cobra®

Version 2018

DATENSCHUTZ-ready

Manual New Features

September 2018

Materials by Harald Borges.

Table of Contents

System requirements CRM PLUS, CRM PRO, CRM BI 4

This is what you will not find in the current version any longer 6

Specifics of CRM PLUS 7

Installing the System as well as Transferring the Data from the 2017 Version 8

New Functions for your Daily Tasks 10

Individual-related Data – an Overview 10

Defining "Personal Data" 10

How to Configure Handling of Personal Data 11

Setting up the System 12

Setting up a Database for Personal Data 15

Edit Views and Entry Masks 33

Working with Personal Data 42

Enter New Data 42

Processing and Transmitting 47

Copy and Duplicate Data Records 48

Synchronizing Data 49

Data Import 54

Overview, Output and Erasing 54

Traditional Deleting of Data 61

Email blacklist 62

Search for Personal Data 65

Data Protection Officer 66

Notes 66

System requirements CRM PLUS, CRM PRO, CRM BI

Single Workstation Installation	Operating system Windows Vista as of SP 2 (32- or 64-Bit) Windows 7 SP 1 (32- or 64-Bit) Windows 8 (32- or 64-Bit) Windows 8.1 (32- or 64-Bit) Windows 10 (32- or 64-Bit) Free memory recommended 1 GB RAM or more Hard disk space 2 GB
Client-/ Server Installation	Client operating system Windows Vista as of SP 2 (32- or 64-Bit) Windows 7 (32- or 64-Bit) Windows 8 (32- or 64-Bit) Windows 8.1 (32- or 64-Bit) Windows 10 (32- or 64-Bit) Server operating System Windows Server 2000, 2003, 2008 (restricted; server installation only, no client installation possible) Windows Server 2008 R2, 2012, 2016 (server as well as client installation possible) The system requirements of the MS SQL Server Express-Version apply also.

Database	MS SQL Server Express Edition 2008, 2012, 2014, 2016, 2017 MS SQL Server 2014 Express (included) The relevant restrictions of the MS SQL Server (Express) installed apply also. The »Mobile user« feature does not function with the Express Version; it requires a professional MS SQL Server.
E-mail integration	Outlook 2007 or higher (32- or partial 64-Bit) Lotus Notes Version 8.5

This is what you will not find in the current version any longer ...

Please note that as of the 2018 version we regard the Novell Groupwise integration as »deprecated«, i.e., it is supplied with the system, but we explicitly recommend not to use it and also guarantee no support for it. Of course, you are free to continue using this integration system.

We also regard bulk recipients and bulk recipients postal codes as »deprecated«. Of course, you are also free to maintain these fields on your own; however, for future versions we do not plan to supply data tables with bulk recipients and bulk recipients postal code any more.

Specifics of CRM PLUS

This documents presents CRM PRO and CRM BI.

In CRM PLUS the following functions of personal data do *not* exist:

- Automatic erasing of personal data. Any data to be erased must be erased manually in the erase schedule.
- Warning email if erasure was not completed. Such a mail would only make sense if erasing was done automatically and is therefore not included in these two versions of the software.

Installing the System as well as Transferring the Data from the 2017 Version

For details on further options of installing, configuring as well as transferring data please refer to the System Manual and the Installation Instructions available as PDF files.

During a patch installation from 2017 to 2018 the old version will be updated and thus completely overwritten. So it will in no way be possible to return to the 2017 version if you have not carried out a complete backup of the old 2017 version before(!).

This is what you must do to carry out a complete backup:

1. Copy the entire server installation, including all folders and sub-folders, to a safe place.

2. In cobra 2017, use the command »File: Data Backup: Database Backup« to backup your SQL databases.

Patch-Installation to Update from cobra 2017 to cobra 2018

You have downloaded the patch file from our customer portal or received it some other way from cobra or your retailer.

During a patch installation your existing cobra 2017 version will be updated to the 2018 version. All existing paths and settings will be retained. So you cannot specify new paths during a patch installation.

Have your activation data for your cobra 2018 version ready since they will be required while the system is updated.

- Close cobra 2017.
- Close the cobra Appointment Manager.
- Close Outlook.
- Doubleclick the patch file. The patch installation will start. It will automatically detect the existing cobra 2017.
- Follow the Wizard steps.

New Functions for your Daily Tasks

Individual-related Data – an Overview

When working with addresses of any type, individual-related data (IRD) will be generated every day.

The data we are dealing with here are data of natural persons, not of legal entities.

The EU General Data Protection Regulation (EU-GDPR): regulates how to deal with such individual-related data.

»The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data.«[1]

Defining "Personal Data"

For the purposes of this Regulation »personal data« means »any information relating to an identified or identifiable natural person […]; an identifiable

[1] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC*

natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person«.

Among the data mentioned here are, for example:

- name, age, marital status, date of birth
- address, phone number, email address
- account-, credit card number
- vehicle chassis number, license plate number
- personal identification number, social security number
- criminal record
- genetic data and medical records
- value judgments, for example, reports

How to Configure Handling of Personal Data

Prerequisite for a user being allowed to not only view, but also handle personal data, are the relevant authorizations and setting. These are system- or database specific. System authorizations apply to the *entire* cobra system, database settings only to that database open at this point.

Setting up the System

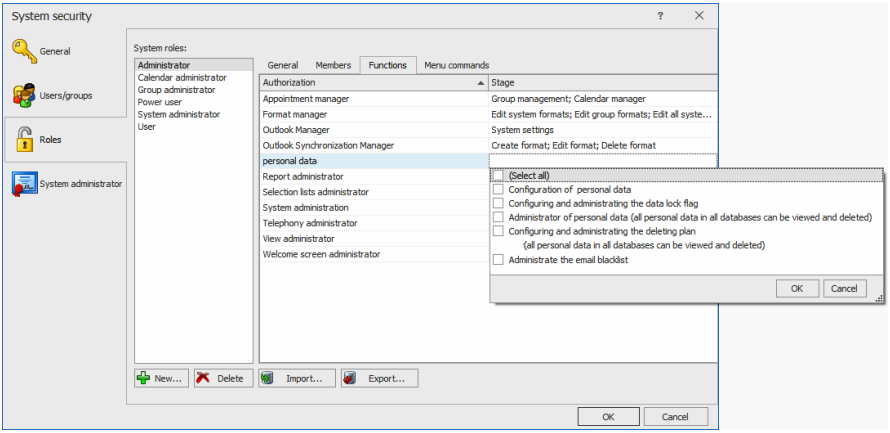
System settings are always effective when working with cobra, that is, independent of which database might be open at this point. In addition, you can also assign authorizations for databases.

The aim of system authorizations is to make the functions described here available to only a few, specialized employees of a company. They are to ensure that only specially trained persons, such as data protection officers, may access some of these functions.

- Issue the command »File: System settings: System settings«.
- Switch to the »User administration« tab.
- Click the »System security« tab.

Here, you can assign specific authorizations at »Roles«. Every user who has a specific role is assigned the authorizations associated with the role. If a user has several roles, the authorizations of all these roles will be accumulated.

- Click a role.
- At »Functions« you will find the settings for personal data.



Configuration of personal data
: This is the authorization to configure settings for personal data. Using this, you can configure handling personal data at »File: Database«.

Configuring and administrating the data blacklist
: This is the authorization to edit the list of such data that may not be created or imported again.

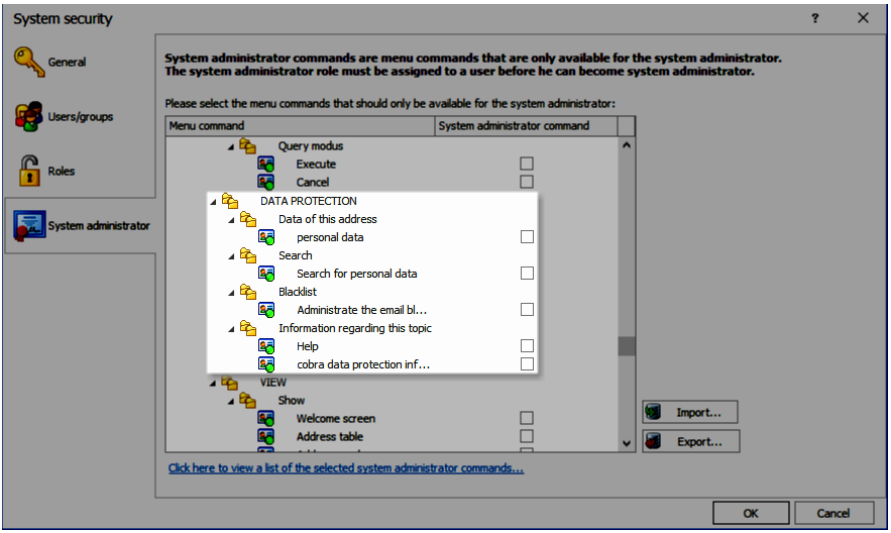
Administrator of personal data
: Persons with this authorization may view, edit and erase all personal data contained in the database. All persons responsible for deleting personal data in accordance with legal stipulations require this authorization.

Configuring and administering the deleting plan
: Persons with this authorization may set up automatic deleting of personal data and edit erase jobs.

Managing the email blacklist
: Persons with this authorization may create, erase and modify the list of email addresses that may not be contacted.

As an alternative, you could also declare commands to be system administrator commands that may only be issued by system administrators.

Switch to the »System administrator« tab.



Here you can declare certain ribbon commands to be system administrator commands. Such commands will then be hidden for all users who do not have the system administrator role. They will only be available for system administrators.

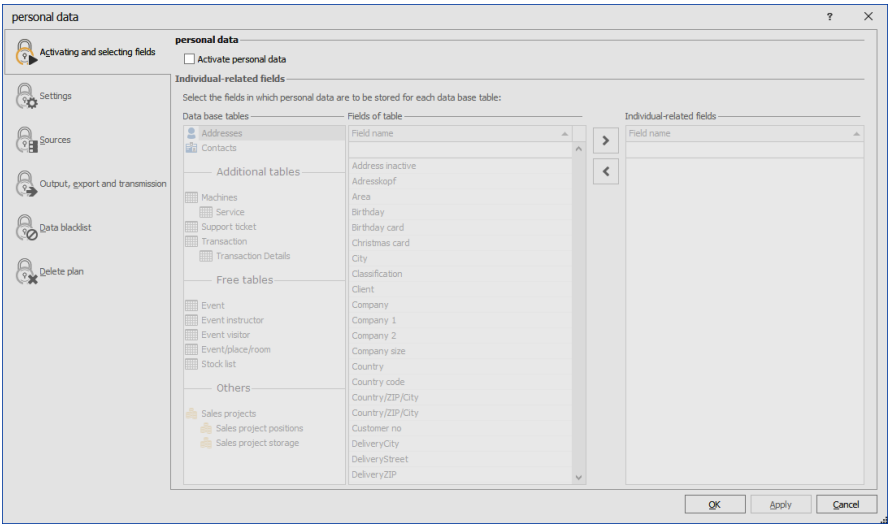
Setting up a Database for Personal Data

There is *no* field type »Personal data« of its own in the database. In fact, in the database configuration you can specify which of the fields of your database are to contain personal data.

In the database structure, you can assign a field the property »Individual-related field (build hierarchy)« (in previous versions, this field was named »Personal field«). This property has nothing to do with the personal data described in this document, but is solely intended to set up address hierarchies. For example, a name field can have both properties and contain personal data for data protection as well as be a personal field for setting up hierarchies.

