



**Product Documentation | PUBLIC**

SAP Logistics Business Network, Global Track and Trace Option

Document Version: LBN 2.0 – 2021-11-23

# Security Guide

# Content

- 1 Introduction. . . . . 3**
- 2 Before You Start. . . . . 5**
- 3 Security Aspects of Data, Data Flow and Processes. . . . . 7**
- 4 User Administration, Authentication, and Authorizations. . . . . 8**
- 5 Data Storage Security. . . . . 9**
- 6 Data Protection and Privacy. . . . . 10**
  - 6.1 Glossary. . . . . 10
  - 6.2 User Consent. . . . . 13
  - 6.3 Read Access Logging. . . . . 13
  - 6.4 Information Report. . . . . 13
  - 6.5 Deletion of Personal Data. . . . . 16
  - 6.6 Change Log. . . . . 24
  - 6.7 Tasks for Audit Specialists. . . . . 25
    - Access the Audit Log Viewer. . . . . 25
    - View Blocked Master Data. . . . . 26
- 7 Other Security-Related Information. . . . . 29**
- 8 Appendix. . . . . 30**
  - 8.1 Manage Personal Data. . . . . 30
    - Provide a Sample Personal Data Record. . . . . 35
  - 8.2 Manage My Personal Data. . . . . 36
  - 8.3 Manage Personal Data Requests. . . . . 40
  - 8.4 Data Transport. . . . . 41

# 1 Introduction

This Security Guide provides an overview of the security-relevant information that applies to SAP Logistics Business Network, global track and trace option.

The target audience for this guide is listed in the following table:

| Role                   | Description  |
|------------------------|--|
| DP&P Specialist        | a business user who can: <ul style="list-style-type: none"><li>• deal with DP&amp;P requests and requirements</li></ul>  |
| Audit Specialist       | a business user who can: <ul style="list-style-type: none"><li>• carry out DP&amp;P audits that include viewing the personal data of all GTT users</li></ul>   |
| Security Consultant    | an aide for general security who can: <ul style="list-style-type: none"><li>• advise on all security matters</li><li>• recommend best practices for security measures</li></ul>                          |
| Solution Administrator | an administrator of a GTT solution who can: <ul style="list-style-type: none"><li>• support the DP&amp;P specialist in the execution of some data protection tasks</li></ul>                             |
| System Administrator   | a supervisor of computer systems who can: <ul style="list-style-type: none"><li>• set and maintain security policies</li><li>• plan, support and maintain the required security infrastructure</li></ul> |

## i Note

This guide does not replace the administration or operation guides that are available for productive operations.

This guide is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.

## Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or

processing time. These demands on security apply likewise to SAP Logistics Business Network, global track and trace option. To assist you in securing your solution, we provide this Security Guide.

#### Disclaimer

Security is a broad topic. SAP Logistics Business Network, global track and trace option is still in development and uses a number of leading-edge technologies that are themselves still being developed. With this in mind, this guide represents the current best approach to applying security. This approach will continue to evolve and improve as the product and its underpinning technologies move forward. Similarly, best practices for applying security in this dynamically changing environment are also likely to move rapidly as well.

#### Overview of the Main Sections

The Security Guide comprises the following main sections:

- **Introduction**  
This section contains information about why security is necessary, how to use this document, and an important disclaimer.
- **Before You Start**  
This section contains information about security for the product, and references to other Security Guides that build the foundation for this Security Guide.
- **Security Aspects of Data, Data Flow and Processes**  
This section provides an overview of security aspects involved throughout the most widely-used processes within the product.
- **User Administration and Authentication**  
This section provides an overview of the following user administration and authentication aspects:
  - Recommended tools to use for user management
  - Standard roles that are delivered with the product
  - Overview of how integration into Single Sign-On environments is possible
- **Data Storage Security**  
This section provides an overview of any critical data that is used by the product and the security mechanisms that apply.
- **Data Protection and Privacy**  
This section provides an overview of Data Protection and Privacy as it applies to the product. It includes a glossary of the basic terminology and explains some of the key aspects.
- **Other Security-Related Information**  
This section provides information about how to apply Session Security Protection and Security Lifecycle Management to the product.

## 2 Before You Start

### → Recommendation

Before you start working through this document, ensure that you have the most recent version of this document that is available from the SAP Help Portal at:

[help.sap.com/gtt](https://help.sap.com/gtt)

SAP Logistics Business Network, global track and trace option is built on top of SAP Business Technology Platform (SAP BTP) and Amazon Web Services (AWS). It uses SAP UI5 as user interface technology as well as SAP Cloud Identity (SAP SCI) for identity and access management.

The security concepts used are from a combination of those used in the following:

- SAP XS Advanced (XSA) Approuter (Multitenant) and
- SAP BTP Cloud Foundry.

The approuter authenticates users of apps with the SAP XS UAA (User Account and Authentication) service, serving static content and invoking calls to their backends. With the multitenant approuter feature, the approuter is shared between multiple tenants.

Users access the cloud service via secure HTTPS protocol. This means that there are no additional security configurations required.

### Additional Information

For additional information about fundamental security topics, see the following table.

| Security-Related Material | Description  |
|---------------------------|--|
| SAP Cloud Solution Brief  | SAP Cloud Solution Overview                                    |
| SAP Data Center           | Data center home page with focus on security and certification |
| SAP Security Certificates | General SAP IT Security Certifications                         |

Table 1: Fundamental Security Information

For a complete list of the available SAP Security Guides, see SAP Service Marketplace at:

<https://service.sap.com/securityguide>

For further information about specific security and related topics, see the Quick Links in the following table.

| Content         | Quick Link  |
|-----------------|---|
| Security        | <a href="https://scn.sap.com/community/security">https://scn.sap.com/community/security</a> |
| Security Guides | <a href="https://service.sap.com/securityguide">https://service.sap.com/securityguide</a>   |

| <b>Content</b>       | <b>Quick Link</b>  |
|----------------------|--|
| Related SAP Notes    | <a href="https://service.sap.com/notes">https://service.sap.com/notes</a><br><a href="https://service.sap.com/securitynotes">https://service.sap.com/securitynotes</a> |
| Released Platforms   | <a href="https://service.sap.com/pam">https://service.sap.com/pam</a>  |
| Network Security     | <a href="https://service.sap.com/securityguide">https://service.sap.com/securityguide</a>  |
| SAP Solution Manager | <a href="https://service.sap.com/solutionmanager">https://service.sap.com/solutionmanager</a>  |
| SAP NetWeaver        | <a href="https://scn.sap.com/community/netweaver">https://scn.sap.com/community/netweaver</a>  |

Table 2: Security and Related Quick Links

# 3 Security Aspects of Data, Data Flow and Processes

The following general security measures are in place, and are applicable to all scenarios:

- Encrypted connection through HTTPS
- User and role mapping with functional restrictions
- Access control lists limiting access to data only to permitted roles, companies and users (instance-based authorization)

Table 3 shows the security measure to be considered for the process step and what mechanism applies.

| Step                      | Description   | Security Measure   |
|---------------------------|---|--|
| User authentication       | Users log on to the system  | Authentication process based on SAML 2.0 Standard takes place.<br><br>Access credentials are not stored on site.<br><br>Invalid session IDs and cookies are intercepted. |
| Document upload           | Users can upload JSONs for their own apps (Metadata Modeling app)                                 | A JSON parser validates structures   |
| User administrative tasks | Administrators can add and remove user accounts, and change the role assignments of user accounts | Division of responsibilities ensures that only company Administrators can carry out the listed user administrative tasks.  |

Table 3: Security Measures that Apply

# 4 User Administration, Authentication, and Authorizations

SAP Logistics Business Network, global track and trace option uses the authentication mechanisms provided by SAP Cloud Identity (SCI) service. The user management itself is product specific and does not rely on any external tools.

## User Management

User management makes use of SCI service facilities.

- **User Administration Tools**  
SAP Logistics Business Network, global track and trace option uses the user administration provided by the SCI to manage users. System Administrators can add, remove and edit users. They can also provide/ revoke multiple pre-defined roles to users. Access control lists limit access to data only to permitted roles, companies and users (instance-based authorization).  
Product-specific roles are predefined including the following:
  - Solution Administrator
  - User Administrator
- **UAA Identity Zone**  
SAP User Account and Authentication Service (SAP UAA) is used as an authorization server. For each tenant, a dedicated UAA instance (sometimes referred to as identity zone) is provided.  
SAP UAA serves the purpose of assigning and checking of functional authorizations. These functional authorizations (also known as UAA scopes) control whether a particular user has the permission to start a given service.  
They are assigned to roles provided by the UAA service. For easier administration, the roles are then bundled to UAA role collections, which in turn are assigned to user groups provided by the SCI service.

## User Authorizations

It's important to consider the security-aspects of creating and configuring users and roles for the applications.

Consider the following security-aspects:

- Grant users only the minimum level of authorization that's necessary.
- Remove a user's authorization as soon as it's no longer required, for example if an employee leaves the company.



# 5 Data Storage Security

SAP Logistics Business Network, global track and trace option stores data in dedicated databases. Access to the databases comes preconfigured with the infrastructure environment.

The databases contain many different types of data including the following:

- personal data (for example user names, email addresses and so on)
- operational business data, as well as
- preferences and configurations.

This data is updated continuously whenever required or requested.

# 6 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data protection and privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries/regions. SAP provides specific features and functions to support compliance with regard to relevant legal requirements, including data protection. SAP does 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 information should not be taken as advice or a 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 landscape and the applicable legal requirements.

## i 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.

## ⚠ Caution

The extent to which data protection is supported by technical means 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.

