How-to Guide

SAP Business One and SAP Business One, version for SAP HANA, 9.3 Patch Level 12 and Higher

Document Version: 9.0 – 2020-08-19

CUSTOMER

How to Manage the Protection of Personal Data in SAP Business One

Typographic Conventions

Type Style	Description
Example	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.
Example	Emphasized words or expressions.
`EXAMPLE`	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE`	Keys on the keyboard, for example, `F2` or `ENTER`.

Document History

Version	Date	Change
1.0	2018-05-03	Document created.
2.0	2018-07-03	Document updated for changes released in SAP Business One version 9.3 patch level 05.
3.0	2018-08-23	Document updated for changes released in SAP Business One version 9.3 patch level 06.
4.0	2018-11-02	Document updated for changes released in SAP Business One version 9.3 patch level 07.
5.0	2018-12-17	Document updated for changes released in SAP Business One version 9.3 patch level 08.
6.0	2019-03-14	Document updated for changes released in SAP Business One version 9.3 patch level 09.
7.0	2019-08-22	Document updated for changes released in SAP Business One version 9.3 patch level 11 and synchronized to SAP Business One version 10 patch level 01.
8.0	2020-01-29	Document updated for changes released in SAP Business One version 9.3 patch level 12. Document updated for changes released in SAP Business One version 10 patch level 01. Added section Personal Data Protection.
9.0	2020-08-19	Document updated for changes released in SAP Business One version 10.0 feature package 2008.

Contents

1 Introduction

This how-to guide will help you to manage the protection of personal data in SAP Business One and SAP Business One, version for SAP HANA (commonly referred to in this guide as "SAP Business One"). SAP Business One contains various features that can help you to manage the protection of personal data, these features are described in this how-to guide.

Personal data is any data that identifies, or can be used to identify, an individual natural person. Personal data can include "metadata", data that provides a link to other data; the metadata may not explicitly identify a person but can be used to indirectly identify a person. Personal data can be captured, processed, controlled and maintained in SAP Business One.

The protection of personal data means, but is not restricted to, protection from actions like unauthorized distribution or access but can also include rights such as persons being able to find out what data companies hold about them. Personal data protection should restrict the capture of personal data to specific purposes that have been consented to and should erase the personal data once the purpose, process and statutory timelines have lapsed.

Personal data protection is covered by various laws and directives in different jurisdictions around the world, such as the *General Data Protection Regulation* of the European Union, the *Personal Information Protection and Electronic Documents Act* of Canada, or the *Personal Information Protection Act* of South Korea. Compliance with the different laws is driven by substantial financial penalties and potential damage claims.

Your company is likely required to follow and comply with personal data protection laws and directives relevant to the jurisdictions in which your company operates. The features of SAP Business One described in this how-to guide can help you to manage your company's obligations towards the protection of personal data, in conjunction with your company's own personal data protection policy.

The information contained in this how-to guide is for general guidance only and is provided on the understanding that SAP is not herein engaged in rendering legal advice. As such, this guide should not be used as a substitute for qualified legal consultation. SAP SE accepts no liability for any actions taken as response hereto. It is the customer’s responsibility to adopt measures that the customer deems appropriate to achieve compliance with data protection laws.

2 Personal Data Protection Management

Personal Data Protection Management in SAP Business One allows you to:

- Determine which data are personal data through the identification of natural persons.
- Manage which data types contain personal data in your business.
- Generate reports on personal data held in the system.
- Clean up and erase personal data held in the system.
- Block and subsequently unblock access to personal data held in the system.

Personal Data Protection Management works with data that is held in the production system of SAP Business One only. Any personal data that has been exported, printed, emailed, backed-up, archived or has otherwise left the production system of SAP Business One, cannot be managed by *Personal Data Protection Management*.

2.1 Personal Data Protection Management Enablement

Personal Data Protection Management is enabled by selecting a checkbox on the *Company Details* window of SAP Business One. Once enabled, the *Data Protection Tools* described in this guide and a *Personal Data Protection* section with *Natural Person* indicator and *Status* in relevant master data become available.

From the SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *Company Details* → *Basic Initialization* tab to view the *Enable Personal Data Protection Management* checkbox.

Personal Data Protection Management is enabled by default for SAP Business One localizations that are for European Union countries, Switzerland and Norway. For all other localizations, *Personal Data Protection Management* is available for enablement through the *Enable Personal Data Protection Management* checkbox. *Personal Data Protection Management* can be disabled if related functionality is not in use.

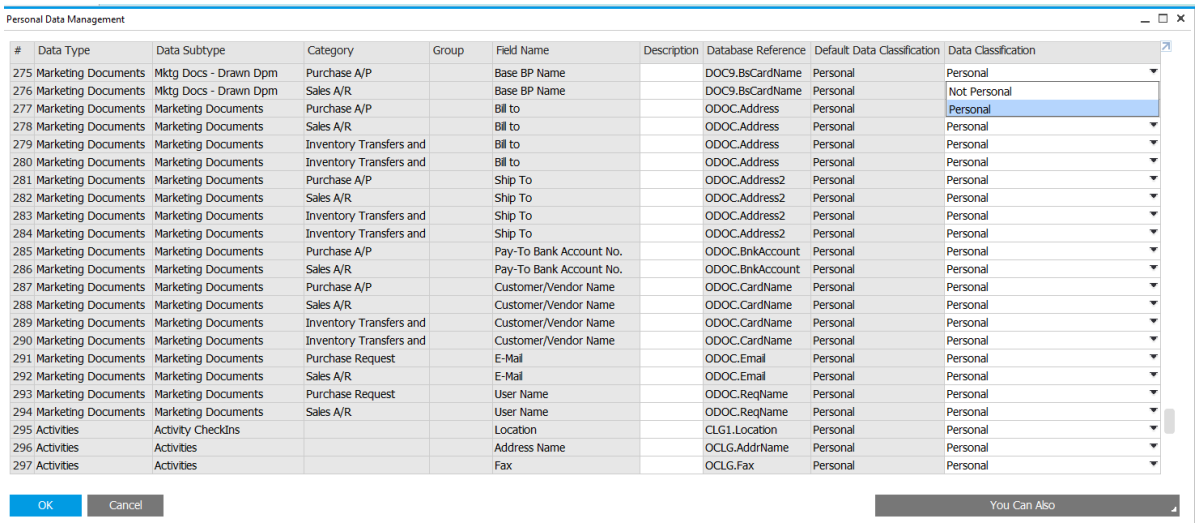
2.2 Personal Data Management

Personal Data Management allows you to identify which types of data contain personal data to help you to fulfill your obligations to protect personal data. Data that is classified as *Personal* or *Sensitive Personal* is included in other personal data processes. You must classify different data properly to allow the *Personal Data Protection Management* tools to work effectively. Not all data can be classified as personal data, only data that are held in areas shown in *Personal Data Management* can be classified as personal data.

Any personal data stored in objects or fields that are not included in *Personal Data Management* cannot be managed by *Personal Data Management* processes, such data must be managed and controlled manually.

SAP Business One can hold personal data in different areas, or objects, of the system. The data held in these predefined objects can be categorized as *Personal* or *Not Personal*. In some special cases the data can be categorized as *Sensitive Personal*. Examples of relevant objects include business partners, employees and marketing documents. Objects that cannot contain personal data do not appear in *Personal Data Management.*

From the SAP Business One *Main Menu*, choose *Administration* → *Utilities* → *Data Protection Tools* → *Personal Data Management*. The *Personal Data Management* window opens.



#	Data Type	Data Subtype	Category	Group	Field Name	Description	Database Reference	Default Data Classification	Data Classification
275	Marketing Documents	Mktg Docs - Drawn Dpm	Purchase A/P		Base BP Name		DOC9.BsCardName	Personal	Personal
276	Marketing Documents	Mktg Docs - Drawn Dpm	Sales A/R		Base BP Name		DOC9.BsCardName	Personal	Not Personal
277	Marketing Documents	Marketing Documents	Purchase A/P		Bill to		ODOC.Address	Personal	Personal
278	Marketing Documents	Marketing Documents	Sales A/R		Bill to		ODOC.Address	Personal	Personal
279	Marketing Documents	Marketing Documents	Inventory Transfers and		Bill to		ODOC.Address	Personal	Personal
280	Marketing Documents	Marketing Documents	Inventory Transfers and		Bill to		ODOC.Address	Personal	Personal
281	Marketing Documents	Marketing Documents	Purchase A/P		Ship To		ODOC.Address2	Personal	Personal
282	Marketing Documents	Marketing Documents	Sales A/R		Ship To		ODOC.Address2	Personal	Personal
283	Marketing Documents	Marketing Documents	Inventory Transfers and		Ship To		ODOC.Address2	Personal	Personal
284	Marketing Documents	Marketing Documents	Inventory Transfers and		Ship To		ODOC.Address2	Personal	Personal
285	Marketing Documents	Marketing Documents	Purchase A/P		Pay-To Bank Account No.		ODOC.BnkAccount	Personal	Personal
286	Marketing Documents	Marketing Documents	Sales A/R		Pay-To Bank Account No.		ODOC.BnkAccount	Personal	Personal
287	Marketing Documents	Marketing Documents	Purchase A/P		Customer/Vendor Name		ODOC.CardName	Personal	Personal
288	Marketing Documents	Marketing Documents	Sales A/R		Customer/Vendor Name		ODOC.CardName	Personal	Personal
289	Marketing Documents	Marketing Documents	Inventory Transfers and		Customer/Vendor Name		ODOC.CardName	Personal	Personal
290	Marketing Documents	Marketing Documents	Inventory Transfers and		Customer/Vendor Name		ODOC.CardName	Personal	Personal
291	Marketing Documents	Marketing Documents	Purchase Request		E-Mail		ODOC.Email	Personal	Personal
292	Marketing Documents	Marketing Documents	Sales A/R		E-Mail		ODOC.Email	Personal	Personal
293	Marketing Documents	Marketing Documents	Purchase Request		User Name		ODOC.ReqName	Personal	Personal
294	Marketing Documents	Marketing Documents	Sales A/R		User Name		ODOC.ReqName	Personal	Personal
295	Activities	Activity CheckIns			Location		CLG1.Location	Personal	Personal
296	Activities	Activities			Address Name		OCLG.AddrName	Personal	Personal
297	Activities	Activities			Fax		OCLG.Fax	Personal	Personal

All object data shown in *Personal Data Management* are initially classified in *Data Classification* according to their *Default Data Classification*. *Personal Data Management* only shows object data that is intended for personal data, not all object data that exist are shown.

Personal Data Management shows the type of data and the specific fields that may contain personal data. User-defined fields or UDFs (excluding system-type user-defined fields) are also shown in *Personal Data Management* when they are connected to personal data objects.

- UDFs with the *Category* of *Inventory Transfers and Requests Sales A/R* and UDFs with the category of *Sales A/R* must have the same *Data Classification*.
- UDFs with the *Category* of *Inventory Transfers and Requests Purchase A/P* and UDFs with the category of *Purchase A/P* must have the same *Data Classification*.

The *Data Classification* column can be amended for individual data items from *Personal* to *Not Personal*. Data items with a *Data Classification* of *Not Personal* are excluded from *Personal Data Management* processes. The *Data Classification* can be changed from *Not Personal* to *Personal*.

Only data that are classified as *Personal* or *Sensitive Personal* and are connected to natural persons are treated as personal data. Natural persons can only be determined in the *Personal Data Management Wizard*. Simply classifying data types as *Personal* or *Sensitive Personal* does not mean that all such data are treated as personal data, the data must be connected to a natural person as well.

The *Database Reference* column indicates a specific table location or a general grouping location. For example, *ODOC.Card.Name,* where the *Category* column is *Sales - A/R,* represents all A/R documents.

Special fields that are classified as *Sensitive Personal* can be changed to *Personal* or *Not Personal.* Only the fields *ID Issued by Authorities*, *Passport No.*, multiple fields related to business partner bank accounts and IBANs (International Bank Account Numbers), *Bank Account* for employees, and some user-defined fields can be classified as *Sensitive Personal* in all localizations. In the Germany localization, the fields *Confession*, *Confession of Partner* and *Social Insurance Number* can also be classified as *Sensitive Personal*. Fields that are classified as *Sensitive Personal* are automatically encrypted and user access is logged and restricted through authorizations. Changing the classification from *Sensitive Personal* to *Personal* or *Not Personal* removes the encryption and relevant user access restrictions.

Multiple special fields *Attachment Entry* exist for various *Data Types*, *Data Subtypes* and *Categories*. *Attachment Entry* is classified as *Not Personal* by default, *Attachment Entry* must be classified as *Personal* to be included in personal data processes. *Attachment Entry* only represents a link to an attachment held outside SAP Business One, the attachment itself must be managed separately for personal data protection purposes.

