Manual

GDPR Toolbox for Microsoft Dynamics 365 Business Central / NAV

Content

Articles

GDPR Toolbox for Microsoft Dynamics 365 Business Central / NAV

The GDPR Toolbox for Microsoft Dynamics 365 Business Central/NAV helps you to meet GDPR requirements for documentation and reporting of your Dynamics 365 Business Central/NAV processes - such as identifying personal data, classifying tables, and generating and processing deletion and anonymization proposals. Respond within the legal deadline, e.g. to requests from affected parties - document these and inform or export the personal data from Business Central/NAV if necessary. Check and document user logons and access rights in Business Central/NAV and reduce your documentation effort with integrated evaluations.

The solution was developed over several months and tested by certified data protection officers and Business Central/ Business Central/NAV partners.

Depending on legal developments, the GDPR Toolbox is continuously expanded by our team of experts and we provide you with the relevant information relating to Business Central/NAV.

Legal notice

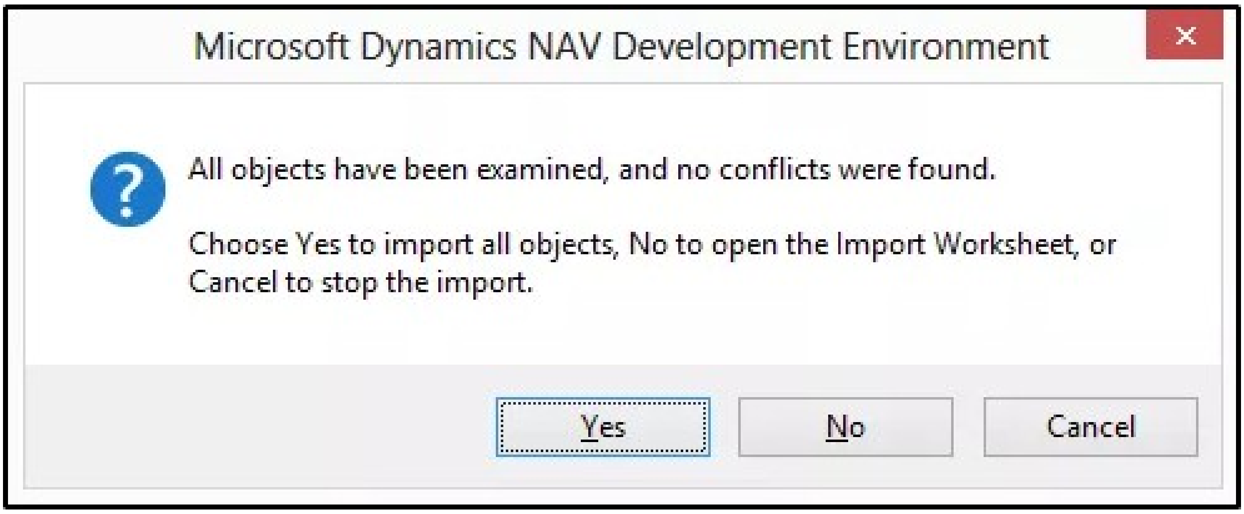
This article serves to inform about issues concerning GDPR. It does not constitute legal advice nor can it replace legal advice.

GDPR Toolbox Integration

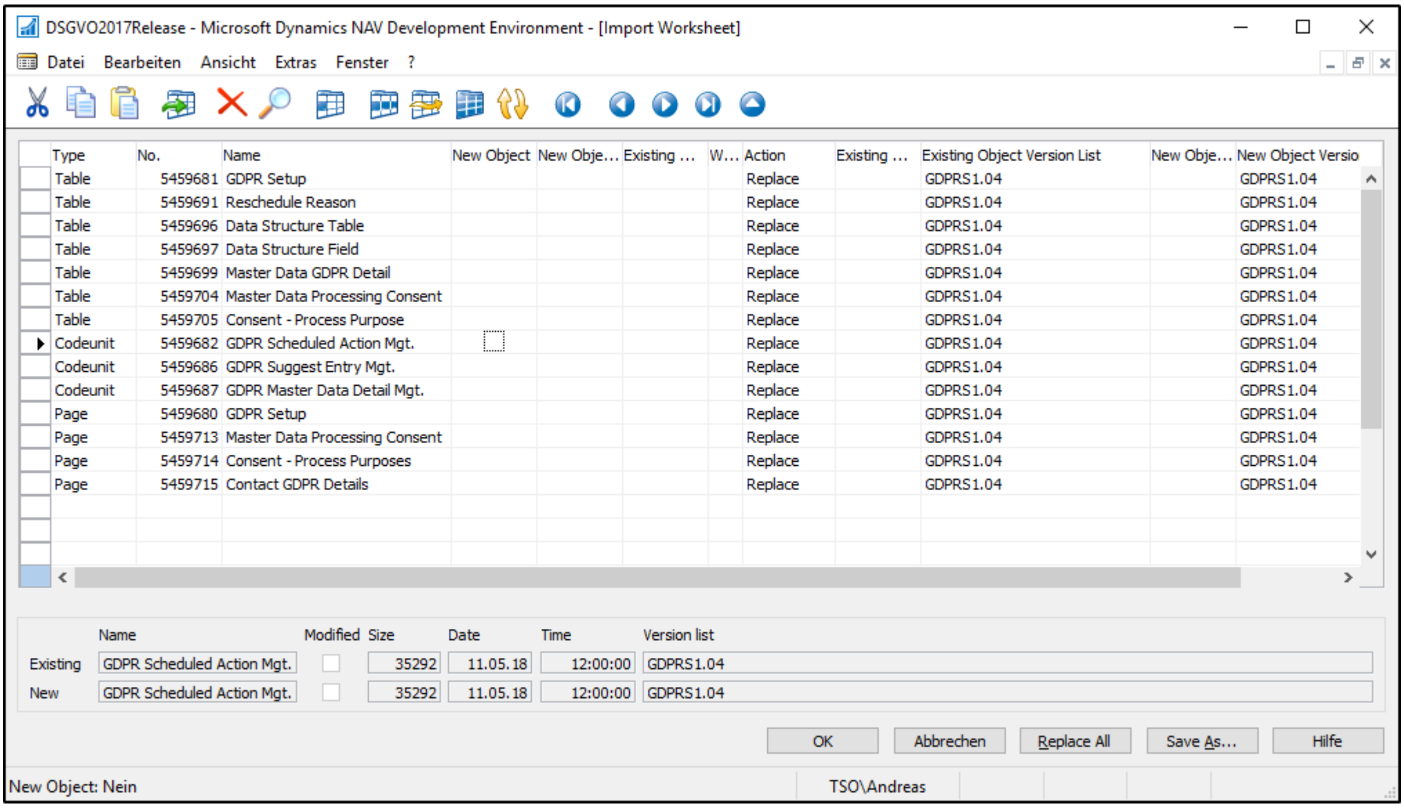
This article describes the integration of the **GDPR Toolbox** based on a standard database version NAV 2017 and requires the corresponding GDPR Toolbox objects for the respective Business Central/NAV version as well as an installed Development Client. These are available on the website www.tso.de/addons/business-central-addons/benutzerlogin/ - via this link you can also download the updates.

Import objects

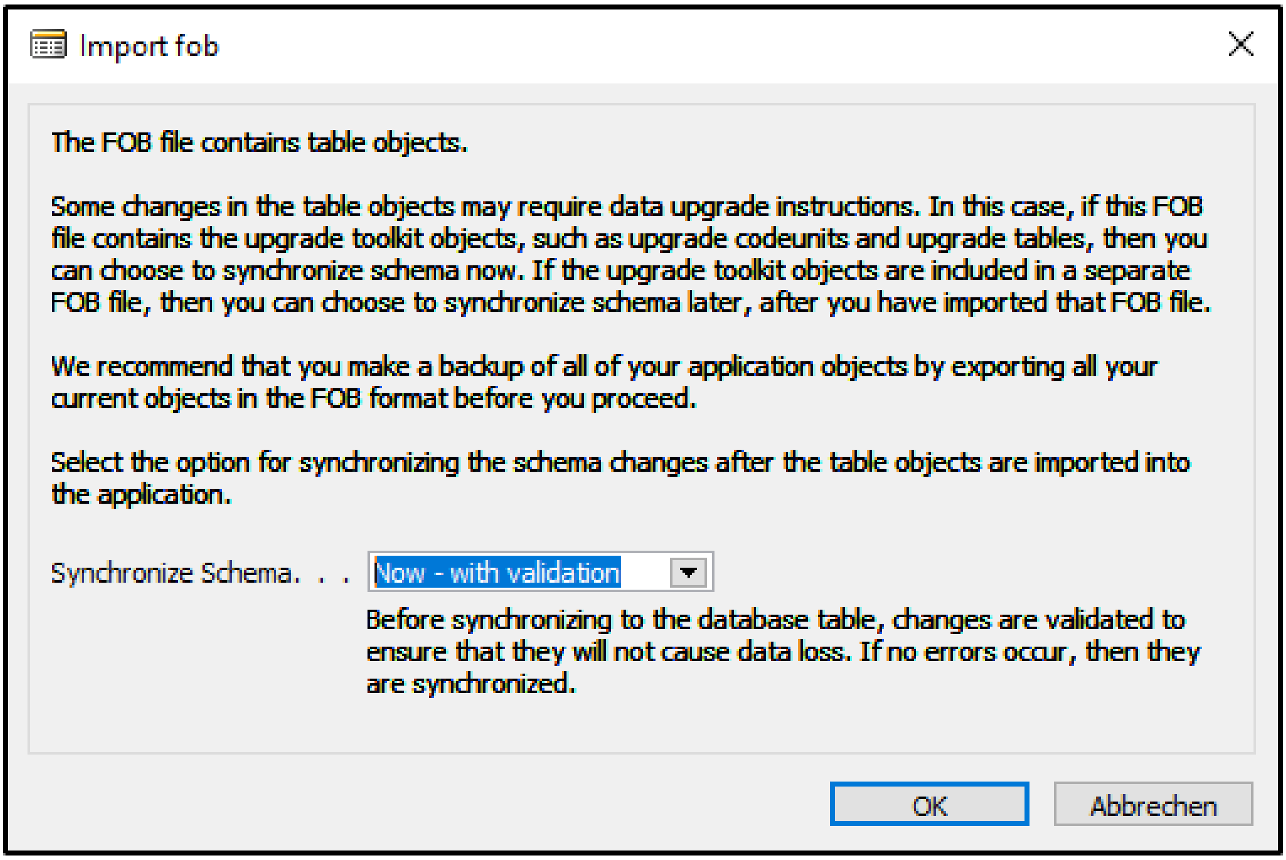
The objects could be imported via the NAV Development Client. To import the objects, call the function [File] [Import] and select the downloaded file. In the displayed dialog, select the option "No".



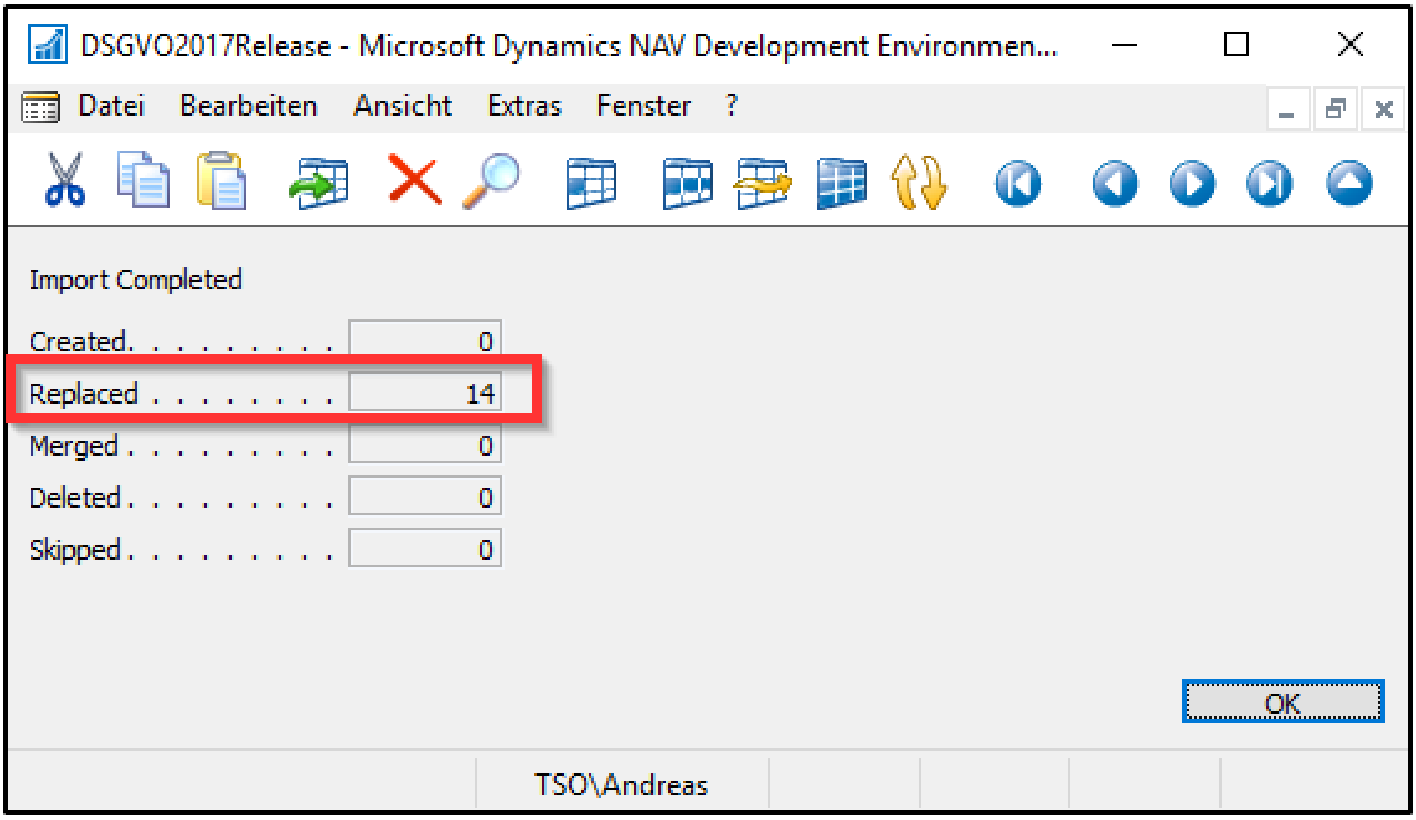
By selecting the option "No", the Import Worksheet is opened and you can get an overview of the corresponding objects.



The objects displayed here show only a part of the objects - the GDPR Toolbox contains more than 80 objects in total. Please select here the function [Replace All] and start the import with [OK]. Since the object package contains tables, the following dialog is displayed.



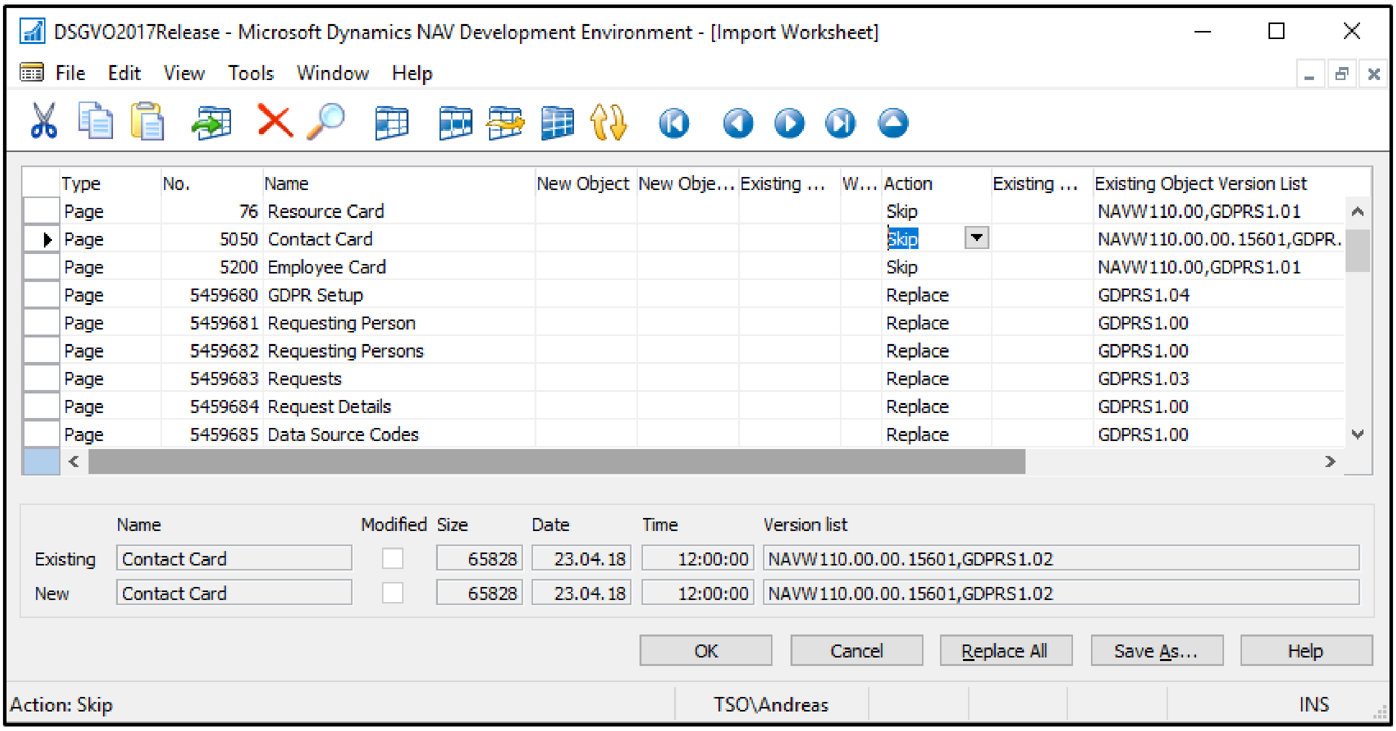
Please select the option "Now - with validation" and confirm with OK. The corresponding table changes are now synchronized with the SQL Server schema and then a status window with the result of the import is displayed.



Please check that the corresponding number of objects is displayed in [Replaced].

Merge Standard Objects

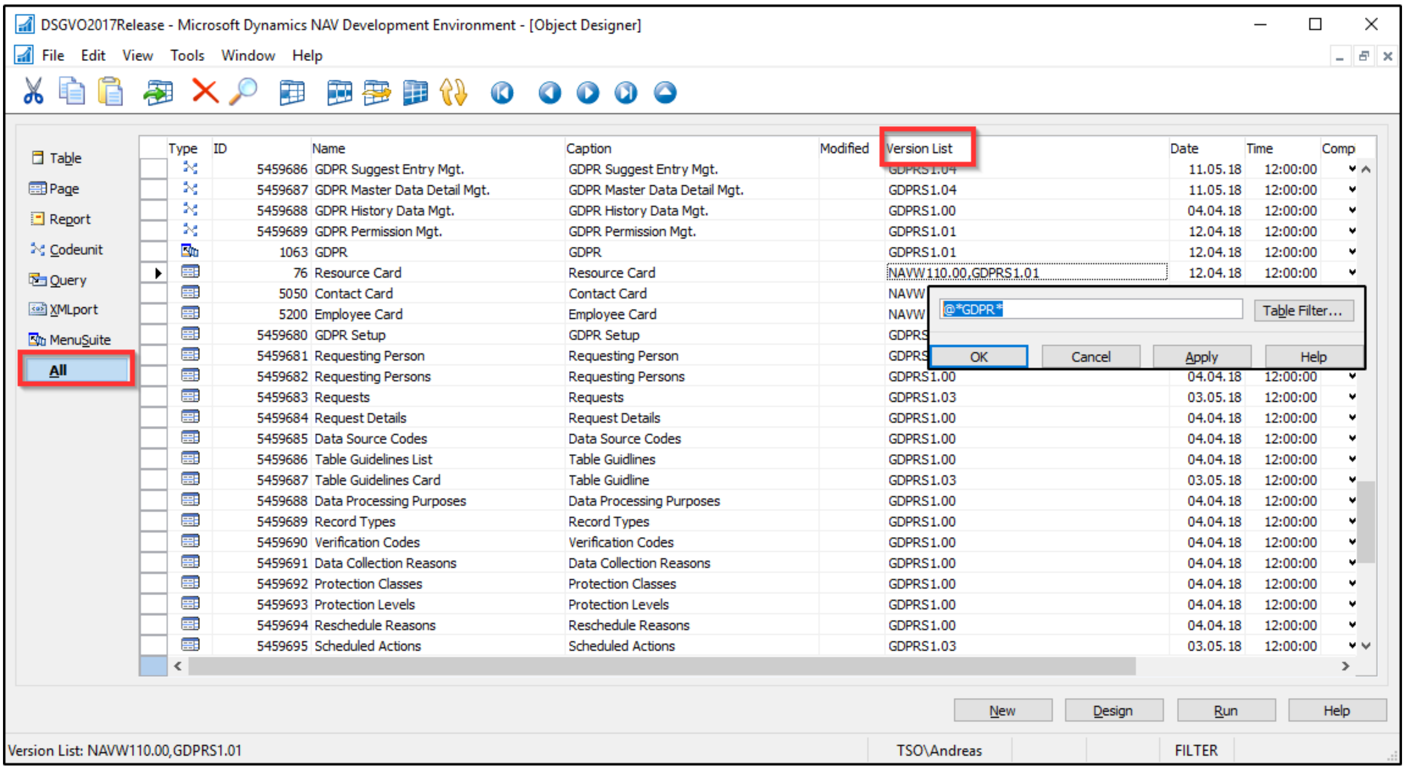
The object package for the GDPR Toolbox contains also changes in three standard objects - that concerns the Pages "Resource Card" (76), "Contact Card" (5050) and "Employee Card" (5200). The action for the GDPR details has been integrated here. If you want to import the objects into a customized customer database or an industry solution, you must merge these objects manually and skip them during the import (see Import Worksheet).