## 6.1 Glossary

The following terms are general to SAP products. Not all terms may be relevant for this SAP product.

| Term                    | Definition  |
|-------------------------|---|
| <b>Blocking</b>         | A method of restricting access to data for which the primary business purpose has ended.  |
| <b>Business Purpose</b> | The legal, contractual, or in other form justified reason for the processing of personal data to complete an end-to-end business process. The personal data used to complete the process is predefined in a purpose, which is defined by the data controller. The process must be defined before the personal data required to fulfill the purpose can be determined. |

| Term                              | Definition  |
|-----------------------------------|---|
| <b>Consent</b>                    | 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.  |
| <b>Data Subject</b>               | 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. |
| <b>Deletion</b>                   | Deletion of <b>personal data</b> so that the data is no longer available.   |
| <b>End of business</b>            | Defines the end of active business and the start of residence time and retention period.  |
| <b>End of Purpose (EoP)</b>       | The point in time when the processing of a set of personal data is no longer required for the primary business purpose, for example, when a contract is fulfilled. After the EoP has been reached, the data is blocked and can only be accessed by users with special authorizations (for example, tax auditors).   |
| <b>End of Purpose (EoP) check</b> | A method of identifying the point in time for a data set when the processing of <b>personal data</b> is no longer required for the primary <b>business purpose</b> . After the <b>EoP</b> has been reached, the data is <b>blocked</b> and can only be accessed by users with special authorization, for example, tax auditors.   |
| <b>Personal Data</b>              | 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. |
| <b>Purpose</b>                    | The information that specifies the reason and the goal for the processing of a specific set of personal data. As a rule, the purpose references the relevant legal basis for the processing of personal data.   |

| Term  | Definition   |
|---|--|
| 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.  |
| Sensitive Personal Data                     | <p data-bbox="804 797 1386 860">A category of personal data that usually includes the following type of information:</p> <ul data-bbox="815 882 1398 1229" style="list-style-type: none"> <li data-bbox="815 882 1398 1046">• Special categories of personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or sex life or sexual orientation.</li> <li data-bbox="815 1059 1294 1081">• Personal data subject to professional secrecy</li> <li data-bbox="815 1095 1374 1158">• Personal data relating to criminal or administrative offenses</li> <li data-bbox="815 1171 1398 1229">• Personal data concerning insurances and bank or credit card accounts</li> </ul>   |
| Technical and Organizational Measures (TOM) | <p data-bbox="804 1267 1398 1431">Some basic requirements that support data protection and privacy are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and privacy and require appropriate TOMs, for example:</p> <ul data-bbox="815 1453 1398 1744" style="list-style-type: none"> <li data-bbox="815 1453 1238 1476">• <b>Access control</b> Authentication features</li> <li data-bbox="815 1489 1227 1512">• <b>Authorizations</b> Authorization concept</li> <li data-bbox="815 1525 1059 1547">• <b>Read access logging</b></li> <li data-bbox="815 1561 1326 1583">• <b>Transmission control/communication security</b></li> <li data-bbox="815 1597 1150 1619">• <b>Input control/change logging</b></li> <li data-bbox="815 1632 1043 1655">• <b>Availability control</b></li> <li data-bbox="815 1668 1398 1744">• <b>Separation by purpose</b> Subject to the organizational model implemented and must be applied as part of the authorization concept.</li> </ul> |

## 6.2 User Consent

Any personal data collected or processed must be linked to a specific, pre-defined purpose, such as the fulfilment of a contract or legal obligation. If there is no other legal basis for the lawful processing of personal data or - in some cases - if the data is to be sent to a third party, you must obtain consent from the data subject to use their personal data. SAP applications ask for consent of the data subject before collecting any personal data. In some cases, the data subject may also be the user. This SAP product provides functionality that allows data subjects to give and withdraw consent to collect and process their personal data. SAP assumes that the user, for example, an SAP customer collecting data, has consent from its data subject (a natural person such as a customer, contact, or account) to collect or transfer data to the solution.

## 6.3 Read Access Logging

Read access to personal data is partially based on legislation, and it is subject to logging functionality. 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. Read access logging enables you to answer questions about who accessed particular data within a specified time frame. Here are some examples of such questions:

- Who accessed the data of a given business entity, for example a bank account?
- Who accessed personal data, for example of a business partner?
- Which employee accessed personal information, for example religion?
- Which accounts or business partners were accessed by which users?

From a technical point of view, this means that all remote APIs and UI infrastructures (that access the data) must be enabled for logging.

Cloud products using SAP HANA XS and SAP HANA standalone use the audit trail and audit policies for change logging. For more information, see the [Auditing Activity section](#) in the SAP HANA Security Guide.

SAP Logistics Business Network, global track and trace option includes a feature that logs accesses of sensitive personal data in the system. The feature helps to analyze data access of sensitive personal data.

The Audit Log Viewer allows you to access audit logs.

- To view the GTT audit logs for a given time period, see the section [Access the Audit Log Viewer \[page 25\]](#).
- For more information on the Audit Log Viewer, see the [Audit Log Viewer for the Cloud Foundry Environment](#).

## 6.4 Information Report

Data subjects have the right to receive information regarding their personal data undergoing processing. The personal data record feature helps you to comply with the relevant legal requirements for data protection by

allowing you to search for and retrieve all personal data for a specified data subject. The search results are displayed in a comprehensive and structured list containing all personal data of the data subject specified, organized according to the purpose for which the data was collected and processed.

The Manage Personal Data (MPD) app uses the Personal Data Manager (PDM) service to extract personal data stored about a data subject. For more information about the MPD app, see the [Appendix \[page 30\]](#).

The company that owns the data is the data controller. If a data subject wants to know which data is stored about him or her, he or she shall contact their data controller.

The following predefined roles are included as standard:

- DP&P Specialist: is authorized to deal with requests from data subjects concerning their personal data and sensitive personal data
- Audit Specialist: is authorized to view, for the purpose of DP&P auditing, all GTT data including personal data and sensitive personal data

### **i** Note

You can use annotations to identify any data that you wish to classify as being personal data or sensitive personal data. For more information, see the [Creating and Deploying GTT Models](#) documentation that is available from the SAP Help Portal under <https://help.sap.com/gtt>.

## **Set up Access to Personal Data**

To set up access for DP&P Specialists to view the personal data of data subjects, you must do the following:

1. Assign the business users to the user group  
You assign the user group *TT\_AUDITOR* or *TT\_DATA\_PRIVACY\_SPECIALIST* to a user using the Administration Console for SAP Identity Authentication Service.  
For further information, see the Onboarding guide under the section: Assign User Groups to a User.
2. View assigned business roles  
You can see the assigned business role, Auditor Specialist or DP&P Specialist, in the user's business role list in the Manage GTT Users (MGU) app.  
For further information, see the Administration guide under the chapter: User Management by Other Roles.

### **i** Note

Both the Onboarding and Administration guides are available from the SAP Help Portal under <https://help.sap.com/gtt>.

## **Retrieve Personal Information**

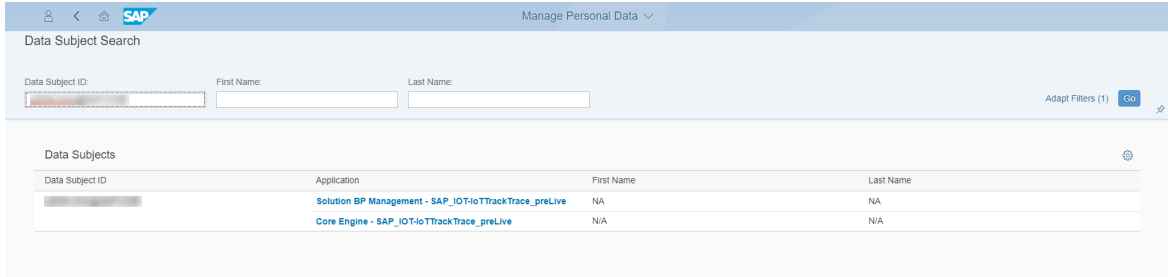
To retrieve personal information about a data subject, you, as the DP&P specialist must do the following:

Prerequisite: You must be able to access the Manage Personal Data (MPD) app of the PDM service.

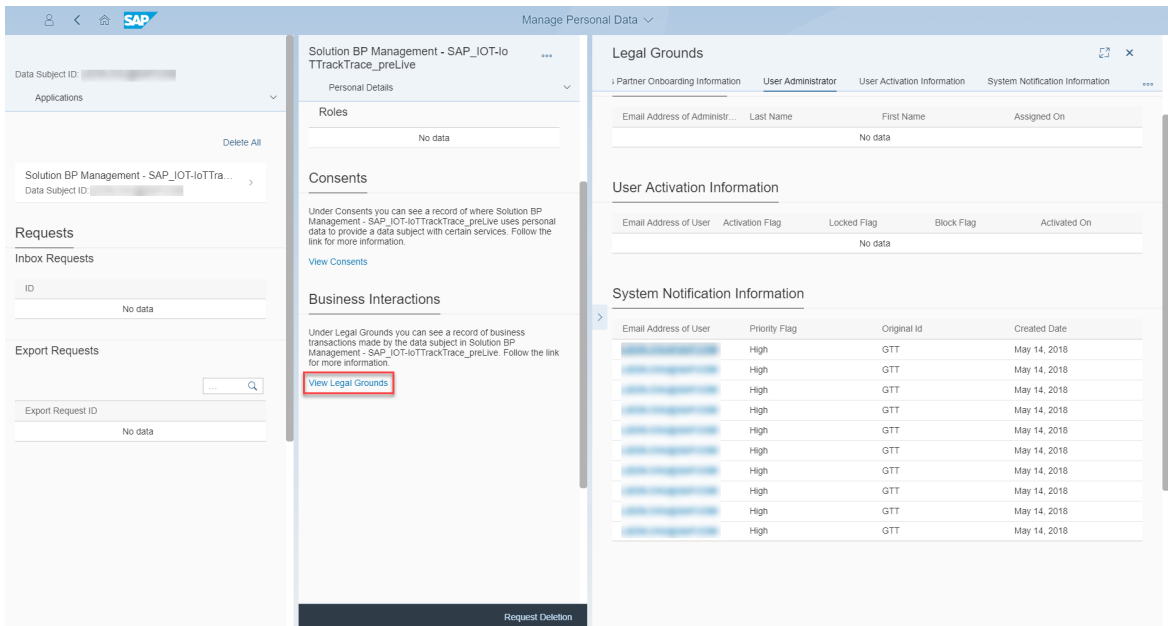
1. Start the MPD app. To do so, in your SAP Cloud Foundry subaccount find the *Personal Data Manager* tile and click *Go to Application*.
2. In the *Data Subject Search* page, enter the email address of the data subject as the *Data Subject ID* and then press the *Enter* key or click the *Go* button.
3. If any personal information is found for the data subject, the data subject is listed in section *Data Subjects*, with one or more links to an application(s). The following links may appear:
  1. Solution BP Management for business partner management.
  2. Master Data Management for master data management.