The field *Employee Code* is for issuing employees with an ID number from SAP Business One, *Employee Code* can be managed by *Personal Data Management* and personal data protection processes. *Employee Code* replaces the function that some companies used *Employee No.* for previously. *Employee No.* cannot be managed by *Personal Data Management* or personal data protection processes and is hidden from view.

Recommendation

Check any related add-ons you use for how personal data is handled. If you have been supplied with add-ons by SAP Partners, check that these will not be affected by the encryption of data. For more information see SAP Note 2633811.

Through the *You Can Also* option, it is possible to change the *Data Classification* for all the fields in the window. Right-click on fields in the window for options like *Reset to Default* for *Data Classification* and *Remove* or *Duplicate* for user-defined field rows. Access to *Sensitive Personal* data is recorded in the *Sensitive Personal Data Access Log*.

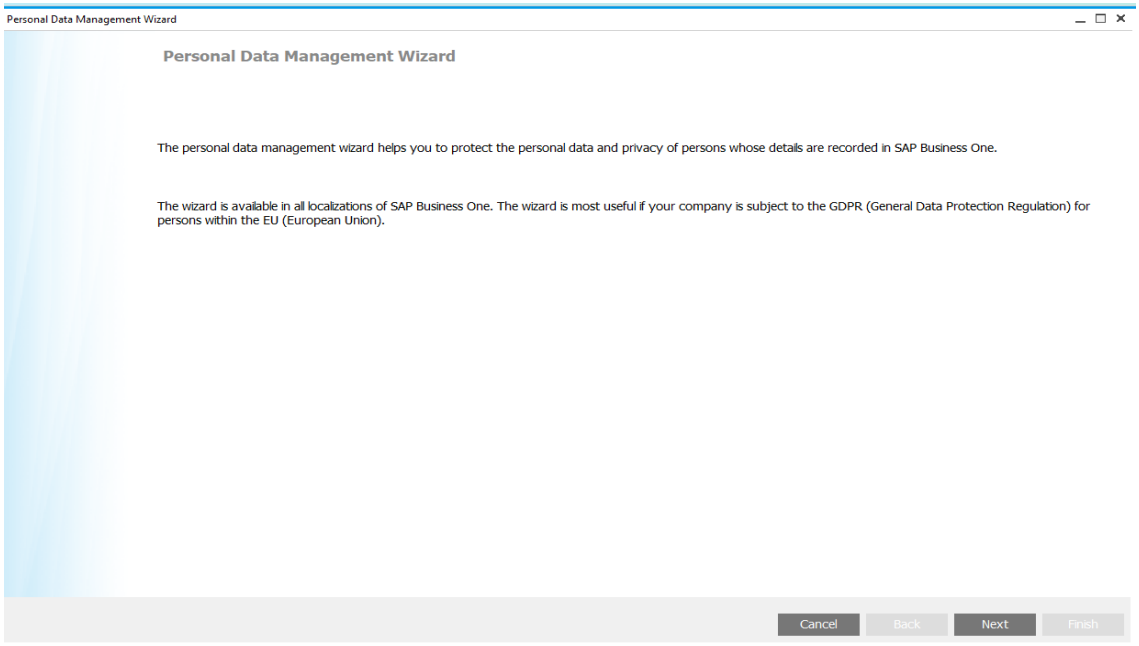
Use the filter option in the toolbar to view specific categories of data in *Personal Data Management* such as *Sensitive Personal* data.

2.3 Personal Data Management Wizard

The *Personal Data Management Wizard* provides six different options to perform a variety of *Personal Data Protection Management* processes:

- *Determine Natural Persons*
- *Reverse Natural Person Determination*
- *Personal Data Report*
- *Personal Data Cleanup*
- *Personal Data Blocking*
- *Personal Data Unblocking*

From the SAP Business One *Main Menu*, choose *Administration* → *Utilities* → *Data Protection Tools* → *Personal Data Management Wizard* to start the wizard. The *Personal Data Management Wizard* opens.



The *Personal Data Management Wizard* works like other wizards in SAP Business One. The wizard guides you through the different available processes in a series of steps, helping you to define what you want to do and which data you want to work with. New wizard runs can be created, or saved wizard runs can be loaded and then refreshed in *Report Results*. Completing or executing the wizard finalizes the changes you have determined in the wizard. When running the wizard, *Data Ownership* is ignored; if a user is authorized to access a wizard action then they can access all business partners through the wizard. Wizard actions apply to personal data that is stored in the inventory and serial/batch engines, to include business partner names in the inventory reporting and internally managed inventory tables.

Not all personal data objects can be managed by the *Personal Data Management Wizard*. The following objects must be managed, and personal data removed, manually:

- *Time Sheets* with *Type* set to *Other*.
- *Target Groups* contained in *Campaigns*.
- Attachments, except from the field *Attachment Entry* which references attachments.
- *Remarks* tab in *Business Partner Master Data*.
- *Content* tab in *Activities*.

2.3.1 Determining Natural Persons

Select the wizard action *Determine Natural Persons* in step 2, *General Parameters,* to identify natural persons that are data subjects and exist in SAP Business One. The wizard is the only way you can identify and determine natural persons in SAP Business One. Once you have determined natural persons, you can manage their personal data appropriately and run other wizard actions for them.

Natural persons are real human beings, as distinguished from entities like corporations. Business partner, employee, user and contact person records may all represent natural persons, but they do not have to. Personal data only relates to natural persons, so *Personal Data Protection Management* is only relevant for natural persons. The same type of data, such as a phone number, may or may not be personal data. A natural person's phone number could be used to identify them, so it is personal data. A company's reception desk phone number cannot be used to identify a natural person, so it is not personal data.

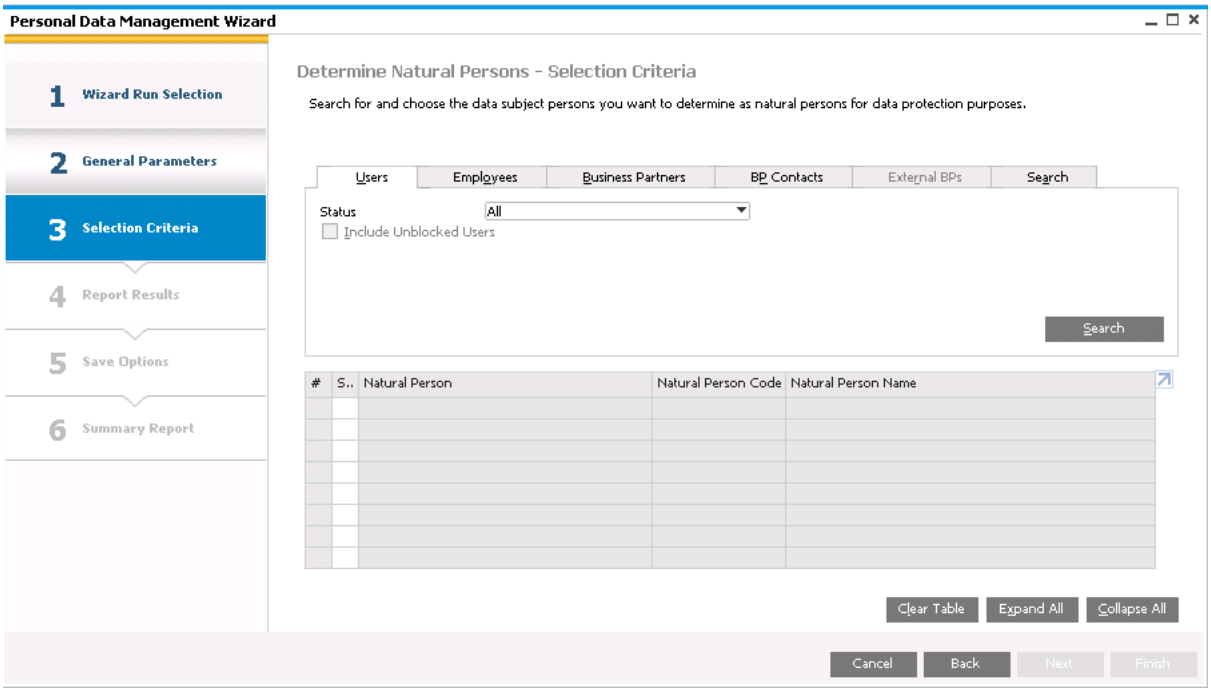
By using the wizard action *Determine Natural Persons*, you can correctly determine which data are for natural persons and which are not. The wizard works by automatically selecting the checkbox *Natural Person* in the *Personal Data Protection* section of related master data windows. You cannot manually select *Natural Person* checkboxes.

Any sensitive personal data for natural persons is encrypted by default and accessible to authorized users only.

> **Recommendation**
>
> Check any related add-ons you use for how personal data is handled. If you have been supplied with add-ons by SAP Partners, check that these will not be affected by the encryption of data. For more information see SAP Note 2633811.

> **Note**
>
> Consent from natural persons to the storage, use, retention and reporting of personal data in SAP Business One needs to be acquired and managed outside SAP Business One. To maintain data and reporting integrity, business partners who are determined as natural persons cannot be duplicated.

In step 3 of the wizard, *Selection Criteria*, search SAP Business One for data subjects that are natural persons.



The different tabs of the wizard allow you to target your search to categories of *Users*, *Employees*, *Business Partners*, *BP Contacts* or to a specific text search. Sales employees and buyers set up in *Sales Employees/Buyers - Setup* cannot be searched for in *Determine Natural Persons* or otherwise determined as natural persons. Clear the search criteria on all tabs by selecting *Clear Selections* on the *Search* tab.

The search results are displayed in a pop-up list where you can choose multiple records for determining as natural persons. Selecting *Choose* places the records in the grid of the wizard, where the *Select* column checkboxes confirm selection. Multiple searches can be performed for different categories, the results of which can be added to the same grid for an individual wizard run. Any data subjects who are already determined as natural persons or have been erased as part of a wizard *Personal Data Cleanup,* do not show in searches.

In step 4 of the wizard, *Report Results,* you can see which data subjects you will determine as natural persons by executing the wizard.

In step 5 of the wizard, *Save Options,* you can either choose *Save Selection Criteria and Exit* or finalize the determinations by choosing *Execute*.

In step 6 of the wizard, *Summary Report*, you can see if the process was successful for the different natural persons.

2.3.2 Reversing Natural Person Determination

Select the wizard action *Reverse Natural Person Determination* in step 2, *General Parameters,* to reverse the identification of natural persons that has been made in SAP Business One previously. The wizard is the only way you can reverse a natural person determination in SAP Business One.

The search, save and results steps work in the same way as for *Determine Natural Persons*.

Once the wizard has been executed, any sensitive personal data for natural persons will be decrypted and so accessible to all authorized users.

2.3.3 Personal Data Reports

Select the wizard action *Personal Data Report* in step 2, *General Parameters,* to report on data held about natural persons recorded in SAP Business One. The wizard is the only way you can report on natural persons in SAP Business One. As a prerequisite, you must have installed Crystal Report runtime before generating *Personal Data Reports*.

Personal Data Reports provide a retrieval function which can be used to inform natural person data subjects about the personal data stored about them. Reports include any personal data for the natural person held in master data and related transactions that is stored in the system. Typically, natural person data subjects have legal rights to request and receive reports about themselves.