In addition to the objects as FOB files, you can also download the objects as TXT files and then merge the corresponding new action "GDPR Details" into the respective existing page of the database.

Compiling Objects

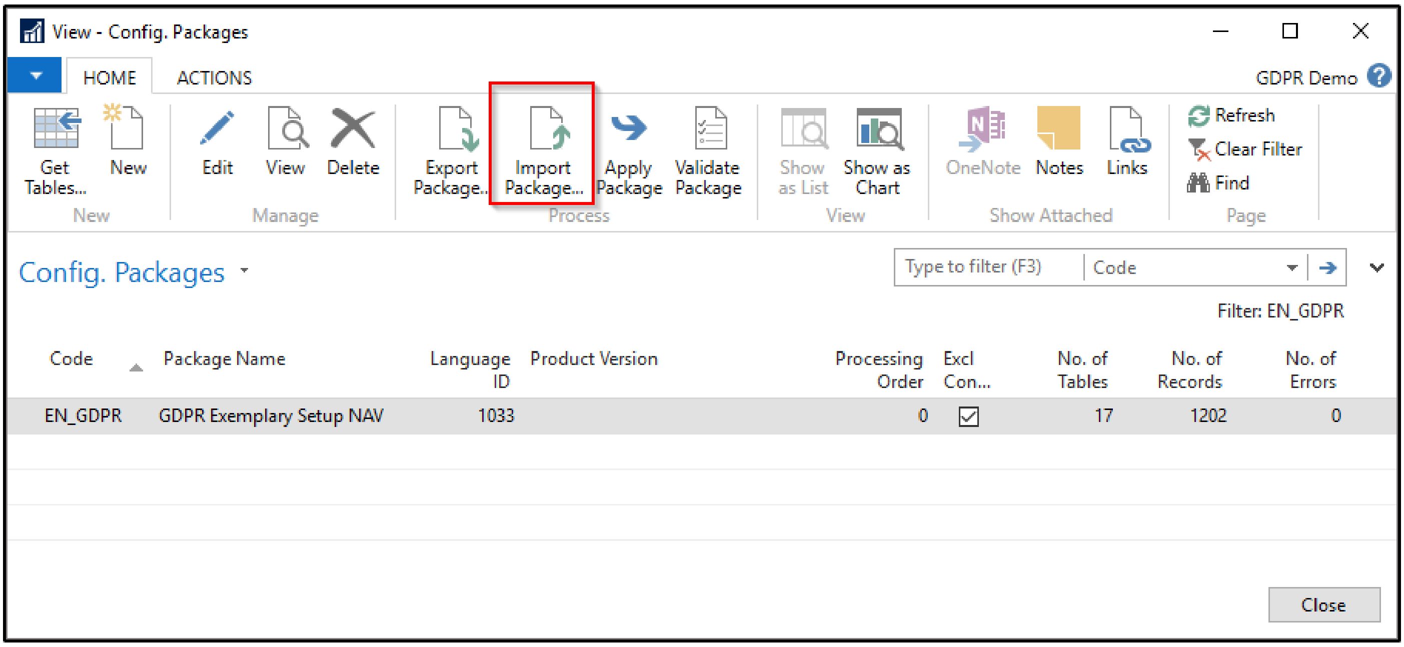
If all objects have been imported and the standard objects have been merged, all objects of the GDPR Toolbox should be compiled. In the NAV Development Client, select the group [All] and filter the objects in the version list to @*GDPR* - this has limited the object list to the corresponding objects.



In this view, select all objects with [Edit], [Select All] and compile the objects with [Tools], [Compile]. If objects cannot be compiled, a corresponding overview window is displayed.

Import Demo Configuration

A configuration package with a demo setup is also provided on the website. This demo setup is not intended for use in a production environment but must first be coordinated with the customer and the data protection officer and tested in a demo environment. To import the demo configuration, call up the configuration packages via the application search and import the file with the extension [.rapidstart] using the [Import Package] action.



With the help of the action [Apply Package] the corresponding demo configuration is accepted.

Note: The ".rapidstart-file" provided and the name of the configuration package may differ from this representation.

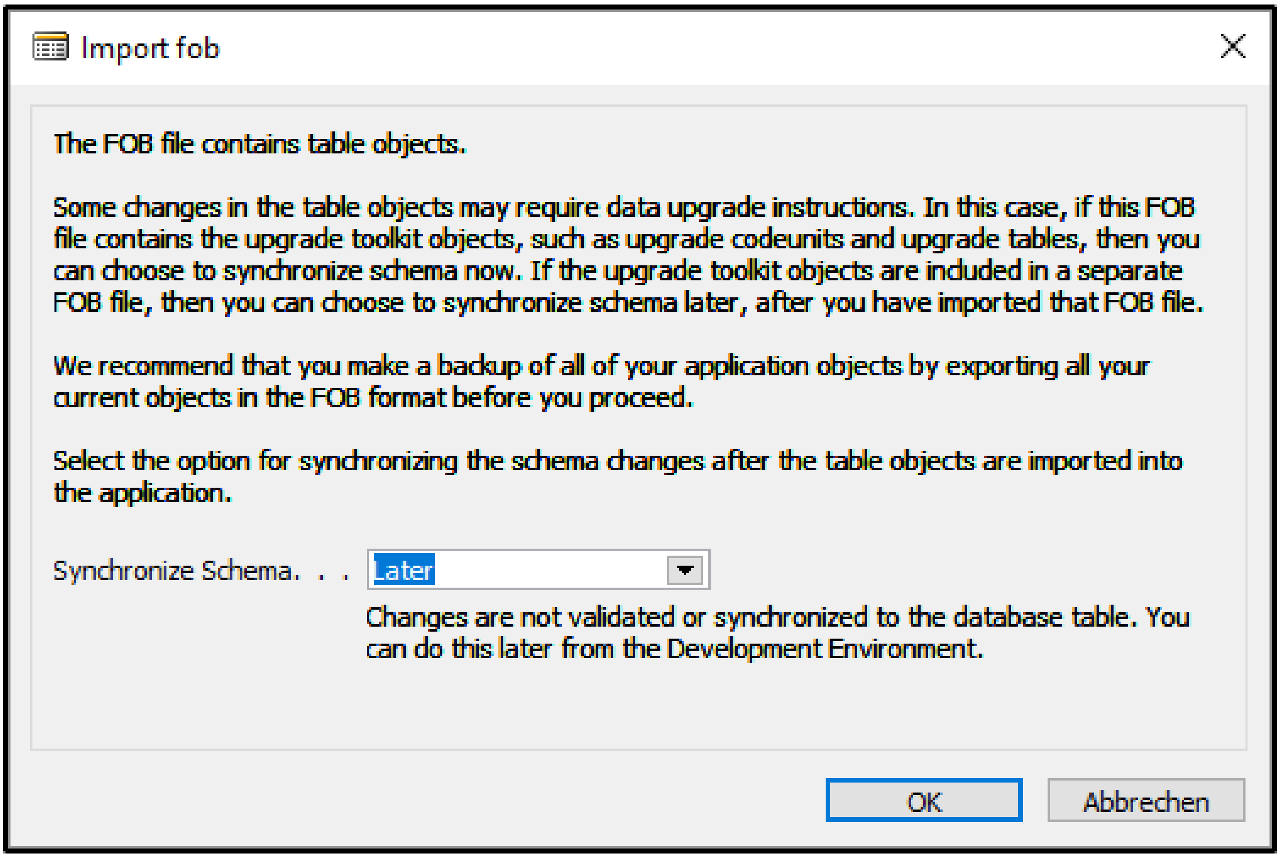
When the import is complete, a status window is displayed showing how much data has been processed and how many errors have occurred. The number of imported records may vary depending on the size - the package has been successfully imported if the number of errors is 0.

Install updates

You will be informed about updates and hotfixes for the GDPR Toolbox via the newsletter. The corresponding updates are available for download at https://www.tso.de/addons/business-central-addons/datenschutz-dsgvo-toolbox/benutzerlogin/ in the form of zip files. The zip file contains the objects as FOB and TXT and, depending on the update, also a separate file for the upgrade objects (as FOB and TXT, starts with Upgrade...). In addition, the zip file also contains the release notes with the documentation for the corresponding changes in this version as well as a note on any existing upgrade objects.

Importing Upgrade Objects

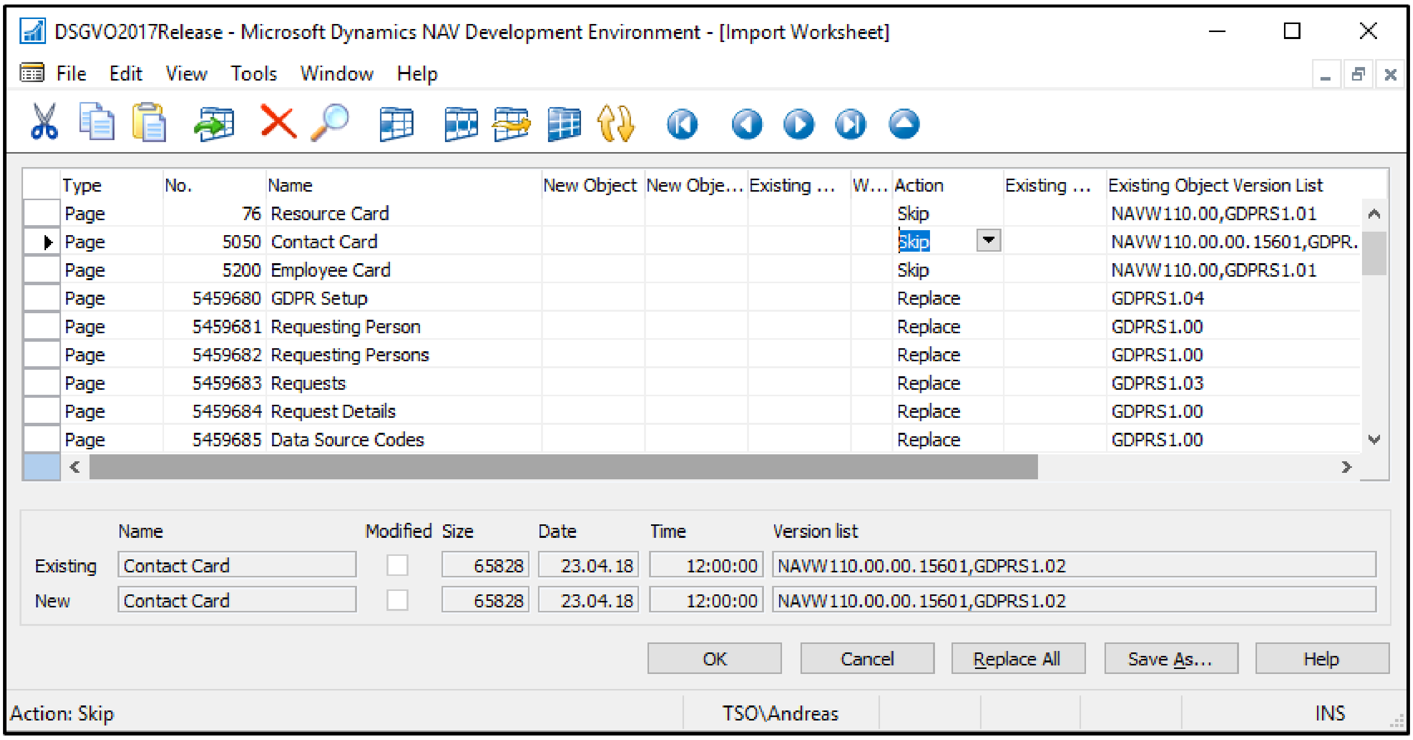
The import of the upgrade objects is described below using the provided FOB file in the Development Client. After you have opened the Development Client, choose [File][Import] and select the corresponding file that contains the upgrade objects. If tables are contained in these upgrade objects, a corresponding dialog is displayed in which you can decide how you want to deal with these table changes.



In this dialog, select the "Later" option, because the table changes are synchronized collectively in a later step.

Importing the Update Objects

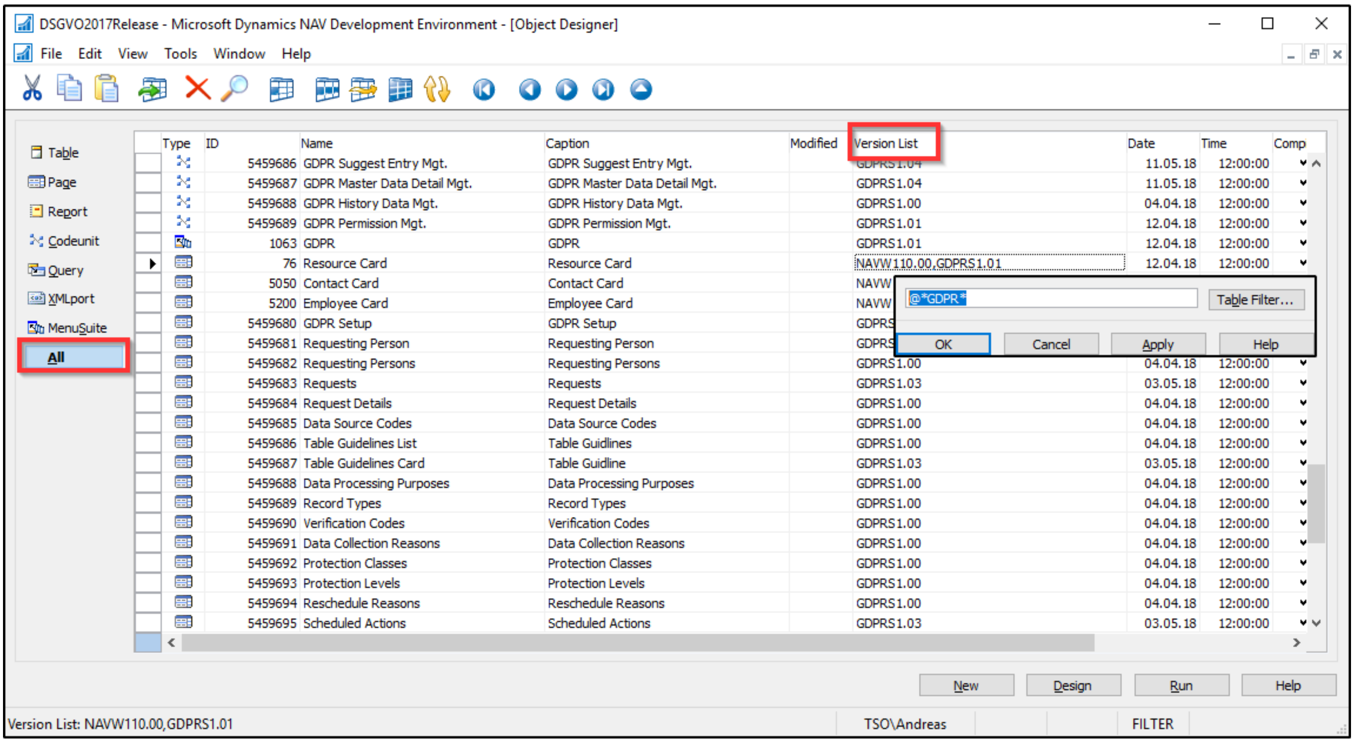
To import the update objects, please open the corresponding FOB file contained in the downloaded zip file. If there are existing objects in the database, you will be notified and you can open the Import worksheet. The objects for the update can also contain changes to standard objects - depending on the version, this can affect the pages "Resource Card" (76), "Contact Card" (5050) and "Employee Card" (5200), among others. The action for the GDPR details has been integrated here. If you want to import the update objects into a customized customer database or an industry solution, you must merge these objects manually and skip them during the import (see Import Worksheet).



If the update objects contain changes to tables, select the "Later" option in the dialog that appears for synchronizing the changes.

Compiling Objects

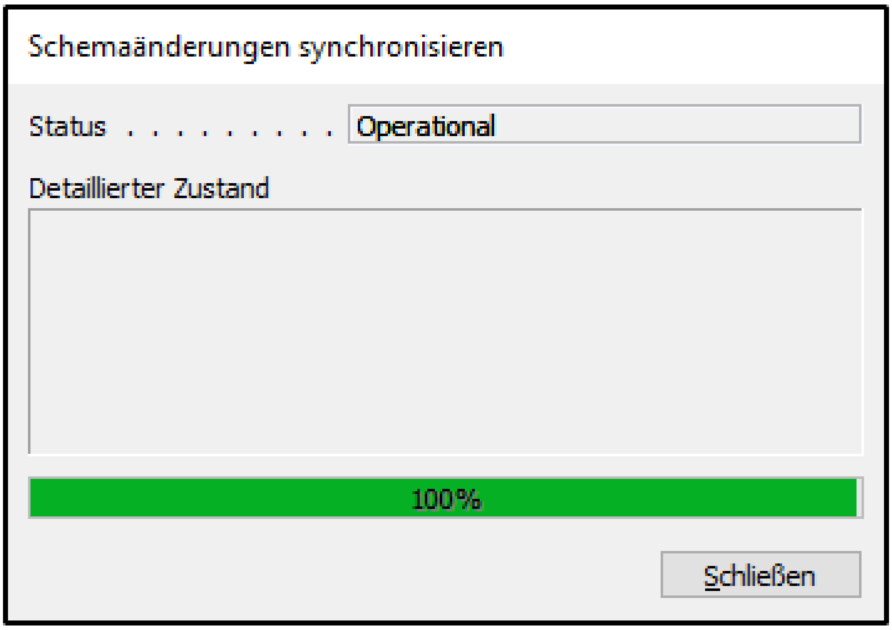
If all objects have been imported and the standard objects have been merged, all objects of the GDPR Toolbox should be compiled. In the NAV Development Client, select the group [All] and filter the objects in the version list to @*GDPR* - this has limited the object list to the corresponding objects.



In this view, select all objects with [Edit], [Select All] and compile the objects with [Tools], [Compile]. If objects cannot be compiled, a corresponding overview window is displayed.