3. Metadata-service for metadata service (that is model management).
4. Core Engine for tracked processes.

An example is shown in the following screenshot:



4. Click the link of the application, and you are navigated to the second page of the *MPD* app.
5. Click the area with the application name and the email address (that is the *Data Subject ID*), a new pane with some detailed information is displayed on the right.
6. In the section *Business Interactions*, click the link *View Legal Grounds* to open further detailed information in a new pane on the right.
7. In the section *System Notification Information* of the new pane, a list of the metadata of the system notifications sent to the data subject is displayed. You can see the *Email Address of User*, *Priority Flag*, *Original ID* and the *Created Date*. This is shown in the following screenshot:



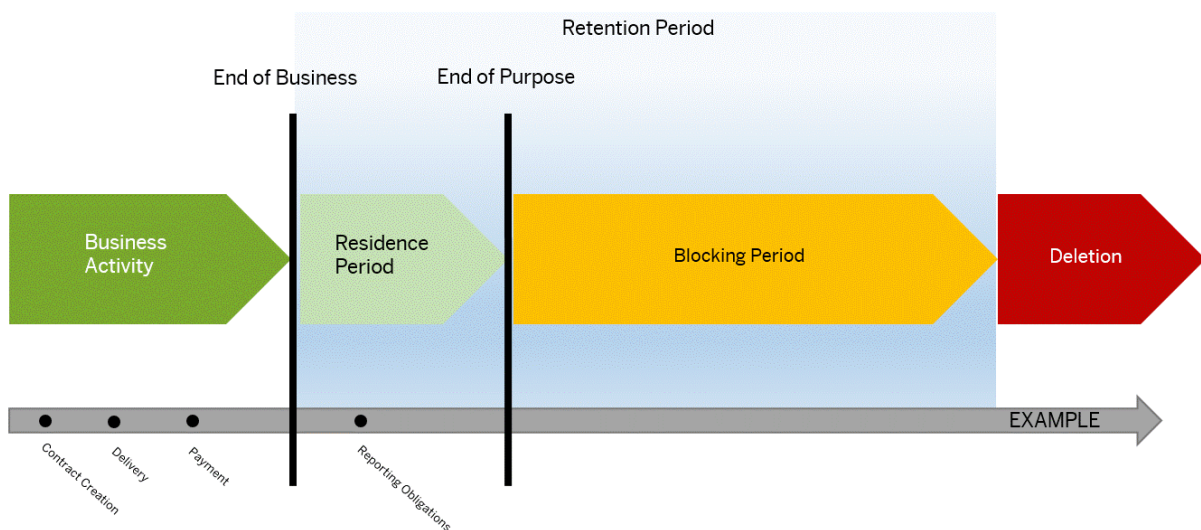
8. Retrieve the personal data and make it available securely to the data subject.

## 6.5 Deletion of Personal Data

### Simplified Blocking and Deletion

An end of purpose (EoP) check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period is part of the overall lifecycle of personal data, which consists of the following phases:

- **Business activity:** The relevant data is used in ongoing business, for example contract creation, delivery or payment.
- **Residence period:** The relevant data remains in the database and can be used in case of subsequent processes related to the original purpose, for example reporting obligations.
- **Blocking period:** The relevant data needs to be retained for legal reasons. During the blocking period, business users of SAP applications are prevented from displaying and using this data. It can only be processed in case of mandatory legal provisions.
- **Deletion:** The data is deleted and no longer exists in the database.



When considering compliance with data protection regulations, it is also necessary to consider compliance with industry-specific legislation in different countries/regions. A typical potential scenario in certain countries/regions is that personal data shall be deleted after the specified, explicit, and legitimate purpose for the processing of personal data has ended, but only as long as no other retention periods are defined in legislation, for example, retention periods for financial documents. Legal requirements in certain scenarios or countries/regions also often require blocking of data in cases where the specified, explicit, and legitimate purposes for the processing of this data have ended, however, the data still has to be retained in the database due to other legally mandated retention periods. In some scenarios, personal data also includes referenced data. Therefore, the challenge for deletion and blocking is first to handle referenced data and finally other data, such as business partner data.



## Deletion of Personal Data

The processing of personal data is subject to applicable laws related to the deletion of this data when the specified, explicit, and legitimate purpose for processing this personal data has expired. If there is no longer a legitimate purpose that requires the retention and use of personal data, it must be deleted. When deleting data in a data set, all referenced objects related to that data set must be deleted as well. Industry-specific legislation in different countries/regions also needs to be taken into consideration in addition to general data protection laws. After the expiration of the longest retention period, the data must be deleted.

In SAP Logistics Business Network, global track and trace option, personal data can be found in the following:

1. GTT model metadata change history
2. Master data
3. Business partner data
4. Core engine
5. Error logs

The following sections detail how to delete personal data from each part that is listed.

### 1. Delete Metadata Change History

By default, the *GTT Model Management (GMM)* app keeps the change history of each GTT metadata model since the model was first deployed. You can delete the change history either by enabling auto deletion or by manually deleting the change history of a specific model.


#### i Note

Once change history is deleted, either automatically or manually, you cannot restore it.

#### Auto Deletion

You can enable auto deletion to let the *GMM* app automatically delete change history that is older than a specified time. Auto deletion runs on a daily basis and applies to all deployed models in your tenant.

To enable auto deletion, proceed as follows:

1. Launch the *GMM* app.
2. In the right-hand *Change History* pane, choose the  icon.
3. In the *Retention Settings* dialog box, specify the number of days in the text box for deleting change history.
4. Choose *OK*.


To disable auto deletion, clear the text box for deleting change history. Then the *GMM* app stops automatically deleting change history.

#### Manual Deletion

You can manually delete all the change history of a specific model by doing either of the following.

To delete a model's change history in the *Search* page:

1. Launch the *GMM* app.

2. In the right-hand *Change History* pane, choose the  icon.
3. In the *Retention Settings* dialog box, choose the *Delete Change History* tab.
4. Specify your target model and choose *OK*.
5. In the confirmation dialog box, choose *Delete*.

To delete a model's change history in the *Model Details* page:

1. Launch the *GMM* app.
2. In the search page, select your target model.
3. In the *Model Details* page, choose the *Change History* tab.
4. Above the changes list, choose *Delete Change History*.
5. In the confirmation dialog box, choose *Delete*.

## 2. Delete Master Data

The *Manage Personal Data (MPD)* app allows DP&P specialists to perform the following tasks on master data (location or business partner):

- block personal data
- delete blocked personal data.

### i Note

In this section, business partner refers to a business entity or organization. To delete personal data of a business partner user, see the section *Delete Business Partner Data*.

#### To block personal data in master data:

### i Note

Currently, it is not possible to unblock personal data once it has been blocked. So, before blocking personal data, check carefully that it is personal data that you actually want to block!

1. Launch the *MPD* app.
2. Specify the data subject ID and the data type (business partner or location), and then select *Go* at the upper-right corner.
3. In the left pane, you then see the personal data of the selected data subject. This has either been created or changed, or it is the email address of the data subject.
4. From the *Business Data* list, select the entry that contains the personal data you want to block. The detailed information of the selected entry is shown on the right pane.

### i Note

You can proceed only when all numbers in both the *Business Active* and *End of Business* columns are zero. If this is not true, the *Block* button is disabled.

5. Choose *Block* at the upper-right corner and confirm.

The tracked process that uses the blocked data is no longer visible to business users. The blocked data cannot be displayed in the *MBP* and *ML* apps. Further, the blocked data cannot be used by new tracked processes.

### i Note

In the *MPD* app, the DP&P specialist can still view the blocked data. The audit specialist can still view the blocked data in the *PDM* service.

#### To delete blocked personal data in master data:

### i Note

Block and delete are linked functions. You can only delete data that has been blocked.

1. Launch the *MPD* app.
2. Specify the data subject ID and the data type (business partner or location), and then select *Go* at the upper-right corner.
3. From the *Business Data* list, select the entry that contains the personal data you want to delete. The detailed information of the selected entry is shown on the right pane.

### i Note

You can proceed only when all numbers in both the *Business Active* and *End of Business* columns are zero. If this is not true, the *Delete* button is disabled.

4. Choose *Delete* at the upper-right corner and confirm.

The selected personal data is immediately deleted. It is not possible to retrieve this deleted personal data.

## 3. Delete Business Partner Data

### i Note

In this section, business partner refers to a business user. To delete personal data of a business partner entity or organization, see the section Delete Master Data.

The *Manage GTT Users (MGU)* app allows DP&P specialists to perform the following tasks on business partner data:

- block the personal information of a user
- unblock the personal information of a user
- delete one or more blocked users from a solution.

Prerequisites: You work for a participant of a solution or the solution owner and you are able to log on to the *MGU* app as a DP&P specialist for data protection.