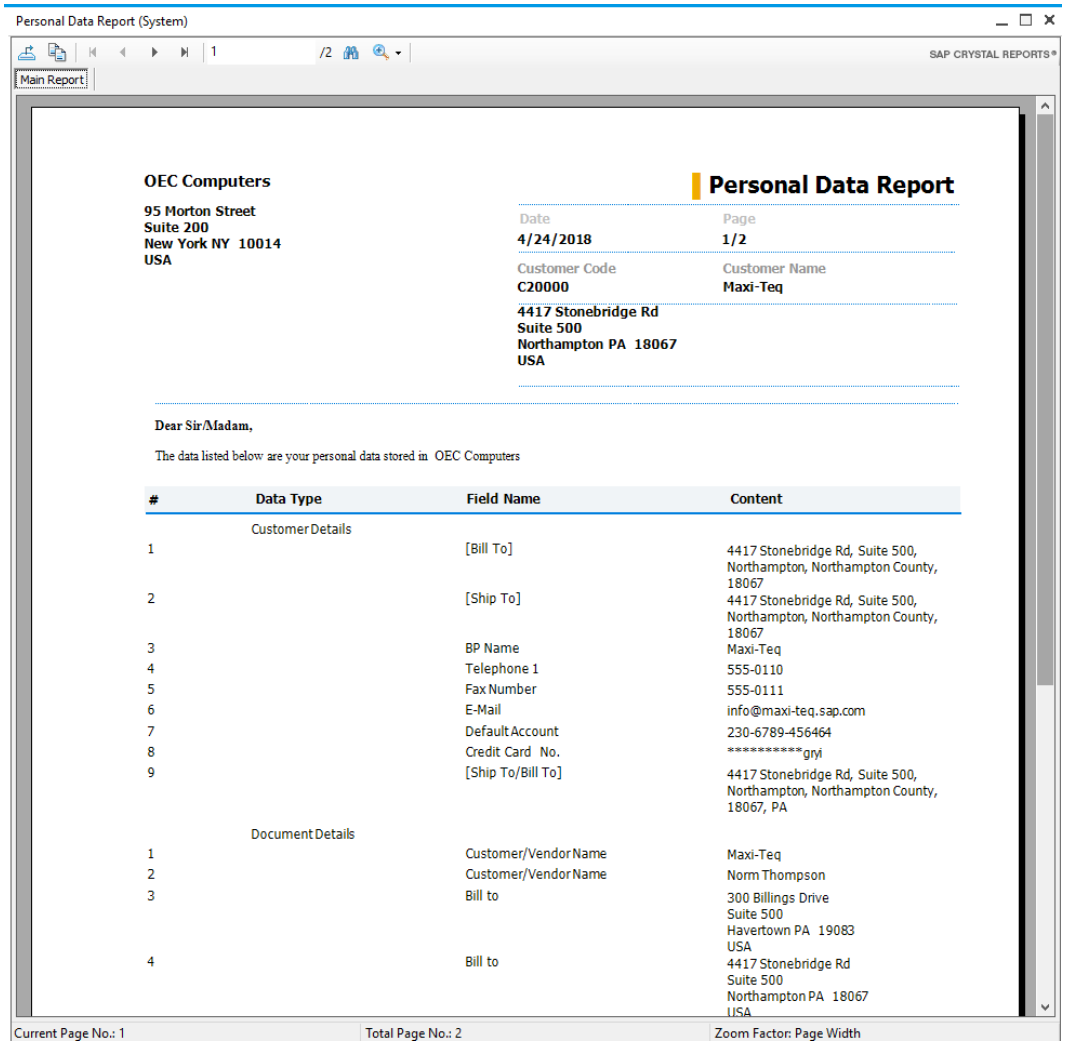
Search for the natural persons you want to report on in step 3 of the wizard, *Selection Criteria*. You can search for multiple natural persons; a separate report will be produced for each person. Select the *Include Contact Persons* checkbox to broaden your search.

In step 5 of the wizard, *Save Options,* you can either choose *Save Selection Criteria and Exit* or finalize the report by printing it or by producing a print preview. Reports can be exported by selecting the *Export Report* icon .

> **Recommendation**
>
> Outside SAP Business One, verify that natural person data subjects have consented to *Personal Data Reports* being produced about them.

Caution

When printing a *Personal Data Report*, the report is saved in a temporary folder on your computer. After completing printing, the report is deleted and a notification states that the report was deleted. If no such notification is received, the report must be deleted manually.



2.3.4 Personal Data Cleanup

Select the wizard action *Personal Data Cleanup* in step 2, *General Parameters,* to erase the data of natural persons that exist in SAP Business One.

According to various regulations around the world, the recording and retaining of personal data should be for specific purposes and processes; once the purposes expire and processes are finished, the personal data should be deleted. Additionally, natural persons can request the erasure of their personal data.

You can use the wizard action *Personal Data Cleanup* to manage your company's obligation to erase the personal data of natural persons held in SAP Business One. *Personal Data Cleanup* works in the following ways:

- Personal data is erased from all areas in which it appears in SAP Business One production.
- Personal data is erased and so removed from areas like master data and transactions, but the entries will continue to exist without the personal data.
- The erasure of personal data cannot be reversed.
- The erased personal data is replaced with asterisks.
- The *Status* in the *Personal Data Protection* section of related master data windows for natural persons is updated to *Erased*.
- When cleaning up external business partners in campaigns, the field *Data Protection Status* on the campaign line is updated to *Erased*. When the status is *Erased*, the line can be deleted but not updated.
- Where the natural person is an employee, business partner or contact person, the record is deactivated in master data; user records are locked. Any employee activities are closed.
- Where employees are owners of business partners (data ownership is managed by business partner) and the business partner *Data Protection Status* is not *Erased*, *Blocked* or *Unblocked*, the employee must be disassociated from the business partner before employee clean up.
- No new transactions can be created for erased natural persons.
- The master data of natural persons cannot be updated after being erased.
- Any customized personal data transfer to journal entries is not affected by *Personal Data Cleanup.*
- Draft documents are not included in *Personal Data Cleanup* so need to be removed or dropped separately. If removal fails, it is likely due to a process which needs to be completed or canceled.
- *Personal Data Cleanups* only affect the production database of SAP Business One, any related backups or other data storage needs to be managed separately.
- The field contents of *Sales Employee Name* in *Sales Employees/Buyers - Setup* is changed to unique dummy data following *Personal Data Cleanup*. The *Data Protection Status* field in *Sales Employee/Buyers - Setup*, for the relevant sales employee, is changed to *Erased* following cleanup.
- For open documents, the system verifies that *Orders* and "higher" marketing documents are closed for the personal data you want to clean up. "Lower" open documents such as *Purchase Quotations* are not verified.
- After cleaning up the field *Attachment Entry*, links in tables such as *OATC* or *ATC1* are cleared so that the *Attachments* tabs in areas such as *Employee Master Data* contain no data.

In step 3 of the wizard, *Selection Criteria*, you can search for natural persons you want to clean up and erase. You can search for multiple natural persons and add them to the same wizard run, just like in the other wizard actions. Use the *No Transaction Since* field on the *Business Partners* tab to manage your company's data retention timelines and find inactive business partners; transactions include marketing documents, journal entries and payments. The *Include Contact Persons* checkbox is automatically selected and cannot be deselected on the *Business Partners* tab.

In step 5 of the wizard, *Save Options,* you can choose to either *Save Selection Criteria and Exit* or finalize the cleanup by choosing *Execute*. Whether the process was successful or not is detailed in step 6 of the wizard, *Summary Report*.

If in the future the natural person needs to be reestablished in the system, a new record will be required.

Recommendation

Remove data as soon as it is not needed, this can be done manually and does not have to be done through *Personal Data Cleanup.* Closely manage your activities, sales opportunities and campaigns to meet your obligations towards the protection of personal data.

2.3.5 Personal Data Blocking

Select the wizard action *Personal Data Blocking* in step 2, *General Parameters,* to block access to the data of natural persons that exist in SAP Business One.

According to various regulations around the world, the recording and retaining of personal data should be for specific purposes and processes; once the purposes expire and processes are finished, the personal data should be deleted. However, after personal data retention periods expire, extensions or overrulings may be given as mandated by law. Personal data access can be blocked but the data can be retained where required.

You can use the wizard action *Personal Data Blocking* to manage your company's obligation to block access to the personal data of natural persons held in SAP Business One.

- Once blocked, the personal data are retained but not accessible or visible unless unblocked.
- Blocked, or subsequently unblocked, natural person records cannot be used in future marketing documents or other business processes.
- Blocking the personal data of selected natural persons encrypts the database records and anonymizes the data on the user interface, in certain cases data is hidden from view.
- When the blocked data are no longer needed, the personal data can go through cleanup after unblocking.
- Business partners who have open marketing documents are excluded and their personal data cannot be blocked.

In step 3 of the wizard, *Selection Criteria*, you can search for natural persons you want to block access to. You can search for multiple natural persons and add them to the same wizard run, just like in the other wizard actions.

In step 5 of the wizard, *Save Options,* you can choose to either *Save Selection Criteria and Exit* or finalize the blocking by choosing *Execute*. Whether the process was successful or not is detailed in step 6 of the wizard, *Summary Report*.

If in the future the natural person needs to be reestablished in the system, a new record will be required.

2.3.6 Personal Data Unblocking

Select the wizard action *Personal Data Unblocking* in step 2, *General Parameters,* to unblock access to the personal data of natural persons that have been blocked previously. The wizard is the only way you can reverse a block on personal data access in SAP Business One.

The search, save and results steps work in the same way as for *Personal Data Blocking*, however previous blocking means that only *Natural Person Code* will be displayed.

Unblocking the personal data of selected natural persons decrypts the database records and makes the data available on the user interface. Once unblocked, the personal data are accessible to all authorized users, but the natural person records cannot be used in future marketing documents or other business processes.

Personal data can be blocked again or if no longer needed can go through a cleanup process. If in the future the natural person needs to be reestablished in the system, a new record will be required.

2.3.7 Default Customers for A/R Invoices and Payments

Default Customers for A/R Invoice and Payment (*One Time Customers*), or simply "default customers", are business partners that are used for generating sales documents, usually invoices and payments, for onetime customers. Since default customer business partner master data is used for multiple onetime customers, normally no personal data is stored for default customer business partners. However, it is possible to hold personal data against the many default customer **transactions**; personal data management options are required for the documents that are created featuring personal data.

Default Customers for A/R Invoice and Payment (One Time Customers) are determined in *G/L Account Determination* (follow path *Administration → Setup → Financials → G/L Account Determination → G/L Account Determination*). Different default customers can be established for different financial periods.

Options for either *Business Partners* or *Default Customers for A/R Invoices and Payments* are available on the *Business Partners* tab of step 3 *Selection Criteria* for the following wizard action types:

- *Determine Natural Persons*
- *Reverse Natural Person Determination*
- *Personal Data Cleanup*

The option *Default Customers for A/R Invoices and Payments* is not selectable for the wizard actions *Personal Data Blocking*, *Personal Data Unblocking* and *Personal Data Report*.

The option *Default Customers for A/R Invoices and Payments* allows for the searching of default customers and related transactions, to apply personal data protection management processes to documents established using those default customers. The option *Business Partners* allows for the searching of regular business partners.

Determine Natural Persons

When selecting the wizard run type *Determine Natural Persons* and choosing *Default Customers for A/R Invoices and Payments*, you can choose the default customers whose transactions feature personal data.

Different default customers can be established for different financial periods so multiple default customer results are possible.

When executing the wizard, sensitive personal data is encrypted in default customer master data and transactions.

Personal Data Cleanup

When determining default customers as natural persons, only their related transactions are considered as personal data. This is different to regular business partners, where both the business partner master data and transactions are considered as personal data. This is because default customers are often used to generate documents for several onetime customers.

For the wizard run type *Personal Data Cleanup*, an additional option *Transactions Posted On or Before* is available for limiting search results by date when *Default Customers for A/R Invoices and Payments* is chosen. The selection of a date in *Transactions Posted On or Before* is mandatory. If a document has no posting date, then the creation date is analyzed. Only closed marketing documents can be searched for.

Once searched for, default customers that are determined as natural persons, so their related transaction rows, can be selected or deselected for personal data cleanup. Different default customers can be established for different financial periods so multiple default customer results are possible.

If a onetime customer requests the removal of personal data, then cleanup is possible as part of a general cleanup of transactions for which the retention period had expired.

2.4 Sensitive Personal Data, Sensitive Personal Data Access Log and Payment Wizard

There are data in all localizations of SAP Business One which can be classified as *Sensitive Personal*:

- *ID Issued by Authorities*
- *Passport No.*
- Data for business partner bank accounts
- Data for business partner IBANs (International Bank Account Numbers)
- *Bank Account* for employees
- User-defined fields that have a *Structure* of *Text* and are connected to objects in *Personal Data Management*.

Bank account and IBAN data are classified as sensitive data by SAP standards but not necessarily by all legal jurisdictions.

Additional pieces of data exist in the Germany localization of SAP Business One that can be classified as *Sensitive Personal*:

- *Confession*
- *Confession of Partner*
- *Social Insurance Number*.