Synchronizing Schema Changes

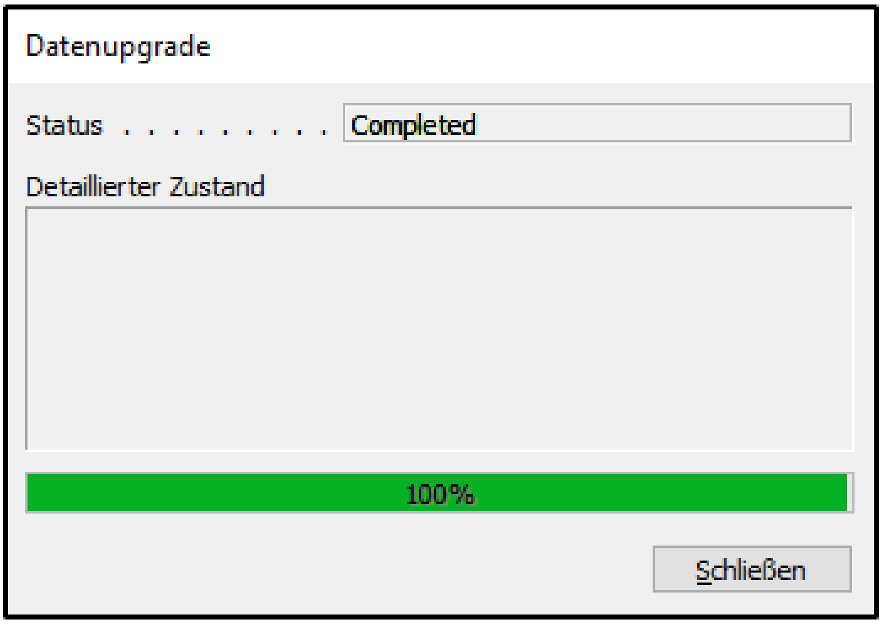
If the schema changes have not yet been synchronized when compiling the objects, you can do this in the menu [Tools] [Sync. Schema For All Tables] [With Validation] - with a successful synchronization you will receive the following status information:



Data upgrade

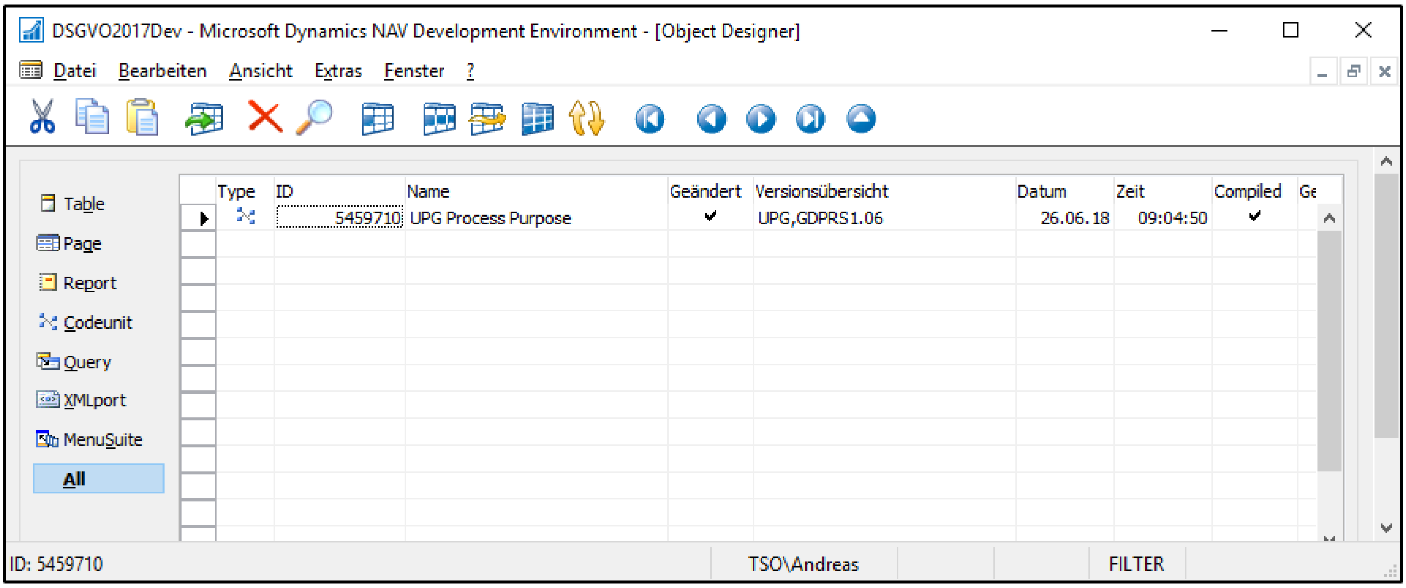
Some of the updates contain upgrade codeunits that transfer the data to the changed structure after the schema changes have been synchronized. If the update package contains these items, they are referenced separately in the Release Notes.

To upgrade the data, call [Tools] [Data Upgrade] [Start] and confirm the corresponding processing duration note with Yes. Select "Parallel" as the execution mode and activate only the indicator for "Show progress". OK starts the data upgrade and displays the progress in the corresponding dialog box. If the data upgrade has been completed successfully, the following overview is displayed:



Delete Upgrade Objects

After the data upgrade has been successfully completed, the upgrade objects can now be deleted from the database. To do this, open the NAV Development Client and select the group [All], filter the objects in the version list to @*UPG* - this restricts the object list to the corresponding upgrade objects. Check the result with the list of upgrade objects from the Release Notes for the update.



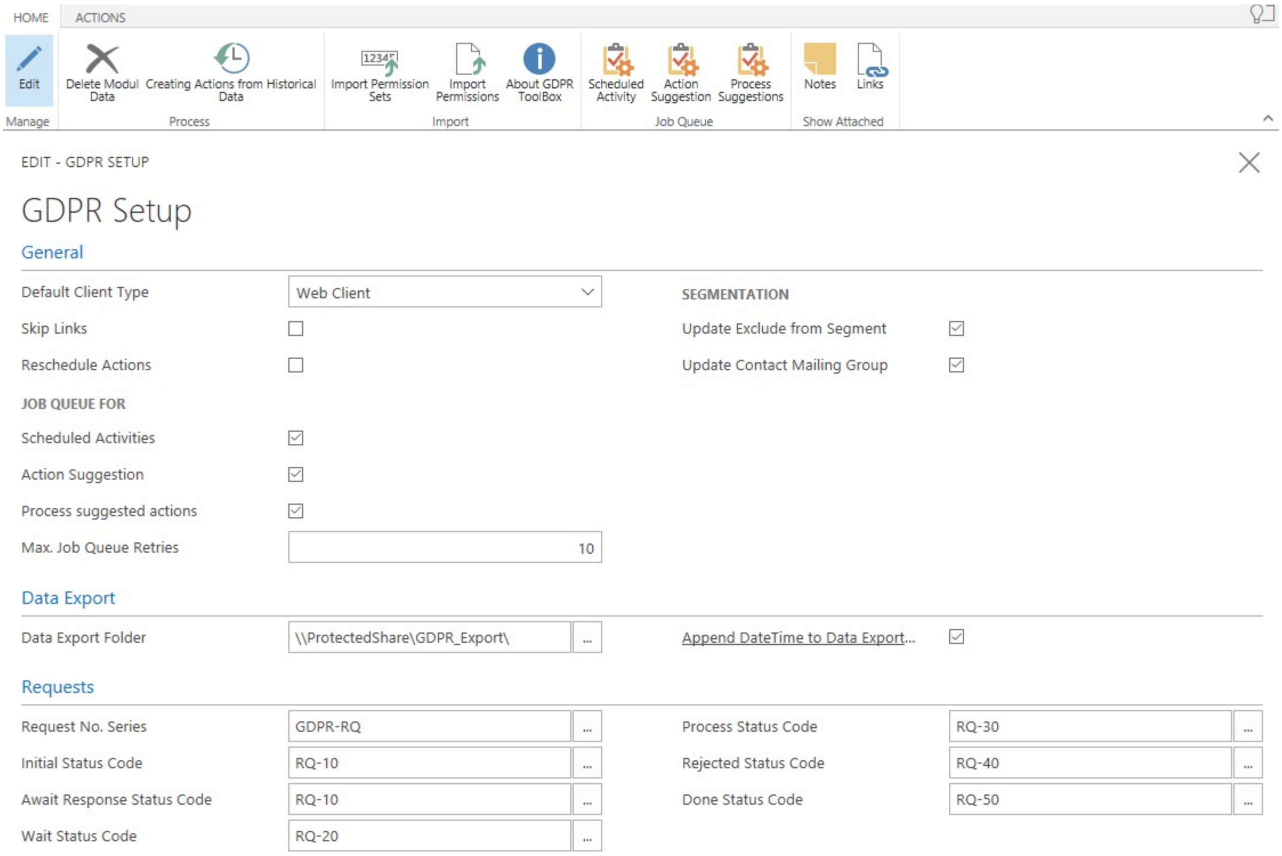
Select all objects and delete them with F4.

GDPR Toolbox Setup

The **GDPR Toolbox** supports the special data protection requirements in Microsoft Dynamics 365 Business Central/NAV. The **General Data Protection Regulation** (**GDPR**) is a European Union regulation unified the rules governing the processing of personal data by private companies and public authorities throughout the EU. This should ensure the protection of personal data within the European Union on the one hand and the free movement of data within the European internal market on the other.

GDPR Setup

In this area the global settings for the GDPR Toolbox are defined. Please note that the screenshots and the data contained therein represent an example and do not claim to be complete. Each company stores personal data differently and elsewhere in Business Central/NAV, therefore all settings and definitions must be agreed and checked with the data protection officer and, if necessary, changed and supplemented. The content described here is merely a prerequisite for the GDPR Toolbox to be technically set up - this facility must be coordinated, adapted and thoroughly tested in a test system before it can be used in a production system.



The following table describes the individual fields of the registers.

Field	Description
Default Client Type	When data records are created in the tables with personal content, planned actions for deleting and anonymizing the data are inserted and links to the data records are also inserted. The advantage of displaying and referring to the planned actions in the form of links is that links are already available in a large number of pages and that the information can therefore be made available in many standard objects without having to make adjustments to standard objects. This field defines the form in which the link for the reference to the planned actions is created. If this setting is subsequently changed, the links in the database are also rebuilt.
Skip Links	With this option you activate that no links are to be created as a connection between created data records and the planned actions if they are not needed. This can have a positive effect on performance, especially when creating scheduled actions for existing data.
Reschedule Actions	If this field is activated, scheduled actions are moved with the standard reschedule reason when their origin data records are updated. The standard reschedule reason can be defined in the reschedule reasons.
Scheduled Activities	You can use this indicator to specify whether the planned actions are not to be created immediately when the data record is created, but afterwards via the job queue. If this option is activated, a job queue item is created and displayed for further processing. Please note that the job queue can be executed automatically ("Manual Scheduled Action").
Action Suggestion	You can use this indicator to specify whether the suggestions are to be created automatically via the task queue. If this option is activated, a job queue item is created and displayed for further processing.
Process suggested actions	You can use this indicator to automatically generate a job queue item that processes (deletes and anonymizes) the suggested actions on a time-controlled basis.
Import Details and Consents	You can use this indicator to automatically generate a task queue item that inserts the GDPR details and declarations of consent from the import transport table in a time-controlled manner.

Update Exclude from Segment	Defines whether the field "Update Exclude from Segment" in the GDPR details for the contact should be updated based on the planned processing purposes. For each planned processing purpose, you can define whether segmentation is allowed. Depending on the planned processing purposes, the system then checks whether at least one processing purpose allows segmenting, otherwise the field "Exclude from Segment" in the contact is activated. **Note:** Removing the "Exclude from Segment" flag is not removed if it was set manually by the user. For this purpose, there is a separate field in the DSGVO Details in the background, which documents the manual setting of this indicator.

Update Contact Mailing Group	Activating this option updates the mailing group on the contact depending on the planned processing purposes. A distribution list can optionally be assigned to each processing purpose.
Data Export Folder	In this field you can select the directory for the file storage. In the case of a request for information and export, the relevant data is stored in this directory. **Note:** It is strongly recommended to enter a specially protected network share so that the data cannot be stored locally, unprotected and viewed without authorization. Storage on a local or mapped drive is not supported.
Append DateTime	This setting defines whether the date and time should be appended to the file names of the files created by data export.
Request No. Series	The request number series is defined here for the requests of concerned persons.
Initial Status Code	When the request is created, the initial processing status in the form of a code is defined in this data record. This field is also used for filtering the requests in the role center.
Await Response Status Code	If there are internal requests regarding the request of the person concerned, this status can be entered here. This field is used to filter the task cues in the role center accordingly.
Wait Status Code	The wait status can be used to classify external requests to the person concerned and display them accordingly in the task cue.
Process Status Code	If the request of the person concerned is processed, the status of the request changes to this corresponding status code.
Rejected Status Code	If the request of a data subject cannot be met (e.g. because legal provisions oppose the request for deletion), then this corresponding status code can be used.
Done Status Code	If the request of the person concerned is completely processed, the status of the request changes to this corresponding status code.

Record Type

The record types are templates with information and specifications that are used when new tables with personal data are defined in the data structures. In addition, the protection class and protection level for the information contained therein are stored in the data types.

For the following protection classes, they are part of the example setup and do not claim to be complete.

Code	Description
SK-1	Normal need for internal data
SK-2	High demand for confidential data
SK-3	Very high demand for particularly secret data

In addition, the following protection levels are available with the example setup.

Code	Description
1	General documents that are to be illegible or voided
2	Internal documents that are to be rendered illegible or voided
3	Sensitive and confidential data and personal data subject to increased protection requirements
4	Particularly sensitive and confidential data and personal data subject to increased protection requirements
5	Confidential information of existential importance to a person, a company or an institution
6	Documents to be kept secret if exceptional safety precautions are to be observed
7	Data to be kept strictly confidential and subject to the highest security precautions

Assignment of protection class and protection levels

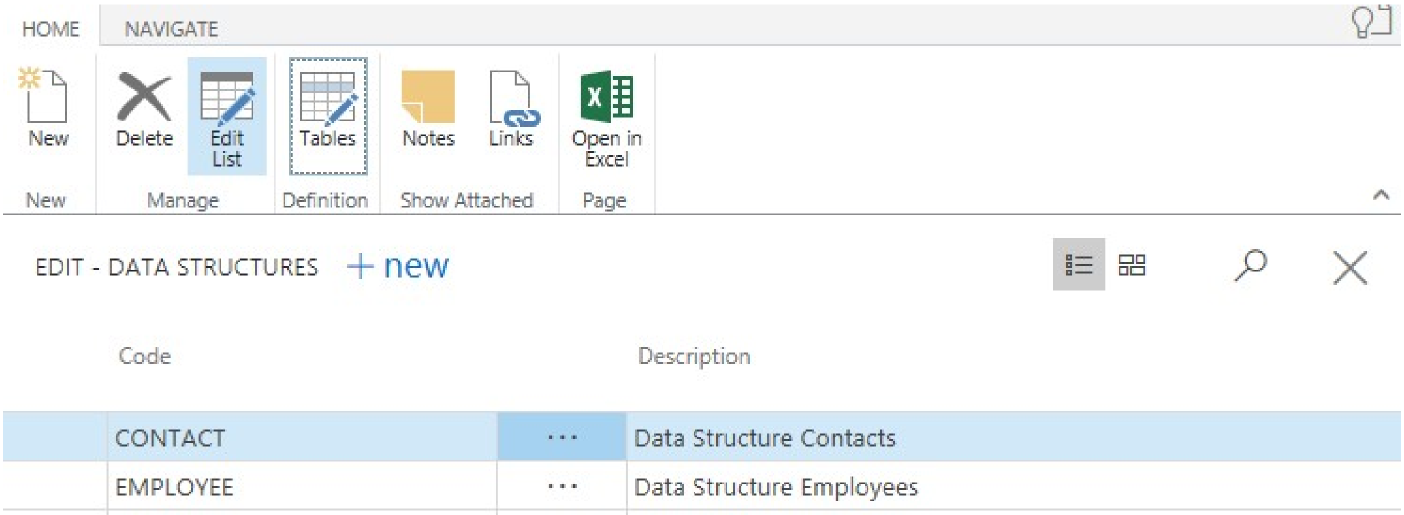
This assignment has already been proposed in the example data. Up to now, only data of protection class 1 and protection level 3 has been provided for the example data.

Request Status

With the request status, requests from concernded persons can be classified with regard to the processing progress and the processing result. This table contains the fields Code and Description and the entries are a prerequisite for the specifications in the GDPR institution.

Data Structures

The data structures contain the configuration for the tables with personal data and the links between the tables. In addition to the tables, the fields with personal contents are also defined here. The display is in a tree structure and the relations and filters for the corresponding tables can be stored on the respective table at the next higher level.



From the respective data structure, you can use the "Tables" action to branch to the setup of tables, fields, relations and specifications for the respective data structure.

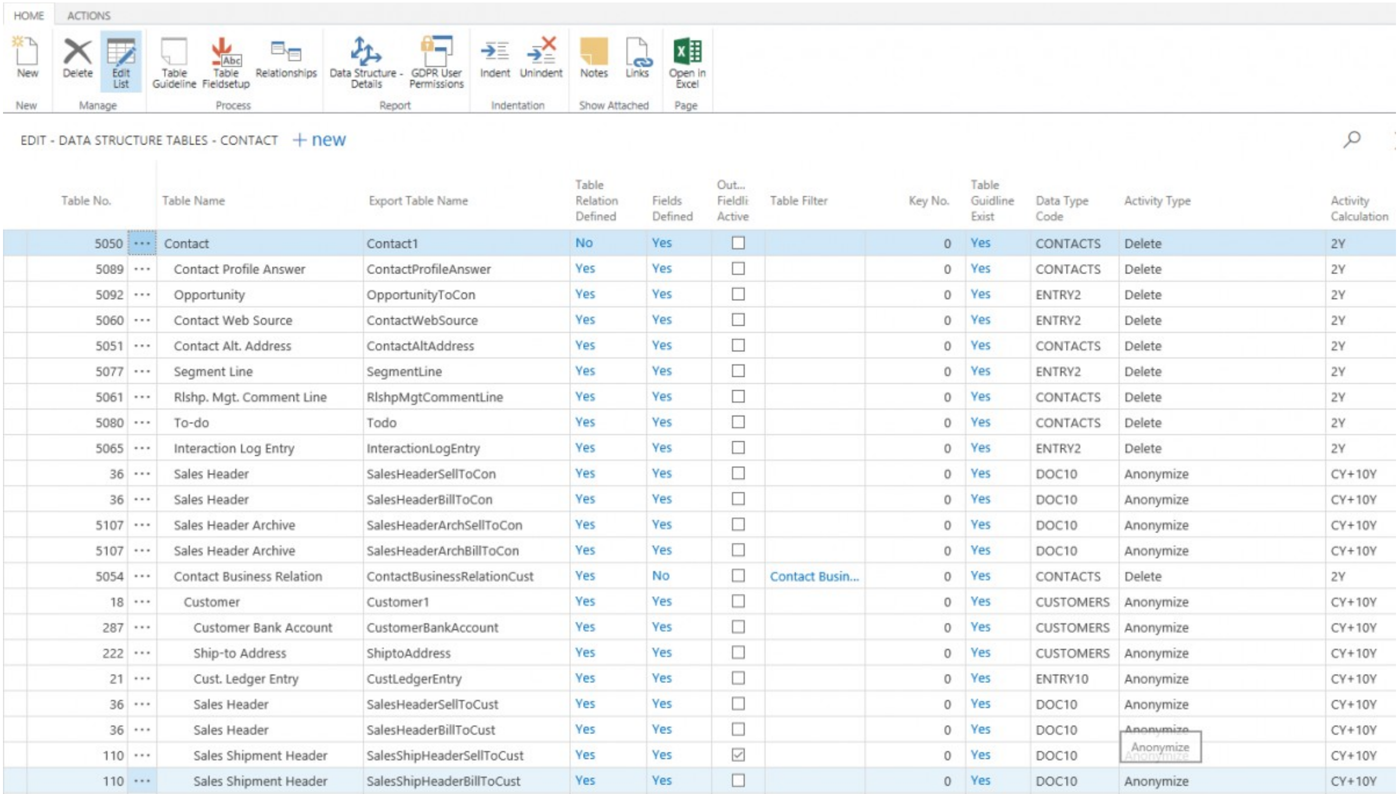
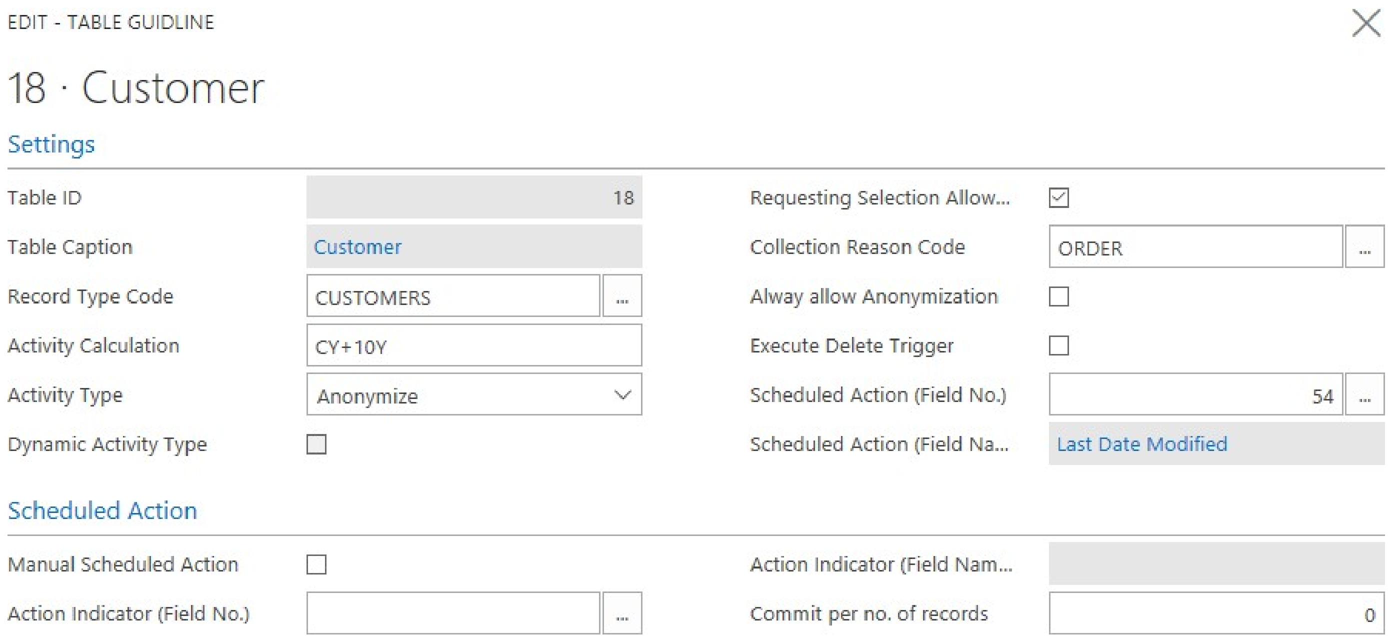