#### To block the personal information for a user:

1. Navigate to the *Active Users* list or the *Locked Users* list.
2. From the list, locate the user whose personal information you want to block, and then click *Block* at the upper-right corner.
3. Click *Block* again to confirm.

After being blocked, the personal information of the user cannot be viewed by other users. However, audit specialists can view the information for auditing purposes.

### To unblock the personal information for a user:

1. Navigate to the *Blocked Users* list.
2. From the list, locate the user whose information you want to unblock and then click *Unblock* at the upper-right corner.
3. Click *Unblock* again to confirm.

After being unblocked, the personal user information of the unblocked user can be viewed again by other users.

### To delete one or more blocked users from a solution:

1. Navigate to the *Blocked Users* list.
2. From the list, use the checkboxes to select the user(s) you want to delete from the solution. From the list, locate the user who you want to delete, and then click *Delete* on the upper right corner.
3. Click *Delete* again to confirm.

The selected users are deleted and are unable to log on.

## 4. Delete Core Engine Data

Within the core engine, you can delete personal data from the following:

1. A Tracked Process

### i. Delete A Tracked Process

A complete tracked process can be automatically deleted at the end of its lifetime and after its residence period. Any personal data in the tracked process is deleted at the same time. Auto deletion of a tracked process is implemented by the event-to-action engine.

You need to establish that the last expected event triggers actions that determine the retention and residence periods. You also need to ensure that at the end of the blocking period, conditions are set so that the complete tracked process is automatically deleted. It can be triggered by any suitable condition and any of the available business rule actions can be used to implement it.

The following example describes how to use the event-to-action engine to automatically trigger deletion of a specific tracked process.

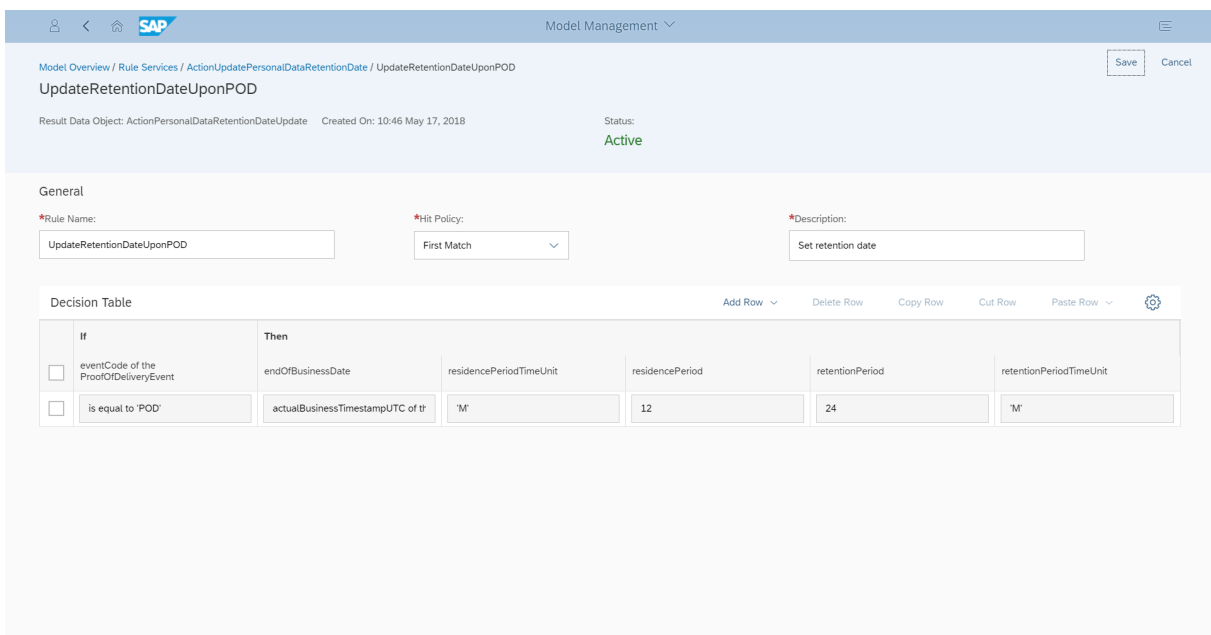
1. An outbound delivery tracking scenario is modeled that includes the following personal data for the responsible planner:

```
@DPP.DataSubjectID
@dpp.PII
planner: String(50) @title:'Responsible Planner Email';
@dpp.PII
plannerMobilePhone: String(50) @title:'Responsible Planner Mobile Phone';
@dpp.PII
plannerFirstName: String(50) @title:'Responsible Planner Mobile Phone';
@dpp.PII
plannerLastName: String(50) @title:'Responsible Planner Mobile Phone';
@dpp.SPI
plannerID: String(50) @title:'Responsible Planner Identity Number';
```

2. Whenever a CDS model is deployed, a background metadata service checks if there are valid DPP.\* annotations. If there are, this tracked process includes personal data and two internal planned events are added as the admissible planned events:

- GTT\_DPP\_BLOCK
- GTT\_DPP\_DELETE

3. You must define a business rule that when a `ProofOfDeliveryEvent` is received, the tracked process is set to end of business for retention. Further, the reference date when the retention rule applies is the actual `BusinessTimestampUTC` of the reported `ProofOfDeliveryEvent`, based on the legal agreement between the customer and the planner. After the residence period (for example 12 months since the related outbound delivery tracked process was set to end of business) only users with special authorization are able to see the planner's personal data. For all other users who access the outbound delivery tracked process, the planner's personal data is not visible. After another 12 months (in total 24 months after the end of business date), the planner's personal data needs to be erased from the related outbound delivery tracked process. This can be done automatically using the following retention rules based on business rule action `ActionUpdatePersonalDataRetentionDate`:



4. The outbound delivery tracked process data is sent to the GTT system.

5. The following business events are posted to the outbound delivery tracked process:

- PickingCompletedEvent
- GoodsIssuedEvent
- ProofOfDeliveryEvent

6. When the `ProofOfDeliveryEvent` is received, the rule `UpdateRetentionDateUponPOD` is triggered with action `ActionUpdatePersonalDataRetentionDate`.

- Update the `personalDataProtectionStatus` in the tracked process from '' to 'End of Business'. A new field is added to the core tracked process entity:

```
personalDataProtectionStatus      : String(20) @title: 'DPP Status' enum {
                                     businessActive = 'BA'
                                     endOfBusiness  = 'EOB'
                                     endOfPurpose   = 'EOP'
                                     @title: 'Business Active';
                                     @title: 'End of Business';
                                     @title: 'End of Purpose';
```

```
} default 'BA';)
```

- If the ResidencePeriod in Time Unit >0, this means there is still some residence period left and the block event is needed. It should update and insert a planned event `GTT_DPP_BLOCK` into the outbound delivery tracked process event directory with the following values: (add M/D/Y etc).

| Field                        | Value  |
|------------------------------|--|
| eventCode                    | GTT_DPP_BLOCK                                |
| eventType                    | com.sap.gtt.core. GTT_DPP_BLOCK              |
| eventStatus                  | PLANNED                                      |
| plannedBusinessTimestampUTC  | ReferenceDate + ResidencePeriod in Time Unit |
| plannedBizTsEarliestUTC      | ReferenceDate + ResidencePeriod in Time Unit |
| plannedBizTsLatestUTC        | ReferenceDate + ResidencePeriod in Time Unit |
| plannedTechnicalTimestampUTC | ReferenceDate + ResidencePeriod in Time Unit |
| plannedTechTsEarliestUTC     | ReferenceDate + ResidencePeriod in Time Unit |
| plannedTechTsLatestUTC       | ReferenceDate + ResidencePeriod in Time Unit |

If the Residence Period in Time Unit is =0 or empty, no insert and update of `GTT_DPP_BLOCK` is needed. If Residence Period in Time Unit is <0, `ActionUpdatePersonalDataRetentionDate` should stop the execution and throw an exception.

- If the Retention Period in Time Unit >0, this means there is still residence period left and the block event is needed. It should update and insert a planned event `GTT_DPP_DELETE` into the outbound delivery tracked process event directory with the following values:

| Field                        | Value                                  |
|------------------------------|--|
| eventCode                    | GTT_DPP_DELETE                         |
| eventType                    | com.sap.gtt.core. GTT_DPP_DELETE       |
| eventStatus                  | PLANNED                                |
| plannedBusinessTimestampUTC  | ReferenceDate + Retention in Time Unit |
| plannedBizTsEarliestUTC      | ReferenceDate + Retention in Time Unit |
| plannedBizTsLatestUTC        | ReferenceDate + Retention in Time Unit |
| plannedTechnicalTimestampUTC | ReferenceDate + Retention in Time Unit |
| plannedTechTsEarliestUTC     | ReferenceDate + Retention in Time Unit |

| Field                  | Value                                  |
|------------------------|--|
| plannedTechTsLatestUTC | ReferenceDate + Retention in Time Unit |

- If the Retention Period in Time Unit is =0 or empty, no `GTT_DPP_DELETE` update and insert is needed.
- If the Retention Period in Time Unit <0 or Retention Period in Time Unit < Residence Period in Time Unit , `ActionUpdatePersonalDataRetentionDate` should stop the execution and throw an exception
- If the Retention Period in Time Unit = Retention Period in Time Unit and both of them > 0, only retention period is considered, thus only `GTT_DPP_DELETE` event is needed

7. If the POD event has been reported or corrected several times, the `UpdateRetentionDateUponPOD` should recalculate the date and update and insert the planned retention events according to logic in the previous step.