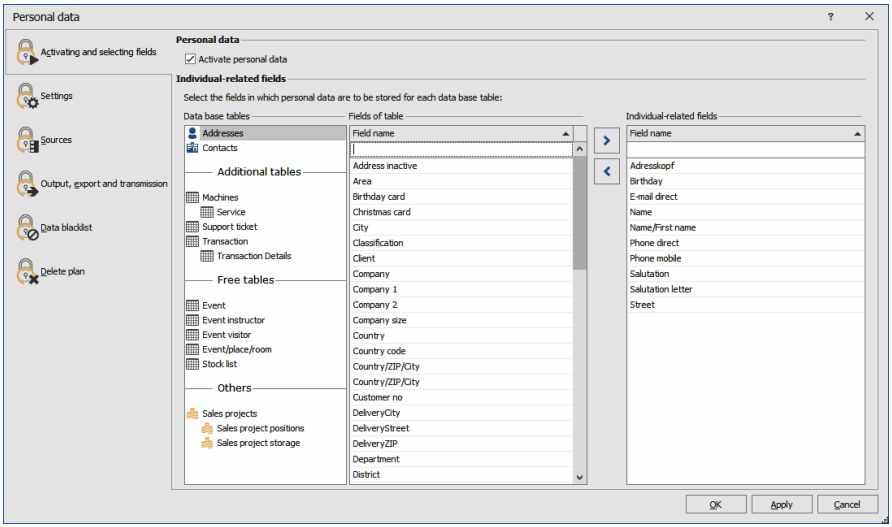
Activating and Selecting a Field

In order to realize the legal right of access, it is essential to identify which fields contain personal data. The standard functions of cobra CRM are not affected here, they apply even if the data protection functions have been disabled. However, managing personal data in accordance with data protection aspects is only possible if they are labeled as such. Here you can label the fields accordingly.



- You activate working with personal data by clicking the option »Activate personal data« right at the top.
- You can switch personal data on and off at any time.
- If you disable working with personal data again by switching off this option, all fields or data tables that you create in the next steps using the configuring function here will be preserved. Reactivating the functions might require repeating sub-steps of the initialization (e.g., if required fields have already been erased from the database structure).

When personal data fields are erased, Yes/No-fields are set to »No«. So consider carefully whether you really want to save personal data in Yes/No-fields.

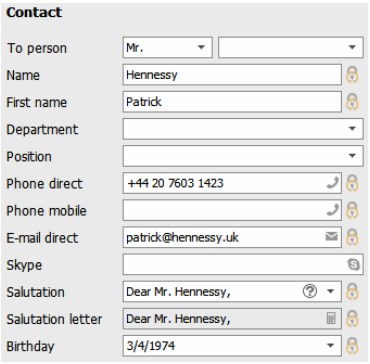


At the left you see the data tables of the database. Generally, personal data might be stored in any of the tables of the database.

At »Fields of table« you can find the data fields existing in the data table concerned. Click a field with personal data and take it over to right into the column for personal data. These fields are now marked as fields with contents worth protection. Only such fields will appear in log files, deleting plans etc.

As rule of thumb it might be assumed that most or all of those data contained in the »Contact« area in the demo provided contain personal data. In addition, especially for single addresses other fields might also contain data covered by the EU-GDPR.

Personal data might also be contained in other data tables than only in the address table.



In the entry masks, fields marked as personal data will be labeled by a small lock icon 🔒.

Personal data

- can be queried at field level,
- will, when edited, be logged by a specific log independent of the modification, covering all changed made,
- can be erased according to schedule,
- can object of a specific report created by a dialog of their own.

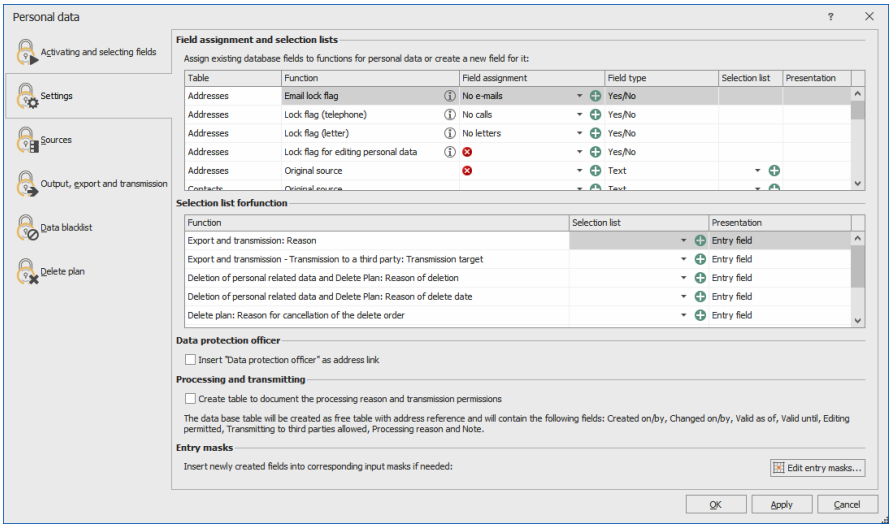
Configuration

Field Assignment and Selection Lists

There are several functions relating to data protection. Some of these functions, such as lock flags for emails, have already existed in earlier versions of cobra.

Using the field assignment function, you can specify which fields are to have which functions. All field functions labeled with a red cross are obligatory.

Fields derived from e.g. the messaging system and the campaign management will not be offered in the field assignment feature.



- In the selection list »Field assignment«, select the field for the function you require. If it does not exist yet, you can create it using the green cross.

cobra users can modify the data structure at will and create new data fields and data tables. Per data table in which at least one field was selected as personal data field, a source field must be specified indicating where the information comes from. Due to the right of access of data subjects, it is required to create log files naming the data source.

You can enter the field with the data source in a suitable entry mask, otherwise the software will request the data source.

- Any field assignments marked with a red icon are obligatory, so you must specify a suitable field of the field type required.

- You can select a field already existing in the database. If there is no such field, click the green icon at the right. Now you can create the field directly in the database structure.

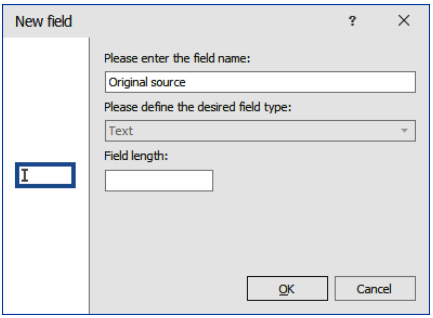


Table ..... The data tables of the database will be listed at the left.

Function ..... There are certain function fields for personal data. Every function requires a specific type of field. In the selection list »Field assignment« you will always be offered only such fields that have the correct type of field.

[Email etc.] lock flag

Lock flags are Yes/No fields which were assigned the relevant field option »Lock flag« by the database structure. If such fields already exist in your database, they will have been preconfigured and will be shown here. If there are no such fields, you can create them here.

Lock flag for editing personal data

To save the personal data stored in a data record from being processed any further, a special lock flag can be attached. This lock flag will also affect contacts, additional- and sub-data of the address, there being some exceptions though. The lock flag will warn any user trying to edit or change personal data. It is intended to sensitize the user to handle these data very conscientiously and not carelessly enrich or alter them. There are several reasons for setting such a lock flag: it can thus be ensured, that a correction of their data requested by data subjects cannot be cancelled. It can thus also be ensured that data scheduled for deleting that should

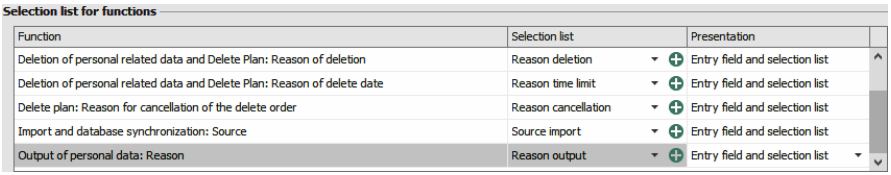
only be erased at a later date due to e.g. legal obligation to retain data, are not modified before.

Source of the original data record
: Enter here in which field you will manage the source of the personal data for each data table.

Selection lists for functions

For certain procedures you must specify certain details, such as the reason for deleting. These functions are hardcoded in the software and, in part, required due to legal provisions.

Here you specify in which selection list you will manage the entries for the relevant field. Using the green icon you can create a new selection list.



By default, in cobra you can enter field contents into selection list entries. However, in this case you may not do so. Selection list entries with field contents will not be shown when working with personal data.

Data Protection Officer

Data protection officer
: Every company must name a data protection officer responsible for complying with the EU-GDPR. You can create a suitable address link indicating the data protection officer of a company (such as: "*John Doe* is data protection officer of *ACME Corporation*").

Processing and Transmitting

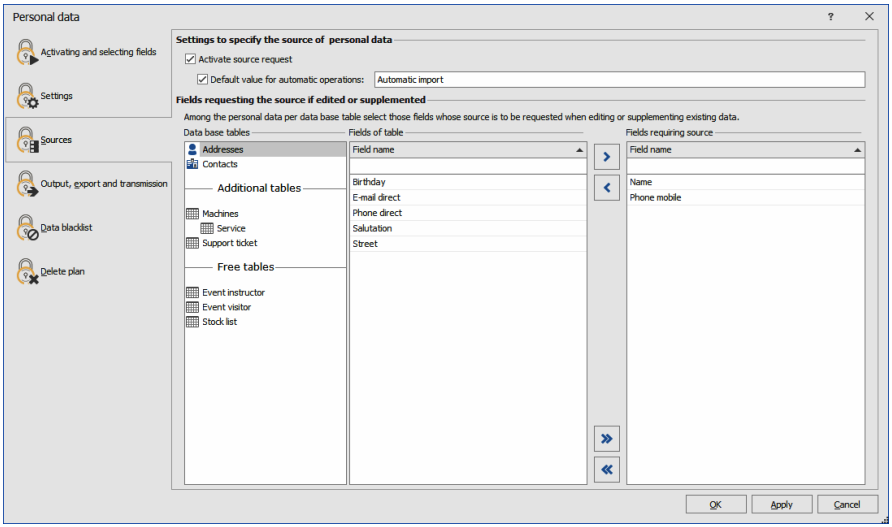
Processing and Transmitting

Here you automatically create a free table in the database structure. It contains the period of validity and information about the explicit permission to process and store personal data. This is useful for all further proceedings such as providing information about, Transmitting or deleting personal data. If this area of the dialog is not active, it means that this table has been created at an earlier date and already exists.

List of Sources

Be sure to specify the sources of an address, such as »Address purchasing«, »Fair contact«, »Telephone canvassing«, »Customer call« etc. Naming one or more sources is necessary due to the right of access of a natural person.

At table level you can store the source of an entire data record. However, if the source of specific fields deviates from the data record source, this must also be stored in order to be able to name the correct source. For example, it can thus be indicated that mere address data come from address purchasing, while other personal data were derived from e.g. an interview with the customer.



Activate source request

Set this option to On in order to ask for the source. When an address is then created, the source will be requested. Requesting the address is done per data record. Should you also want to have such a request for a field, you can configure that in the lower part of the dialog.

Default value for automatic operations

If you import addresses or carry out some other automatic procedure, you can specify a default value here that will then be entered as source of these addresses. This option ensures that the source field will not remain empty. If required, you can search for the contents of these fields later and replace them.

Fields requiring the source [...]

This function is important to meet legal requirements. If you select fields here, their data sources will be requested not only when data are created, but also whenever they are modified or enriched. You will be offered all fields that you have marked as personal data fields. Form these, select a

subgroup of fields where you want to activate querying the source whenever they are modified and/or enriched. We recommend to select all personal fields. Comment fields might be exceptions here.

Modifications of personal data are logged per field. The original source will be stored in the data record. Any later modifications will be documented in the log. Not the subject of the modification will be stored, but only the fact that there was a modification.

Outputting, Exporting and Transmitting

Here you specify how personal data are to be put out and exported. This will affect, e.g., the functions to be found in the »Output« tab of the ribbon.

In cobra CRM, personal data can be exported and forwarded in a variety of ways . From a legal point of view, it is required to disclose to data subjects to whom personal data were passed on if they exercise their right.