Table No.	Table Name	Export Table Name	Table Relation Defined	Fields Defined	Out... Fieldli Active	Table Filter	Key No.	Table Guidline Exist	Data Type Code	Activity Type	Activity Calculation
5050	Contact	Contact1	No	Yes	☐		0	Yes	CONTACTS	Delete	2Y
5089	Contact Profile Answer	ContactProfileAnswer	Yes	Yes	☐		0	Yes	CONTACTS	Delete	2Y
5092	Opportunity	OpportunityToCon	Yes	Yes	☐		0	Yes	ENTRY2	Delete	2Y
5060	Contact Web Source	ContactWebSource	Yes	Yes	☐		0	Yes	ENTRY2	Delete	2Y
5051	Contact Alt. Address	ContactAltAddress	Yes	Yes	☐		0	Yes	CONTACTS	Delete	2Y
5077	Segment Line	SegmentLine	Yes	Yes	☐		0	Yes	ENTRY2	Delete	2Y
5061	Rlshp. Mgt. Comment Line	RlshpMgtCommentLine	Yes	Yes	☐		0	Yes	CONTACTS	Delete	2Y
5080	To-do	Todo	Yes	Yes	☐		0	Yes	CONTACTS	Delete	2Y
5065	Interaction Log Entry	InteractionLogEntry	Yes	Yes	☐		0	Yes	ENTRY2	Delete	2Y
36	Sales Header	SalesHeaderSellToCon	Yes	Yes	☐		0	Yes	DOC10	Anonymize	CY+10Y
36	Sales Header	SalesHeaderBillToCon	Yes	Yes	☐		0	Yes	DOC10	Anonymize	CY+10Y
5107	Sales Header Archive	SalesHeaderArchSellToCon	Yes	Yes	☐		0	Yes	DOC10	Anonymize	CY+10Y
5107	Sales Header Archive	SalesHeaderArchBillToCon	Yes	Yes	☐		0	Yes	DOC10	Anonymize	CY+10Y
5054	Contact Business Relation	ContactBusinessRelationCust	Yes	No	☐	Contact Busin...	0	Yes	CONTACTS	Delete	2Y
18	Customer	Customer1	Yes	Yes	☐		0	Yes	CUSTOMERS	Anonymize	CY+10Y
287	Customer Bank Account	CustomerBankAccount	Yes	Yes	☐		0	Yes	CUSTOMERS	Anonymize	CY+10Y
222	Ship-to Address	ShiptoAddress	Yes	Yes	☐		0	Yes	CUSTOMERS	Anonymize	CY+10Y
21	Cust. Ledger Entry	CustLedgerEntry	Yes	Yes	☐		0	Yes	ENTRY10	Anonymize	CY+10Y
36	Sales Header	SalesHeaderSellToCust	Yes	Yes	☐		0	Yes	DOC10	Anonymize	CY+10Y
36	Sales Header	SalesHeaderBillToCust	Yes	Yes	☐		0	Yes	DOC10	Anonymize	CY+10Y
110	Sales Shipment Header	SalesShipHeaderSellToCust	Yes	Yes	☑		0	Yes	DOC10	Anonymize	CY+10Y
110	Sales Shipment Header	SalesShipHeaderBillToCust	Yes	Yes	☐		0	Yes	DOC10	Anonymize	CY+10Y

The corresponding tables are stored in the line structure. The hierarchy can be influenced by the actions "Indent" and "Unindent". In addition, this view provides an overview of the detailed facilities from the table specifications, the field list, the relations and the corresponding filters.

Table Guidelines

The table guidelines define the rules for which actions are to be performed with the personal data in this table. You can also define the record type and the data collection reason in the table specifications.

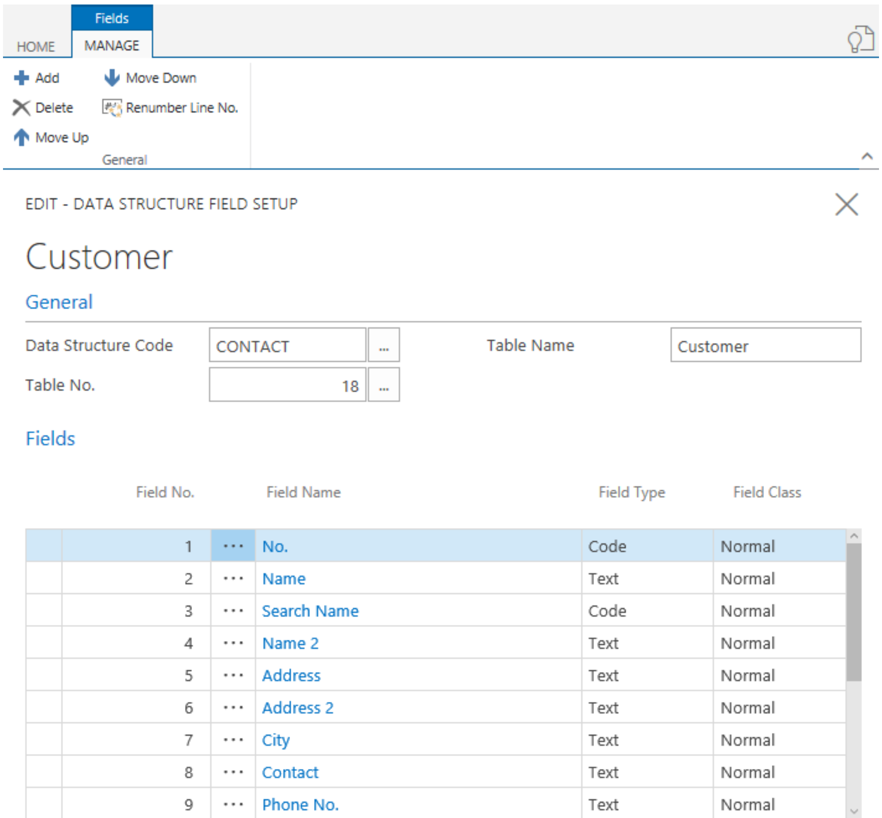


The following fields can be stored in the table specifications:

Field	Description
Table ID	Number of the table from the data structure
Table Caption	Name of the table from the data structure
Record Type Code	Select the data type from the Data Types table. The specifications contained in this table are copied to this table and can be overridden here.
Activity Calculation	The Activity Calculation refers to the action type and determines how long it is intended to store the data in this table and thus determines the time when the corresponding action type is to be executed for the data records.
Activity Type	The action type defines how the data in this table is to be handled if the reason for saving the data is no longer given. Here you can distinguish between deleting and anonymizing.
Dynamic Activity Type	This controls whether the activity type can subsequently be changed to "Anonymize" for an action type "Delete". This can be useful, for example, if you create a sales activity and do not want to delete it in any other transactions with the sales activity within the defined period. In the case of contacts from which, for example, a customer is created and sales transactions take place, the contact should be anonymized. The dynamic activity type is only used in conjunction with the action type "Delete" and is checked when proposals for deletion/anonymization are created. For data in underlying data structures, the action type with the indicator activated is set from "Delete" to "Anonymize".
Requesting Selection Allowed	You can use this indicator to define that this table is permitted for selecting and assigning the link between the requester and the corresponding master data record.
Collection Reason Code	The specification in this field determines the standard data collection reason for the generated data records in this table. This information is not copied into the individual data records of the table, but is defined here as a global default.
Alway allow Anonymization	Regardless of the activity type defined for the table, you can use this setting to define that anonymization of the data in this table is always permitted.
Execute Delete Trigger	This indicator defines that the deletion trigger of the corresponding table and thus the business logic for deletion is to be taken into account. This field is preset with "Yes" for new data records.
Scheduled Action (Field No.)	With this field you can select a date field from the corresponding table which is used for the subsequent creation of "Scheduled Actions" to determine the date on which the activity type for this table is to be executed in combination with the "Activity formula" field.
Scheduled Action (Field Name)	This field displays the field name for the selected field according to the "Scheduled action (field no.)".

Field List

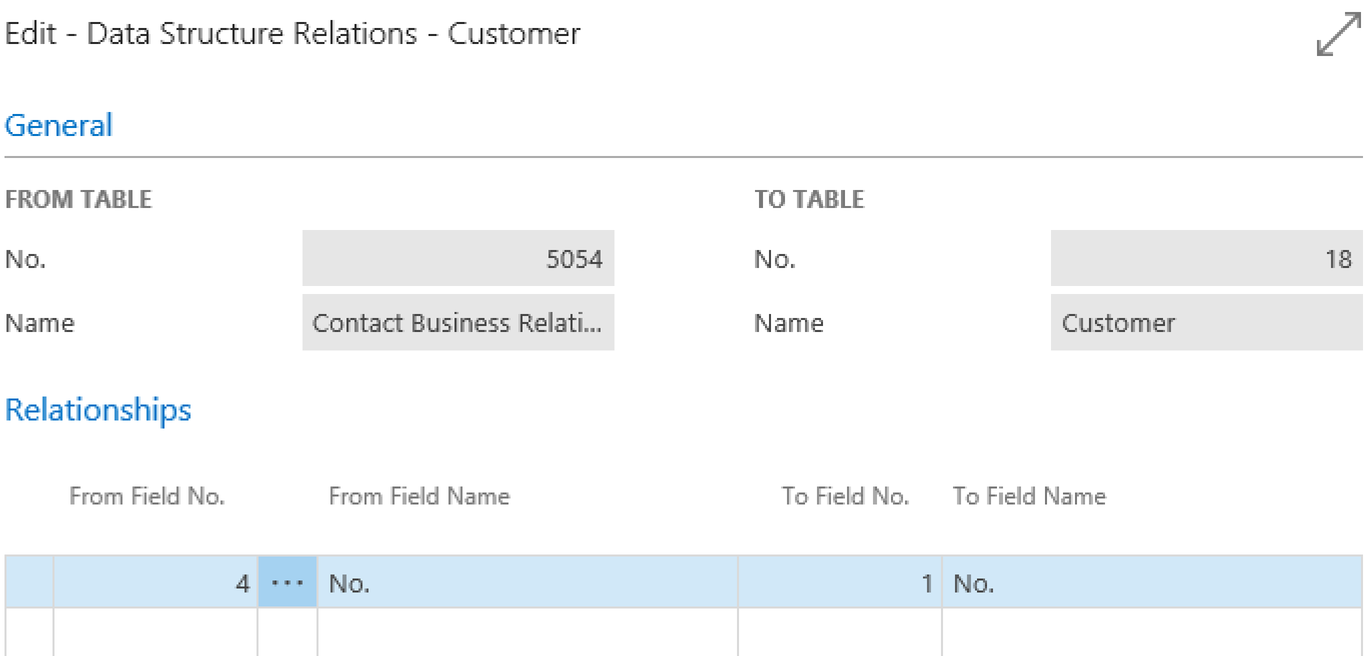
The field list defines the fields of the table that can contain personal data.



The "Add" actions can be used to add new fields and the "Move Up" and "Move Down" actions can be used to change the order of the fields in the list.

Relations

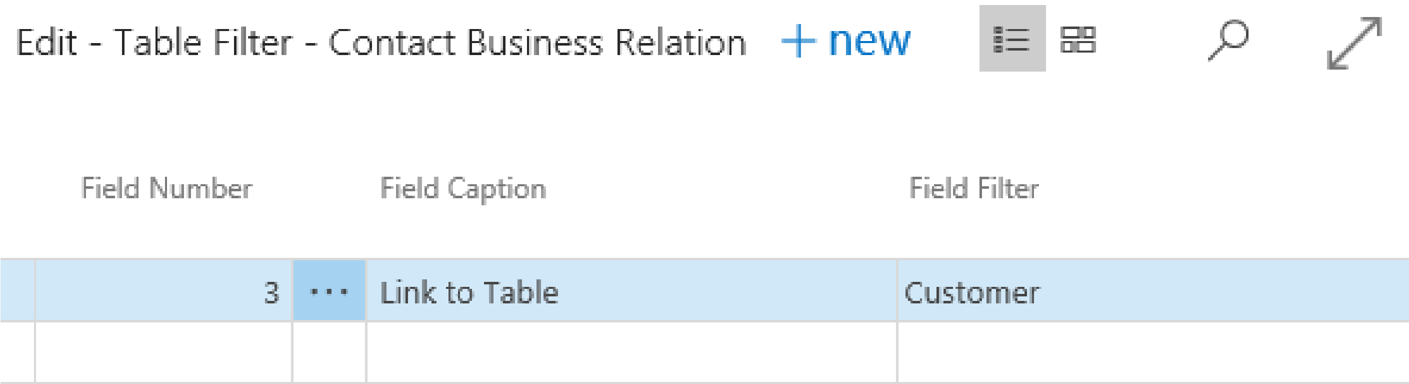
The relations define the connections to the table on the next higher data level. The "From Table" and "To Table" are displayed in the view. The corresponding fields are defined in the line-oriented view of the window.



In this example, the relations from the "Contact Business Relationship" and "Customer" tables are displayed.

Table filter

In the Table Filters column of the Data Structure view, you can define fixed table filters in the form of a table using the AssistEdit button.



In the Table Filter column of the Data Structure Tables view, you can use the AssistEdit button to call a table in which the fixed fields between the current table level and the table level above it are defined. In this case, a fixed filter is created between the Contact and Contact Business Relation table. Since the customer is to be considered in this branch of the data structure tree, the filter is defined here as a fixed value for the customer.

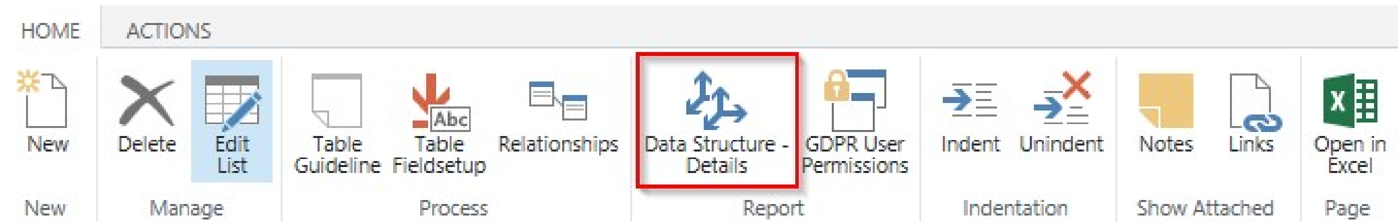
Multiple entries of a table

Tables can be inserted several times in the data structure. Different relations/filters and field lists can be used. If, for example, you want to filter the sales invoices once according to the "Sell-to Cust. No." and according to the "Bill-to Cust. No.", you can consider these filters/relations in two different rows. In addition, you can define the field lists for the export, the information and the anonymization of information per row, so that there are separate field lists with the "Sell-to" fields for the relation on "Sell-to Cust. No." as well as a separate field list with the "Bill-to" fields for the relation can be mapped to "Bill-to Cust. No.".

Translated with www.DeepL.com/Translator

Report data structure details

The configuration of tables and fields with personal content can be evaluated with the help of the provided report "Data structure details". This report can be called directly from the view of the tables for the respective data structure.



Data Structure - Details
CRONUS AG (EN)

11.07.2018 11:39
Page 1 of 40

Data Structure: Code: CONTACT

Code CONTACT
Description Contact

Table with personal data

Table No.	Table Name	Level	Fields defined	Table Guideline exists	Scheduled Action Date	Anonymization always allowed
5050	Contact	0	No	No		No

Table Guideline

Record Type Code	Activity Calculation	Activity Type	Collection Reason Code	Request selection allowed	Always allow anonymization	Excecute delete trigger
CONTACTS	2Y	Delete	ORDER	Yes	No	Yes

Field List

Field No.	Field Name	Field Type
1	No.	Code
2	Name	Text
3	Search Name	Code
4	Name 2	Text
5	Address	Text
6	Address 2	Text
7	City	Text
9	Phone No.	Text
10	Telex No.	Text
15	Territory Code	Code
84	Fax No.	Text
85	Telex Answer Back	Text
86	VAT Registration No.	Text
91	Post Code	Code
92	County	Text
102	Email	Text
103	Home Page	Text
5054	First Name	Text
5055	Middle Name	Text
5056	Surname	Text
5058	Job Title	Text
5059	Initials	Text
5060	Extension No.	Text
5061	Mobile Phone No.	Text
5062	Pager	Text
5063	Organizational Level Code	Code
5101	Salutation Code	Code
5102	Search Email	Code
5105	Email 2	Text

Data Collection Reason

The legal reasons for the collection of the data can be stored in this table of institutions. The legal reason can be used as a template in the table definition for the personal data.

HOME

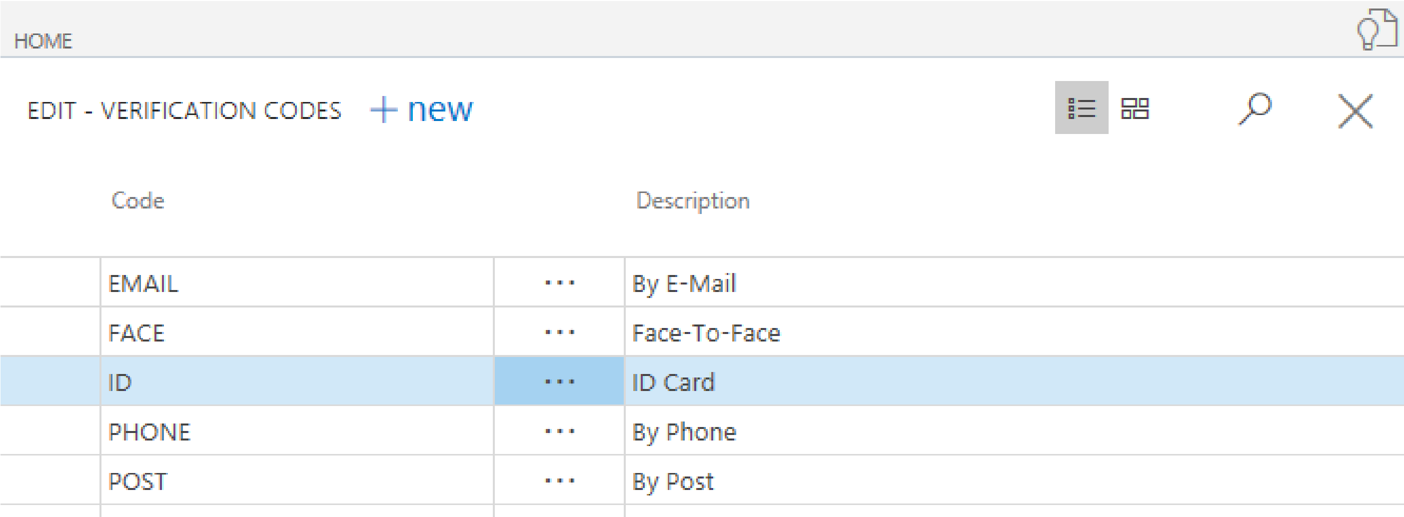
EDIT - DATA COLLECTION REASONS + new

Code	Description
CONSENT	Consent
ECOM	Online Shop / Marketplace
FAIR	Fair
INTERNAL	Internal Processes
NEWSLETTER	Newsletter Subscription
OBLIGATION	Legal Obligation
ORDER	Order Processing

The data collection reasons can be defined in the form of a code and a description and are a prerequisite for the specifications in the data types.

Verifications

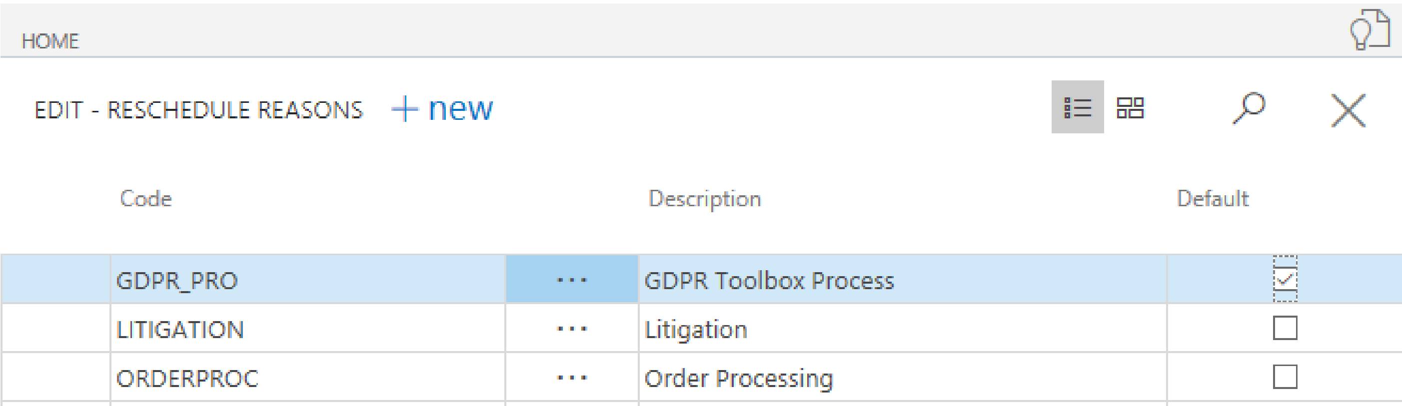
The verifications are used in the module area for the inquiries of persons concerned and define the verification of the inquiring person, i.e. by using default values it can be documented how it was checked that the inquiring person is actually the person who claims to be. This verification process is currently not supported by a procedure within the GDPR Toolbox, but only by documenting the result of a verification.