8. Now if a business user starts the *Global Track and Trace (GTT)* app and views this completed outbound delivery, he or she sees two new planned events, `GTT_DPP_BLOCK` and `GTT_DPP_DELETE`, each with the status `Planned`:

| Event                 | Event Status | Event Reason                                      | Location | Planned Business Time               | Actual Business Time                | Created By                      | Created At               |
|-----------------------|--------------|---|----------|-------------------------------------|-------------------------------------|---------------------------------|--------------------------|
| Picking completed     | Planned      |   |          | Mar 16, 2018, 01:38:48 PM Etc/GMT-8 |                                     |                                 |                          |
| Delayed               | Unplanned    | Traffic Jam At 2018-03-16T13:38:52                |          |                                     | Mar 16, 2018, 01:38:52 PM Etc/GMT-8 | int_coreintegration_comfortcars | Mar 16, 2018, 1:39:00 PM |
| Proof of delivery     | Reported     | Proof of Delivery Received At 2018-03-16T13:38:54 |          | Mar 16, 2018, 01:48:48 PM Etc/GMT-8 | Mar 16, 2018, 01:38:54 PM Etc/GMT-8 | int_coreintegration_comfortcars | Mar 16, 2018, 1:39:04 PM |
| In Transit            | Reported     | InTransit Location Update At 2018-03-16T13:38:55  |          | Mar 16, 2018, 01:48:48 PM Etc/GMT-8 | Mar 16, 2018, 01:38:55 PM Etc/GMT-8 | int_coreintegration_comfortcars | Mar 16, 2018, 1:39:08 PM |
| Goods issued          | Planned      |   |          | Mar 16, 2018, 01:43:48 PM Etc/GMT-8 |                                     |                                 |                          |
| Personal Data Blocked | Planned      |   |          | Mar 16, 2018, 01:48:48 PM Etc/GMT-8 |                                     |                                 |                          |
| Personal Data Deleted | Planned      |   |          | Mar 16, 2018, 01:48:48 PM Etc/GMT-8 |                                     |                                 |                          |

9. When the residence period ends (in this case 12 months later), the overdue batch job detects `GTT_DPP_BLOCK` is overdue. The overdue job does the following:

- Instead of update `GTT_DPP_BLOCK` status to `Overdue`, report an actual event to `GTT_DPP_BLOCK`, no overdue internal event is needed.
- Update the field `DataProtectionStatus` from 'End of Business' to 'End of Business Purpose'.

10. Now in the *GTT* app, if a business user checks the tracked process, he or she can find it and see that `GTT_DPP_BLOCK` has been reported. But he or she can't see the tracked process anymore.

### Note

If a DP&P specialist checks the tracked process in the *GTT* app, he or she also finds that `GTT_DPP_BLOCK` has been reported. However, unlike the business user, he or she can still see the tracked process and the planner's personal data.

11. When the blocking period ends (in this case another 12 months later), the overdue batch job detects `GTT_DPP_DELETE` is overdue and the overdue job does the following:

- Delete the complete tracked process and all related process event directory entries.
- The Audit service log is triggered to record the deletion action.

12. At this point if a business user checks the tracked process in the [GTT](#) app, he or she cannot find it. All data has been deleted, so even the DP&P specialist cannot see anything.

## 5. Set the Retention Period for Error Logs

The Manage Advanced Settings app contains a DP&P-related option for setting the retention period for error logs displayed in the Monitor Processing Errors app. Error logs older than the specified retention period are deleted.

Prerequisite: You must have a user with the role solution administrator.

Procedure

1. In the SAP Fiori Launchpad, open the Manage Advanced Settings app.
2. Click the [Parameter Settings](#) tab.
3. In the [Retention Period](#) area, click the [Edit](#) button and set the retention period (default=90 days). You can either type in the text box or use the slider. The retention period must be an integer between 1 and 365 inclusive.
4. Click [Save](#).

Result

The retention period for error logs displayed in the Monitor Processing Errors app is changed to the value you saved.

### **i** Note

There is a delay of around 24 hours before the new retention period becomes active.

## 6.6 Change Log

Creation and change of personal data need to be documented. Therefore, for review purposes or as a result of legal regulations, it may be necessary to track the changes made to this data. When these changes are logged, you should be able to check which employee made which change, the date and time, the previous value, and the current value, depending on the configuration. It is also possible to analyze errors in this way.

Cloud products using SAP HANA XS and SAP HANA standalone use the audit trail and audit policies for change logging. For more information, see the [Auditing Activity section](#) in the SAP HANA Security Guide.

There is a feature that logs changes of personal data and sensitive personal data in the GTT system. The feature helps to analyze modification of personal data and sensitive personal data.

The Audit Log Viewer allows you to access change logs. To view the GTT change logs for a given time period, see the section [Access the Audit Log Viewer \[page 25\]](#). For more information on the Audit Log Viewer, see the [Audit Log Viewer for the Cloud Foundry Environment](#).



## 6.7 Tasks for Audit Specialists

Audit specialists are authorized to view, for the purpose of DP&P auditing, all GTT data and can do the following:

- [Access the Audit Log Viewer \[page 25\]](#)
- [View Blocked Master Data \[page 26\]](#)

### 6.7.1 Access the Audit Log Viewer

#### Context

Prerequisites:

To access the audit log viewer, you need to be assigned:

- the role solution administrator and
- the role audit specialist

#### Procedure

1. Log on to the SAP Business Technology Platform cockpit.
2. Choose your global account and cloud foundry subaccount.
3. Choose *Subscriptions*.
4. Find the tile, *Audit Log Viewer*, and click *Go to Application*.
5. Fill in your account information and log in.
6. Select the *Time Range* and click *Reload*. You can see the audit logs for your selected time range.
7. To view the information for all users, navigate to the *Users* list.

#### Results

You can see the audit logs for your selected time range. Depending on your authorization, the list displays all users from either the solution participant or solution owner.

##### **i** Note

The list includes blocked users but not deleted users.

For more information on the [Audit Log Viewer](#), see the [Audit Log Viewer for the Cloud Foundry Environment](#).

## 6.7.2 View Blocked Master Data

Audit specialists can view blocked master data in a specific subdomain via the following Restful API.

```
<homepage URL>/saplbnmanageLocationservice.saplbnmanageLocations/odata/v2/BlockingStoreService/BlockingStore?$format=json
```

For example, an audit specialist can view the blocked master data in the “first-shipper” subdomain by accessing the following Restful API.

```
https://first-shipper.cfapps.sap.hana.ondemand.com/saplbnmanageLocationservice.saplbnmanageLocations/odata/v2/BlockingStoreService/BlockingStore?$format=json
```

To enable an audit specialist to view blocked master data in a specific subdomain, you must create the `<subdomain>_lbn_md_auditor` role collection and then assign it to the audit specialist.

If the name of a subdomain contains one or more hyphens ('-'), replace them with underscores ('\_') when composing the role collection name. Take the subdomain 'first-shipper' for example, use `first_shipper_lbn_md_aditor` as the role collection name.

The response of the API is as follows:

### Sample Code

```
{
  "d": {
    "results": [
      {
        "_metadata": {
          "id": "https://first-shipper.cfapps.sap.hana.ondemand.com/odata/v2/BlockingStoreService/BlockingStore('61e878f9-b8de-4b96-ad86-51c29d2b34ff')",
          "uri": "https://first-shipper.cfapps.sap.hana.ondemand.com/odata/v2/BlockingStoreService/BlockingStore('61e878f9-b8de-4b96-ad86-51c29d2b34ff')",
          "type": "BlockingStoreService.BlockingStore"
        },
        "Blocking_Store_GUID": "61e878f9-b8de-4b96-ad86-51c29d2b34ff",
        "External_GUID": "2e4b503d-a8bf-4091-a257-911d8ef00a24",
        "App_GUID": "LocationService-GUID",
        "End_Of_Business_Date": "/Date(1478850840000)/",
        "End_Of_Residence_Date": "/Date(1573458840000)/",
        "End_Of_Blocking_Date": "/Date(1668066840000)/",
        "Created_On": "/Date(1573458841000)/",
        "Updated_On": "/Date(1573458841000)/",
        "Sub_Domain_Id": "first-shipper",
        "Status": "Blocked",
        "App_Name": "LocationService",
        "Data": "{\"to_Address_Id\":null,\"to_LocationTextDescription\":{\"id\":\"530cd578-f069-4710-ad7a-ea33693059bf\",\"languageCode\":null,\"locationDescription\":\"New Nanjing Office #5\",\"location_Id\":null,\"location\":null,\"to_LocationText\":[],\"to_MultipleLocationType\":[],\"to_AlternativeIdentifier\":[],\"to_ObjectType\":null,\"to_Address\":{\"to_DefaultFax\":null,\"to_DefaultWorkplaceAddress\":null,\"to_DefaultMobilePhone\":null,\"to_DefaultEmail\":{\"id\":\"051b19b2-2826-4fdd-afdf-eaf24237c0a4\",\"parent_Id\":null,\"validityStartDate\":null,\"validityEndDate\":null,\"isDefaultEmailAddress\":true,\"emailAddress\":null},\"to_DefaultPostalAddress\":{\"to_CountryCode
```

```

\":null,\"to_CorrespondenceLanguageCode\":null,\"to_RegionCode\":null,
\"to_PoBoxDeviatingRegionCode\":null,\"to_PoBoxDeviatingCountryCode\":null,
\"id\":\":null,\"parent_Id\":null,
\"scriptCode\":\":null,\"correspondenceLanguage\":null,\"poBox\":null,
\"poBoxIsWithoutNumber\":null,\"poBoxPostalCode\":null,\"poBoxDeviatingCountry
\":null,\"poBoxDeviatingRegion\":null,\"postalCode\":\":250005\",
\"companyPostalCode\":null,\"streetName\":null,\"streetPrefixName\":null,
\"additionalStreetPrefixName\":null,\"streetSuffixName\":null,
\"additionalStreetSuffixName\":null,\"houseNumber\":null,
\"houseNumberSupplementText\":null,\"cityCode\":null,\"cityName\":\":Nan_Jing
\",\":null,\"district\":\":Gulou District\",\":country\":
\":CN\",\":region\":null,\"addressTimeZone\":null,\"county\":null,\"building
\":null,\"floor\":null,\"roomNumber\":null,\"careOfName\":null,
\"poBoxLobbyName\":null,\"poBoxDeviatingCityName\":null,\"latitude\":null,
\"longitude\":null,\"deliveryServiceNumber\":null,\"deliveryServiceTypeCode
\":null,\"to_DefaultPerson\":null,\"to_DefaultOrganization\":null,
\"to_DefaultLandlinePhone\":\":{\"to_CountryCode\":null,\"id\":\":6a2c5a6d-
f8ba-43af-8c39-254d3470207d\",\":parent_Id\":null,\"validityStartDate\":null,
\"validityEndDate\":null,\"isDefaultPhoneNumber\":null,
\"destinationLocationCountry\":null,\"numberType\":\":1\",
\"numberExtension\":null,\"to_PostalAddressTextDescription\":null,
\"to_DefaultWeb\":null,\"to_WorkplaceAddress\"::[],\"to_Fax\"::[],\"to_Person\":
:[],\"to_LandlinePhone\"::[],\"to_PostalAddress\"::[],\"to_Web\"::[],\"to_Email\":
:[],\"to_Organization\"::[],\"to_MobilePhone\"::[],\"to_pcmtc\":null,\"id\":
\":f89995fd-637b-42fe-a15d-5bf248fd3abc\",\":addressType\":null,
\"prfrdCommMediumType\":null,\"to_LocationType\":null,\"id\":\":2e4b503d-
a8bf-4091-a257-911d8ef00a24\",\":modifiedAt\":1571220187000,\"createdAt\":
1571128173000,\"createdBy\":\":testuser@firstshippertest.com\",\":modifiedBy\":
\":testuser@firstshippertest.com\",\":tenantId\":null,\"serviceInstanceId
\":null,\"latitude\":null,\"longitude\":null,\"objectType\":\":Customer\",
\"sourceSystem\":\":LBN\",\":locationExternalId\":\":NANJING OFFICE NEW 005\",
\"locationId\":\":LBN:NANJING_OFFICE_NEW_005\",\":sourceUniversalObjectId\":
\":xri://sap.com/
id:LBN#9000001:LBN:Location:Customer:NANJING_OFFICE_NEW_005\",\":locationType
\":null,\"accessDateTime\":1478850840000},
  \"Tenant_Id\": \"d03a83e4-e354-4918-95cb-1c7dde769630\"
},
{
  \"metadata\": {
    \"id\": \"https://first-shipper.cfapps.sap.hana.ondemand.com/odata/v2/
BlockingStoreService/BlockingStore('fecae2b2-757f-43e0-9a0a-a5a29cc2f7d2')\",
    \"uri\": \"https://first-shipper.cfapps.sap.hana.ondemand.com/odata/v2/
BlockingStoreService/BlockingStore('fecae2b2-757f-43e0-9a0a-a5a29cc2f7d2')\",
    \"type\": \"BlockingStoreService.BlockingStore\"
  },
  \"Blocking_Store_GUID\": \"fecae2b2-757f-43e0-9a0a-a5a29cc2f7d2\",
  \"External_GUID\": \"cda2b4fa-f9dd-4ee5-ba80-e9e0b340f93d\",
  \"App_GUID\": \"LocationService-GUID\",
  \"End_Of_Business_Date\": \"/Date(1478850840000)/\",
  \"End_Of_Residence_Date\": \"/Date(1573458840000)/\",
  \"End_Of_Blocking_Date\": \"/Date(1668066840000)/\",
  \"Created_On\": \"/Date(1573458841000)/\",
  \"Updated_On\": \"/Date(1573458841000)/\",
  \"Sub_Domain_Id\": \"first-shipper\",
  \"Status\": \"Blocked\",
  \"App_Name\": \"LocationService\",
  \"Data\": \"{\":to_Address_Id\":null,\"to_LocationTextDescription\":\":{\"id
\":\":bf1d73f7-d32b-4d1f-937b-9c9c23d5c93c\",\":languageCode\":null,
\"locationDescription\":\":Beijing Office 002\",\":location_Id\":null,\"location
\":null},\"to_LocationText\"::[],\"to_MultipleLocationType\"::[],
\"to_AlternativeIdentifier\"::[],\"to_ObjectType\":null,\"to_Address\":
{\":to_DefaultFax\":null,\"to_DefaultWorkplaceAddress\":null,
\"to_DefaultMobilePhone\":null,\"to_DefaultEmail\":\":{\"id\":
\":a911bcdcf-9ddc-45c6-b271-2d9582da1a58\",\":parent_Id\":null,
\"validityStartDate\":null,\"validityEndDate\":null,\"isDefaultEmailAddress
\":true,\"emailAddress\":null},\"to_DefaultPostalAddress\":\":{\"to_CountryCode
\":null,\"to_CorrespondenceLanguageCode\":null,\"to_RegionCode\":null,
\"to_PoBoxDeviatingRegionCode\":null,\"to_PoBoxDeviatingCountryCode\":null,

```

```

\id\": \"259ffdc6-f894-4f30-a16e-829e7f6caa76\", \"parent_Id\": null,
\"scriptCode\": \" \", \"correspondenceLanguage\": null, \"poBox\": null,
\"poBoxIsWithoutNumber\": null, \"poBoxPostalCode\": null, \"poBoxDeviatingCountry
\": null, \"poBoxDeviatingRegion\": null, \"postalCode\": \"100125\",
\"companyPostalCode\": null, \"streetName\": \"Tianze Rd\", \"streetPrefixName
\": null, \"additionalStreetPrefixName\": null, \"streetSuffixName\": null,
\"additionalStreetSuffixName\": null, \"houseNumber\": \"16\",
\"houseNumberSupplementText\": null, \"cityCode\": null, \"cityName\": \"Beijing\",
\"additionalCityName\": null, \"district\": \"Chaoyang\", \"country\": \"CN\",
\"region\": null, \"addressTimeZone\": null, \"county\": null, \"building\": null,
\"floor\": null, \"roomNumber\": null, \"careOfName\": null, \"poBoxLobbyName
\": null, \"poBoxDeviatingCityName\": null, \"latitude\": null, \"longitude\": null,
\"deliveryServiceNumber\": null, \"deliveryServiceTypeCode\": null},
\"to_DefaultPerson\": null, \"to_DefaultOrganization\": null,
\"to_DefaultLandlinePhone\": {\"to_CountryCode\": null, \"id\":
\"44a4a0b7-5308-46e8-aeb8-3dec81d11356\", \"parent_Id\": null,
\"validityStartDate\": null, \"validityEndDate\": null, \"isDefaultPhoneNumber
\": null, \"destinationLocationCountry\": null, \"number\": null, \"numberType\":
\"1\", \"numberExtension\": null}, \"to_PostalAddressTextDescription\": null,
\"to_DefaultWeb\": null, \"to_WorkplaceAddress\": [], \"to_Fax\": [], \"to_Person\":
[], \"to_LandlinePhone\": [], \"to_PostalAddress\": [], \"to_Web\": [], \"to_Email\":
[], \"to_Organization\": [], \"to_MobilePhone\": [], \"to_pcmtc\": null, \"id\":
\"a049e2d5-3873-43a2-aa23-339cf72f52db\", \"addressType\": null,
\"prfrdCommMediumType\": null}, \"to_LocationType\": null, \"id\": \"cda2b4fa-
f9dd-4ee5-ba80-e9e0b340f93d\", \"modifiedAt\": 1569828259000, \"createdAt\":
1569572138000, \"createdBy\": \"testuser@firstshippertest.com\", \"modifiedBy\":
\"testuser@firstshippertest.com\", \"tenantId\": null, \"serviceInstanceId
\": null, \"latitude\": null, \"longitude\": null, \"objectType\": \"LogisticLocation
\", \"sourceSystem\": \"LBNTEST\", \"locationExternalId\": \"BJ_OFFICE_001\",
\"locationId\": \"LBNTEST:BJ_OFFICE_001\", \"sourceUniversalObjectId\": \"xri://
sap.com/id:LBN#90000001:LBNTEST:Location:LogisticLocation:BJ_OFFICE_001\",
\"locationType\": null, \"accessDateTime\": 1478850840000},
  \"Tenant_Id\": \"d03a83e4-e354-4918-95cb-1c7dde769630\"
}
]
}
}

```

## 7 Other Security-Related Information

SAP Logistics Business Network, global track and trace option is an SAP UI5-based application, and as such makes use of HTML5 and JavaScript. Active content (at least HTML5 and JavaScript) has to be enabled. This is mandatory, as the product will not work without it.

### Session Security Protection

SAP Logistics Business Network, global track and trace option is restricted to operating with Secure Socket Layer (SSL) and activated cookie handling in the browser only.

### Security Lifecycle Management

SAP Logistics Business Network, global track and trace option is operated by SAP. The Cloud Operations, Business Operations, DevOps, and Development Teams continuously monitor security-relevant issues and keep the system and software up to date.

# 8 Appendix

## i Note

In this standard appendix the following texts within the section Manage Personal Data, do not apply:

- Delete Personal Data – instead refer to the Data Protection and Privacy chapter under [Deletion of Personal Data \[page 16\]](#)
- Withdraw Consent.

## 8.1 Manage Personal Data

Find data subject records and inform data subjects about their personal data used and stored by applications.

In the [Manage Personal Data](#) application, you can search for a specific data subject record using a refined search. You can also adjust the settings to search with more parameters or display more information when you have found the desired data subject record.

After you have identified the data subject, you can see information about which applications store their personal data and how their personal data is used by those applications. You can see if the data subject has made any requests for correction or deletion of their personal data. You can also download a machine-readable or human-readable report of all a data subject's personal data being stored and processed by applications.