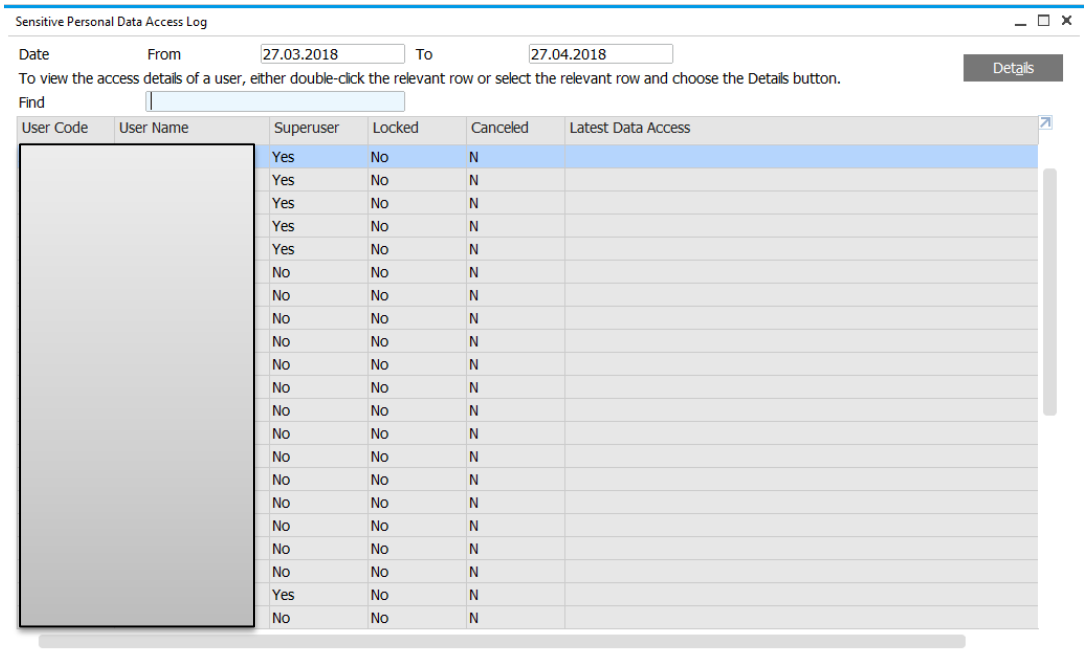
A natural person's sensitive personal data is encrypted by default and hidden from view for all users once a natural person has been determined. Only authorized users can view the data by right-clicking on the fields in question and choosing to display the sensitive data. The action of right-clicking on the data is logged and recorded in the *Sensitive Personal Data Access Log*. Once the sensitive data is accessed, it can be amended.

Business partner bank account data, unlike other sensitive data, is encrypted except for the last 4 digits. If the business partner bank account data has only 4 digits, then all 4 digits are encrypted. Business partner bank account and IBAN data is encrypted in *Business Partner Master Data* and any related forms or documents that display the data, like incoming payments, deposits, bills of exchange, the payment wizard and payment results tables.

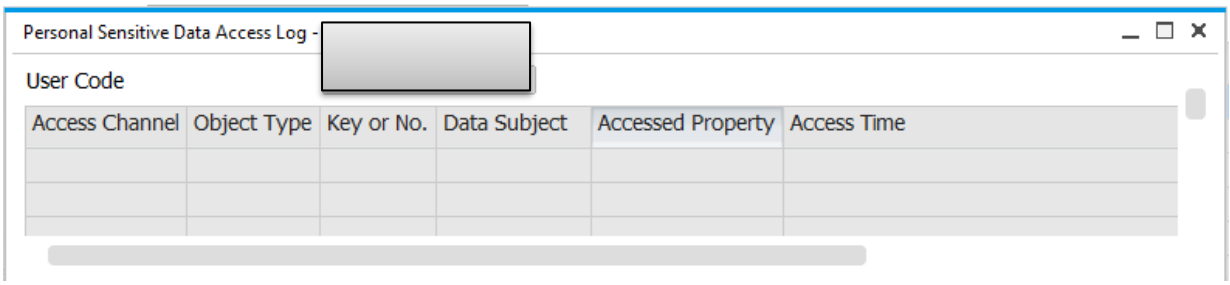
Sensitive Personal Data Access Log

The *Sensitive Personal Data Access Log* allows you to track who has accessed sensitive personal data in SAP Business One. When sensitive personal data is viewed through the *Personal Data Management Wizard* action *Personal Data Reports*, the access is recorded in the *Sensitive Personal Data Access Log*. When sensitive personal data is accessed by DI API or *Payment Wizard*, the access is recorded in the *Sensitive Personal Data Access Log*. When sensitive personal data is exported in a query or spreadsheet, the sensitive personal data is encrypted and so no access is logged.

From the SAP Business One *Main Menu*, choose *Administration* → *Utilities* → *Data Protection Tools* → *Sensitive Personal Data Access Log*. The *Sensitive Personal Data Access Log* window opens.



By selecting individual users in the log, you can see which objects were accessed for which data subjects, at what time and through which method.



Creating Bank Files in the Payment Wizard with Sensitive Personal Data

From the SAP Business One *Main Menu*, choose *Banking → Payment Wizard* to access the *Payment Wizard*.

The bank file generation process through the *Payment Wizard* is affected when working with sensitive personal bank data for natural persons. When updating *Payee Bank Account* and *Payee Bank IBAN* (*Data Type* category *Payment Results Table* or the *OPEX* table), the data are encrypted before being entered. When generating bank files through the *Payment Wizard*, the business partner bank account and IBAN data are taken into the bank file after decryption.

Creating bank files is logged as an action accessing sensitive personal data.

When creating bank files, the *Payment Wizard* decrypts the relevant bank data, so the bank file can subsequently be used to make payments, provided a single *Bank Format File Type* is chosen.

To create bank files with decrypted data, only one category of *Bank Format File Type* can be selected in step 6 of the wizard. Two *Bank Format File Types* exist, *EFM* and *DLL*, selecting rows with *EFM* and *DLL* in the same run will create an *EFM* bank file with encrypted data that cannot be processed by banks. A warning message appears when a wizard run involves both *EFM* and *DLL* formats.

When the *Bank Format File Type* is *DLL*, then the decryption of the data is handled by DI service (more information is available in SAP Note 2633811). This service is called by the payment add-on. The payment add-on identifies the fields to be decrypted based on the setup in *Personal Data Management*.

3 Personal Data Protection

Personal Data Protection is a separate and distinct feature to *Personal Data Protection Management*. *Personal Data Protection Management* has many more features and covers much more data than *Personal Data Protection* which was introduced before *Personal Data Protection Management*.

Personal Data Protection automatically encrypts, so hides from view, and restricts the editing of data contained in a limited number of fields. The viewing and editing of the encrypted data are controlled through *Authorizations*. Data in the following fields are encrypted by *Personal Data Protection*:

- *ID No.* on the *Personal* tab of the *Employee Master Data* window. All but the first 7 standard characters are encrypted.
- *Passport No.* on the *Personal* tab of the *Employee Master Data* window. All characters are encrypted.
- *ID No. 2* on the *General* tab of the *Business Partner Master Data* window. All but the first 7 standard characters are encrypted.

By changing *Authorizations* for users, the underlying data can be viewed and edited. From the SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *Authorizations* → *General Authorizations* → *General* → *Access to Masked Data*. The following *Authorization* settings determine what data users can view and amend in the fields that are encrypted by *Personal Data Protection*:

- *No Authorization*. Data cannot be amended and can be viewed in an encrypted form only. Default setting for regular users.
- *Read Only*. Data can be viewed in an unencrypted form but not amended.
- *Full Authorization*. Data can be viewed and amended in an unencrypted form.

As Crystal Reports access the database directly, you can use the "SAPB1CRDecryptAndMaskGenerate(encryptedString, fieldType)" function to decrypt the data. In the "encryptedString" parameter, you define the string to be decrypted. The "fieldType" parameter specifies the field as follows: "0 ... Credit Card No.", "1 ... Business Partner Master Data ID No. 2", "2 ... Employee Master Data ID. No.", "3 ... Employee Master Data Passport No.". Although initially decrypted, the data is displayed in an encrypted form in Crystal Reports.

4 Authorizations

Authorizations allow specific users in SAP Business One to view, create, and update parts of the system that they have been assigned to, following data ownership definitions. By default, new users have no authorizations. Each user can have only one manager who assigns permissions.

By controlling who has authorization to access different parts of the system, you control access to the data in the system. Through authorizations, you can control access to, and so can protect, personal data.

Just like for other areas of SAP Business One, access to personal data protection tools like the *Personal Data Management Wizard* and viewing sensitive data can be controlled in *Authorizations*. The viewing of just personal data in different objects cannot be controlled by *Authorizations*, users can either see everything with personal data or nothing at all.

You can define users as either regular users or superusers.

Regular Users:

- Can perform certain actions, for example, award discounts, change prices, or access confidential accounts, with the proper authorizations.
- Cannot assign authorizations to other users.

Superusers:

- Have full and unrestricted authorization to access users in the system, apart from to their own logins.
- Automatically have full authorization to access all functions in the system.
- Can define authorizations and permissions for other users.

You define authorizations in the *Authorizations* window. From the SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *Authorizations* → *General Authorizations*.

Users can be given authorization to access individual modules, like *Sales - A/R,* and the different areas under the individual modules. Authorizations are affected by combinations of settings. For example, if a user has permission to display business partner master data but lacks permission to see account balances of business partners, the system does not display account balances in the *Business Partner Master Data* window.

Users who do not have permission to alter authorizations do not have the *Authorizations* option in their view of the *Administration* module.

Prerequisites

You have defined users in the system and specified which users are superusers.

Features

You can give users authorization to only display information or exclude users from a function altogether. You can restrict user access to documents. For example, you can limit access to sales quotations within a certain number series only, to quotations in other series, or you can deny access completely.

You can override authorizations in specific circumstances. For example, if a user has no permission to create a certain sales document, but attempts to do so, the system prompts the user to request an authorized user to approve and enter their user name and password. This enables the unauthorized user to save the document for that specific occurrence only.

You can define approval processes for the purchasing and sales transactions in the system that override the standard permissions. For example, if a user is authorized to add an invoice, even if it exceeds the customer's credit limit, you can activate an additional release procedure whenever the credit limit is exceeded by a specific amount.

4.1 Defining Authorizations

SAP Business One is equipped with a comprehensive authorization facility that can be tailored to every user. During the implementation phase, the system administrator should devise an authorization policy to prevent unauthorized access to the database. By assigning the correct authorizations, changes to document fields can be restricted.

Certain precautions must be taken to ensure that access to data is monitored. In the *General Ledger*, users who do not have authorization for the document journal, but are authorized for journal entries, can use the data record pushbuttons to scroll through the database and view documents. In this way, they can display other entries, even though they are not authorized to display lists, for example, in the document journal.

You should grant authorizations to each user according to the user's roles and responsibilities. SAP Business One provides the following authorization options:

- *Full Authorization*: users can display and modify data for that function.
- *Read Only*: users can only view, but not change, data.

  This option targets data only, so it is not available for functions that require user operations (for example, removing business partners).
- *No Authorization*: users have no access to that function.

  Note

  Superusers have full authorizations for all functions and these authorizations cannot be modified.

Each user's authorizations are displayed in the *Authorizations* window. Various authorizations are displayed for modules with mixed authorizations, such as full authorization for some submodules and read-only for others.

Prerequisites

- You are a superuser.
- You have created regular users in the system.
- You have assigned users to appropriate authorization groups.

Procedure

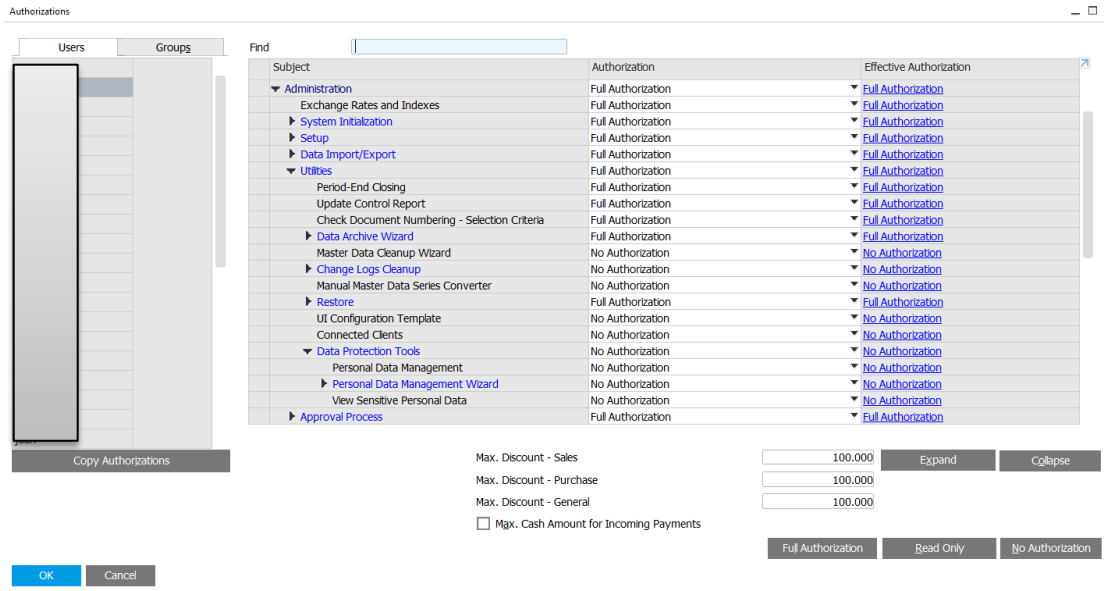
1. From the SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *Authorizations* → *General Authorizations*. The *Authorizations* window opens.
2. On the *Authorization Groups* tab of the *Authorizations* window, define authorizations for each authorization group. Each authorization group's authorizations are automatically applied to all users within the group.
3. On the *Users* tab, fine-tune each user's authorizations to ensure appropriate effective authorizations for all permission items.
4. Choose the *Update* button to save the changes in the *Authorizations* window.