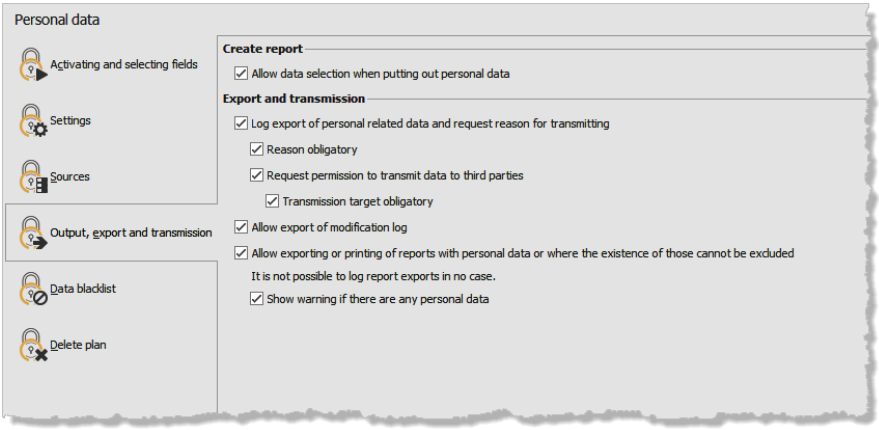
However, that does e.g. not apply if data are forwarded within the same company.

cobra CRM can only log what happens within cobra CRM or was initialized by cobra CRM. For example, it can be logged that personal data were sent by mail to an address XY if that address exists in cobra.

But it is not, for example, possible to log the address forwarded to if personal data were transferred to Outlook for mailing and then recipient addresses are entered manually in Outlook.

Of course, cobra cannot log after an export whether exported data were forwarded, since cobra is no longer responsible for the exported data.

The functions offered here serve to document such forwarding manually. This is why the user is asked whether personal data are to be forwarded and to whom and what the reason is.



Output

Allow data selection [...]

If you activate this option, you can specify exactly which data are to be put out when personal data are put out. If you do not check the option here, all data will be put out automatically.

Export and Disclosure

For each export (except the exports of reports and the modification log) the user can be asked to give the reason for exporting - and this reason will be recorded. The user can also be asked whether the exported data are to be disclosed and to whom. There is a special view showing disclosure of the export, it can be put out as PDF or CSV file.

Export and Transmission

Users will be asked about the reason why they are exporting personal data. There are many possible reasons, for example exporting addresses for a serial letter or forwarding to a third party.

Reason obligatory

If you activate this option, entering the rea-

son for exporting becomes obligatory. This means that exporting can only be completed if the user has entered a reason.

Request permission to transmit data to third parties
: It will be asked whether the data may be disclosed.

Transmission target obligatory
: If the data are to be transferred later, entering the target can be made obligatory. This means that exporting can only be completed if the user has entered a reason.

Allow export of the modification log
: The modification log can be exported and put out. This export will not be recorded.

Allow exporting or printing of reports [...]
: If you activate exporting and printing of reports, you are doing so at your own risk.

Exporting personal data in reports will not be recorded.

Show warning [...]
: Since it cannot be excluded that a report might also contain personal data, a warning can be shown while exporting data and creating a report.

Data Blacklist

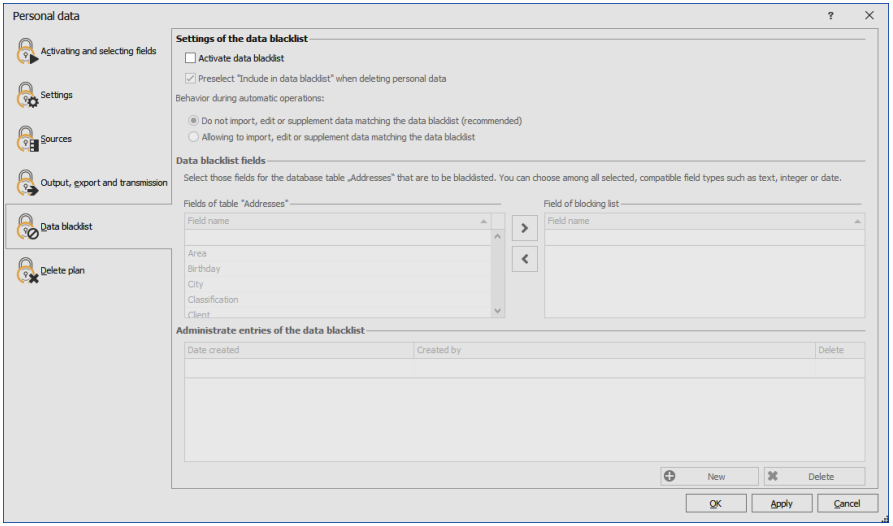
This list will document which data may not be added to the system (again). If the data have been erased once, it will thus be prevented that the same data are entered or imported again later. When trying to import or create again a locked data record, users will be warned.

Addresses may
- either be entered manually in this list
- or be entered automatically into the blacklist when entire addresses are erased or individual personal data field contents are added to the blacklist.

It can thus be prevented that addresses are imported to cobra or created there again manually.

If importing is done automatically, it is predefined how addresses are to be handled that have been added to the blacklist.

This blacklist will only supervise data in the »Addresses« data tables, not in other data tables.



Settings

Activate data blacklist
: Here you activate the blacklist.

Preselect “Include in data blacklist” […]
: Activating this option will lead to the function of adding erased data to the blacklist being offered automatically as default setting.

Behavior during automatic operations
: If you have data imported automatically, e.g. via the Automation Server, you can prevent importing of data records listed in the blacklist. However, this option will not be effective if you synchronize databases or mobile users.

Fields of the data blacklist

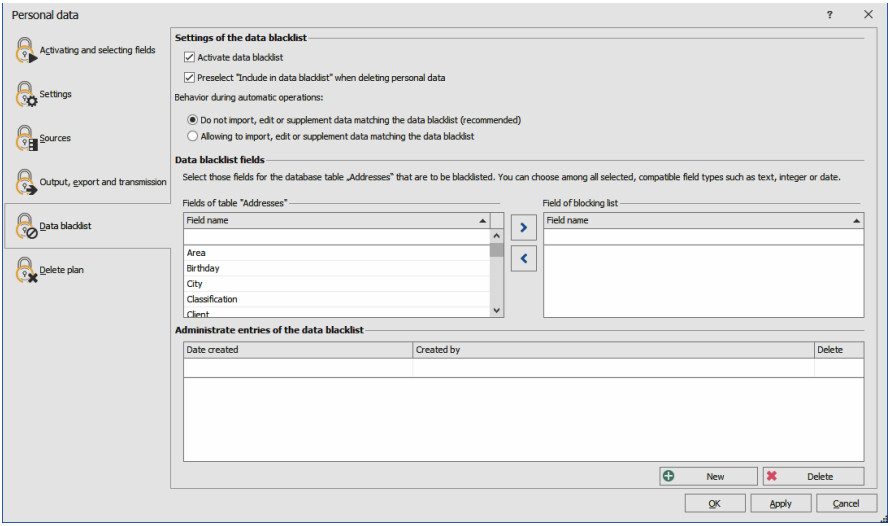
In order to lock data they must be uniquely identifiable. To do so, you can select fields from the address table whose content will be checked by cobra. These fields are assigned an AND link and will be checked whenever an address is created or imported as well as whenever an address is modified. It is thus determined whether the data in all these fields match. Here you select which fields are to be added to the data blacklist.

If you should add additional fields to the data blacklist later, you must complete any entries existing already.

Should you later remove fields from the data blacklist, the blacklist data will also be erased permanently.

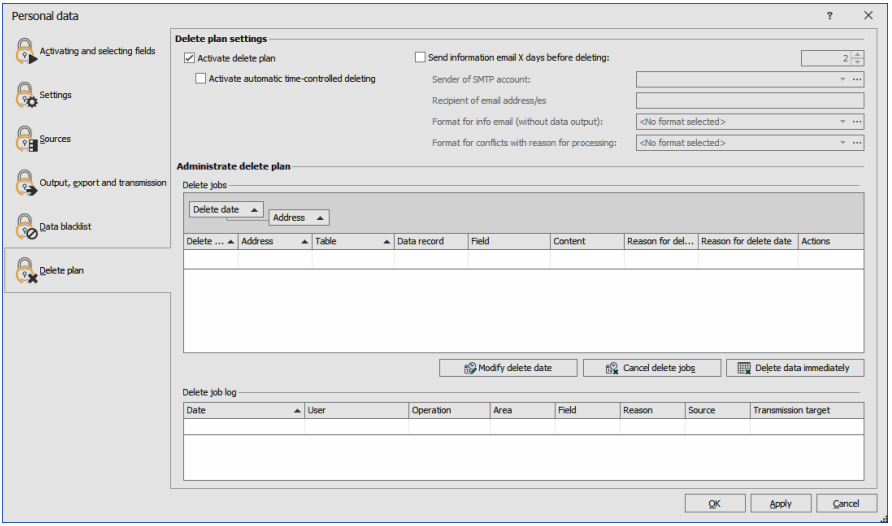
Managing data blacklist entries

In this dialog you can manually add data records to the blacklist. Click the »New « button. Enter the data to be locked.



Delete plan

Time-controlled erasure of personal data is done according to an erase schedule. The plan documents future as well as already overdue erasures. Any modifications of the erase schedule are recorded.



Activate delete plan
: Here you activate the deleting plan.

Activate automatic time-controlled deleting (CRM PRO and CRM BI)
: Should you select this option, the data will be erased automatically when their period of validity has expired.

Send information email [...]
: Specify here how many days before deleting an email is to be sent. In this email (e.g. to the data protection officer) you can inform about the erasure.

SMTP account ... Automatic email transmission is done via an SMTP account. Select that account here or create it. This account must be in the »System« area and not in a user or group area.

Recipients ..... Enter the email addresses of the addressees in the mail. Separate multiple addresses by a semicolon.

Format for info email
Enter here the content of the mail informing about the scheduled erasure.

Format for conflicts [...]
It is possible that the date specified in the data table »Processing and disclosure« in the »Valid until« field is later than the erase date planned in the erase schedule. This means that there is a conflict that can be reported by mail. Specify here the format of the email reporting the conflict.

Managing the erase schedule

In this area you manage erase tasks. Personal data are to be erased if there is no purpose or legal obligation to retain them. If erasure is overdue, they are highlighted in color.

Whenever cobra is started or the erase schedule activated, it is checked whether there are data to be erased. ,

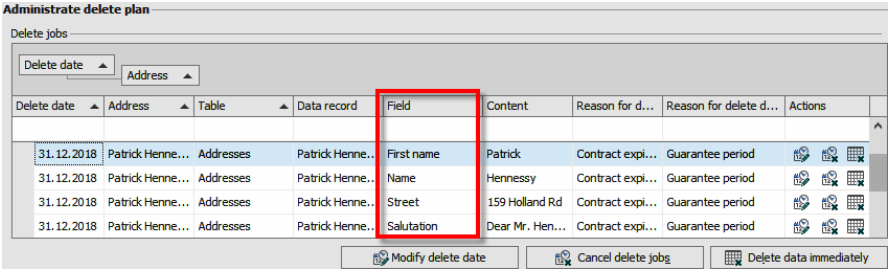
- If that is the case and automatic erasing has been activated, the data are erased if they do not have a purpose any longer. If data are not erased automatically due to their purpose, they are highlighted in color. After the purpose has expired, data are erased automatically then.

- If automatic erasure has not been activated, any erasures falling due are highlighted in color.

Actions

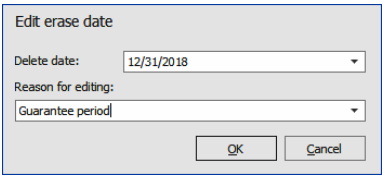
- Mark one or more erase tasks in the erase schedule to be able to execute further actions in the erase schedule.

Erase tasks always relate to only one field of a data record. This is shown in the »Field« column.



