cleaned up after the retention period.