> **Note**
>
> If you grant a user full or read-only authorization for a certain function, make sure that you have assigned an appropriate license to the user. Otherwise, the authorization setting is not effective.

4.2 Defining Authorizations for Personal Data Protection

Access to personal data protection tools like the *Personal Data Management Wizard* and the viewing of sensitive data can be controlled in *Authorizations*.

From the SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *Authorizations* → *General Authorizations*. In the main *Authorizations* grid, select *Administration* → *Utilities* → *Data Protection Tools* for individual users.



When running the *Personal Data Management Wizard*, *Data Ownership* is ignored; if a user is authorized to access a wizard action then they can access all business partners through the wizard. For users authorized to use wizard actions, data ownership is not applied when selecting business partners, when accessing business partners or documents for generating personal data reports or for executing personal data cleanups.

4.3 Defining User Groups

Prerequisites

You are a superuser.

Context

Employees in a company can be grouped according to their roles (for example, sales people, accountants, managers and so on). Generally, different roles require different settings for their functions, features, and data within SAP Business One. You can assign SAP Business One users to different user groups, based on the users' actual roles.

SAP Business One supports the following user group types:

- *Authorization*: According to users' different roles, you can assign them to the appropriate authorization groups. An authorization group's authorizations are automatically applied to all users within this group.
- *Form Settings*: With a form settings group, you can copy the form settings of one user to a group. This helps you save time when adding new users or changing the table columns to be displayed for a group of users.
- *Cross All Types*: The settings of each of the above group types are automatically applied to all the groups in this type. If you intend to create the groups containing the same users in each of the above types, we recommend that you create just one group under *Cross All Types*.

After assigning users to specific settings groups (for example, authorization groups), you can grant the settings at the group level and then fine-tune each individual user's settings.

As in real life, each SAP Business One user may belong to more than one group. These groups are either in a same type or in different types. For example, an accounting manager may have the roles of an accountant and a manager. The `Accountant` and the `Manager` groups both may be in the *Authorization* type; or the `Accountant` group may belong to the *Authorization* type and the `Manager` group may belong to the *Form Settings* type.

> **Note**
>
> A group name is unique within all user group types.

Procedure

1. To open the *User Groups* window, from the SAP Business One *Main Menu*, choose *Administration* → *Setup* → *General* → *User Groups*.

The *User Groups* window appears. In the left pane, you can select the group types and the corresponding existing groups displays. You can select each group to edit the group name and group type, add users to this group, and so on.

> **Note**
>
> Once you change the group type for a specific group, this group will lose all properties of the former group type.

2. To define a new group, in the *User Groups* window, choose the *Create Group* button. The *OK* button changes to *Add*.
3. Enter a name, an optional description and a type for the group.
4. Select appropriate users for this group.
5. Choose the *Add* button.

   A new group is created.

Results

When you create an authorization group, you can define a due date range for the group. In addition, you can also specify a due date range for any specific user in this group.

Defining an active date range for an authorization group:

- Specify the date range (*Active From...To...*) in the header of a user group.
- The date range entry applies to all users in the group.
- Once the validity period of this group has expired, all users in the group will lose the corresponding authorizations of this group. The users remain with their authorizations (if any) granted in other groups.

Defining an active date range for a specific user:

- Specify a date range (*Active From...To...*) in the lines of users.
- The date range entry applies only to the selected user.
- Once the validity period of this user has expired, this user will lose the corresponding authorizations of this group. This user remains with his other authorizations (if any) granted in other groups. At this point, if the group's date range is still valid, the other users in this group remain with this group's authorizations until their own active dates have expired.

A user's active date range must be within the corresponding group's active date range.

> **Example**
>
> You create an authorization group named `Sales`, assigning `Sam` and `Jack` into the group.

- The active date range for the group `Sales` is defined as being from 01.01.2017 to 31.12.2017.
- The user's active date range for `Sam` is defined as being from 01.02.2017 to 30.06.2017.
- The user's active date range for `Jack` is defined as being from 20.01.2017 to 30.09.2017.

4.4 Copying Authorizations for Other Users or Authorization Groups

Context

You can copy authorizations between authorization groups and between users. This function is especially useful in the following situations:

- Between authorization groups:
  - Members of two authorization groups play similar roles in the company but are divided into two groups because they belong to different business units or branches.
  - There is considerable overlap between two authorization groups in terms of members.

    For example, Group A is included in Group B. Both groups require the same authorizations for nearly all permission items, except that Group A requires higher authorizations for certain permission items. As a result, you can first define authorizations for Group B, then copy Group B's authorization profile to Group A, and lastly, fine-tune Group A's authorizations.
- Between users:
  - Two users play the same role and have exactly the same responsibilities. Therefore, they may have the same authorization profile.
  - Two users' responsibilities are very similar and differ only in a few aspects.

> **Note**
>
> You cannot copy a superuser's authorization profile for regular users. Although you can grant full authorization to a regular user throughout the system, only superusers can perform certain functions (for example, assigning authorizations, data ownership, and licenses).

Procedure

> **Note**
>
> If you want to copy authorizations only between two users or between two authorization groups, you can use an alternative drag-and-drop method. For example, you can drag a user name to another user name, and then release the mouse button. This can also apply the first user's authorizations to the second user after your confirmation.

1. From the SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *Authorizations* → *General Authorizations*. The *Authorizations* window is displayed.
2. Select the user or authorization group whose authorization profile is to be copied.
3. Choose the *Copy Authorizations* button.
4. In the *Copy Authorizations* window, select appropriate users or authorization groups, and then choose the *OK* button.
5. To save the changes, choose the *Update* button in the *Authorizations* window.

4.5 Modifying Authorizations

When an authorization for a module or a parent function is granted, the authorization is automatically copied to all the child functions. For example, if *No Authorization* is granted for the *Sales* module, the user does not have any authorizations for any function throughout the entire module.

Only superusers can modify permissions for other users. However, superusers cannot modify authorizations for themselves.

Procedure

To define or restrict different authorizations for individual functions in an application:

1. Choose *Administration* → *System Initialization* → *Authorizations* → *General Authorizations*. The *Authorizations* window displays.
2. Choose the user name in the left column.
3. Select the  icon to the left of an application or function in the list to expand to the next level of authorizations. To show or hide all the functions of an application at once, choose *Expand* or *Collapse*, respectively.
4. To change a user's authorization for a function or an entire module, single-click the authorization in the list to the right. A dropdown list appears with the possible authorizations for the function or application. Choose an entry from the list to select it.
5. Once a user has been selected, display and change the corresponding authorizations as required. Superusers appear in gray in the list, as their permissions cannot be altered.

4.6 Personalizing Main Menu According to Authorizations

Depending on user authorizations for system functions, users may be restricted from opening some windows in the SAP Business One *Main Menu*. Users will still see, but can hide, menu entries that are not accessible.

Procedure

The *Main Menu* is not automatically updated according to each user's authorizations. To display or hide menu entries according to the user authorizations, do the following:

1. Log on to SAP Business One as, for example, user A, and make sure that the *Main Menu* is active.
2. On the tool bar, click  .
3. In the *Form Settings - Main Menu* window, choose the *Apply Authorization* button.
4. To save the changes, choose the *Update* button.

4.7 Authorizations for Specific Windows and Documents

Prerequisites

To display windows that the user may not have permission to display, choose the *Main Menu - Settings* icon from the toolbar and make all the required options *Visible*.

Context

Authorizations can be overridden in specific circumstances. For example, if a manager is out of the office, they can permit one of their staff to add a document on a one-time basis. In addition, this function permits those without authorizations to view reports and other windows to which they may not otherwise have access. The user who lacks permissions is challenged each time for the overriding permissions.

Procedure

1. Open the required document. A system message displays stating that the user does not have permission to perform this action.
2. Choose *Authorization by Another User*.
3. Enter the user name (code) and password of the manager or user with the required permissions.
4. The transaction is then completed as required.

4.8 Tracking Changes in Authorizations

Prerequisites

To view changes in authorizations, full authorization to the *Change Log* option, under *General* is required. Super users in the system have full authorizations automatically.

Each time a user updates the *Authorizations* window, the system creates a new instance of the *Authorizations* window, and saves it in the *Change Log* window along with the date and the user who made the update.

Context

All the changes in authorizations that were made in any category and by any user can be tracked. These include a detailed list of the changes, who made them and when they were made. In addition, the *Authorization* window as it was on a specific date, or after a specific update can be displayed.

Procedure

1. Open the *Authorizations* window from *Administration* → *System Initialization* → *Authorizations* → *General Authorizations*.
2. Choose the user for whom the changes are to be tracked.
3. From the *Tools* menu, choose *Change Log*. The *Change Log* window displays.
4. In the *Change Log* window, double-click a row to display the required instance of the *Authorizations* window. The instance provides a view of the *Authorizations* window as it was after the update.
5. Choose the *Show Differences* button to view a detailed list of the changes made in the selected instance.

4.9 Authorizations Window

Use the *Authorizations* window to assign permissions to each user. Superusers have full permissions that cannot be altered. Regular users can have full or partial permissions, for each module and sub-module.

To access the *Authorizations* window, choose *Administration* → *System Initialization* → *Authorizations* → *General Authorizations*.

> **Note**
>
> You have defined your users as either regular or superusers.

Authorizations Window Fields

Users

This tab displays authorizations for every SAP Business One user. We highly recommend that you follow the steps below to define authorizations for individual users:

1. Assign each user to appropriate authorization groups, based on the user's role (for example, sales person or manager).
2. Define authorizations for each authorization group first. Each authorization group's authorizations are automatically applied to users within the group.
3. Fine-tune each user's authorizations to arrive at appropriate effective authorizations.

Authorization Groups

This tab displays authorizations for every authorization group. An authorization group's authorizations are automatically applied to all users within this group. For more information, see Defining Authorizations.

Effective Authorization

The resultant authorization that a user has over an object or operation.

Various levels of authorization can be applied to a user at both the user and the authorization-group levels. The effective authorization is the highest level of authorization that is applied to the user.

> **Example**
>
> User U001 is assigned to Group A and Group B. For a particular permission item:

- U001 authorization = Read-only
- Group A authorization = Full
- Group B authorization = None

As a result, the effective authorization = max{Read-only, Full, None} = Full.

Max. Discount – Sales

Specify the maximum discount that the user is authorized to enter in sales business documents. If you enter 0, the user is not able to enter any amounts for which automatic rounding has been defined, because automatic rounding represents a discount.

Max. Discount – Purchasing

Specify the maximum discount that the user is authorized to enter in purchasing business documents. If you enter 0, the user is not able to enter any amounts for which automatic rounding has been defined, because automatic rounding represents a discount.

Max. Discount – General

Specify the maximum discount that the user is authorized to enter for the followings:

- Business partner master data
- Payment terms
- Goods issue, goods receipt, and inventory transfer
- Special prices

If you enter 0, the user is not able to enter any amounts for which automatic rounding has been defined, because automatic rounding represents a discount.

Max. Cash Amount for Incoming Payments

Select and enter the maximum cash amount the regular user is authorized to enter in an incoming payment (*Payment Means* window, *Cash* tab). This can be overridden for specific documents with a supervisor's permission. This option is not active for superusers.

Full Authorization

Choose to grant full authorization to a user for all functions in all applications.

Read Only

Choose to grant read-only authorization to a user for all functions in all applications. The user can then display all data but cannot make any changes.

No Authorization

Choose to grant no authorizations for any functions in any application. The user will be unable to display or change any data.

4.10 Additional Authorization Creator

Use this window to create and add a new permissions object for user-created forms.

Additional Authorization Creator

Authorization ID, Name

Specify unique ID and name for the additional authorization.

Option

Sets permission options for the new authorization:

- *Full/Read/None*
- *Full/None*

Item

Indicates if the authorization is of *Item* type or *Form* type

Permissions set to a form apply to all its subordinates. Permissions set to an item do not apply to the parent form.