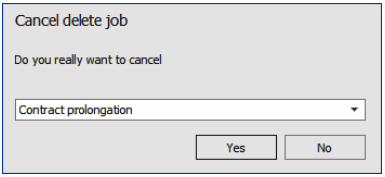
Modify delete date

Using this function, you can set a different erase date. Click this button to edit the highlighted erase tasks. Enter the new erase date and state why the date has been modified.



Cancel delete jobs

Using this function you cancel the erase task for a field. You can thus undo an erase task, e.g., if a customer prolongs an expiring contract indefinitely. Mark the relevant task or tasks and click this button. Enter a reason for canceling erasure.

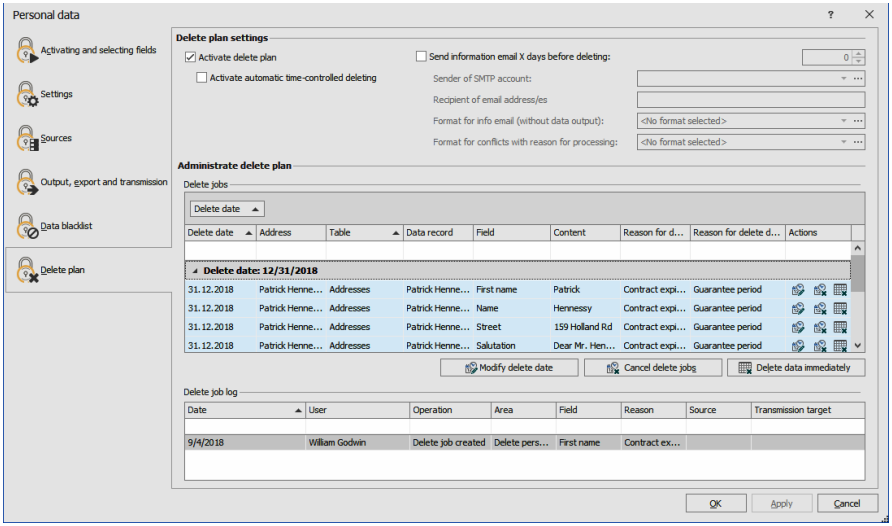


Delete data immediately

Clicking this button will erase the data highlighted immediately.

Delete job log ... If you click a task in the erase schedule, you can view the report to see how this task was modified. The report is

stored separately and linked to the data record. Thus it will be retained even after the erase schedules have been executed and can be viewed somewhere else.



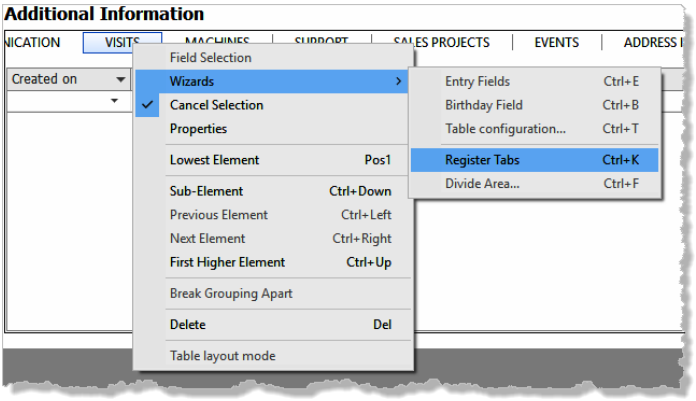
Edit Views and Entry Masks

Table and Entry Mask for Processing and Forwarding Data (CRM PLUS, CRM PRO, CRM BI)

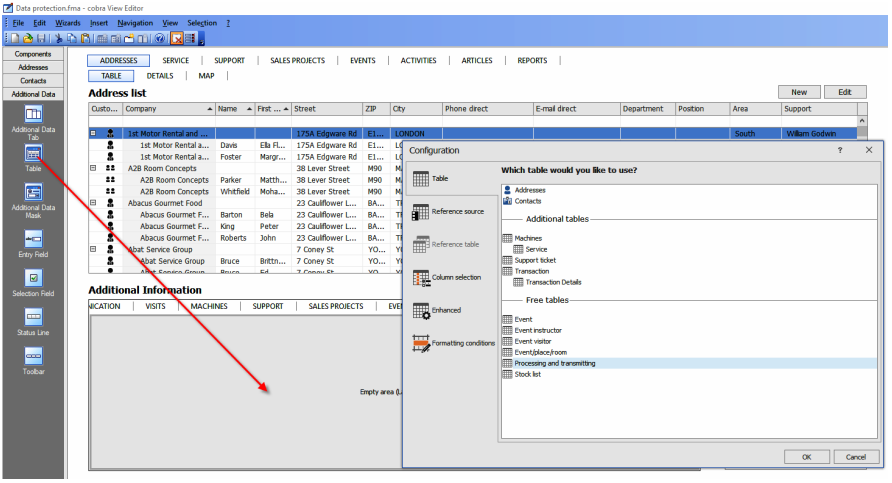
In order to be able to work constructively with the free table »Processing and forwarding«, it is recommended to integrate it in a view and, in addition, specify an entry mask for recording data.

1. Step

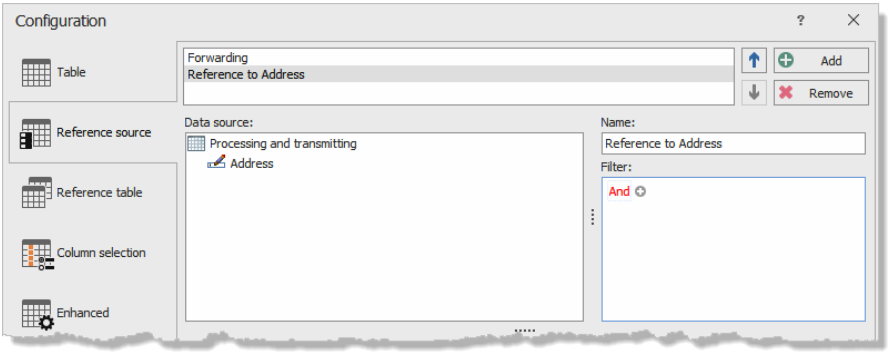
- Use the command »File: View: Edit view.« to access the view editor.
- In the table, click under the address list.
- From the context menu, issue the command »Wizards: Register Tabs«.



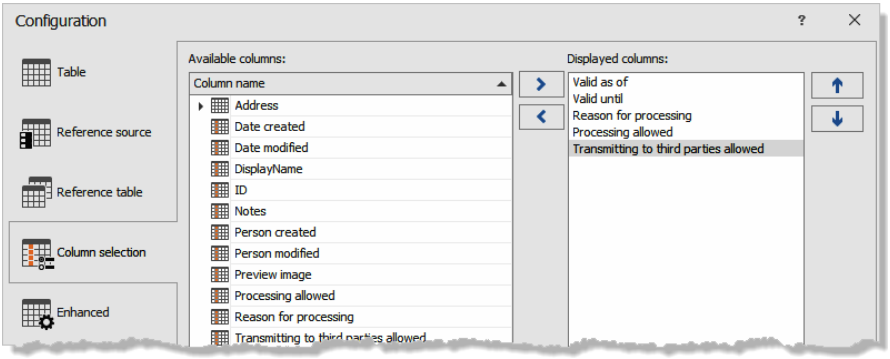
- Create a new tab. Assign a name to it, such as »Processing and forwarding«.
- Drag an additional data table into the empty tab area.



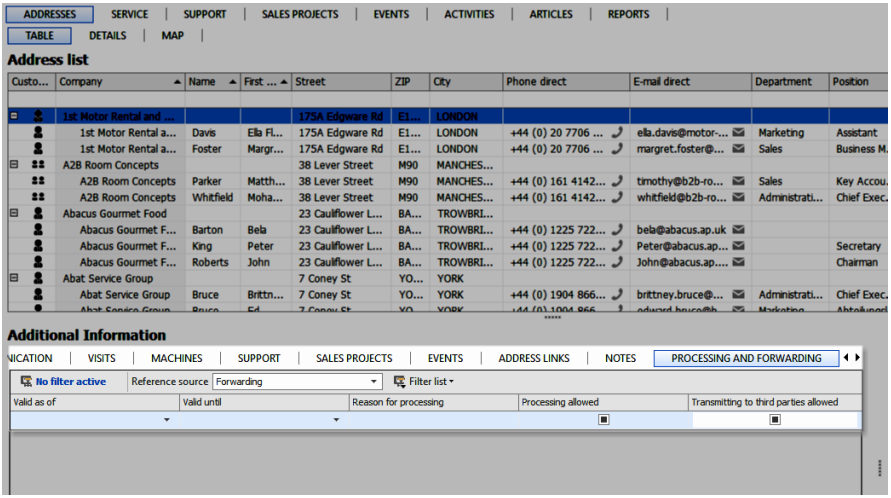
- Configure the table.



- Specify which columns are to be displayed in the table.



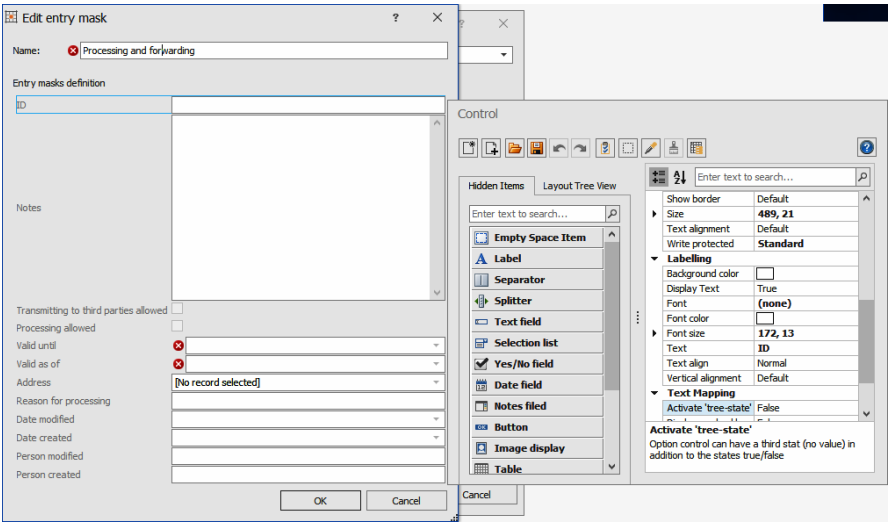
You have thus created an additional tab containing information on handling personal data in the area below the address table.



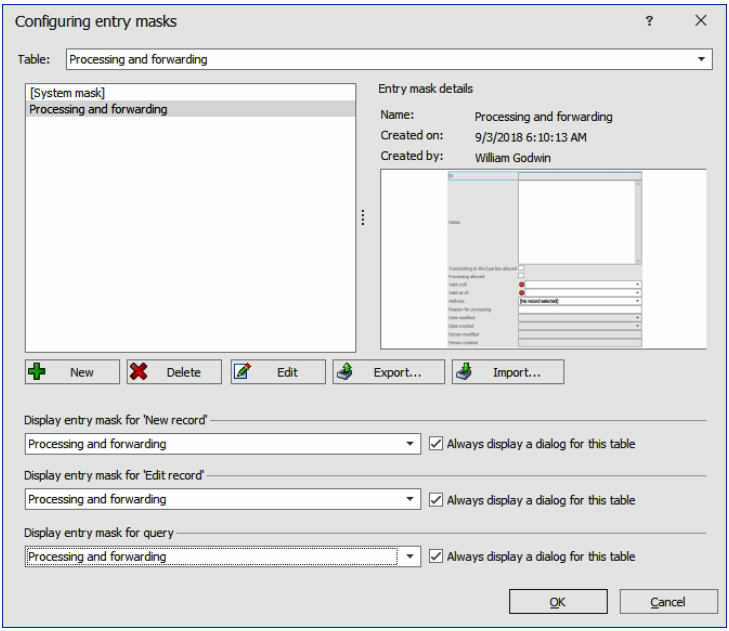
2. Step

In this step you create an entry mask for entering details.