Code	Description
EMAIL	By E-Mail
FACE	Face-To-Face
ID	ID Card
PHONE	By Phone
POST	By Post

Reschedule Reasons

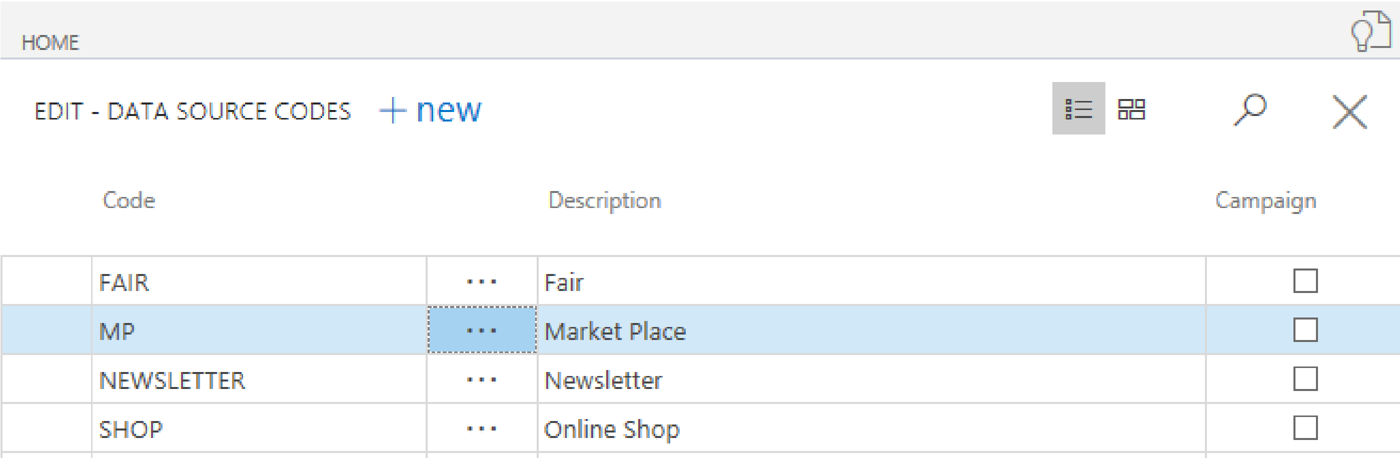
These reschedule reasons are used to document the manual or automatic shifts of planned actions.



Code	Description	Default
GDPR_PRO	GDPR Toolbox Process	☑
LITIGATION	Litigation	☐
ORDERPROC	Order Processing	☐

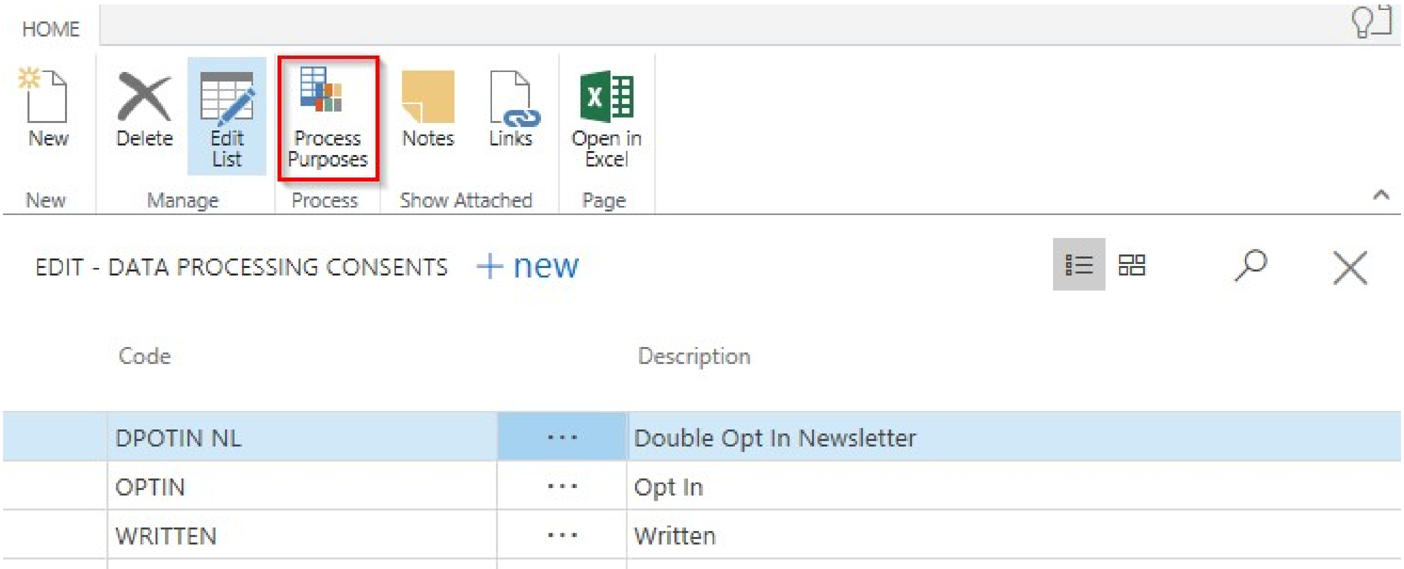
Data Source Codes

The origin of a data record, such as a contact, can be documented when the data record is created. This allows you to answer the question about the origin of the data when an enquiry is made by a person concerned. The corresponding table "Data Source Codes" defines the possible selection of origin codes with the values Code and Description. In addition, a flag can be activated in the "Campaign" field that activates the additional Source Campaign Field in the GDPR Details view, e.g. for the contact. In this field you can specify then the specific campaign through which the contact was made.



Data Processing Consents

The GDPR requires the consent of the data subject for the collection and processing of the data. This table defines the possible declarations of consent that the user can select when creating or editing master data.



The consents can be filed for contact and used for inquiries from data subjects and can be used for the answers to the question "When and in what form did I give my consent to the processing of the data".

Process Purposes

In addition to the Data Processing consents, the planned processing purposes are also deposited. These are defined in the respective declaration of consent and added to the contact when the declaration of consent is issued. This view defines the possible processing purposes.

EDIT - PROCESS PURPOSES - DPOTIN NL · DOUBLE OPT IN NEWSLETTER + new

Processing Purpose Code		Description
NL_MEN	...	Newsletter Men
NL_WMN	...	Newsletter Woman

These processing purposes can be included in the consent forms and are automatically added to the contact when the consent is documented. The following view shows the guidelines for the processing purposes for the e-mail declaration of consent.

If, for example, a contact withdraws its Data Processing consents, the corresponding processing purposes will also be removed.

Import DSGVO details and declarations of consent

Existing or historical declarations of consent, as well as DSGVO details can be imported via two separate tables. This data is maintained in the DSGVO setup under Actions > Import DSGVO Details or Actions > Import Consent. The processing takes place by a further task queue. This can also be achieved in the GDPR Setup under Action > Process Import Details and Consents.

User Permissions

The user permissions for the users of the GDPR Toolbox are defined in three groups. These groups and the corresponding authorization records define a proposal for the authorizations to map typical tasks of the different user groups of the GDPR Toolbox. The definition of the task area for the respective user group can vary depending on the company, so that extensions and adjustments must be made to the authorizations described here and this institution is not legally binding and does not claim to be complete.

Import

The import of permission sets and permissions can be called up directly via the action buttons in the GDPRS Setup.

Basic User

For this user there is an authorization set "GDPR-BASIC" - this is assigned to all users who have to access tables with personal contents or read the setup of the GDPR Toolbox and is comparable to the standard authorization set "BASIC".

In order to set up a user in the order entry area and create the functions such as contact creation, customer and enter and book orders, at least the following permission records must exist for this user in a standard NAV database.

Permission Set	Name
BASIC	Basic User (All Inclusive)
DATAEXCH-SETUP	Data Exchange Setup
GDPR-BASIC	Basic User GDPR Toolbox
RM-CONT, EDIT	Edit contacts
S&R-Q/O/I/R/C, POST	Post sales orders, etc.
S&R-Q/O/I/R/C	Create sales orders etc.
S&R-CUSTOMER, EDIT	Edit customers
S&R-POSTED S/I/R/C	Read posted shipments, etc.

GDPR Officer

The authorization record "GDPR-OFFICER" has been provided for the officer who has to record and process the requests from the persons affected. To perform the usual tasks of the agent, the users must be assigned at least the following authorization records.

Permission Set	Name
BASIC	Basic User (All Inclusive)
DATAEXCH-SETUP	Data Exchange Setup
GDPR-OFFICER	Officer GDPR Toolbox
S&R-POSTED S/I/R/C	Read posted shipments, etc.

The rights to information and export can be mapped in this permissionset - not the rights, e.g. to data correction. To do this, it may be necessary to assign additional permission records from the standard authorization records.

GDPR Administrator

For users who have to set up the GDPR Toolbox, the "GDPR-SETUP" permission set is provided, which enables full access to all relevant tables of the GDPR Toolbox.

The users for setting up the GDPR Toolbox must have assigned the following authorization records.

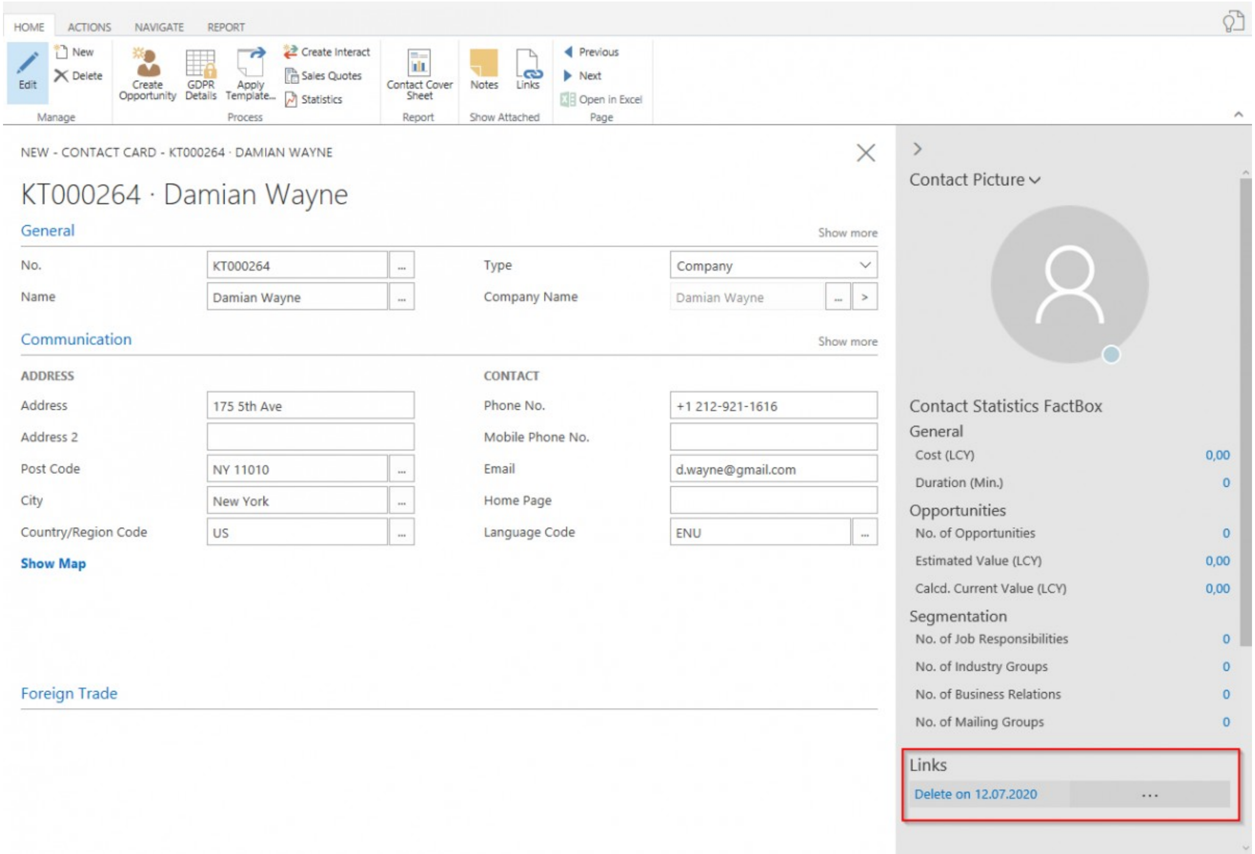
Permission Set	Name
BASIC	Basic User (All Inclusive)
DATAEXCH-SETUP	Data Exchange Setup
GDPR-SETUP	Setup GDPR Toolbox

GDPR Toolbox Operation

The **GDPR Toolbox** supports the special data protection requirements in Microsoft Dynamics 365 Business Central/NAV within the framework of the **General Data Protection Regulation** (**GDPR**). In this part of the documentation, the operation of the GDPR Toolbox is presented using example processes. Since each company works individually and the characteristics of data protection are manifold, the documentation of these example processes is to be understood as a suggestion and basis for the possibilities. The processes presented here do not claim to be complete and must therefore be checked, revised and supplemented in cooperation with the data protection officer.

Contact Creation

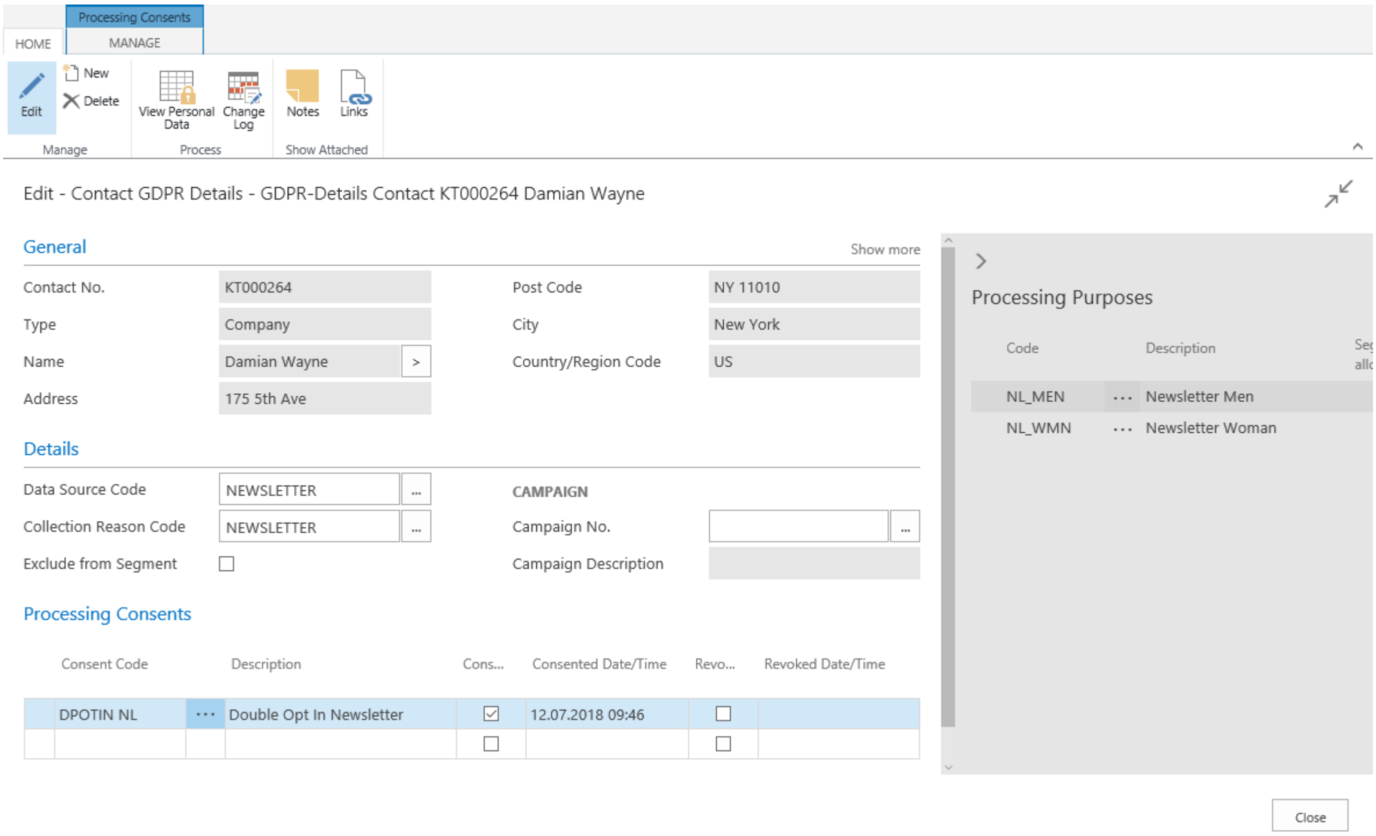
If the user creates a new contact, the time for which the data for this contact is to be retained/saved is defined as soon as the contact is created. During creation, the table specifications from the data structure setup are interpreted and a planned action date as the action type (delete or make anonymous) are determined and inserted in the "Planned actions" table. In addition, a link is created with the reference to this entry in the table and displayed to the contact - this link establishes a connection between the contact and the planned action (in this case "Delete").



The links are created for the client type defined in the GDPR Setup.

GDPR Details

The GDPR relevant contact details are provided as a separate page in the form of the "GDPR Details" campaign on the contact card.



This page shows some information about the contact itself (name, address,...). The "Exclude from segment" field is also displayed here and synchronized with the contact card. In addition, the origin of the data can be defined in the information register "Data origin" in the form of a data origin code and due to the setting in the data origin code campaign, also an origin campaign.

The data processing consents for this contact can be documented in the data processing consents register. The "Agreed" indicator documents the corresponding processing purposes in the "Processing purposes" info box. Should a contact revoke the data processing consent, the processing purposes will be removed automatically. If overlapping processing purposes have been defined in different consent declarations, the data record will only be removed in the Processing Purposes infobox if all corresponding consent declarations have been revoked.

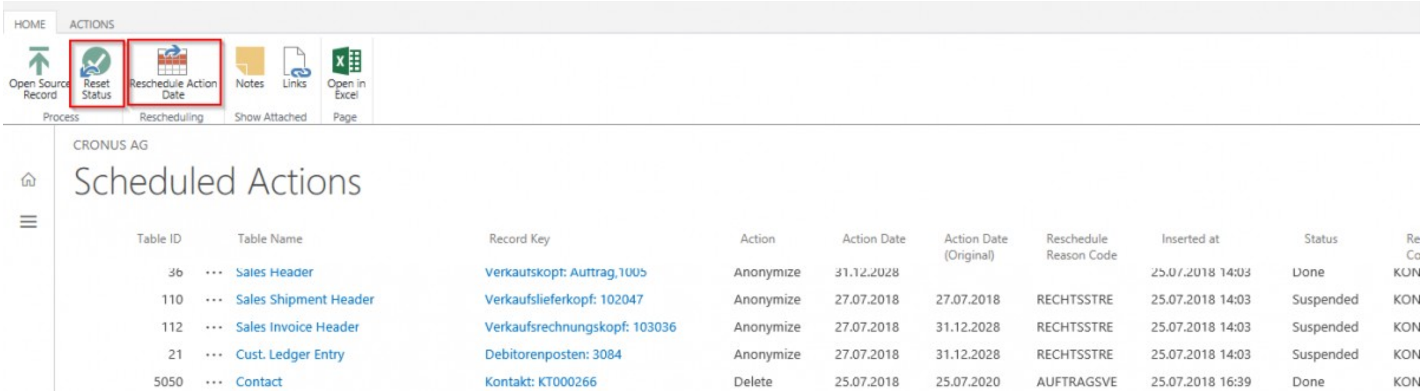
With the action "View Personal Data" the personal data of the contact and the corresponding data structure, in which the table "Contact" is contained, can be called up directly from this view. If the change log is activated for the table "DSGVO-Details", you can use the action "Change log" to view the logged changes for this contact.

Customer Creation

The creation of the customer is entered according to the same principle as for the contacts link and a data record in the planned actions of the GDPR Toolbox. In this example, the function "Create as customer" was used for a company contact.

Scheduled Actions

With the link on the data set you can call up the scheduled actions for this data set - alternatively the planned actions can also be called up directly from the menu of the GDPR Toolbox.



In this view, it is possible to reset the status "Suspended" to "Waiting" so that the check can be carried out again in "Create suggestions". You can also specify the postponement and a newly planned date for the "Delete/anonymize" action and a reason from the "New Reschedule Reasons" table.

This table also forms the basis for the creation of proposals to carry out the actions for deleting/anonymizing the data records. These suggestions are used in the GDPR Toolbox to monitor the planned actions and that the user has the possibility to check and override the results or the execution, based on the settings at the table defaults, before executing the action.

Automatically update scheduled actions

The scheduled actions can also be updated using the job queue. The entry and the call of the job queue item can be reached from the DSGVO Toolbox setup. In addition to this activation, the subsequent update must be activated in the corresponding table defaults (tab " Scheduled action ").

The indicator "Manual scheduled actions" defines that the planned actions are updated downstream. To be able to select this option, an integer field for the update (update progress) must exist in the respective table and be created if necessary. For details see GDPR Toolbox Customization.