Level

Sets hierarchy level for the object.

Parent ID

Selects a parent item when you add a subordinate object.

Display Order

Selects the location of a subordinate or sibling object within the permission hierarchy.

Forms ID/Edit

Opens the *User Authorizations – Forms ID* window. Assigns the authorization object to a user-form of your choice by entering the form ID.

Add Same-Level

Choose to define new additional authorization with the same level of the selected one.

Add Sub-Level

Choose to define new additional authorization with level lower than the level of the selected one. Subordinate authorizations can be created for additional authorizations of levels one to four.

4.11 Authorization for Changing My Personal Settings

Use the *Authorization* window to assign permissions to each user to change all or some attributes for themselves.

To access *Authorization - Change My Personal Settings*, from the SAP Business One *Main Menu*, choose *Administration*→ *System Initialization*→ *Authorizations*→ *General Authorizations*, and then enter `Change My Personal Settings` in the *Find* box.

You can change the authorization of *Change My Personal Settings* by choosing the following options:

- *Full Authorization* (This option is by default selected.)
- *Read-Only*

- *No Authorization*

The following table explains the dependencies between the *Users* authorization and the *Change My Personal Settings* authorization:

Authorization of *Users*	**Authorization of** *Change My Personal Settings*	**Behavior**
Full Authorization	Full Authorization	The user can access and change all enabled attributes in *the Users - Setup* window for the current user and other users.
Read Only	Full Authorization	The user can access the *Users - Setup* window, navigate and view the details of all the users, but can change: • Only the following details of the current user: *E-mail*, *Mobile Phone*, *Mobile Device ID*, *Fax*, *Defaults* • The values on the *Services* and *Display* tabs.
No Authorization	Full Authorization	The user can access the Users - Setup window, view and change: • Only the following details of the current user: • The following settings: *E-mail*, *Mobile Phone*, *Mobile Device ID*, *Fax*, *Defaults* • The values on the *Services* and *Display* tabs.
Full Authorization	Read Only	The same behavior as when a user has *Full Authorization* in *Users*.
Read Only	Read Only	The user can access the *Users - Setup* window, navigate and view the details of all the users, but cannot make any updates.

No Authorization	Read Only	The user can access the *Users - Setup* window, only view the details of the current user, but cannot make any updates.
Full Authorization	No Authorization	The same behavior as when a user has *Full Authorization* in *Users*.
Read Only	No Authorization	The user can access the *Users - Setup* window, navigate and only view the details of all the users, but cannot make any updates.
No Authorization	No Authorization	The user has no access to the *Users - Setup* window.

5 Data Ownership

Data ownership allows you to control who owns data within SAP Business One. With the data owner function, you can define the owner of data and information. Therefore, personal data can be secured and protected by predefined authorizations. Information and data can be accessed by permitted roles and users only.

To enable data ownership functions, from the SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *General Settings*. On the *BP* tab, select the *Enable Data Ownership* checkbox.

To set up data ownership, proceed as follows:

- To define data authorizations, from the SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *Authorizations* → *Data Ownership* → *Data Ownership Authorizations*.
- To define the rules for sharing the ownership of documents and business partners, from the SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *Authorizations* → *Data Ownership* → *Data Ownership Sharing Options*.

When running the *Personal Data Management Wizard*, *Data Ownership* is ignored; if a user is authorized to access a wizard action then they can access all business partners through the wizard. For users authorized to wizard actions, data ownership is not applied when selecting business partners, when accessing business partners or documents for generating personal data reports or for executing personal data cleanups.

5.1 Enabling Data Ownership

In SAP Business One *Main Menu*, choose *Administration* → *System Initialization* → *General Settings* → *BP*, and then select the option *Enable Data Ownership* to enable the data ownership management function.

Manage Data Ownership By

This field is available only if you have selected the *Enable Data Ownership* checkbox.

You can manage data ownership by following methods:

- Document Only

  Manage data ownership per document. That is, owners are directly defined for different type of documents. And the ownership authorization is determined by document owner.
- Business Partner Only

  Manage data ownership per business partner. That is, owners are defined for business partners. The ownership authorization to the documents is determined by the owner of the business partner for which the documents are created.

> **Note**
>
> The field *Allow BP Without an Owner* will appear when you have selected *Business Partner Only* in *the Manage Data Ownership By* dropdown list. Select the *Allow BP Without an Owner* option to allow business partners without owners exist.

- Business Partner and Document

  When the business partner has an owner, the ownership authorization to the document is determined by the owner of the business partner used in that document;

  When the business partner has no owner, the ownership authorization to the document is determined by document owner.

- Branch

  Manage data ownership by branch. That is, user access to marketing document, business partner, reporting and account information is authorized through branch assignment. For example, a user is only able to access a business partner if both the user and business partner are assigned to the correct branch. Data ownership by branch does not apply to *Super Users* or other users where *Ignore Data Ownership* is enabled.

  > **Note**
  >
  > For purchase requests, data ownership is directly determined by the document owner.
  >
  > For blanket agreement, data ownership is not determined by the owner defined on it, but determined by the owner of the business partner that the blanket agreements are created for.

5.2 Data Ownership Authorizations Window

This window displays each employee with each of their permissions per object. Only employees who are linked to users in the *Employee Master Data* window can view this window and all other windows in the *Authorizations* folder.

Authorizations can be granted per user, so that the user has the same permissions throughout the system. Authorizations can also be individualized, so that each user has different permissions for different objects.

Since superuser authorizations cannot be altered, user permissions are shown as grayed out. Employees that are linked to superusers have full permissions. All other users by default have no permissions.

Data ownership is driven by the owner field in business partners, sales opportunities, and sales A/R and purchasing A/P documents. The owner can only be an active employee that is associated to a user. Data ownership can be turned on or off either system wide, or by object, or even by individual window or report. A user can access the business partner, sales opportunity, and sales or purchasing document as long as he or she has a defined relationship with the owner and has been granted either *Read Only* or *Full* data ownership permission for that relationship.

Relationships include:

- Peer: the user and the owner share the same manager on their corresponding employee records
- Manager: the owner is the user's manager per the manager field on the user's employee record
- Subordinate: the user is the owner's manager per the manager field on the owner's employee record
- Branch: the user and the owner are members of the same branch. The branch is read from the corresponding employee records.
- Department: the user and the owner are members of the same department. The department is read from the corresponding employee records.
- Team: the user and the owner are members of the same team. Team membership is defined on the corresponding employee records
- Company: the user can define the ownership on the company level.

For each of these relationships, the user can be granted *Full*, *Read Only* or *No Authorization*.

In the event that more than one relationship exists between the user and the owner, the more lenient authorization is granted. For example, the user and the owner are in the same branch and department. If the user has *Read Only* for the branch but *Full* authorization for the department, the user is granted *Full* authorization to the sales opportunity or sales or purchasing documents in question.

In the situation whereby different authorizations are granted to the same object, the more lenient authorization is granted. For example, if the user has *Read Only* authorization for *Peer* but *Full* authorization for *Company*, the user is granted *Full* authorization to the object company-wide.

To display this window, choose *Administration* → *System Initialization* → *Authorizations* → *Data Ownership* → *Data Ownership Authorizations*.

> **Note**
>
> According to the method you select to manage the data ownership, different objects are displayed in this window. You can manage data ownership by the following methods:

- Document Only - displays sales and purchasing documents
- Business Partner Only - displays business partner and purchase request
- Business Partner and Document - displays business partner, sales and purchasing documents

5.3 Data Ownership Sharing Options Window

In this window, you define which objects can be viewed, either fully or partially, or whether only the name of a document appears in a report while the document itself cannot be viewed.

If a document or sales opportunity has no owner, then any user can access it as if no data ownership is in place. Any user can assign an owner to a document or sales opportunity that does not have an owner. Once an owner is assigned, only the owner's manager or a superuser can change the owner.

Define object owners according to the following data ownership management methods:

- Data Ownership Sharing Options: Manage By Document Only
- Data Ownership Sharing Options: Manage By Business Partner Only
- Data Ownership Sharing Options: Manage By Business Partner and Document

5.3.1 Data Ownership Sharing Options: Manage by Document Only

Documents Tab

Define data owners for documents listed on this tab. You can define document owners with the following options:

- No Restriction

  Data ownership function is bypassed for the document.
- Header Owner

  Owner is defined as the owner specified on the document header.

  The documents are visible to the owner and to all those users that have a defined relationship to the owner and have the requisite permission for the specific relationship.
- Header and Row Owner

  Owner is defined as both the owner specified on the document header and the owner specified in the document lines or in the opportunity stages.

  The documents are visible to the owner and to all those users that have a defined relationship to the owner and have the requisite permission for the specific relationship

Windows Tab

Define the data owners for windows listed on this tab. You can define object owners with the following options:

- No Restriction

  Data ownership function is bypassed for the document.
- Header Owner

  Owner is defined as the owner specified on the document header.

  The documents are visible to the owner and to all those users that have a defined relationship to the owner and have the requisite permission for the specific relationship.

For a document, if the owner option you select on the *Document* tab is inconsistent with the owner option you select for reports on the current tab, and the reports use this document as data source, the following happens:

- When the owner option you select on the *Document* tab is *No Restriction*, the data ownership function for this document is by passed.

  You can view all records of the bypassed document in related reports (for which you have defined a different owner on the current tab) with *Full* authorization.
- When the owner option you select on the *Document* tab is other than *No Restriction*, the following happens:
  - The owner defined on the current tab is *No Restriction*:

    In related reports for which you have defined a different owner on the current tab, you can view all records of this document with *Read Only* authorization.
  - The owner defined on the current tab is *Header Owner*:

In related reports for which you have defined a different owner on the current tab, you can view only the records for which you have a defined relationship to the header owner and have the requisite permission for the specific relationship.

5.3.2 Data Ownership Sharing Options: Manage by Business Partner Only

Documents Tab

Define data owners for purchase requests. There is no business partner in purchase requests. Therefore, the owner of a purchase request is defined directly.

You can define the owner with the following options:

- No Restriction

  Data ownership function is bypassed for purchase request.
- Header Owner

  Owner is defined as both the owner specified on the purchase request header and the owner specified in the purchase request lines.

  Purchase requests are visible to the owner and to all those users that have a defined relationship to the owner and have the requisite permission for the specific relationship.
- Header and Row Owner

  Owner is defined as both the owner specified on the purchase request header and the owner specified in the purchase request lines.

  The documents are visible to the owner and to all those users that have a defined relationship to the owner and have the requisite permission for the specific relationship.

Business Partner Tab

Define data owners for business partners. The data owner of the documents listed in the tab is determined by the owner of the business partner for which the documents are created.

You can define the object owner with the following options:

- No Restriction

  Data ownership function is bypassed for the documents.
- Business Partner Owner

  Owner is defined as the owner of the business partner for which the documents are created.

  The documents are visible to the owner and to all those users that have a defined relationship to the owner and have the requisite permission for the specific relationship.

  Note

  The data ownership of blanket agreements is determined by the business partner owner only, as follows:
- The owner you specify on the *General* tab of the *Sales Blanket Agreement* window *or Purchase Blanket Agreement* window has no effect on data ownership management.
- When a business partner has an owner, the data ownership of the sales or purchase blanket agreements created for it is determined by that business partner owner.

- When a business partner has no owner, data ownership of the sales or purchase blanket agreements created for it is bypassed.

Windows Tab

Define the data owners for windows listed on this tab. You can define object owners with the following options:

- No Restriction

  Data ownership function is bypassed for the document.
- Header Owner

  Owner is defined as the owner specified on the document header.

  The documents are visible to the owner and to all those users that have a defined relationship to the owner and have the requisite permission for the specific relationship.

For a document, if the owner option you select on the *Document* tab or the *Business Partner* tab is inconsistent with the owner option you select for the reports on the current tab, and the reports use this document as a data source, the following happens:

- When the owner option you select on the *Document* tab or the *Business Partner* tab is *No Restriction*, the data ownership function for this document is by passed.

  You can view all records of the bypassed document in related reports (for which you have defined a different owner on the current tab) with *Full* authorization.
- When the owner option you select on the *Document* tab or the *Business Partner* tab is other than *No Restriction*, the following happens:
  - The owner defined on the current tab is *No Restriction*:

    In related reports for which you have defined a different owner on the current tab, you can view all records of the object with *Read Only* authorization.
  - The owner defined on the current tab is *Header Owner*:

    In related reports for which you have defined a different owner on the current tab, you can view only the records for which you have a defined relationship to the header owner and have the requisite permission for the specific relationship.

5.3.3 Data Ownership Sharing Options: Manage by Business Partner and Document

Documents Tab

When the business partner for which the listed objects are created has no data owner, the data owner of the listed objects is determined by the owner option defined on this tab.