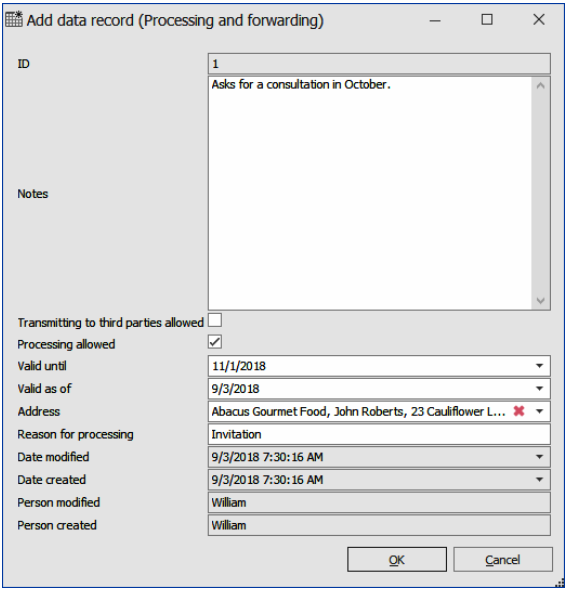
- Issue the command »File: View: Edit entry mask«.
- Select the table »Processing and forwarding«.
- Click the »New« button.
- The system will automatically suggest an entry mask already containing all the fields of the table. You can now move and edit fields and drag them back from the entry mask to the control elements. But you are also free to take over the entry mask as shown.



- Confirm with »OK«.
- You can access this entry mask as a dialog. Configure that in the lower part of this dialog.


Configuring entry masks
Table:
Processing and forwarding
[System mask]
Processing and forwarding
Entry mask details
Name:
Processing and forwarding
Created on:
9/3/2018 6:10:13 AM
Created by:
William Godwin
New
Delete
Edit
Export...
Import...
Display entry mask for 'New record'
Processing and forwarding
Always display a dialog for this table
Display entry mask for 'Edit record'
Processing and forwarding
Always display a dialog for this table
Display entry mask for query
Processing and forwarding
Always display a dialog for this table
OK
Cancel

When entering and editing data, a suitable dialog will open from the new register tab in future.



Lock flags

The lock flags you set in the »Configuration« tab are important for working with personal data. They can be integrated into an entry mask for the users. In this example that is done in the entry mask for creating and editing addresses.

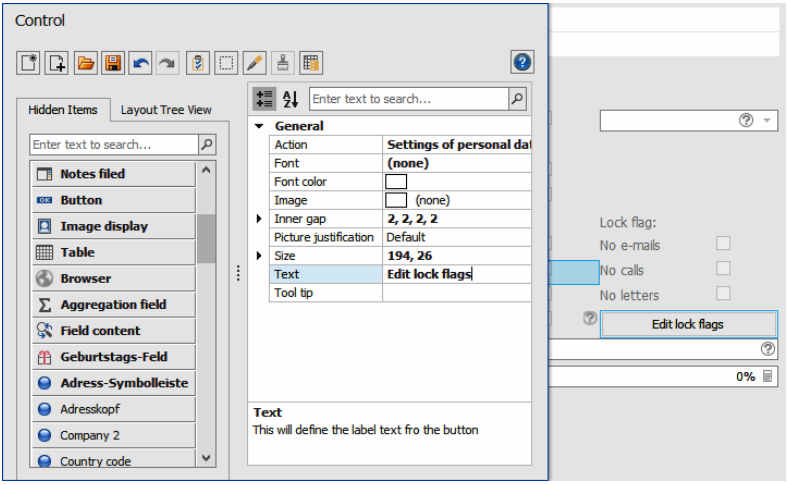
Lock flags always belong to an address, whereas the button to handle lock flags can be integrated not only in address-, but also contact entry masks.

You can

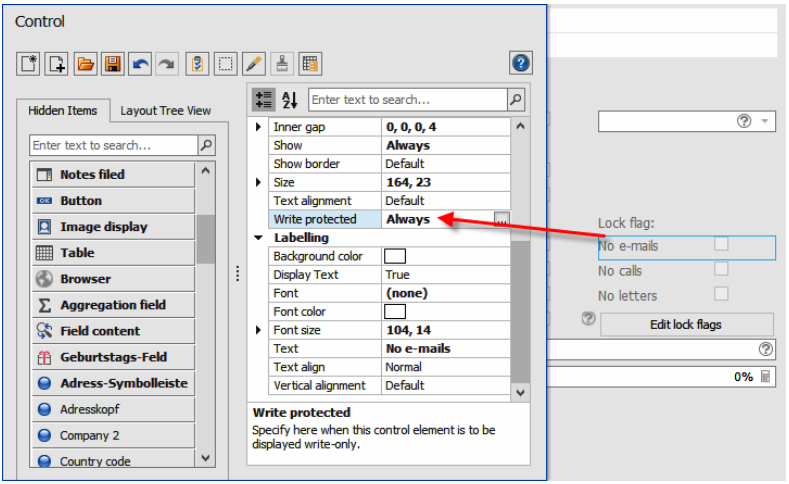
- either display them as Yes/No fields directly in the address entry mask
- or access them via a button in the address or contact entry mask as a dialog. Accessing them via a dialog has the advantage that any modifications of the lock flags will be recorded here.

You can combine both and make the entry fields in the entry mask write-protect, as we have done in our demo view. Then you can modify the lock flags in the dialog, and any settings configured there will be displayed directly in the entry mask.

- Issue the command »File: View: Edit entry mask«.
- Select the address table and the relevant mask.
- Drag an empty button into the entry mask.
- As caption, enter »Edit lock flags«.
- Click the »Action« button.

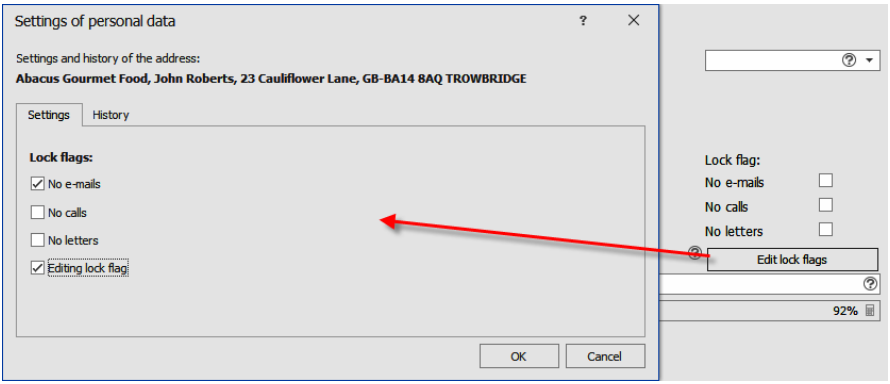


- At »Further commands« select »Settings of personal data«. Confirm with »OK«.
- Now mark a lock flag in the entry mask. Activate the write protect function.



- Repeat the procedure for the other lock flags.
- Close the entry mask editor.

In the entry mask itself there now is a suitable button accessing a dialog.



In this dialog you activate the lock flags required. You can also view a history there. All modifications of lock flags will be recorded here.

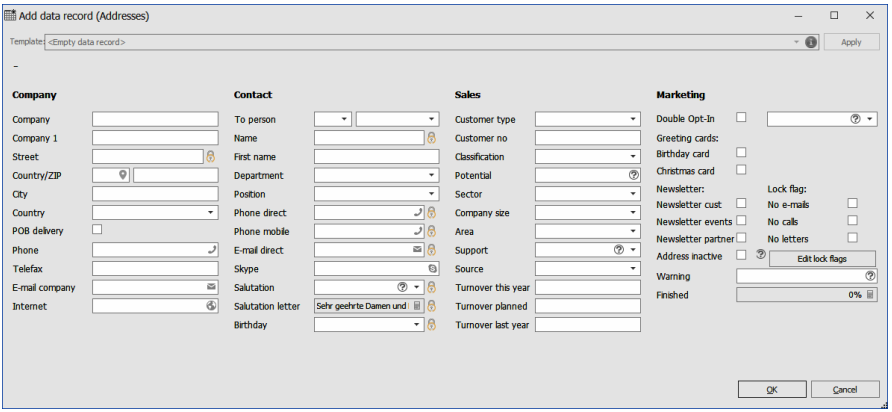
Working with Personal Data

In the following examples we will assume that you have already configured the database for personal data.

Depending on the configuration of your system it might be that some of the input and output functions will not be available and you cannot view specific dialogs.

Enter New Data

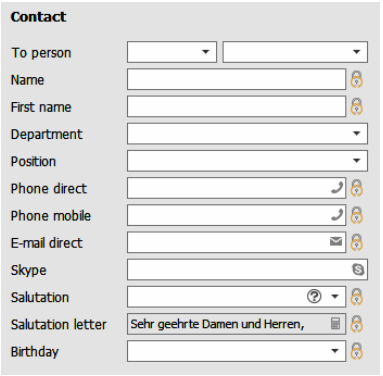
Issue the command to create new data, such as a new address.



You can identify the fields for personal data by the padlock icon .

At the right-hand side you see an area for lock flags.

Complete the dialog as usual.



Lock flags

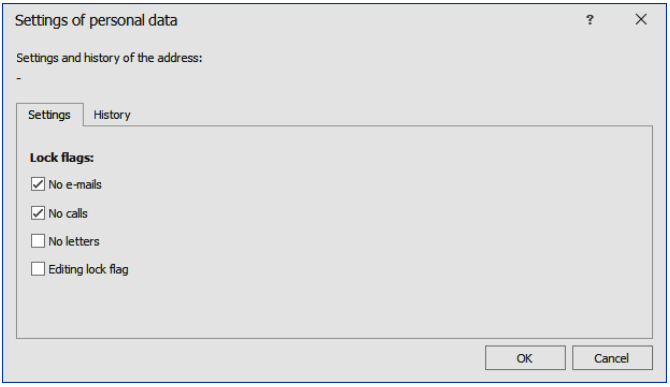
Lock flags control creating and editing data as well as communication with users. They will not suppress such actions, but will ensure that the user concerned is warned by the system that he is working with personal data. So if, e.g., customers do not wish to be called or receive emails, this is where to enter it. A lock flag affects all email addresses, telephone numbers etc. of the data record concerned.

The email blacklist works differently. Any email address entered there is blocked for all data records in which it appears.

This could, e.g., be important if a customer cancels a contract and forbids any further contact, but you must retain the customer data for any further warranty claims for a certain period of time.

- Click the »Edit lock flags« button.

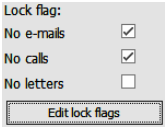
A dialog will open.



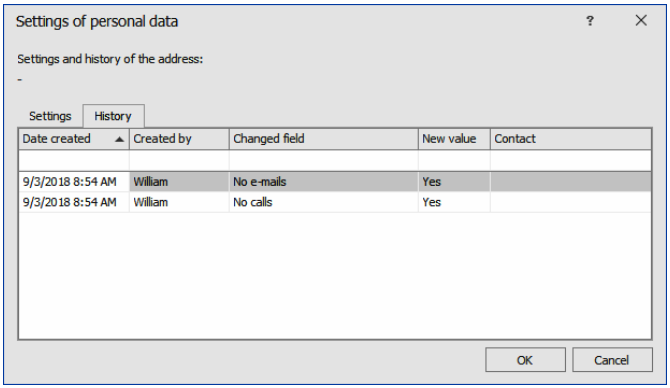
Here you can mark the lock flags you want.

Here you can also set an »Editing lock flag« for modifying personal data. This lock flag will warn about any modifications of personal data within the data record concerned.

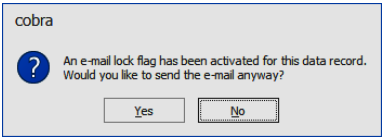
The figure shows lock flags also displayed directly in the dialog for editing addresses.