### Searching for a Data Subject Record

To find a data subject record, you must search using one of the following formats:

- Data subject ID
- First name, last name, and date of birth
- First name, last name, and email address

You can refine your search by adding additional fields. To add additional search fields, select [Filters](#) on the Manage Personal Data screen. In the popup that appears, select the search fields you want to add. However, for every search either [Data Subject ID](#) or [First Name, Last Name](#), and [Date of Birth](#) or [First Name, Last Name](#), and [Email Address](#) are mandatory fields.

### Corporate Customer Search

In Personal Data Manager, you can also search for corporate customer by company.

To find a data subject record for a corporate customer, you must search using the following formats:

- First name, last name, and company ID
- First name, last name, and company name
- Email address and company ID
- Email address and company name

### **i** Note

The fields *Company ID* and *Company Name* are only available if they are provided to Personal Data Manager by your solution.

The search looks for all relevant applications in the application repository and then performs a search for all information related to the data subject across these applications.

## Inform the Data Subject

The *Manage Personal Data* application allows you to view the following information:

The search results for the data subject are sorted according to data subject ID and grouped by application. The data subject role in each application is also displayed. If a search for corporate customers is enabled, the company ID and company name are also displayed in the search results.

To display more detailed information for an application, choose the application name to open the details view.

If you want to display information for only certain data subject roles in an application, mark the checkbox next to the data subject role and choose *Display Details*.

This opens an overview of applications and requests associated with the data subject. To open the details view for an application and data subject role, choose the line with the data subject role for which you want to view more information in the section *Application*. Only the information associated with the data subject role you selected is displayed in the application detail view. Additionally, any requests you make related to the personal data used in an application only apply to the data subject role you selected.

Each application has its own detail view. The data subject role you selected is displayed in the header. The detail view includes these sections:

- *Personal Data*: This section displays all the personal data used by an application, including personal details, addresses, email addresses, and phone numbers. If the entry for a field is longer than 32 characters, it becomes a link, and you can select the link to display the complete entry. You can request the deletion or correction of personal data for a specific application in this section. If you request the deletion of personal data from the *Personal Data* section, only the personal data used by that specific application will be deleted when the request is processed. The *Edit* and *Request Deletion* buttons are only active if there are no requests with the status *New* or *In Progress* for that application.
- *Business Purposes*: This section displays all business purposes associated with a data subject ID. Business purpose details include the following information:
  - *Business Purpose Ends On*: The date on which the organization's business with a user ends.
  - *Business Purpose Status*: Whether there is ongoing business with a user.
  - *Business Purpose Starts On*: When the business purpose begins. This is used calculate the end date for the business purpose.
  - *Business Purpose Name*: The name of the business purpose.
  - *Legal Entity Value*: The value assigned to the legal entity to which the business purpose belongs, for example, the company from which a purchase was made.

- *Legal Entity*: The type of legal entity.
- *Condition Field*: The attribute or property in the business purpose that is used to calculate the end of purpose (EoP).
- *Condition Value*: The value of the condition field.

### **i** Note

The *Business Purpose* section is only available if you are using Personal Data Manager with Data Retention Manager.

- *Where the data subject's personal data is used*: This section displays selected business transactions made by the data subject in an application. You can display more business transactions by choosing *More*.
- *Long Text Data*: Personal Data Manager can also display long text data stored by an application. You can view the following text types:
  - *Email Conversations*: You can select an email to open a dialog box with more information about the email, including the text and other recipients.
  - *Comments*
  - *Chats*
  - *Attachments*: Personal Data Manager only displays the name of attachments related to an application for a data subject role.

The text types are grouped according to transactions associated with the text, if any, and displayed in descending order with the most recent text first. Long texts are displayed as links. To display the complete text, choose the link to open a dialog box containing the complete long text. You only can download or export long text data in a machine-readable format.

## Export Personal Data

You can export your personal data including information for your business transactions and business purposes in a human-readable or machine-readable format

You can download the information for each application and data subject role separately:

1. On the overview page, choose an application to open the details view for that application.
2. On the the application details page, choose *Export* to create a request to download the information.
3. In the dialog box, choose *Email* or *Download*.
  1. For *Email*, select an email address from the dropdown menu and choose a file format for the exported data. You can choose from PDF, JSON, or XML. PDF files are human readable, and JSON and XML files are machine readable.
  2. For *Download*, choose a file format for the download: PDF, JSON, or XML.

In both cases, if you select PDF, you can choose to export all transaction data. If you do not choose this option, only five transaction data records are exported. By default, all transaction checkboxes are selected if you choose any of the machine readable formats, for example JSON or XML.
4. Choose *Export* in the dialog box.
  1. If you chose *Email*, an email containing a link to the document and a second email containing a one-time password that will allow you to access the document will be sent to the email address you selected in step 3.
  2. If you chose *Download*, a download request will be created. You can download the files from the *Export Requests* section under *Requests* once the request is complete.



3. Once a download is created for certain criteria, such as the following, another request for the same criteria can only be created after the existing request is completed (downloaded or canceled):
  - Application name
  - Data subject role (for example, customer or vendor)
  - Download type (PDF, XML, JSON)
  - Browser download or export via email)
  - Data Subject ID

## Delete Personal Data

You can make a request to delete personal data processed by the applications listed on the overview page. You can request the deletion of data for one application or all applications listed.

To request the deletion of all data from all applications, choose [Delete All](#) under [Applications](#) and confirm the action. All personal data for all applications and data subject roles will be deleted when the request has been processed.

To request the deletion of personal data from one application for one role, open the application details view, choose [Request Deletion](#), and confirm the action. The personal data for the application and data subject role you selected will be deleted when the request has been processed.

## Requests

Under [Requests](#), you can see all requests that have been created for a data subject. You can monitor the progress of a request and assist with further processing if necessary.

After you have created a request, it will appear in the list of existing requests, either under [Inbox Requests](#) or [Export Requests](#).

### Inbox Requests

You can find the following types of requests under [Inbox Requests](#):

- Correction
- Deletion

You can find the following information in the list of requests:

- The application related to a request. If a user has requested the deletion of all personal data from all applications, the value for this column will be [All](#) instead of an application name.
- The data subject role associated with the request.
- The status of the request: new, in progress, completed, rejected or revoked.
- The date the request was created.

You can also get more information about an individual request by navigating to the details view for that request.

Under [Request Details](#), you can find the following additional information:

- The request ID

- The name of the person who made the request
- Which business objects are affected by the request
- Any comments entered about the request

When you make a correction request, *Corrected Fields* appears on the details page. It displays the fields that need to be correct and what the new values for those fields are.

### i Note

Deletion requests can be processed using either Data Retention Manager or an application-specific retention manager.

## Export Requests

Each time you export personal data, a corresponding export request is created. In the *Export Requests* section, you can find a list of all export requests that have been created and the following information about each request:

- The request ID
- The application associated with the request
- The data subject role associated with the request
- The date the request was created
- The request status
- The type of download

The list also provides an option to cancel the export request even after the documents are ready for download. This option becomes unavailable once the document is downloaded or the revoke request is raised

An export request can have the following statuses:

- *Request received*: The export request has been received but processing has not yet started.
- *Information retrieved*: The information required for export has been retrieved from the application.
- *Information not retrieved*: The information required to export the personal data requested could not be retrieved from the application.
- *Document created*: The document was created and sent to the SAP Document Center.
- *Document could not be created*: Document creation failed.
- *Document link sent*: The email containing a link to the document in the SAP Document Center was sent to the email provided.
- *Document link could not be sent*: An email containing a link to the document could not be sent.
- *One-time password could not be sent*: The email containing a one-time password for accessing the document could not be sent.
- *One-time password sent*: The email containing a one-time password for accessing the document was sent. When a request has this status, the export process is complete.
- *Ready to download*: The documents are ready to be downloaded.
- *Downloaded*: The documents have already been downloaded.
- *Ready for download (Partial Download)*: The documents are created and ready for download but some data fetch calls failed.
- *OTP sent successfully (Final Status with Partial Download)*: The documents are created and OTP sent but some data fetch calls failed.

## Processing Requests

Requests can either be processed automatically or manually:

- **Automatic:** For requests to be processed automatically, the application must provide an end point or an API to trigger the process for automatic correction or deletion of personal data. If a request cannot be completed automatically and further processing is required by the application, the request receives the status *In Progress*. The request then becomes available to the operations clerk for further manual processing.
- **Manual:** After the request is created, it is sent to the operations clerk to be processed.

### Provide a Sample Personal Data Record

You can use Personal Data Manager to create a sample personal data record to show how an application processes personal data before a data subject begins to use this application. A sample personal data record is designed to show what kind of personal data is processed and how it is processed without including any actual personal data.

To create a sample personal data record, complete the following steps in the landscape where you can simulate your application:

1. In your application, create a profile for a sample data subject.
2. Search for your sample data subject in the **Manage Personal Data** application in Personal Data Manager.
3. Select the application to see the personal data stored in that application for the sample data subject in a sample personal data record.

To display sample information about business purposes, and legal grounds, you also need to create this sample information.

4. You can also use the export function to provide sample data in a machine-readable or human-readable format.

### [Related Information](#)

[Manage Personal Data](#)

## 8.1.1 Provide a Sample Personal Data Record

Provide information about data processing procedures.

You can use Personal Data Manager to create a sample personal data record to show how an application processes personal data before a data subject begins to use this application. A sample personal data record is designed to show what kind of personal data is processed and how it is processed without including any actual personal data.

To create a sample personal data record, complete the following steps in the landscape where you can simulate your application:

1. In your application, create a profile for a sample data subject.
2. Search for your sample data subject in the [Manage Personal Data](#) application in Personal Data Manager.
3. Select the application to see the personal data stored in that application for the sample data subject in a sample personal data record.

To display sample information about consents, business purposes, and legal grounds, you also need to create this sample information.