Define data owners for documents listed on this tab. You can define document owners with the following options:

- No Restriction

  Data ownership function is bypassed for the document.
- Header Owner

  Owner is defined as the owner specified on the document header.

The documents are visible to the owner and to all those users that have a defined relationship to the owner and have the requisite permission for the specific relationship.

- Header and Row Owner

  Owner is defined as both the owner specified on the document header and the owner specified in the document lines or in the sales opportunity stages.

  The documents are visible to the owner and to all those users that have a defined relationship to the owner and have the requisite permission for the specific relationship

Business Partner Tab

When the business partner for which the listed objects are created has a data owner, the data owner of the listed objects is determined by the owner option defined on this tab.

You can define the object owner with the following options:

- No Restriction

  Data ownership function is bypassed for the documents.

- Business Partner Owner

  Owner is defined as the owner of the business partner for which the documents are created.

  The documents are visible to the owner and to all those users that have a defined relationship to the owner and have the requisite permission for the specific relationship.

  > **Note**
  >
  > The data ownership of a blanket agreement is determined by business partner owner only, as follows:

- The owner you specify on the *General* tab of the *Sales Blanket Agreement* window or *Purchase Blanket Agreement* window has no effect on data ownership management.
- When a business partner has an owner, the data ownership of the sales or purchase blanket agreements created for it is determined by that business partner owner.
- When a business partner has no owner, data ownership of the sales or purchase blanket agreements created for it is bypassed.

Windows Tab

Define the data owners for windows listed on this tab. You can define object owners with the following options:

- No Restriction

  Data ownership function is bypassed for the document.

- Header Owner

  Owner is defined as the owner specified on the document header.

  The documents are visible to the owner and to all those users that have a defined relationship to the owner and have the requisite permission for the specific relationship.

For a document, if the owner option you select on the *Document* tab or the *Business Partner* tab is inconsistent with the owner option you select for the reports on the current tab, and the reports use this document as a data source, the following happens:

- When the owner option you select on the *Document* tab or the *Business Partner* tab is *No Restriction*, the data ownership function for this document is by passed.

  You can view all records of the bypassed document in related reports (for which you have defined a different owner on the current tab) with *Full* authorization.

- When the owner option you select on the *Document* tab or the *Business Partner* tab is other than *No Restriction*, the following happens:
  - The owner defined on the current tab is *No Restriction*:

    In related reports for which you have defined a different owner on the current tab, you can view all records of the document with *Read Only* authorization.
  - The owner defined on the current tab is *Header Owner*:

    In related reports for which you have defined a different owner on the current tab, you can view only the records for which you have a defined relationship to the header owner and have the requisite permission for the specific relationship.

6 Change Log Window

Use the change log to gain an overview of the changes made in many windows of SAP Business One. By tracking the change log, you can more easily verify and audit changes to data. Access to change logs is dependent on user credentials.

Each time you update, for example, personal data management, tax groups, withholding tax, house banks, freight, credit card, authorizations, employee master data, sales, purchasing documents, production orders, or charts of accounts, the application records the change and can show it as required in the *Change Log* window.

To access the change log, open a window in SAP Business One, make changes if necessary, and then (with the window still open) choose *Tools*→ *Change Log...*. To display the log of a certain change instance, in the *Change Log* window, double-click the line of the instance. The *... History Instance #...* window appears. The window displays the read-only details of the change instance.

> **Note**
>
> Updates to *Natural Person* determination by the *Personal Data Management Wizard* are not recorded in the *Change Log*. Only manual changes are recorded in the *Change Log*.

Change Log Fields

Instance

The sequential number of the change made. 1 is assigned to the first change, 2 is assigned to the second change, and so on.

Object Code

Displays the unique code of the record that is changed.

> **Example**
>
> If you have updated an account in the Chart of Accounts window, the G/L account code of the updated account appears in this field.

Updated

Displays the date on which the element was updated

User Name

Displays the name of the user who updated the element

Show Differences

Opens the *Differences* window for the selected instance.

The window provides detailed information on the changes that were made.

6.1 Differences Window

Use this window to review detailed information about the selected document instance.

To open this window:

1. In the SAP Business One menu bar, choose *Tools*→ *Change Log...*→ *Show Differences*.
2. In the *Change Log...* window, choose the *Show Differences* button.

Differences Window Fields

Date

Date on which the change was made.

Changed Field

The field that was changed.

Previous Value

Value of the field before the change.

New Value

Value of the field after the change.

User Name

Name of the user who made this change.

6.2 Change Logs Cleanup Window

Use this utility to delete the change log entries for various documents and master data up to a desired date. This helps to free up space within your company database.

> **Recommendation**
>
> Deleting the change log entries is irreversible. Back up all data before executing a cleanup.

General Area Fields

Change Logs Cleanup

Select whether to start a new cleanup according to defined parameters, or to load and view the results of the last executed cleanup.

Cleanup Scenario

Enter a name to indicate the scenario for the current cleanup.

Cleanup Date

Display the system date on which to execute the cleanup.

Logs Clean Up To

Specify the date till which you want the change log entries to be deleted. It must be earlier than the Cleanup Date.

Remarks

If required, enter any comments for the cleanup.

Table Area Fields

Select

Select the documents and master data for which you want the change log entries to be deleted.

Module

Display the modules that support the change logs cleanup function.

Document Name

Display the names of the documents and master data for which the change logs can be deleted.

Current Size (MB)

Displays the size of the change log files for the document and master data.

Status

Displays the status or the results of the cleanup for each selected document and master data.

Total

Displays the following content:

- The total of the current size of all selected documents and master data.
- The total number of change log entries that were successfully deleted.

Execute

Choose this button to start the cleanup according to defined parameters.

Cancel, Finish

Choose this button to exit the window.

- The *Cancel* button is available when the cleanup has not started yet.
- The *Finish* button is available after the cleanup is completed.

7 Access Log Window

The *Access Log* window displays the access details of SAP Business One users who have logged on and logged off with one of the following:

- SAP Business One client
- DI API

  > **Note**
  >
  > The *Access Log* window does **not** display the access details of users who have logged on and logged off using one of the following:

- SAP Business One integration platform
- Web tools
- SAP HANA (if you are using SAP Business One version for MS SQL)
- Microsoft SQL Server (if you are using SAP Business One, version for SAP HANA)

To open the *Access Log* window, in the SAP Business One menu bar, choose *Tools*→ *Access Log*.

Access Log Fields

Date From, To

Specify a date range to display detailed results for the selected user.

> **Note**
>
> If you do not specify a date range, the *Access Log Details* window does not display any results for the selected user.

Superuser

Displays one of the following:

- Yes

  Yes, the user is a superuser.
- No

  No, the user is not a superuser.

Locked

Displays the current lock status of each user as follows:

- Yes

  Yes, the user is locked.
- No

  No, the user is not locked.

> **Note**
>
> For more information about users and locking, see the online help topic Users - Setup Window.

Latest Logon Status

Displays the date and time of the latest logon for each user. If the user is currently logged on to SAP Business One, the line for the user is highlighted.

Latest Access Status

Displays one of the following statuses for each user's previous logon:

- *Succeeded*

  Indicates that the user's previous logon was successful.
- *Failed*

  Indicates that the user's previous logon failed.

Latest Logoff

Displays the date and time of the latest logoff for each user.

Last Password Change

Displays the date and time at which the password was last changed. In addition, it shows which user performed the change.

No. of Failed Access Attempts

Displays the number of failed access attempts since the last successful logon for each user, if the user's last access attempt failed.

7.1 Access Log Details Window

The *Access Log Details* window displays a list of actions and details related to a specific user's access activity in SAP Business One.

To open the *Access Log Details* window, in the *Access Log* window, double-click the table row of a user whose access information you want to display.

Access Log Details Fields

Action

Displays one of the following actions for each user:

- `Logon Succeeded`

  Indicates that the previous logon attempt succeeded.
- `Logon Failed`

  Indicates that the previous logon attempt failed.
- `Logoff`
- `Created`

  Indicates that a new user code has been created.
- `Superuser Selected`

Indicates that the user's status has changed to superuser.

- `Superuser Deselected`

  Indicates that the user's superuser status has been removed.
- `Locked`
- `Unlocked`
- `Password Changed`

  Indicates that the user password has changed since the previous logon.
- `Screen Unlock Failed`

  The SAP Business One application screen is locked after a certain time of inactivity and the user must log on again by entering the user credentials. The Screen Unlock Failed status indicates that attempting to log on again by unlocking the SAP Business One screen failed.

Action By

Displays the user ID of the user who has performed the action indicated in the Action column.

Client IP

Displays the IP addresses of the SAP Business One client computer in use by the user shown in the Action By column.

Client Name

Displays the name of the SAP Business One client computer in use by the user shown in the Action By column.

Date and Time

Displays the date and time of the action indicated in the Action column.

8 Data Archive Wizard

The *Data Archive Wizard* allows you to remove transactional data permanently from your SAP Business One database and archive the removed data.

> **Note**
>
> The *Data Archive Wizard* is available only if you are using SAP Business One version for Microsoft SQL, the wizard is not available in SAP Business One, version for SAP HANA.

From the SAP Business One *Main Menu*, choose *Administration* → *Utilities* → *Data Archive Wizard* to start the *Data Archive Wizard*.

Companies who have worked with SAP Business One for longer than two years can use the wizard to remove closed transactional data relating to previous financial periods that have been closed. Closed transactional data can include closed sales and purchasing documents and reconciled journal entries.

With the data archive wizard, you can:

- Simulate a data archive wizard run – the simulation gives you a preview of the expected results of the wizard run. The preview shows:
  - Which data will be removed.
  - The expected reduction in database size.
- Initiate a data archive wizard run – when the run is complete, some data is permanently removed from the database. This action is irreversible.

  > **Note**
  >
  > SAP Business One automatically backs up, or archives, the database before any data is removed. If needed, you can restore the backup file, review the database, generate reports, and print documents. The database you restore is in read-only mode, so you cannot change or add any data to it.

  The data removed depends both on the database size and on the preparations done before the data archive wizard run started.
- Load a saved data archive wizard run – if needed, you can check whether a specific document was archived.

> **Caution**
>
> The data archive wizard may require a long time to run to completion, depending on the database size, during which time SAP Business One will not be available for other tasks. The wizard results are irreversible. More information is available in online help and in the how-to guide for data archiving. You can view these document on the SAP Help Portal.

9 Frequently Asked Questions

1. Why is there so much focus on protecting personal data currently?

Answer: High profile new regulations, such as GDPR for the European Union, are increasing legal obligations to protect personal data and introducing strict new penalties. As digitization and big-data affects more and more people, personal data protection is becoming increasingly relevant to everyone. Data breaches affecting companies both large and small are frequently in the news headlines having an impact on reputations and values.

2. Why would you delete data instead of anonymizing the data within the change log?

Answer: Entries with personal data are not dropped. Personal data only in any entry which relates to natural persons (in main object and in the change log) is replaced by an asterisk. The system predefined fields which were determined as personal are fields by which a natural person can be identified. That is why this data should be removed (replacement by asterisk is for indicating that the fields which went through the personal data cleanup).

3. Will turning on the personal data protection functionality require immediate further actions to be performed to continue working with the system (directly after an upgrade) or can a user upgrade and then gradually start defining personal data functionality?

Answer: Turning on the personal data protection functionality (in *Company Details*) doesn't require any immediate further actions. Users can upgrade and then gradually start defining personal data protection functionality.

4. Are all the features you have shown to be compatible with SAP Cloud (CDS) and SAP HANA?

Answer: Yes.

5. You can anonymize data in the system. For companies that want to keep the change log, can you only anonymize data from users that needs to be anonymized?

Answer: Once a natural person requests the removal of their personal data or the purpose for holding this data no longer exists, the data will not be accessible to anyone (not from the main object nor from the related change log).

6. Can attachments be protected, attachments can contain a lot of personal information?

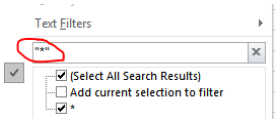
Answer: No, attachments are held externally to SAP Business One so this is not supported currently, protection of attachments must be managed separately. However, the field *Attachment Entry* for various data types in *Personal Data Management* can be managed by personal data protection processes. *Attachment Entry* represents the link held in database tables to reach an attachment, not the attachment itself.

7. For personal data that was erased and is shown as asterisks "*". How will searching for data with asterisks work?

   Answer: There will be no impact on searching. Searching by "*" will retrieve all results, including those cases when the search field includes "*".

8. How does text filtering work for asterisks when exporting employees, business partners, contacts, users to Microsoft Excel?