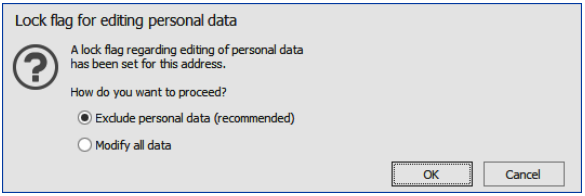
In the lock flags dialog there is also a »History« tab. .Here it is recorded which user has modified the settings for lock flags and when.



A lock flag will not completely prevent approaching a contact or modifying data. It will rather issue a warning whenever someone is on the verge of doing so.

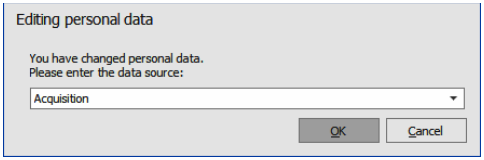


This can also happen when personal data are modified.



If you exclude personal data, modifications of data that are not personal will be stored.

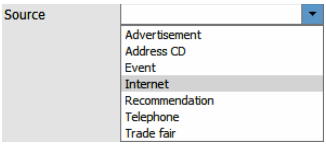
If you decide to modify personal data, you will be asked about the source of the data.



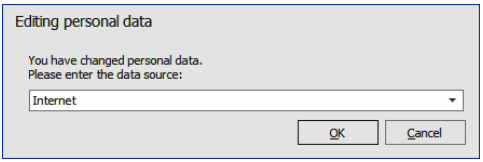
The data source will be recorded.

Data source

If there is a field for selecting or entering a data source in the entry mask, you can specify there where the data entered come from.



When the data record is closed and stored, the system will automatically check whether a data source was named. If not, you will asked to enter the source.



An example:

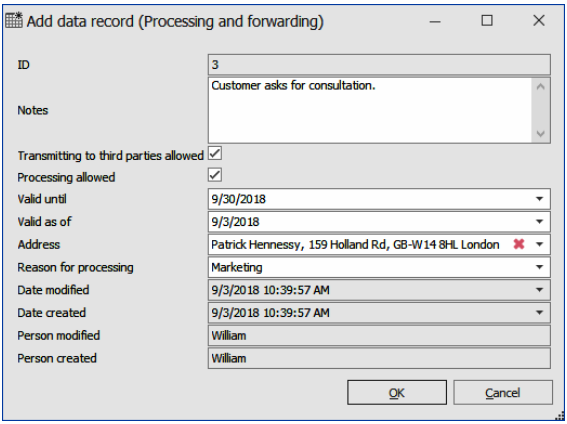
When you enter an address, in the field »Source« you enter the source of the personal data in the address. This source is valid for the entire data record with all the details available at this point. The source - also termed »original source« - will 1. be stored in the database field »Source« and 2. documented in the record.

Should you later modify the personal data contained in the address or enrich them with additional data, you must specify where this new detail comes from. To make sure that is done, the source is always requested when saving the modifications. This source is documented for every single field in the record. Only the last source will always be documented, previous source data of this field will be overwritten. If field contents are erased, the source data will also be erased.

Processing and Transmitting

In the table »Processing and transmitting« you specify for how long the personal data of an address are to be valid and what may be done with these data.

- Right-click the table and from the context menu issue the command »New«.



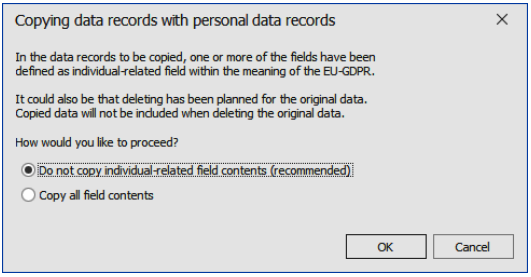
- Enter a processing purpose.
- If the data subject concerned allows processing and transmitting of his or her data, click the relevant options. This is merely informative. Transmitting and processing of data will work nonetheless.
- Validity specifies for how long the personal data of the address may be processed or transmitted.
- These details will be recorded in this table so that you can comply with your obligation to communicate.
- Here you can enter any amount of purposes with varying validities. Example: If a customer has several contracts with you, enter here the purpose and validity of each of these contracts.

- As long as no valid purpose has been entered, personal data of this data record will not be erased automatically. After the validity of the latest purpose has expired, data will be erased automatically.
- Processing purposes are valid for an entire address and its data such as additional and contact data. They cannot be assigned to single fields.

Copy and Duplicate Data Records

When you copy or duplicate data records containing personal data, you will be warned.

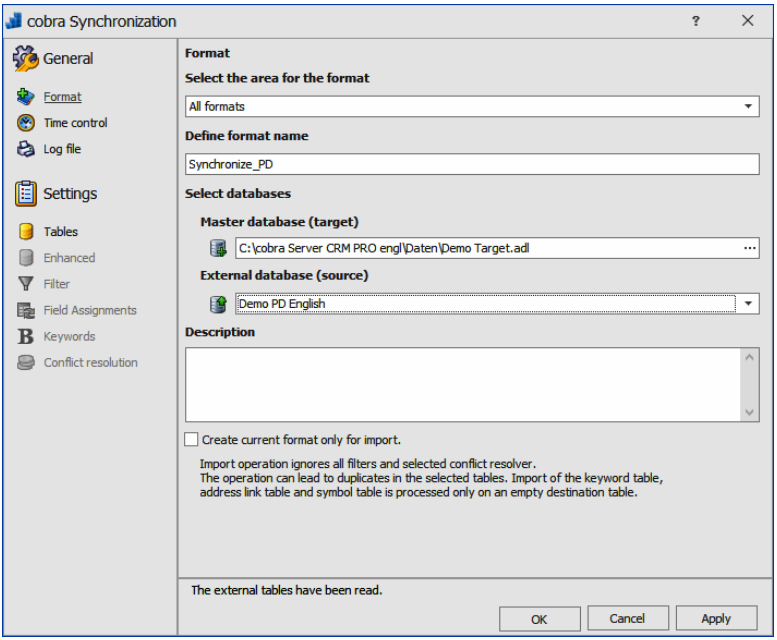
Personal data in data records that have been copied or duplicated will be retained even after the original data have been deleted. Configuration of settings for processing and transmitting will not be taken over into the new data record.



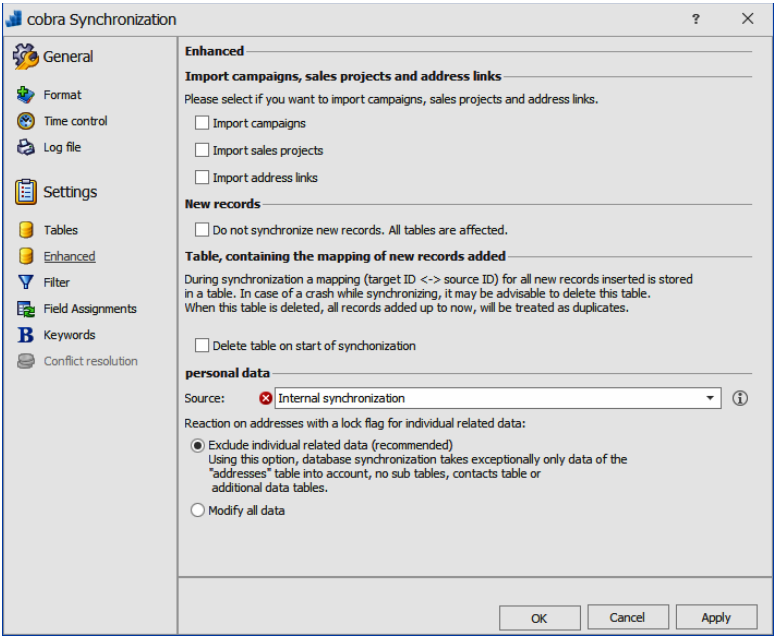
Synchronizing Data

The synchronizing data function has various settings for personal data. One of its aims is to prevent that, whenever data are synchronized, addresses that are listed in the blacklist are taken over into the target database. Also, the content of locked personal data fields will not be modified.

- Issue the command »Data: Data exchange: Synchronization«.
- Select the format required.



You set the options for individual-realted data in the »Enhanced« register tab. These are those data that have been marked as personal data in the *Target* database.



Source ..... Enter here the source of the data. This default value will be used when data are synchronized. It is also the default value presented to the user when querying the source.

Reaction on addresses [...]

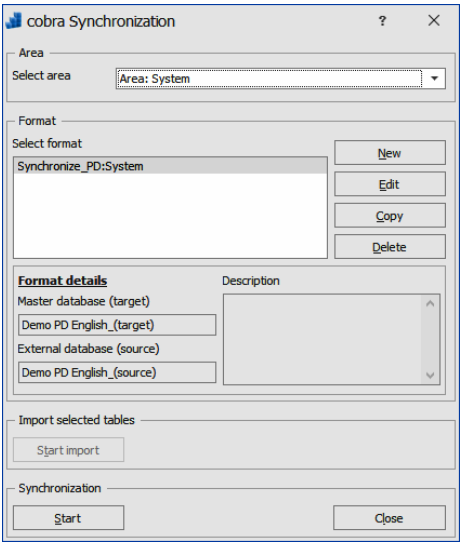
Enter here what is to be done if a lock flag has been set for personal data in the target database.

»Exclude ... data« means that no data from the source file will be taken over into personal data fields of the target database. However, contents of other fields not related to personal data will be taken over.

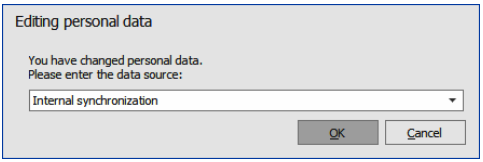
There is an exception though: whenever data are synchronized, this is done only for fields of the address table, but not for fields of other tables such as contact-, additional- or other subdata sources!

Modify all data .. Use this function to import the contents of the source database, even if in the target database the field contains personal data and the lock flag »Lock flag for editing personal data« has been set.

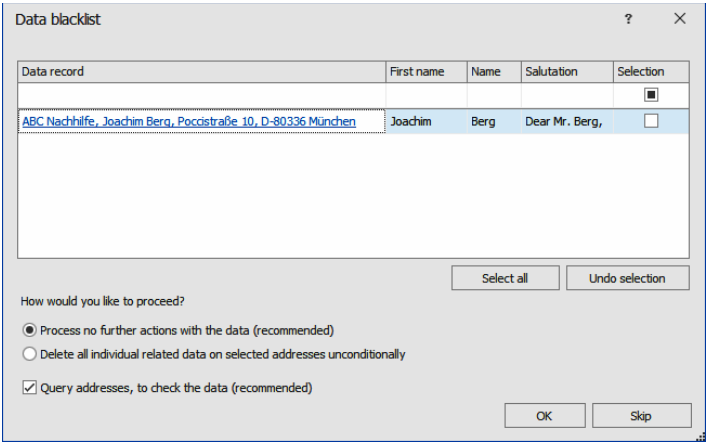
After you have completed configuring the format, start synchronization.



Now you need to specify the source of the personal data, the value entered in the format will be suggested. It will be applied to all data imported during synchronization.



The software will synchronize the databases. Should, after synchronizing, it be found that the data records imported are listed in the data blacklist, such records will be listed.



Data record ..... The addresses in this list are links. If you click such a link, the address will be opened in the editing mask where you can verify and modify it.

Columns of the data blacklist
The fields of the data blacklist will be shown as columns.

Selection ..... Click here those data records to which the action selected below is to be applied.

Process no further actions
Any modifications of data of the target database done during synchronizing will be retained.

Delete all individual related data [...]
All personal data will be erased from the addresses, even those which were not affected during synchronizing.

Use this function only if you are very sure that you want to erase permanently *all* personal data from the data records selected!