4. You can also use the export function to provide sample data in a machine-readable or human-readable format.

## Related Information

[Manage Personal Data \[page 30\]](#)

## 8.2 Manage My Personal Data

Learn how to use the self-service cockpit in Personal Data Manager.

The *Manage My Personal Data* application in Personal Data Manager provides a self-service cockpit that enables you to view which of your personal data is being processed and stored by the different services you use.

### Information

In the self-service cockpit, you can see the following types of information:

- A list of applications that you have allowed to use your personal data
- The personal data used by each of the applications listed
- Any requests you have made for the correction, deletion, or export of your personal data
- Business purposes, consents, and business transactions associated with your data subject ID, for example, an email address or mobile phone number.

On the overview page for your user profile, there is a list of all the applications that use personal data and the data subject roles associated with each application, for example, a customer or vendor. You can also find a list of requests for correction, deletion, or export of personal data.

For more detailed information about the personal data used by an application, choose the line with the data subject role for which you want to display more information. Only the information associated with the data subject role you selected is displayed in the application detail view.

Additionally, any requests you make related to the personal data used in an application only apply to the data subject role you selected.

When you open the application, the first data subject role for the first application in the list is already displayed.

Each application has its own detail view. The data subject role you selected is displayed in the header. The detail view includes these sections:

- *Personal Data*: This section displays all of your personal data that an application uses, including personal details, addresses, email addresses, and phone numbers. If the entry for a field is longer than 32 characters, it becomes a link. To display the complete entry, choose the link to display the complete entry. You can make a request to delete or correct your personal data for a specific application in this section. If you request the deletion of your personal data from the *Personal Data* section, only the personal data used

by that specific application and data subject role will be deleted when the request has been processed. The [Edit](#) and [Delete](#) buttons are only active if there are no requests with the status [New](#) or [In Progress](#) for that application.

- **Business Purposes:** This section displays all business purposes associated with your data subject ID. You can find the following information under [Business Purpose Details](#):
  - [Business Purpose Ends On](#): When an organization's business with you ends.
  - [Business Purpose Status](#): Whether an organization has ongoing business with you.
- **Where my personal data is used:** This section displays a selection of business transactions in an application that contain your personal data.
- **Long Text Data:** Personal Data Manager can also display long text data stored by an application. You can view the following text types:
  - [Email Conversations](#): You can select an email to open a dialog box with more information about the email, including the full text and other recipients of the email.
  - [Comments](#)
  - [Chats](#)
  - [Attachments](#): You can view the name of any attachment related to an application and your data subject role in that application.

The text types are grouped according to the business transaction associated with the text, if any, and displayed in descending order with the most recent text first. Long texts are displayed as links. If you want to read a complete text, choose the link to open a dialog box containing the complete long text. You can only download or export long text data in a machine-readable format.

## Export Your Personal Data

You can export your personal data including information for your business transactions and business purposes in a human-readable or machine-readable format

You can download the information for each application and data subject role separately:

1. On the overview page, choose an application to go to the details view for that application.
2. On the application details page, choose [Export](#) to download or export the information.
3. In the dialog box, choose [Email](#) or [Download](#).
  1. For [Email](#), select an email address from the dropdown menu and choose a file format for the exported data. You can choose from PDF, JSON, or XML. PDF files are human readable, and JSON and XML files are machine readable.
  2. For [Download](#), choose a file format for the download: PDF, JSON, or XML.

In both cases, if you select PDF, you can choose to export all transaction data. If you do not choose this option, only five transaction data records are exported.

4. Choose [Export](#) in the dialog box.
  1. If you chose [Email](#), an email containing a link to the document and a second email containing a one-time password that will allow you to access the document will be sent to the email address you selected in step 3.
  2. If you chose, [Download](#), a download request will be created. You can download the files from the [Export Requests](#) section under [Requests](#) once the request has been processed.
  3. Once a download is created for certain criteria, such as the following, another request for the same criteria can only be created after the existing request is completed (downloaded or canceled):

- Application name
- Data subject role (for example, customer or vendor)
- Download type (PDF, XML, JSON)
- Browser download or export via email)
- Data Subject ID

### i Note

For a complete list of all business transactions and business purposes, you must export the data in a machine-readable format. By selecting [Export all transaction data](#) you can download the data in a human-readable format.

## Delete Your Personal Data

You can make a request to delete personal data processed by the applications listed on the overview page. You can request the deletion of your data for one application or for all applications listed.

To request the deletion of your data from all applications, choose [Delete All](#) under [Applications](#) and confirm the action. All your personal data being used by all applications and data subject roles will be deleted once your request has been processed.

To request the deletion of your personal data from one application, open the application details view, choose [Request Deletion](#), and confirm the action. All of your personal data that is being used by the application and data subject role you selected will be deleted when the request has been processed.

## Requests

After you have created a request, it appears in the list of existing requests, either under [Inbox Requests](#) or [Export Requests](#).

You can find the following types of requests under [Inbox Requests](#):

- Correction
- Deletion

You can see the following information in the list of requests:

- The application related to a request. If you have requested the deletion of your personal data from all applications, the value for this column will be [All](#) instead of an application name.
- The data subject role associated with your request.
- The type of request: deletion, correction, or withdraw consent
- The date the request was created

You can also get more information about an individual request by navigating to the details view for that request.

Under [Request Details](#), you can find the following additional information:

- The request ID
- The name of the person who made the request

- The business objects affected by the request
- Any comments entered about the request

When you make a correction request, *Corrected Fields* is displayed on the details page. It shows you which fields need to be corrected and the new values you provided for those fields.

## Export Requests

Each time you export your personal data, a corresponding export request is created. In the *Export Requests* section, you can find a list of all export requests that have been created and the following information about each request:

- The request ID
- The application associated with your request
- The data subject role associated with your request
- The date you created the request
- The status of your request
- The type of download

The list also provides an option to cancel the export request as long as the documents are not yet downloaded or the one-time password has not yet been sent.

Your export request can have the following statuses:

- *Request received*: The export request has been received but processing has not yet started.
- *Information retrieved*: The information required for export has been retrieved from the application.
- *Information not retrieved*: The information required to export the personal data requested could not be retrieved from the application.
- *Document created*: The document was created and sent to the SAP Document Center.
- *Document could not be created*: Document creation failed.
- *Document link sent*: The email containing a link to the document in the SAP Document Center was sent to the email provided.
- *Document link could not be sent*: An email containing a link to the document could not be sent.
- *One-time password could not be sent*: The email containing a one-time password for accessing the document could not be sent.
- *One-time password sent*: The email containing a one-time password for accessing the document was sent. When a request has this status, the export process is complete.
- *Ready to download*: The documents are ready to be downloaded.
- *Downloaded*: The documents have already been downloaded.
- *Ready for download (Partial Download)*: The documents are created and ready for download but some data fetch calls failed.
- *OTP sent successfully (Final Status with Partial Download)*: The documents are created and OTP sent but some data fetch calls failed.

## 8.3 Manage Personal Data Requests

Process personal data requests.

The *Manage Personal Data Requests* application lets you process requests from data subjects for correction or deletion of their personal data. After you complete the request in all the relevant applications and for all associated data subject roles, you can update the status of the request.

### Requests List

*Manage Personal Data Requests* provides you with a list of personal data requests that you are authorized to process.

The standard fields visible in the application are as follows:

- *Request ID*: The unique identifier assigned to the request.
- *Status*: The status of the request. A request can have the following status values: new, in progress, completed, rejected, or revoked. If a request has the status revoked, it means that the data subject has cancelled their request for correction or deletion of his or her personal data.
- *Type*: The type of request made. The following request types are available:
  - Correction
  - Deletion
- *Requested On*: The date the request was made.
- *Due In*: The number of days left to process a request. This field will not be displayed if a request has been completed or rejected.
- *Due On*: The date the request is due. This field will not be displayed if a request has been completed or rejected.
- *Application*: The application using the personal data for which the request was made.
- *Changed On*: The date the request was last updated.

You can search for personal data requests using *Request ID*, *Status*, and *Type*.

You can adapt the standard fields according to your business needs. You can also add or remove columns as necessary.

After you have found the request you need, you can navigate to the request details page.

### Request Details

On the request details page, you can find a detailed description of the request, including the data subject ID and the data subject role in the application, for example, customer or vendor. If the request applies to all data subject roles associated with a data subject ID in an application, the value for *Data Subject Role* is *All*. If it is a correction request, you can see the field that needs to be corrected, the current value of the field, and the requested value of the field.



## Processing a Personal Data Request

When you begin working on a new request, you can change the status of the request to in progress. This option is only available on the details page for new requests. Once you set the request to in progress and confirm the status change, it is assigned to you for further processing.

If you are working on a correction request, you have to add comments before you can finish processing the request. This field is mandatory for all correction requests. You can also add a comment to the request without completing or rejecting the request. Enter your comment in the text box and choose [Save Comment](#). All comments related to the request are displayed under [Comments](#).

Once you have finished processing the request, you can choose [Complete](#) or [Reject](#) depending on how you process the request. If you choose [Complete](#), it means that the request can be finished and no further processing is required. After you confirm this action, the status of the request will change to [Completed](#). If you choose [Reject](#), it means that you cannot finish processing the request and further information or processing may be required. After you confirm this action, the status of the request will change to [Rejected](#).

## 8.4 Data Transport

Export the personal data stored by Personal Data Manager.

Logs and requests are generated during the use of Personal Data Manager. Personal Data Manager stores the following types of information in logs and requests:

- [Requests](#): all the inbox requests, including correction and deletion, and export requests that were created for a data subject.
- [Activity Log](#): the user who accessed the data, which data set was accessed, and the fields that were accessed.



To export this data, select at least one data type and choose [Export](#) to download a ZIP file containing a JSON file for each entity.

# 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.

## Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

## 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.

## Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.



© 2021 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.