Create an order / post a delivery and invoice

An order, a posted delivery and a posted invoice are created from the customer. For the tables of the posted documents, you have defined in the table specifications for the data structure that these documents are to be made anonymous.

Scheduled Actions

Table ID		Table Name	Record Key	Action	Action Date	Action Date (Original)	Reschedule Reason Code	Inserted at	Status	Record Code
5050	···	Contact	Kontakt: KT000267	Delete	30.07.2020			30.07.2018 06:58	Waiting	CONT
18	···	Customer	Debitor: D00070	Anonymize	01.01.2021	31.12.2018	LITIGATION	30.07.2018 07:02	Waiting	CONT
5054	···	Contact Business Relation	Kontakt Geschäftsbeziehung: KT000267,...	Delete	30.07.2020			30.07.2018 07:02	Waiting	CONT
36	···	Sales Header	Verkaufskopf: Order,1007	Anonymize	31.12.2028			30.07.2018 07:02	Done	CONT
110	···	Sales Shipment Header	Verkaufslieferkopf: 102049	Anonymize	31.12.2028			30.07.2018 07:26	Waiting	CONT
112	···	Sales Invoice Header	Verkaufsrechnungskopf: 103038	Anonymize	31.12.2028			30.07.2018 07:26	Waiting	CONT
21	···	Cust. Ledger Entry	Debitorenposten: 3089	Anonymize	31.12.2028			30.07.2018 07:26	Waiting	CONT
5050	···	Contact	Kontakt: KT000268	Delete	30.07.2020			30.07.2018 08:17	Waiting	CONT

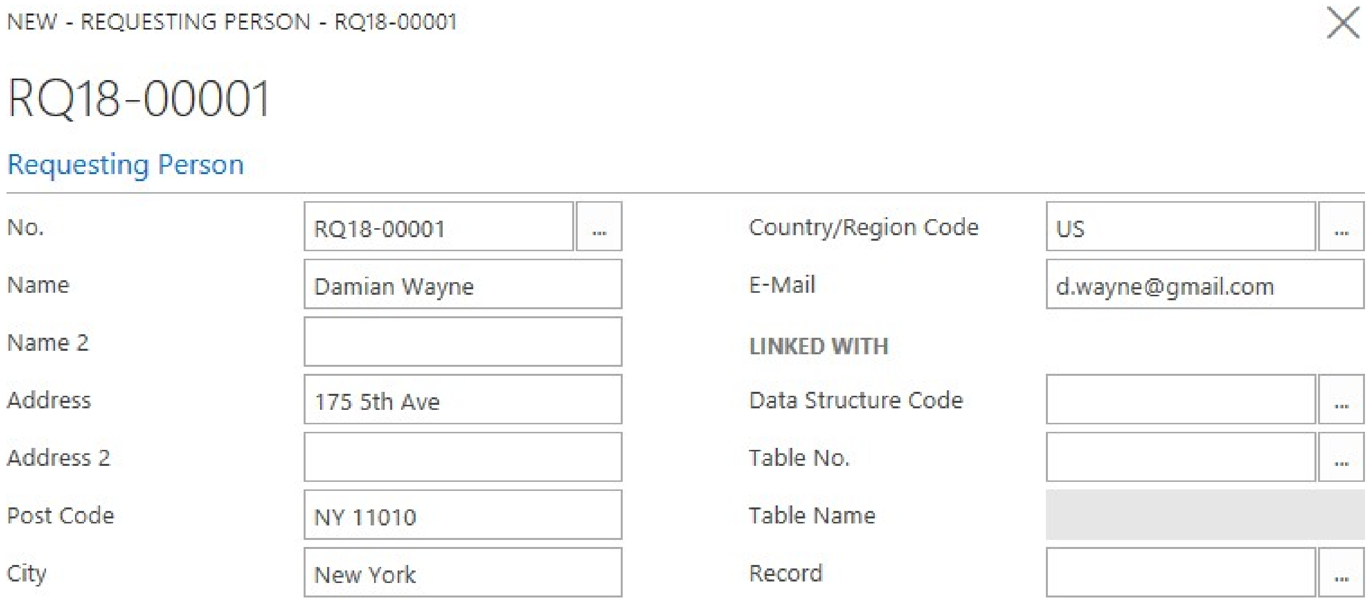
Request from concerned persons

With the GDPR, private individuals have more rights to the stored data and can make inquiries to companies and public authorities and request information about the stored information. The administration and documentation of these requests are supported by the GDPR Toolbox. The following rights of the data subjects are supported:

- Information - right to information
- Correction - right to correction
- Export - right to data transferability
- Delete - right to delete stored data

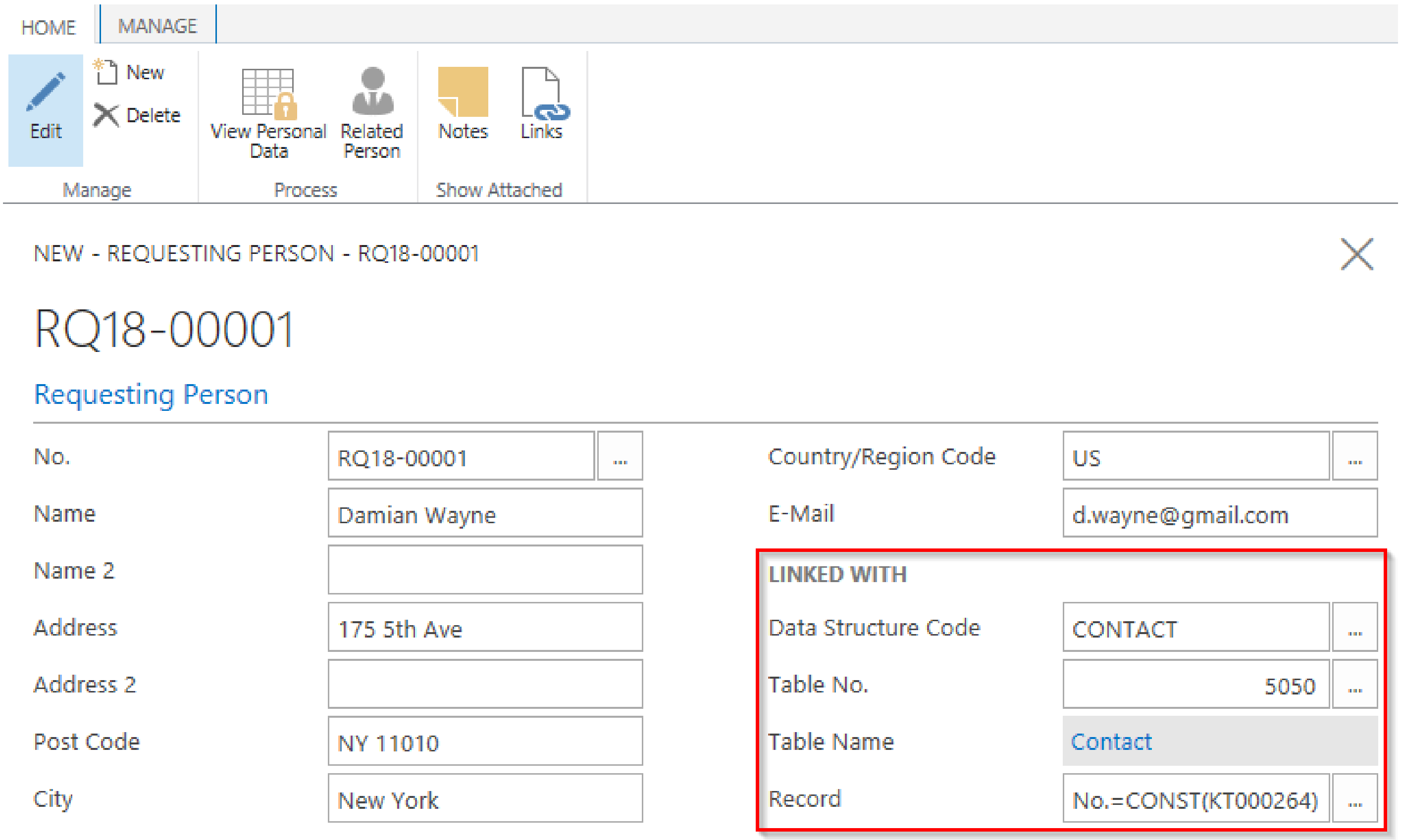
Creation of the requesting person

The inquiries of the persons concerned are filed in the "Requesting Persons" section. First, the name, address and communication information of the person making the request is recorded.



Link to master data

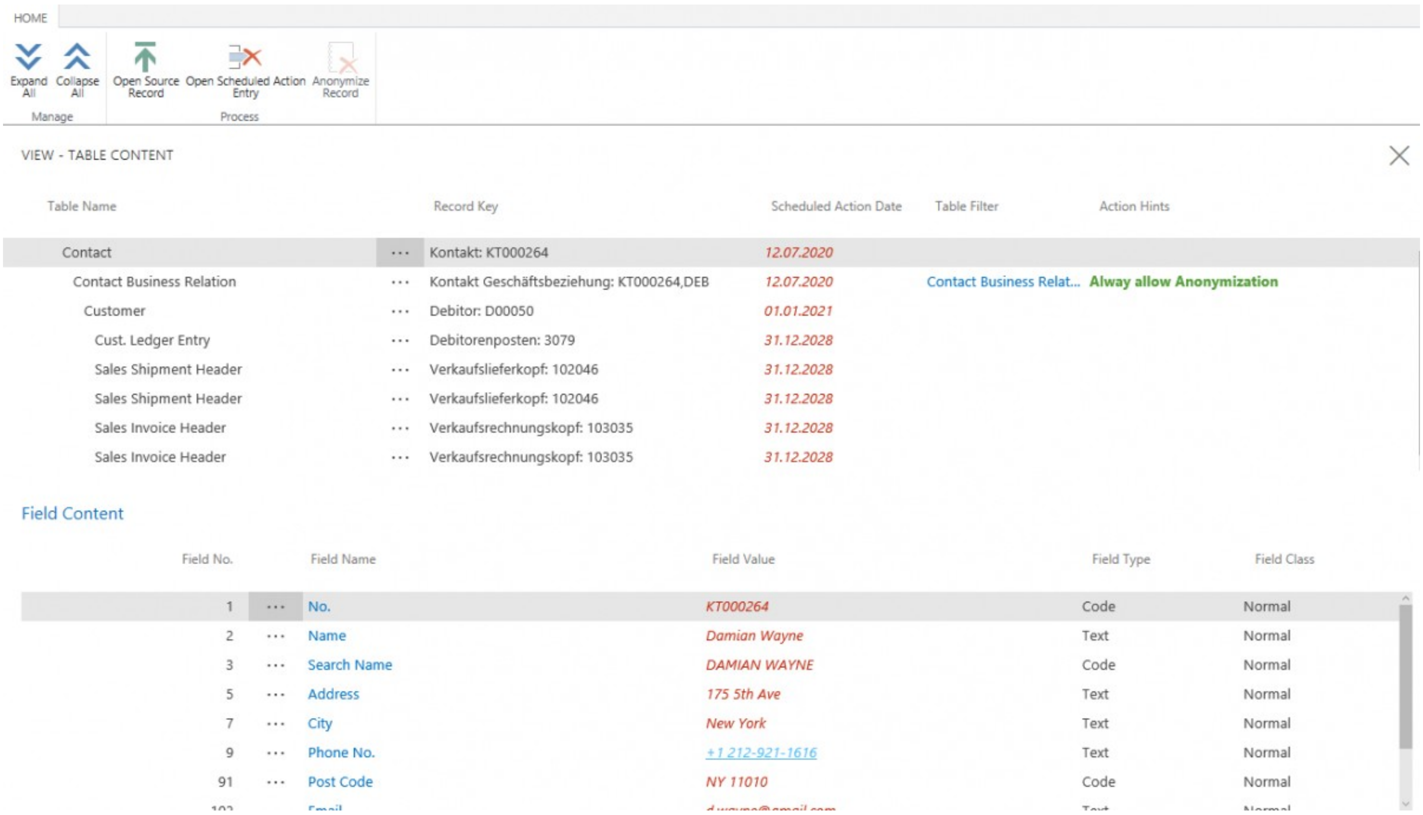
In addition, a reference must be established between the requesting person and the respective master data record. For this purpose, the "Linked to" area is provided in the map view for the person making the request. First you have to decide for a data structure, based on this corresponding example structure you have to define whether the inquiring person is a contact, employee or a resource (e.g. a service provider). You can select the corresponding data structure and store it in the field *Data structure code*.



In the data structure, links can be defined at different levels, for example at contact, customer or vendor level. The tables allowed for selection are defined in the table specifications in the data structures ("Allow table for query" field). In the above example of a request, the "Contact" table was defined as a reference to the master data. In the field *Data set* the corresponding number of the contact can be selected.

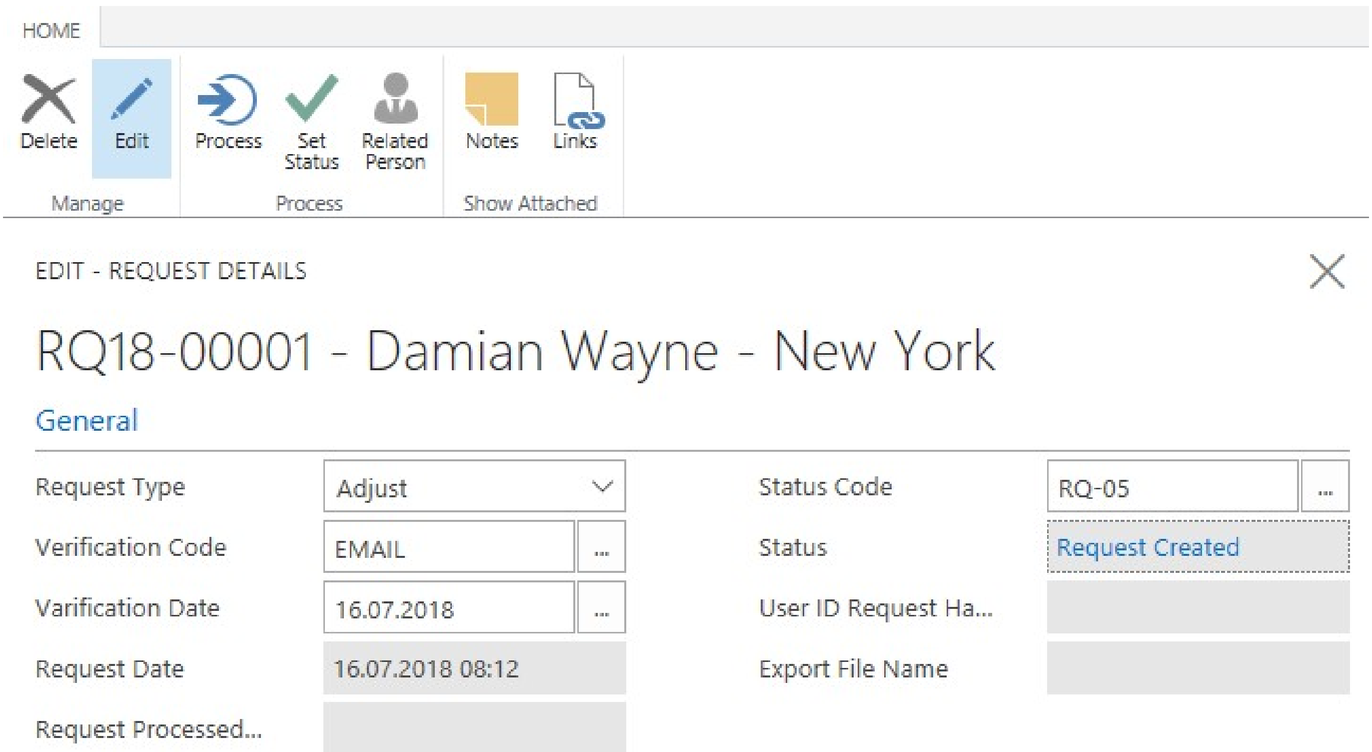
Note: The assignment of the data level in the form of the table number is relevant for the subsequent processes such as information and export of personal data. Only data for the underlying tables of the data structure is taken into account, that is, if a query is to be linked and contacts are used, the contact table and the contact number must also be specified and access at customer level must not be selected, otherwise the contact data is ignored.

Once the links have been defined, you can use the "Personal data" action to obtain an overview of the stored information in accordance with the defined data structure and the initial table.



Include request

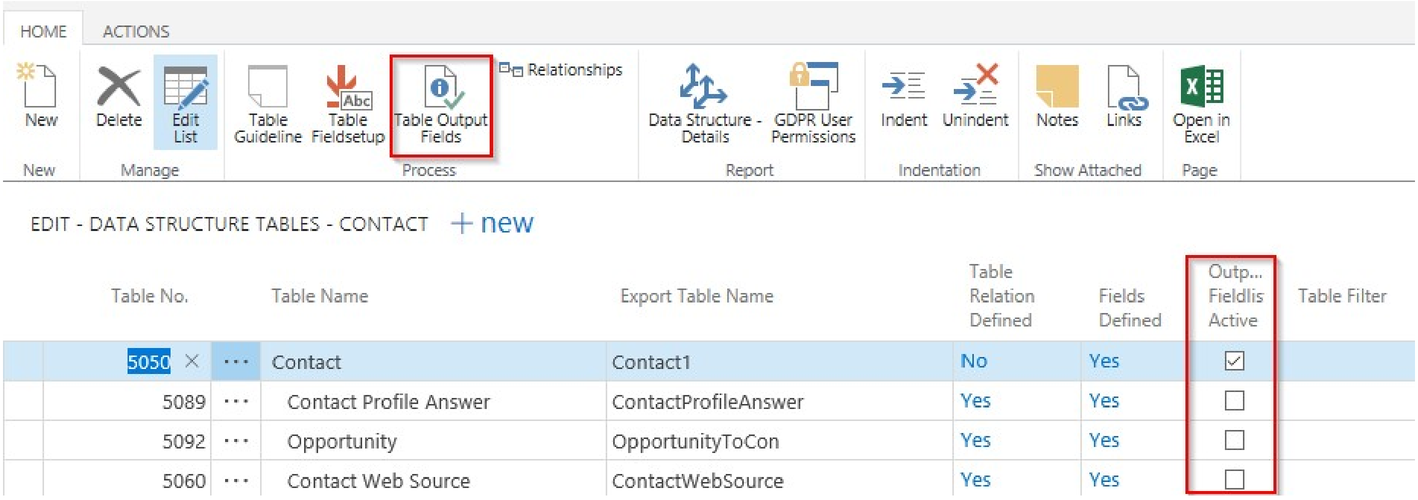
In the lower part of the inquiry one or more requests of the inquiring person can be recorded. It can also be used to document whether and when the person has already made inquiries in the past. New calls can be entered via the "New line" button in the Requests group in the ribbon.



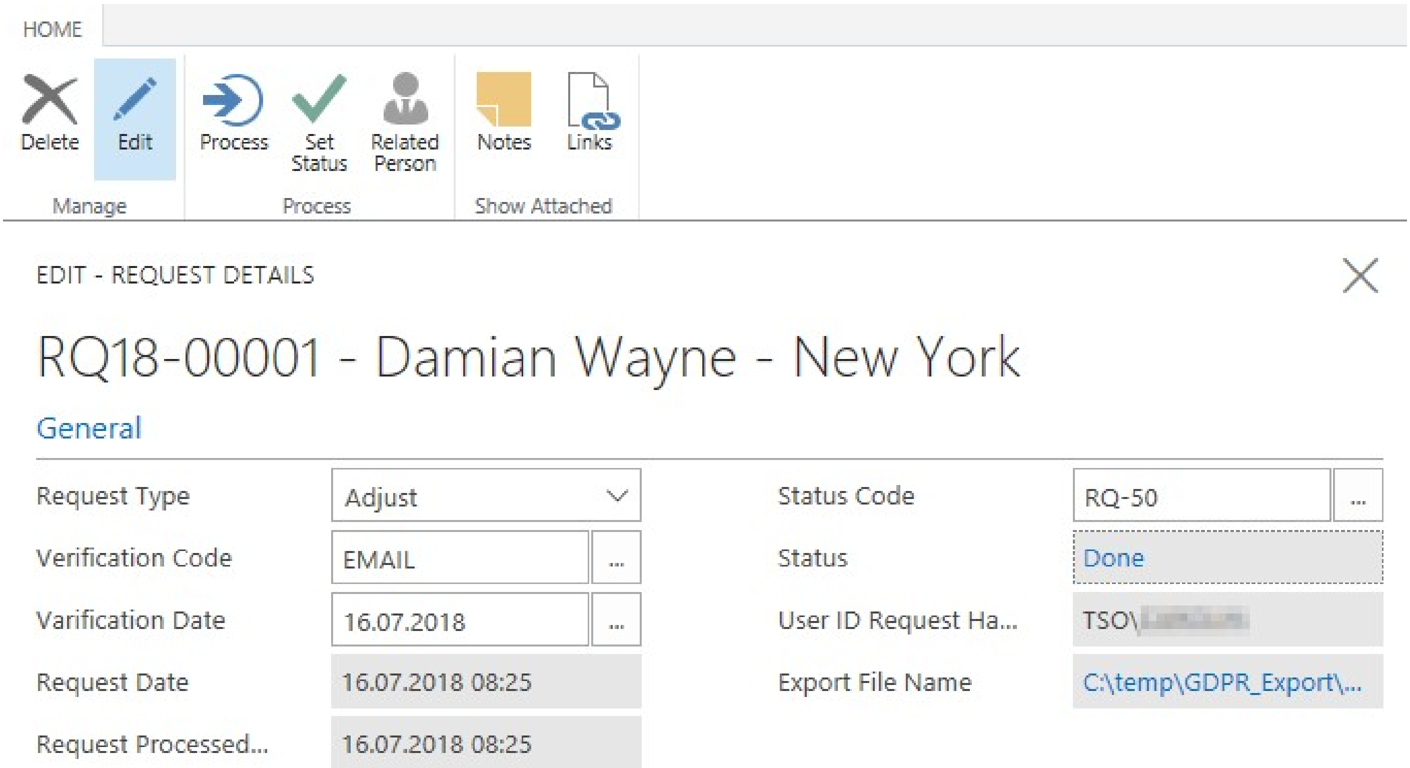
With the field Request type, the request type can be classified into a group for the rights of the requesting person. The request type also controls the executed "Process" function. With the verification code and the verification date, proof of the identity of the person making the request can be documented. In addition, a status for the status of processing can be selected from the "Request status" table. Depending on the selected status, the request is displayed in the corresponding stack of the role center.