Query addresses

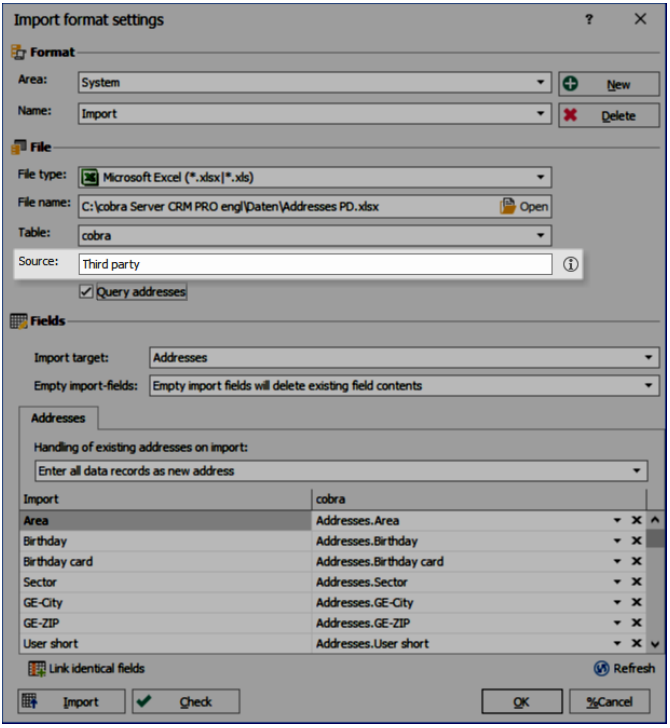
As soon as you have completed the procedure with »OK«, the addresses selected have been queried in the database and you can now edit them manually.

Skip ..... If you click this button, you will leave the dialog without having performed any action or queried anything.

Data Import

When data are imported, a source must be named for the data to be imported. It will be stored with the new as well as any data records modified.

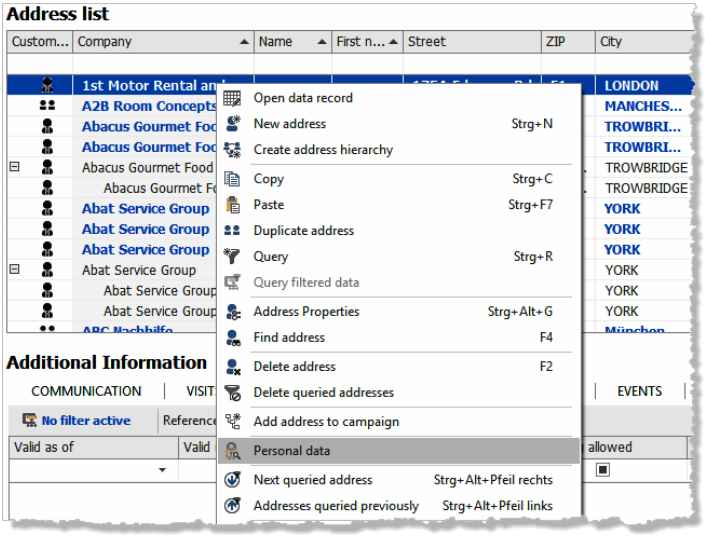
You enter the source in the import format.



Overview, Output and Erasing

To erase or put out records containing personal data, go to the relevant table.

- There, right-click the relevant data record.
- From the context menu, issue the command »Personal data«.

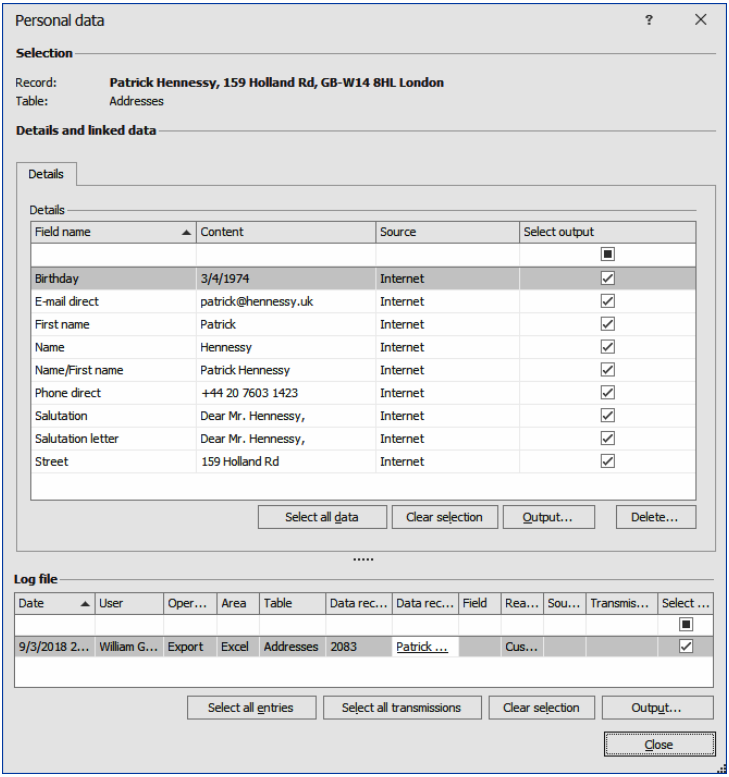


- Or, in the ribbon, issue the command »Data protection: Data of this address: Personal data«.

The dialog is organized in two areas:

- »Details« with personal contents and contents of the contact- and additional data records.
- »Log file« with an overview of modifications, transmittings, upcoming erasures etc.

Details



In the upper part of this dialog, at »Details«, you can view which personal data are contained in this record.

There you can mark specific fields or use buttons to select all data or cancel the existing selection.

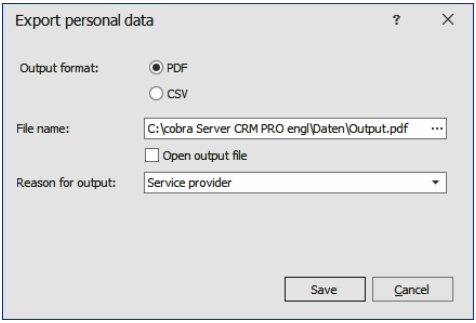
- Mark the data to be put out.

Putting out details

Putting out personal data must be justified and will be entered in the record.

- Click the »Output« button.

You will asked about the reason for putting out the data.



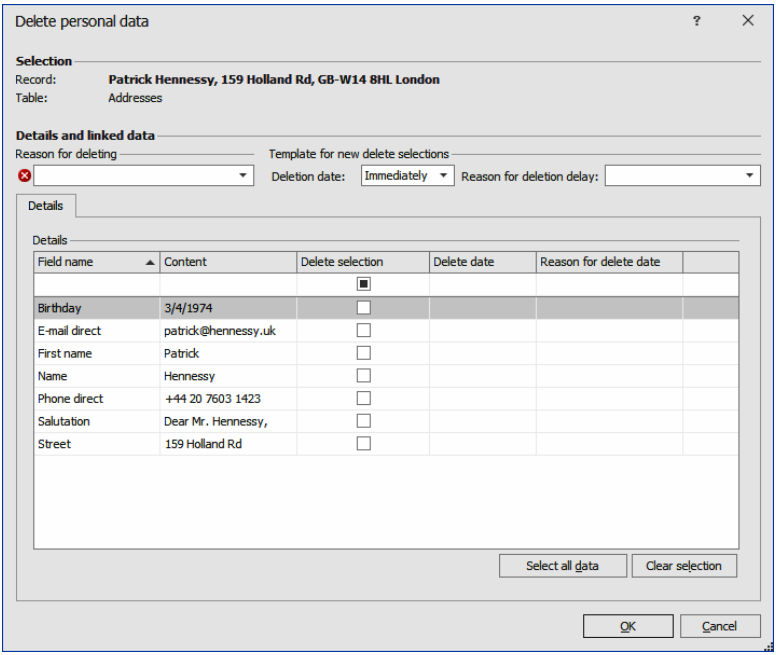
- If the data are transmitted to a third party, you must also enter to whom these data will be transmitted.
- After the data have been put out, there will be a new item in the record.

Erasing

- Click the »Delete« button.

A dialog will appear where you can configure erasing personal data. You can define erasing specifically for any field. Data you do not need any longer, such as the date of birth of a customer, can be erased immediately. Other data you might require e.g. to process later warranty claims, can be marked to be erased later. You do so by selecting an erase date.

- Data are erased immediately if you close the dialog with »OK«.
- Any later erase jobs that you enter here are taken over into the erase schedule.



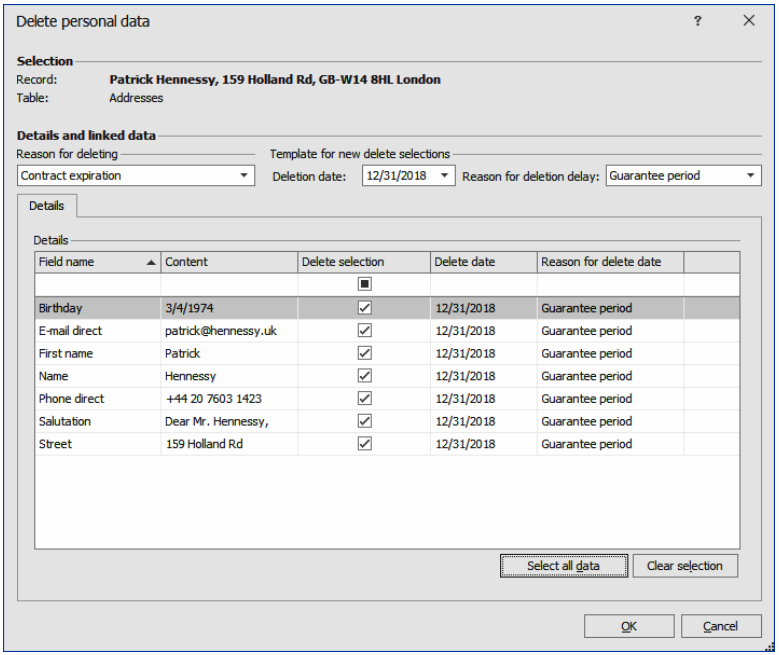
Reason for deleting

Select a reason for erasing the personal data.

Template for new delete selections

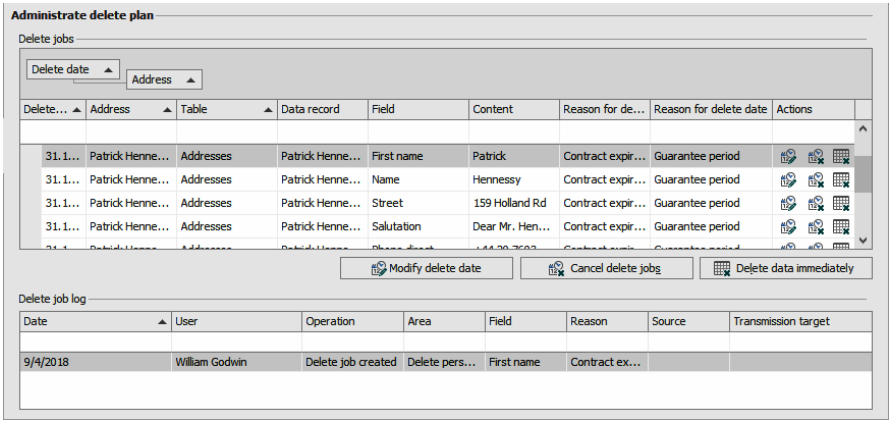
These are default values to be entered if you select an erasing option at »Details«.

Details..... Here you mark those fields whose contents are to be erased. As date and reason for erasing those default values will be suggested that you have entered at »Default«. But you can still define individual dates and reasons for the fields. It might be, e.g., that a date of birth is to be erased immediately, whereas other data might be subject to different legal obligations to retain data. Here the deadlines set by the Commercial Code need to observed. An erase date can be specified as of one day later.