Answer: Use quotation marks and an asterisk as a workaround.



9. Is it possible to set the natural person checkbox at the same time as when creating a new business partner?

Answer: No. Business partners need to be established first; then natural person determinations can be set via the *Personal Data Management Wizard*, *Natural Person Determination* action.

10. Can you also determine user defined tables (UDTs) and user defined objects (UDOs) as personal data, so that data can be erased when necessary?

Answer: No, this is not supported.

11. Can user defined fields (UDFs) be identified as personal data or sensitive personal data?

Answer: UDFs for personal data objects (objects included in personal data management such as BP master data, employee master data, users, contacts, marketing documents, service documents) can be added to personal data management and determined as personal data or sensitive personal data.

12. Is it possible to add standard fields to the personal data management setup window, or is this only for UDFs?

Answer: No, adding standard system fields is not supported. Only UDFs connected to personal data objects can be managed through the personal data management setup window.

13. BP master data addresses could have UDFs, will these be supported?

Answer: Yes. Adding UDFs is supported for any personal data protection object or sub-object, which is included in personal data management, and for which UDFs can defined.

14. When adding a new UDF to BP master data, do we need to run the personal determination wizard again. for all data?

Answer: If you plan to store personal data in the newly added UDF and you have BPs which were determined as natural persons, or you plan to determine certain BPs as natural persons, then you should add the UDF to personal data management. Only then, when running the personal data report or personal data cleanup, will the new UDF be considered as personal data.

15. How are options relevant for Germany activated, is it by database localization?

Answer: Yes. Sensitive personal employee master data will be automatically encrypted after the employee is determined as a natural person via the wizard action natural person determination. Certain sensitive personal data are only available in the German localization.

16. Certain fields that carry sensitive personal data can only be seen when you have special authorizations. Can different fields be set the same way?

Answer: No. Sensitive personal data is supported for certain special fields only, these fields are categorized in *Personal Data Management*.

17. How does encrypted data appear in marketing documents? Asterisks in card names for example.

Answer: Asterisks replace any personal data in master data and transactions, including card names, addresses and phone numbers.

18. Can a customer or user define their own passphrase for encryption?

Answer: No. Encryption is executed by the system only. Sensitive personal data fields are automatically encrypted when a data subject is determined to be a natural person.

19. What about queries? Is the hiding of personal data only at the user interface (UI) level or is it also applied to user defined queries?

Answer: Regular personal data is not hidden. Only sensitive personal data is hidden. Only certain data are defined as sensitive personal data. These sensitive data fields are encrypted by default and can be viewed in the UI by users who are authorized to view sensitive data. When querying those fields the retrieved value is encrypted. As to DI API access, there is a specially developed DI service which enables the decrypting of data (to read the data or updated the data).

20. Can personal data reports be exported?

Answer: Yes, via the export option.

21. Is there a solution to read encrypted data when using Crystal Reports or a simple SQL query?

Answer: No. Values can be retrieved via the UI or DI only.

22. How are encrypted data retrieved in Crystal Reporting?

Answer: Data cannot be retrieved in Crystal Reports, this is not supported.

23. If the data is under GDPR in SAP, will the encryption restrictions be via the application front end only or applicable via other ways of data consumed, like reporting tools?

Answer: The encrypted fields are accessible via the UI or DI only.

24. Can we check what personal data was extracted through queries?

Answer: No.

25. Will add-ons be impacted by the encryption of sensitive personal data, confession and partner confession in the Germany localization?

Answer: Add-ons provided by SAP will not be affected by the encryption of sensitive personal data. Check with your SAP Partner to see if any add-ons they have supplied will be affected by sensitive personal data encryption. For more information see SAP Note 2633811.

26. Can data that was removed by the wizard action *Personal Data Cleanup* still exist in backups or elsewhere?

Answer: Yes, the wizard action *Personal Data Cleanup* affects the existing SAP Business One database in production only. Your company is responsible for the protection of personal data wherever it exists, so backups or other records need to be managed correctly. Following a wizard *Personal Data Cleanup,* it is recommended to delete any relevant backups and back up again.

27. When running the wizard action *Personal Data Cleanup*, does the system check for open connections to the company database and does it require single user mode?

    Answer: No, single user mode is not required.

28. Can I restrict or authorize the viewing of just personal data so that users can see related information without the personal data?

Answer: No, this is not possible. Authorizations can restrict access to sections of SAP Business One, including the data protection tools. Data ownership can restrict access to certain business partners. Neither authorizations nor data ownership can restrict access to just the personal data of the areas controlled.

29. Is access to personal data recorded?

    Answer: No, only access to sensitive personal data is recorded.

30. Are multi-language translation field contents considered to be personal data?

Answer: When managing translations for a personal data field, the field translations are considered as personal data. As a result, the wizard actions for reporting, cleanup, blocking and unblocking are applied to the translations. When sensitive fields have translations, the field and the related translations are encrypted and accessible to authorized users only.

31. How can I manage my company's personal data retention timelines?

Answer: In step 3, *Selection Criteria*, of the wizard action *Personal Data Cleanup*, you can search for natural persons you want to clean up and erase. Use the *No Transaction Since* field on the Business Partners tab to manage your company's data retention timelines and find inactive business partners; transactions include marketing documents, journal entries and payments (the service module is excluded).

32. How will personal and sensitive personal data be handled in *Quick Copy* (*Administration* → *System Initialization* → *Implementation Center* → *Implementation Tasks* → *Data Management* tab → *Copy Data Between Companies* option) when moving data from one database to another?

    Answer: When creating or updating an object in a target database:

- The *Natural Person* checkbox of any data subjects (employees, BPs, contact persons, users) is automatically not selected, whether *Enable Personal Data Protection Management* is selected, or not selected, in the target database.
- If the source field contains sensitive personal data, the system transfers a dummy data value to the target database. No decryption of the source value takes place, the target value can be overwritten.
- If the source field was included in a *Personal Data Cleanup*, the asterisk is copied to the target field, but the status *Erased* is not transferred.
- The dummy value or asterisk must be a valid value for the target field otherwise the copying fails. For example, asterisks are not valid for the *Confession* field in *Employee Master Data* in the Germany localization of SAP Business One.
- Consider your company's personal data protection policy when transferring personal data.

33. When selecting the wizard actions *Personal Data Report* or *Personal Data Cleanup*, why is the choose from list for the selected data subject empty or certain data subjects are not included?

    Answer: Potentially, no data subjects were determined as natural persons or natural persons exist, but the natural person status has been erased.

34. Why is the *BP* choose-from list empty or some BPs are excluded when selecting *Personal Data Cleanup*?

    Answer: Choose from lists only include natural person business partners for whom no open marketing document exist.

35. Can I duplicate business partners that are determined to be natural persons?

Answer: No. To maintain data and reporting integrity, business partners who are determined as natural persons cannot be duplicated.

36. Why does the *Personal Data Management Wizard* fail to run even though authorizations exist for the wizard actions?

    Answer: Users need authorization to view sensitive data.

37. How can I generate a personal data report or execute cleanup for a natural person with a *Personal Data Protection Status* of *Blocked*?

Answer: The blocked natural person must be unblocked first. When subsequently selecting the actions *Personal Data Report* or *Personal Data Cleanup*, the various *Include Unblocked...* search options like *Include Unblocked Users* or *Include Unblocked Employees* must be selected.

38. Do I have to block a natural person again after unblocking?

Answer: Unblocking should be executed according to legal requirements and based on your legal counsel.

39. How can I manage consent to the storage, use or reporting of personal data in SAP Business One?

    Answer: Consent needs to be acquired and managed outside of SAP Business One.

40. How can I identify transactions that have been through a personal data cleanup?

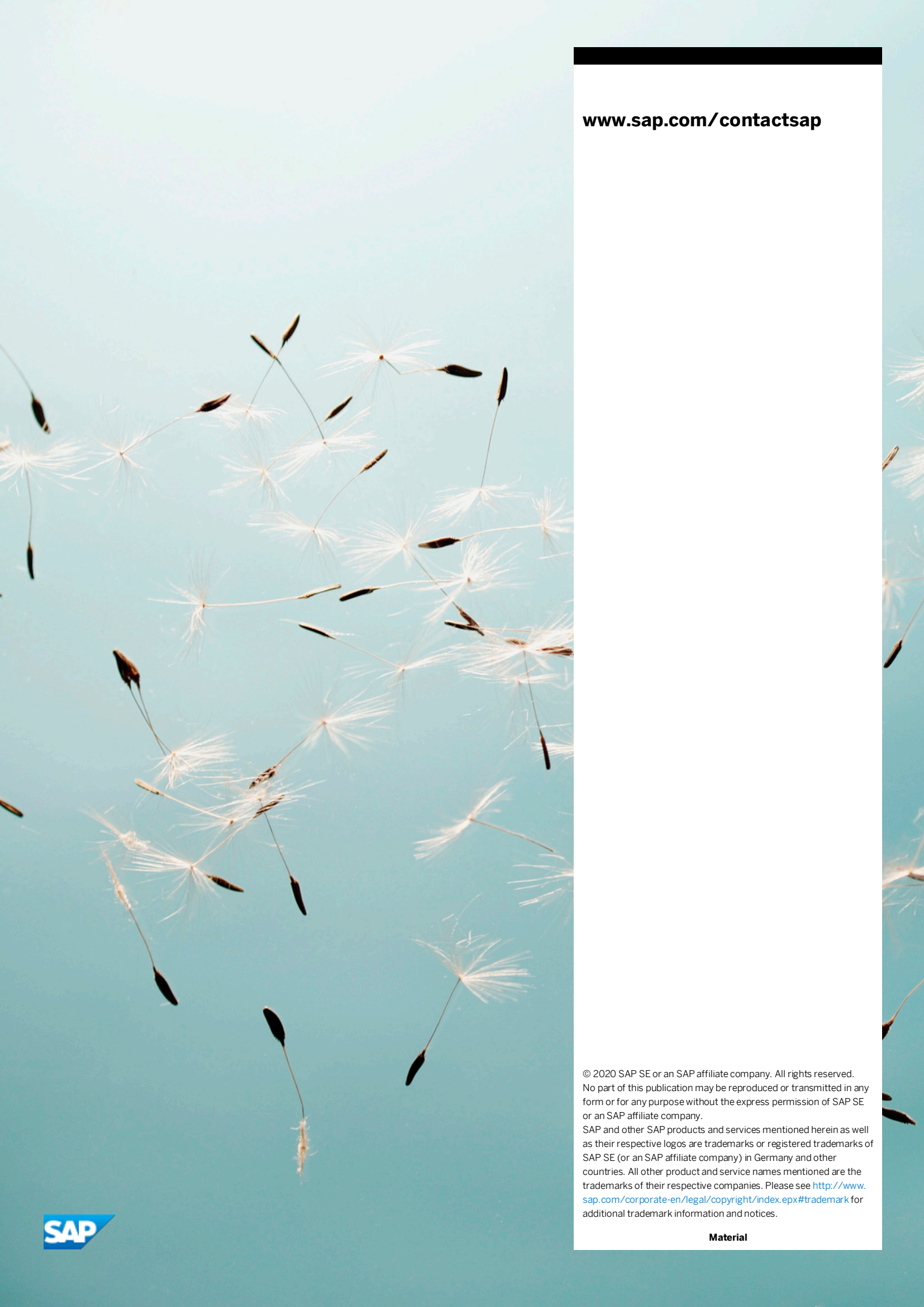
    Answer: Documents can be identified by the internal flag *Data Protection Status*. The default value is "N", once deleted the value is changed to "D".

41. In previous patches of SAP Business One, before the system distinguished between regular business partners and default customers, I was able to block the personal data of a default customer. After moving to the new patch, blocking default customers is no longer supported. How can I unblock the personal data of the default customer?

    Answer: Remove the default customer from *G/L Account Determination*. As the business partner is now a regular business partner, you can unblock the data or apply any action that is supported for regular business partners.

10 Glossary of Terms

Term	Definition
Natural person	A real human being, as distinguished from entities like corporations.
Data subject	An identified or identifiable natural person who is the subject of data held. An identifiable natural person is someone who can be identified, directly or indirectly, 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.
Personal data	Any information relating to an identified or identifiable natural person who is a data subject.
Sensitive personal data	A category of personal data that usually includes the following type of information: Special categories of personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health status, sex life or sexual orientation. Personal data subject to professional secrecy. Personal data relating to criminal or administrative offenses. Personal data concerning financial accounts or insurance policies.
Consent	The action of a data subject confirming that the usage of their personal data shall be allowed for a given purpose.
Deletion	Deletion of personal data so that the data is no longer available.
Purpose	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.



www.sap.com/contactsap

Material