Right to information

The Requesting person has a right to information about the stored data. This right is represented in the GDPR Toolbox by a report that determines and outputs the tables and field contents according to the data structure and this report can be made available to the inquiring person in the form of a PDF. If you want to override this standard setting - that is, you want to display even more data or, if necessary, less data - you can solve this problem with an additional field list "Output Field List" in the Data Structure Table. As soon as data is contained there, the standard is overridden. The change is displayed in the data structure using the "Output Fieldlist Active" indicator.



In the request for the person concerned, the request type "Information" is selected and the corresponding report is created using the "Process" action and a link to this report is provided in the field *Export file name*.



The file is then sent manually, e.g. by e-mail. In the view Request details you can set a manual status using the available actions "Set status" or branch to the assigned master data record via Linked person. The "Process" action has already automatically set the corresponding status from the field *Done Status Code* of the GDPR institution.

The report on the stored data on the person making the request contains the fields defined in the assigned data structure (field list).

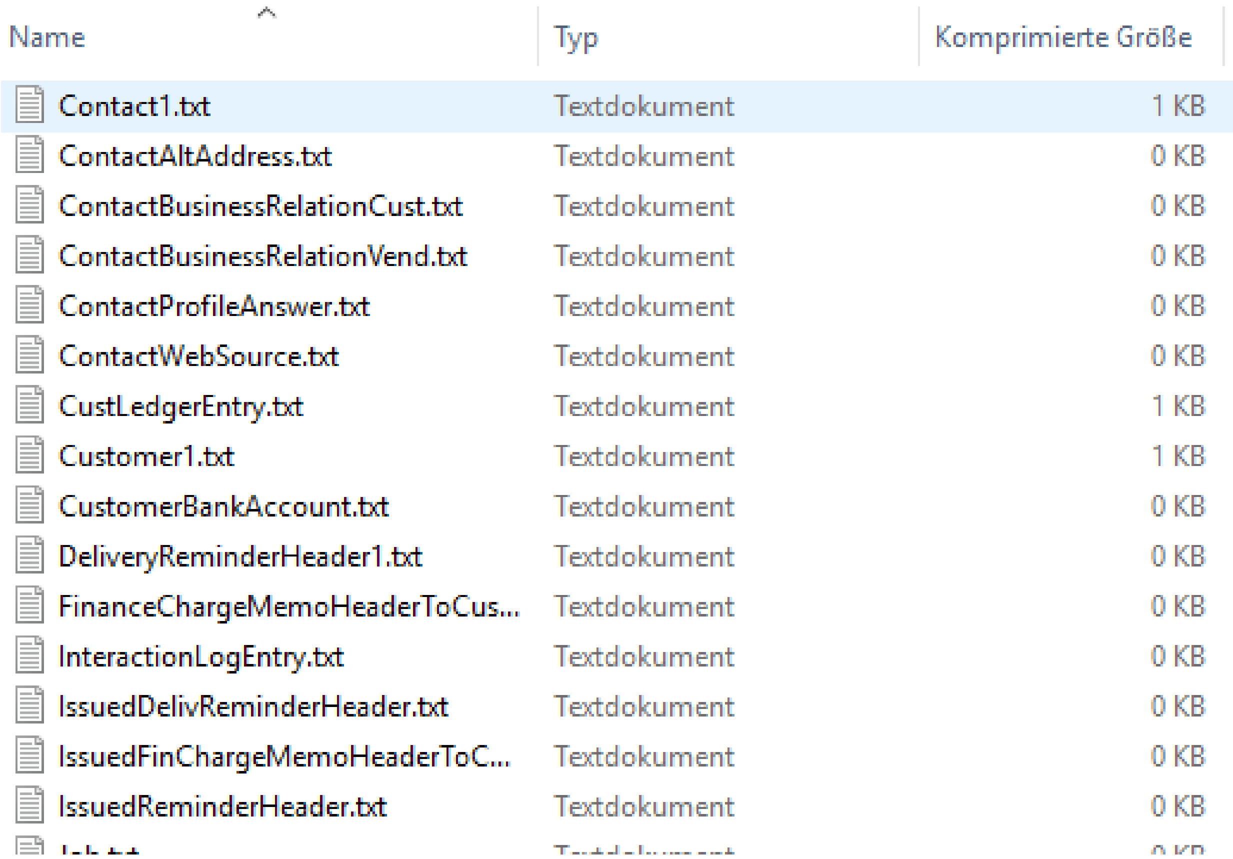
Personal Data - Request - List
CRONUS AG (EN)

Montag, 16. Juli 2018
Page 1

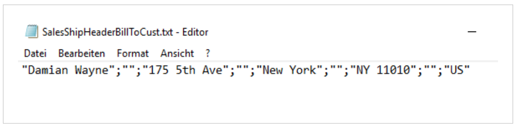
Contact	Table Record ID	Field Name	Field Value
Sales Shipment Header	102046	Bill-to Address	"175 5th Ave"
		Bill-to City	"New York"
		Bill-to Contact No.	"KT000264"
		Bill-to Country/Region Code	"US"
		Bill-to Name	"Damian Wayne"
		Bill-to Post Code	"NY 11010"
		Sell-to Address	"175 5th Ave"
		Sell-to City	"New York"
		Sell-to Contact No.	"KT000264"
		Sell-to Country/Region Code	"US"
		Sell-to Customer Name	"Damian Wayne"
		Sell-to Post Code	"NY 11010"
		Ship-to Address	"175 5th Ave"
		Ship-to City	"New York"
		Ship-to Country/Region Code	"US"
		Ship-to Name	"Damian Wayne"
		Ship-to Post Code	"NY 11010"
Sales Invoice Header	103035	Bill-to Address	"175 5th Ave"
		Bill-to City	"New York"
		Bill-to Country/Region Code	"US"
		Bill-to Name	"Damian Wayne"
		Bill-to Post Code	"NY 11010"
		Sell-to Address	"175 5th Ave"
		Sell-to City	"New York"
		Sell-to Country/Region Code	"US"
		Sell-to Customer Name	"Damian Wayne"
		Sell-to Post Code	"NY 11010"
		Ship-to Address	"175 5th Ave"
		Ship-to City	"New York"
		Ship-to Country/Region Code	"US"
		Ship-to Name	"Damian Wayne"
		Ship-to Post Code	"NY 11010"
Cust. Ledger Entry	3079	Description	"Order 1004"
Customer	D00050	Address	"175 5th Ave"
		City	"New York"
		Country/Region Code	"US"
		Email	"d.wayne@gmail.com"
		Name	"Damian Wayne"
		No.	"D00050"
		Phone No.	"+1 212 [illegible] 1616"

Right to transfer

The data subject is granted the right to transfer data under the GDPR. This right is represented in the query details by the query type "Export". When the request is processed, the data is exported in the form of a CSV file and all tables with the corresponding data and fields from the specified data structure are taken into account and stored as a zipped text file. Alternatively, the setup in the output field list is also taken into account here (see above). This data can then be made available to the inquiring person.



The format for exporting the data has not been defined yet in the GDPR, so the fields are exported as CSV in the order of the field list.



The used file names are created according to the table name and can be adapted in the data structure in the column *Export table name*.

Right to correction

The concerned person also has the right, that the stored data will be corrected. This right is represented by the request type "Correction". The correction requests can be varied, so that the actual correction takes place, for example, via the master data. The possibility of changing posted documents does not exist and is also not permitted due to the guidelines for storage. The correction is supported by

- the call of the linked person
- manual correction of data
- the documentation of the correction by describing the changes in the notes and possibly links to the request details
- the status for processing the corrections

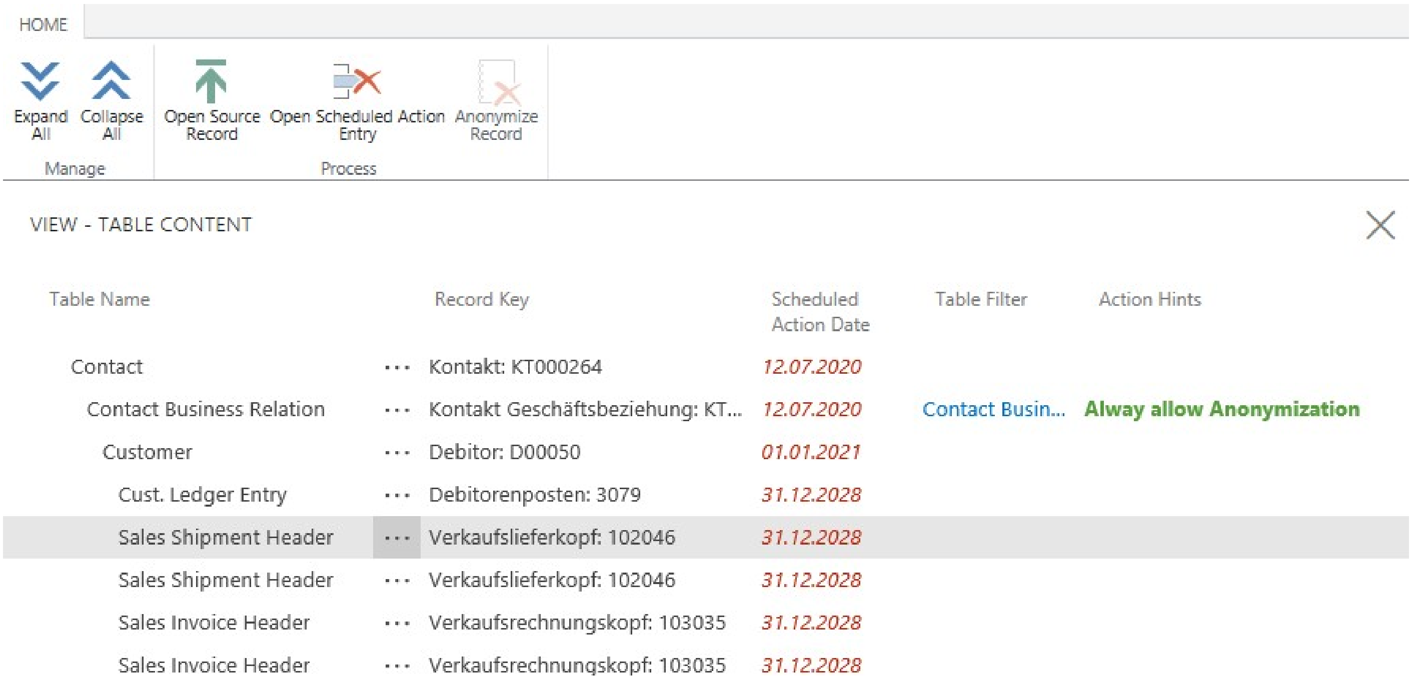
The action "Process" sets a corresponding information in the form of a PDF file and sets the status of the corresponding request. In this case, the report is to be understood as documentation and can be sent to the person concerned for correction.

Right to delete

The rights of the GDPR also provide for the deletion of personal data. In principle, you cannot always comply with this right, because there are different, competing requirements for this right, such as the retention periods for booked documents. The corresponding intervals and action dates are set up using the table specifications of the data structure. For this institution, the deadlines are to be chosen in such a way that both the requirements of the GDPR and the retention periods are met. In this demo scenario, we have therefore provided for the "Posted sales invoices" table to be stored for 10 years as a non-legally binding example. As an alternative to deletion, the function Anonymize can also be used in the GDPR Toolbox. In contrast to the deletion of data records, the defined fields are overwritten with anonymizing default values when data records are made anonymous.

If data records are to be deleted, not some selective data records are removed from the tables, but all data of the entire structure for a master data record is always deleted or made anonymous. The planned actions form the basis for checking whether deletion/anonymization is possible. If the date for the execution of the deletion/anonymization is exceeded in all planned actions, the corresponding deletions/anonymizations can be executed.

For the request of a person concerned, this means that the request for deletion can only be met if the corresponding date in all linked data records of the data structure also permits deletion/anonymization. Users of the GDPR Toolbox can call up the stored personal data of the inquiring person directly from the inquiring person ("View Personal Data" action) and determine whether deletion is already possible via the "Scheduled action date" column.



If the detail data allows deletion, a corresponding entry is inserted in the proposed actions when you execute the "Process" action. If deletion is not possible, this can be stored in the notes and the person making the request can be informed.

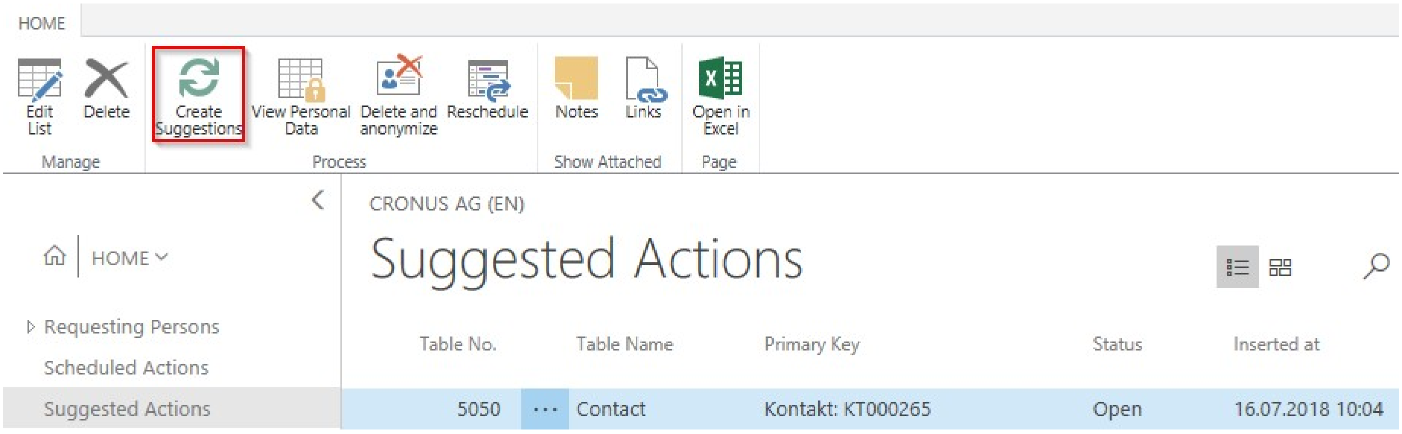
Suggestions for deleting/anonymizing

In the "Proposed actions" of the GDPR Toolbox, the master data intended for deletion or anonymization are inserted. The proposed actions are updated from this view with the action "Create proposals". A fully automated deletion is currently not yet planned and the deletion or anonymization of the corresponding data takes place in two phases:

1. Make suggestions for deleting and anonymizing
2. Execution of the proposed actions for delete/anonymize

Create Suggestions

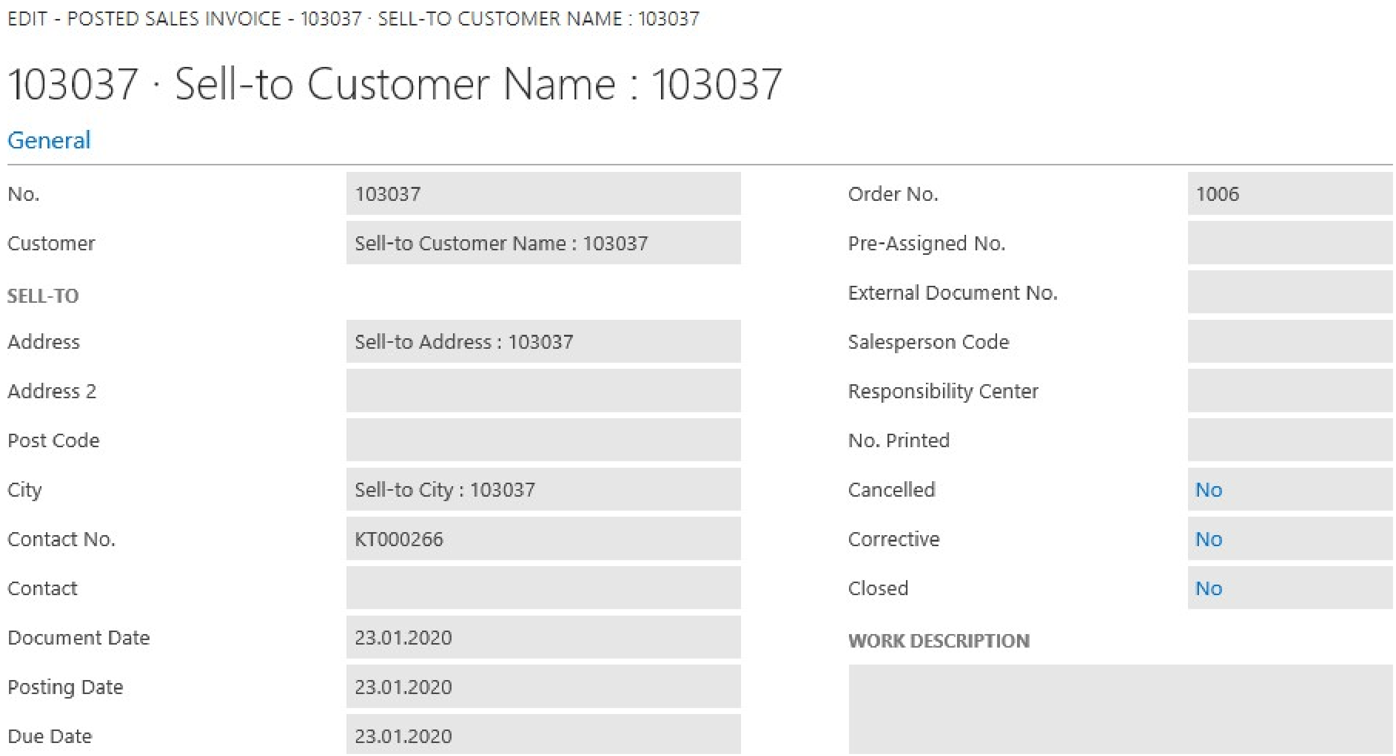
The function of the same name for creating proposals checks whether the corresponding action date for deleting/anonymizing has been reached for an unchecked data record and then determines all associated data records based on the data structure and checks whether the corresponding action date has been reached or already exceeded. If all other data records are also allowed for deletion/anonymization, a corresponding master data entry according to the data structure at the highest level, e.g. contact, is proposed in the proposals.



The corresponding proposals can be checked using the "Personal data" action or, alternatively, the corresponding date for the execution of the action can be postponed. To avoid unwanted deletions and anonymization, it is strongly recommended to check the proposals. The rules for deleting and anonymizing are defined in the data structure, the table specifications, the relations and the field list. If several data records are to be processed simultaneously, you can select the desired rows and then execute the action.

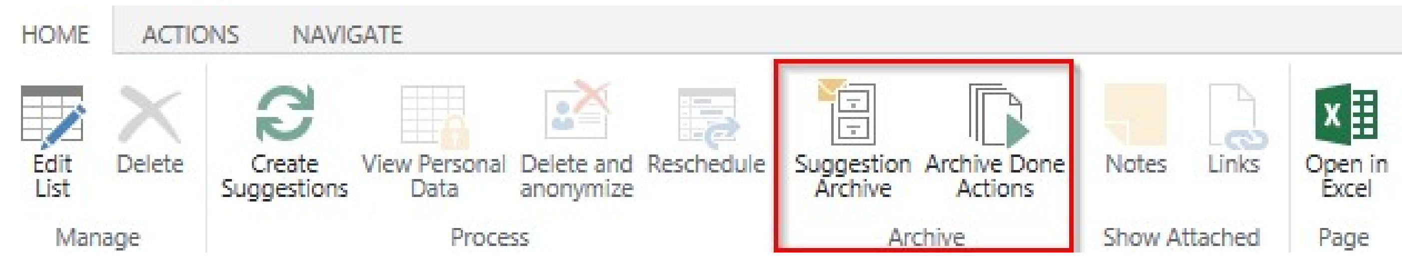
Delete and Anonymize

Based on the proposals created and the checks performed, the user can decide that the planned actions should be performed. The "Delete and make anonymous" action can be used to either delete the data records from the database or make the fields anonymous according to the defined field list. The following is an example of an anonymous sales invoice - the corresponding field contents are displayed with the field name and the reference to the primary key.