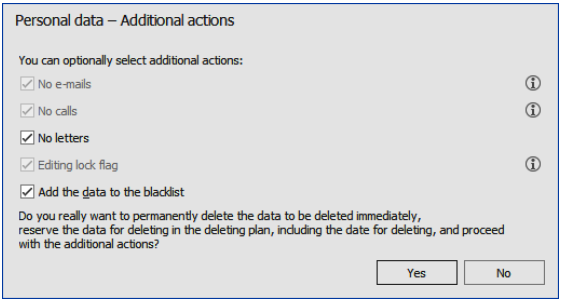
Confirm with »OK«.

In the erase schedule that will look like this:



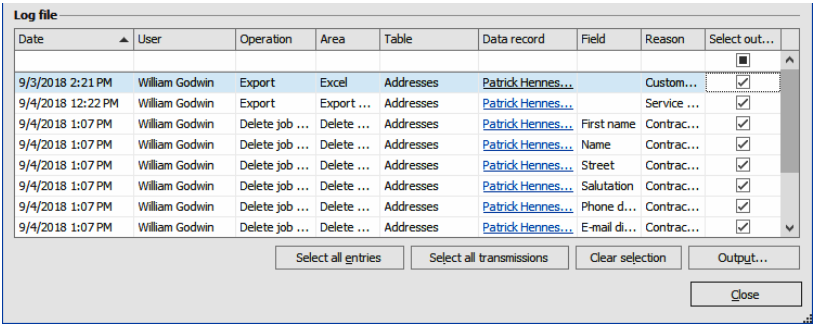
During erasing the contents of obligatory fields will also be erased. When you edit the data record again, cobra will force you to enter these data again.

If you erase personal data, these can be added to the blacklist. You can thus prevent that the same data will have to be created or imported again at a later date.



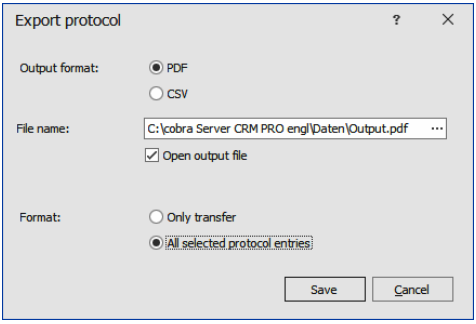
Record

The record will log erase tasks, data modifications and other operations performed at a specific data record. You can thus document that you have observed the legal provisions for protecting data.



- Using the »Select all transmissions« button, you will select only those entries logged that affect transmitting data, such as data export or transmitting an index card. You can thus comply with the right to obtain communication of a data subject.

- Using the »Output« button you will export the record.
- Select format and target of the output file.

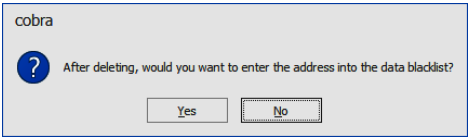


Traditional Deleting of Data

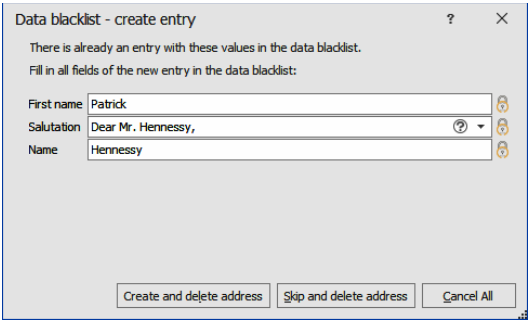
You can also delete a data record containing personal data the traditional way, i.e. not within the dialog mentioned above.

- Mark the data record.
- From the context menu, issue the command »Delete address«.
- There will be no warning about personal data. In fact, the data record will be deleted completely.

You will, however, be asked whether you want to add the data record to the blacklist. You can thus prevent that the same data will have to be created or imported again at a later date.



If not all fields of a data record that are to be added to the blacklist contain data, you can now edit them. To do so, a dialog will open. In this dialog you are presented those fields that constitute the data blacklist.



Here those data fields that have no content are marked by a red icon.

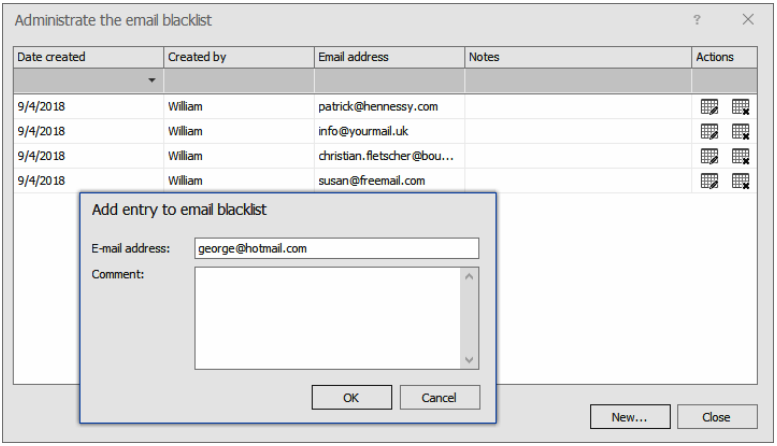
- Either you complete the data required here and click »Create and delete address«.
- Or you do not enter anything and click »Skip and delete address«. Then nothing will be entered in the data blacklist and the address will be deleted.
- Should you not have the authorization to view some of the field contents, this field will remain empty in this dialog. You must then enter the correct value manually to be able to add the address to the blacklist.

Email blacklist

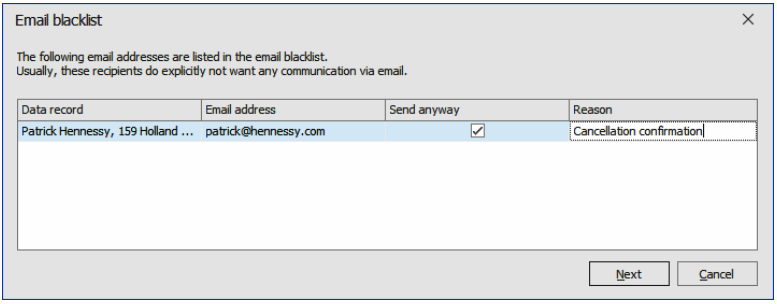
This list documents email addresses that may not be contacted. Any email address entered there is blocked for all data records in which it appears.

An email lock flag works differently: it will affect all email addresses in the data record it was activated in.

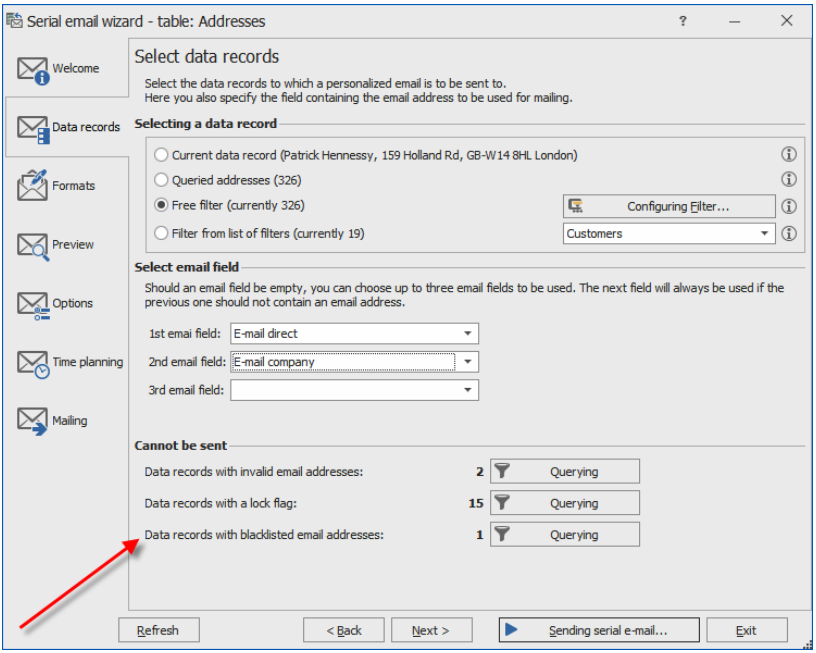
- In the ribbon, issue the command »Data protection: Administrate the email blacklist«.



If you try to send an email to this address, you will now receive a warning. if you still want to send the mail, you will have to enter the reason.



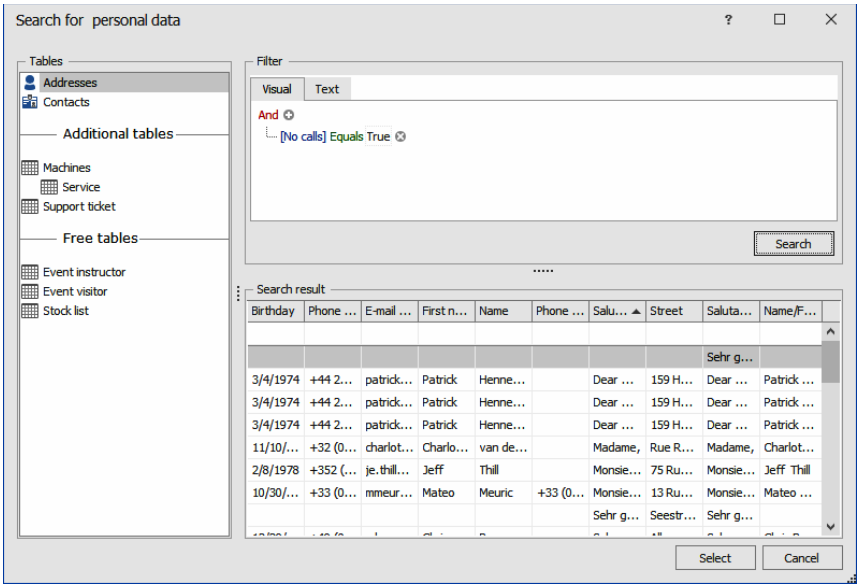
The serial email function has a special feature. It will not send any mails to addresses of the email blacklist and will also not ask about sending. It will show how many data records are listed in the blacklist and will allow querying them.



Search for Personal Data

You can search deliberately in personal data only.

- Issue the command »Data protection: Search: Search for personal data«.



Here you will find the familiar filtering options.

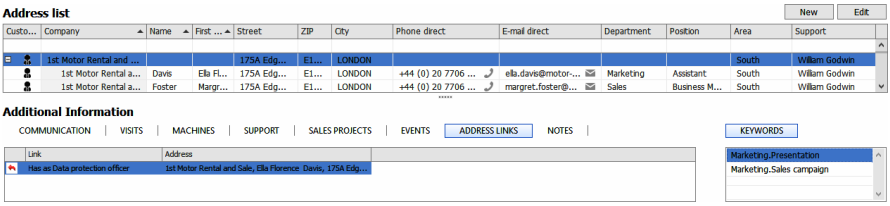
If you mark a data record and then click the »Select« button, you see the personal data of that data record.

Data Protection Officer

By entering an address link, you can specify who is responsible for whom as data protection officer.

On the one hand, you can specify here who is responsible for data protection in your company and thus also for erasing addresses.

On the other hand, you can also indicate the data protection officers of other companies. These address links can be queried.



Notes

Additional Data

If a new data record is created in which personal data fields are to be filled with »default values« only, it is assumed that this data record will *not* contain any personal data. Such default values are entered by cobra, not the user. In consequence, there will be no request for the source nor will the data record be checked for a lock flag.

If in such a data record the default value field or any other personal data field is modified, the logic of checking for a source or a lock flag will apply again and will also affect the personal data fields with default values.

Reports

It is not possible to log the export of reports. This is why it can also not be logged which personal data might be contained in the reports and are exported also.

Modification log

If you work with the modification log, all data and modifications since the log was set up will be logged there. This includes any personal data you have erased and modified in the meantime.

So you might consider not adding personal data to the modification log.

cobra - computer's brainware GmbH
Weberinnenstraße 7
D-78467 Konstanz

Telefon 07531 8101-0
Telefax 07531 8101-22
info@cobra.de

www.cobra.de