Archiving

If the suggested actions have been processed according to their settings, they are automatically archived and can be viewed via the menu item "Suggestion Archive". In case of an update of the GDPR Toolbox from an older version, which did not contain this archiving yet, the archiving can be done manually via "Archive Done Actions".



GDPR actions for historical data

For the historical data you can create the planned actions with the help of the batch processing "Create actions from historical data" in the menuband of the GDPR institution. Note that the determination of the action date must be created depending on the field contents of the respective tables - for example, a posted invoice with the posting date 03/15/2013 could be made anonymous as of 12/31/2023. The corresponding definition for the baseline date for calculating the action date is stored in the table specification in the field *Planned action date (field number)*. If no field is specified in the table specifications, field *Planned action date (field number)*, the current date is used as the base date for the cost estimate.

In the table specifications you can define whether the scheduled actions are to be created immediately, i.e. when the data record is created or alternatively downstream. The advantage of downstream creation, particularly for tables with many data records, is that the job queue data writes the transaction and the data to the database at defined intervals or depending on the number of data records processed using the "Commit by number of data records" parameter, closes the transaction and starts a new transaction. This avoids locks on tables. The batch processing described above creates the scheduled actions within a database transaction for all tables and all data records, which can lead to locks when processing many data records. Details of the setup for the downstream actions can be taken from the table specifications in the Setup area.

User Permissions

For the documentation of access rights in the course of the implementation of the GDPR, a report is available which evaluates user access to the tables with personal content across data structures. This report can be accessed directly from the GDPR Toolbox role center.

GDPR User Permissions - List
CRONUS AG (EN)

Mittwoch, 1. August 2018
Page 1

Table No.	Table Name	User Name	Read Permission	Insert Permission	Modify Permission	Delete Permission	Execute Permission
0		TSO\	Yes	Yes	Yes	Yes	Yes
18	Customer	TSO\NAVRECHTE	Yes	Indirect	Indirect		
21	Cust. Ledger Entry	TSO\NAVRECHTE	Indirect	Indirect	Indirect		
23	Vendor	TSO\NAVRECHTE	Yes	Indirect	Indirect		
36	Sales Header	TSO\NAVRECHTE	Yes	Indirect	Indirect		
38	Purchase Header	TSO\NAVRECHTE	Yes	Indirect	Indirect		
110	Sales Shipment Header	TSO\NAVRECHTE	Indirect		Indirect		
112	Sales Invoice Header	TSO\NAVRECHTE	Indirect		Indirect		
114	Sales Cr.Memo Header	TSO\NAVRECHTE	Indirect				
120	Purch. Rcpt. Header	TSO\NAVRECHTE		Indirect			
122	Purch. Inv. Header	TSO\NAVRECHTE	Indirect				
156	Resource	TSO\NAVRECHTE	Yes				
167	Job	TSO\NAVRECHTE	Yes				
222	Ship-to Address	TSO\NAVRECHTE	Yes	Indirect	Indirect		
287	Customer Bank Account	TSO\NAVRECHTE	Yes				
5050	Contact	TSO\NAVRECHTE	Yes	Indirect	Indirect		
5051	Contact Alt. Address	TSO\NAVRECHTE	Yes				

The report evaluates the access rights based on the Users and Access Rights tables at the TableData level. The relevant tables are determined from the table specifications of all data structures.

GDPR Toolbox Customization

This article describes the possibilities to extend the DSGVO-Toolbox by individual customizations and thus special requirements in combination with the use of industry solutions or customer customizations. This article contains information that is primarily relevant for Business Central/NAV developers.

The described adjustments and entry points are provided in the NAV versions 2016 and higher and Business Central, in the form of events/subscribers. Starting with NAV version 2015 and lower, these enhancements are provided as "function calls".

Create the scheduled actions

The "scheduled actions" are created or changed in the course of the "Insert/Delete/Rename Trigger" and possibly (depending on the configuration) also during the processing of the "Modify Trigger". In order to enable individual rules for the creation of "scheduled actions", the codeunit "Cust. Scheduled Action Mgt. (ID 5459720)" can be used.

Here different functions (3 each) are available for Insert, Modify, Delete and Rename transactions. Below are the three functions provided for the "Insert Trigger":

```
Documentation()...
OnRun()...
LOCAL [EventSubscriber] HandleOnBeginInsertScheduledActionEntry(RecRef : RecordRef;TableGuideline : Record "Table Guideline";VAR ScheduledActionEntry : Record "Scheduled Acti
// The event is triggered when the data record (RecRef) is inserted. Control the influence on ScheduledActionEntry before the standard logic is executed,
// disable complete standard logic by setting Handled to TRUE

LOCAL [EventSubscriber] HandleOnBeforeInsertScheduledActionEntry(RecRef : RecordRef;TableGuideline : Record "Table Guideline";VAR ScheduledActionEntry : Record "Scheduled Act
// The event is triggered before the ScheduledActionEntry.Insert command is executed.

LOCAL [EventSubscriber] HandleOnAfterInsertScheduledActionEntry(RecRef : RecordRef;TableGuideline : Record "Table Guideline";VAR ScheduledActionEntry : Record "Scheduled Acti
// The event is triggered after the ScheduledActionEntry.Insert command is executed.

LOCAL [EventSubscriber] HandleOnBeginModifyScheduledActionEntry(RecRef : RecordRef;VAR ScheduledActionEntry : Record "Scheduled Action Entry";VAR Handled : Boolean)...
LOCAL [EventSubscriber] HandleOnBeforeModifyScheduledActionEntry(RecRef : RecordRef;VAR ScheduledActionEntry : Record "Scheduled Action Entry")...
LOCAL [EventSubscriber] HandleOnAfterModifyScheduledActionEntry(RecRef : RecordRef;VAR ScheduledActionEntry : Record "Scheduled Action Entry")...
LOCAL [EventSubscriber] HandleOnBeginDeleteScheduledActionEntry(RecRef : RecordRef;VAR ScheduledActionEntry : Record "Scheduled Action Entry";VAR Handled : Boolean)...
LOCAL [EventSubscriber] HandleOnBeforeDeleteScheduledActionEntry(RecRef : RecordRef;VAR ScheduledActionEntry : Record "Scheduled Action Entry")...
LOCAL [EventSubscriber] HandleOnAfterDeleteScheduledActionEntry(RecRef : RecordRef;VAR ScheduledActionEntry : Record "Scheduled Action Entry")...
LOCAL [EventSubscriber] HandleOnBeginRenameScheduledActionEntry(RecRef : RecordRef;VAR ScheduledActionEntry : Record "Scheduled Action Entry";VAR Handled : Boolean)...
LOCAL [EventSubscriber] HandleOnBeforeRenameScheduledActionEntry(RecRef : RecordRef;VAR ScheduledActionEntry : Record "Scheduled Action Entry")...
LOCAL [EventSubscriber] HandleOnAfterRenameScheduledActionEntry(RecRef : RecordRef;VAR ScheduledActionEntry : Record "Scheduled Action Entry")...
```

The event for the subscriber "HandleOnBeginInsertScheduledActionEntry" is executed at the beginning of the standard function for inserting the "scheduled actions". At this point it is possible to intervene before the standard code is executed. The parameter "Handled" can be used to define whether the standard code is to be executed afterwards or whether the standard call is to be terminated with an EXIT.

The event for the subscriber "HandleOnBeforeInsertScheduledActionEntry" is executed immediately before the insert into the table "Scheduled Action Entry". The event for the subscriber "HandleOnAfterInsertScheduledActionEntry" is executed immediately after the insert into the table "Scheduled Action Entry".

For the provided functions, the data record (RecRef), the table specifications of the data structure (Table Guideline), the Scheduled Action Entry and, depending on the function, a base date for the calculation of the action date can be passed as parameters. In addition to influencing the "planned action", the effects on the actual data, e.g. in connection with an intercompany logic, can also be mapped here.

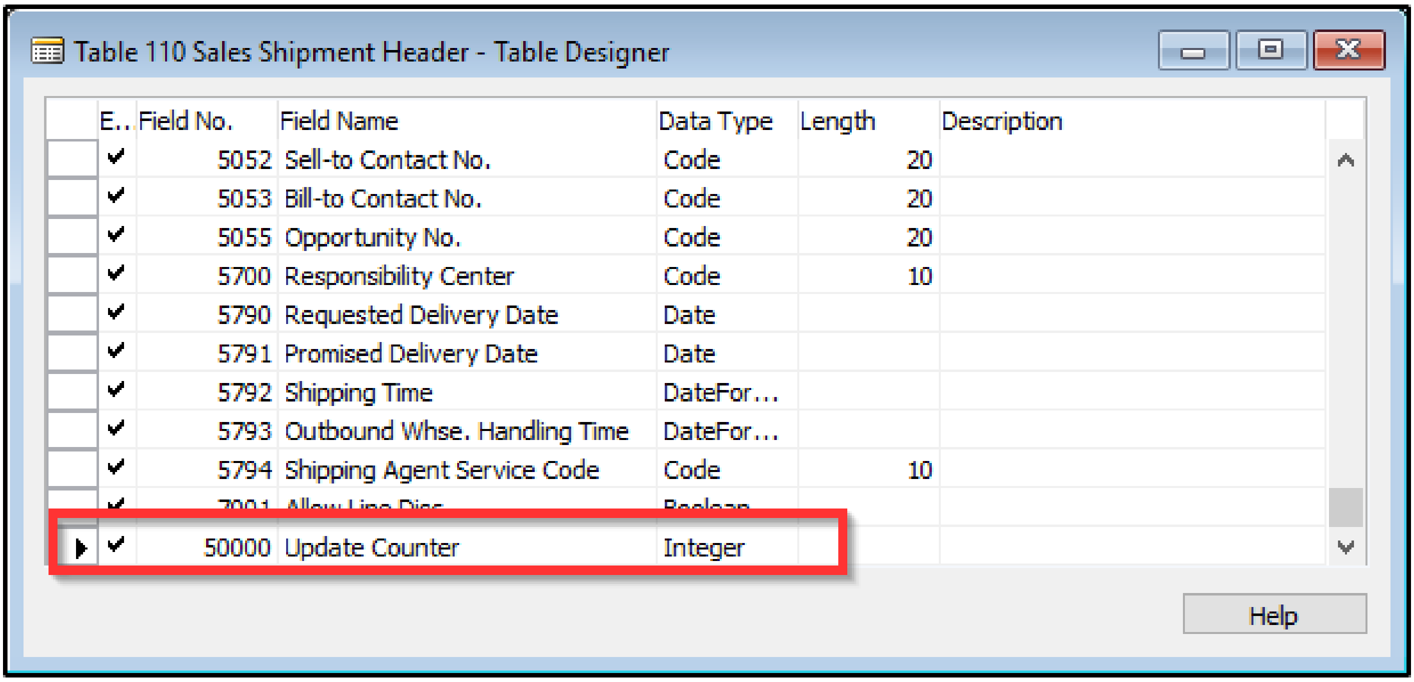
Update scheduled actions via the job queue

The scheduled actions can also be updated using the job queue. The entry and the call of the job queue item can be reached from the DSGVO Toolbox setup. In addition to this activation, the subsequent update must be activated in the corresponding table guidelines (tab " Scheduled action ").

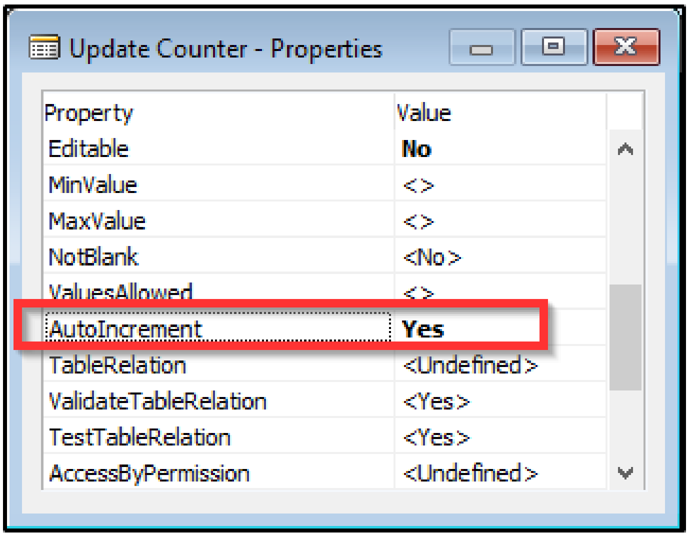
The " Manual Scheduled actions" indicator defines that the scheduled actions are no longer created (or possibly updated) in the "OnInsert" tab of the data record, but are added later. To be able to select this option, an integer field for the update (update progress) must exist in the respective table and be created if necessary. In addition, an index must exist for this field.

Note:' A developer license is required to create the field and the index! Without a corresponding integer field and an index for this field, this option cannot be used.

Below we have created the corresponding field for the Sales Delivery Header table as follows:

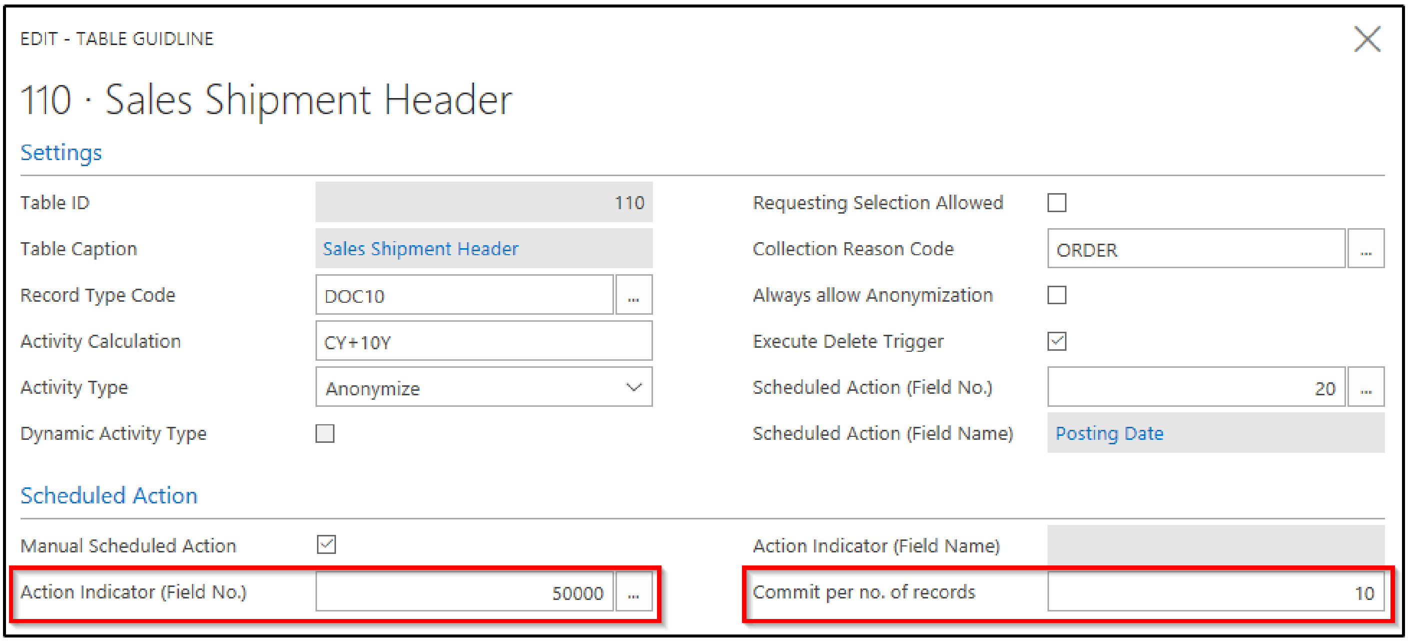


In this example we have decided to use an AutoIncrement in the properties of the field, because in this example the option "Move action" is not used.



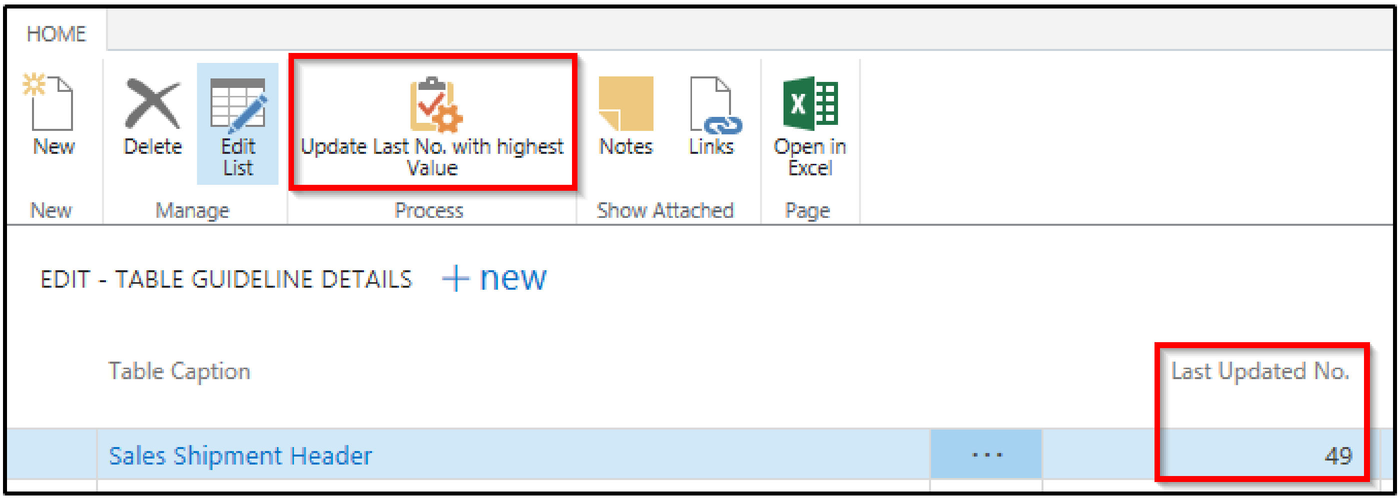
If you want to use the option "Move action" and want to influence the creation of the scheduled actions there depending on the field contents, it can be useful to implement your own business logic for updating the field, which then updates this counter each time a data record is updated.

In addition to specifying the field for identifying the scheduled actions to be created (field), you can also use a commit ("Commit per" field) depending on the number of processed data records.



By specifying a value in the Commit by Number of Records field, you can avoid table locking for large update actions. The corresponding progress or counter value for the last record processed can be viewed with the "Update details" action.

Here you can also generate the last updated entry if you activate it later.



Delete and Anonymize

Many customers use industry-specific solutions. These require special procedures for the processing of planned deletions and anonymizations, for example in connection with intercompany processes.

In order to be able to implement these special features centrally, the code unit "Cust. Deletion Mgt." (ID 54597). (ID 5459721) has been made available. The following functions are available:

```
Documentation()

OnRun()

LOCAL [EventSubscriber] HandleOnBeforeDeleteRecord(VAR RecRef : RecordRef;VAR Handled : Boolean)
// set Handled to TRUE to ignore standard code

LOCAL [EventSubscriber] HandleOnAfterDeleteRecord(VAR RecRef : RecordRef)

```

The parameter "Handled" can be used in this subscriber to define whether the standard code of the GDPR Toolbox is to be run through after this logic has been executed, or whether the logic implemented here is to consider a completely individual logic.

The special features for anonymizing information in fields can be defined in the code unit "Cust. Anonymization Mgt." (ID 54597). (ID 5459722) can be implemented. Similar functions are available in this code unit:

```
Documentation()

OnRun()

LOCAL [EventSubscriber] HandleOnBeforeAnonymizeField(VAR RecRef : RecordRef;VAR FieldRef : FieldRef;VAR Handled : Boolean)
// set Handled to TRUE to ignore standard code

LOCAL [EventSubscriber] HandleOnAfterAnonymizeField(VAR RecRef : RecordRef;VAR FieldRef : FieldRef)

```

In these functions, the table and the field to be anonymized are passed within a loop according to the field list in the data structure, so that the creation of the field content for anonymization can be influenced here.

Authorizations at object level

Many data structures contain objects that are not assigned the appropriate permissions to modify and delete records in a customer license. Some permissions, primarily to posted document tables, are already assigned in the default objects of the GDPR Toolbox, so these actions are possible for these tables.

A new code unit (ID 5459723 - Cust. Permission Assignmnt.) has been provided to provide customers and partners with a central location for assigning permissions. The following functions are available in this codeunit:

```
Documentation()

OnRun()

LOCAL [EventSubscriber] HandleOnDeleteAndPermissionIsMissing(VAR RecRef : RecordRef;RunDeleteTrigger : Boolean)
RecRef.DELETE(RunDeleteTrigger);

LOCAL [EventSubscriber] HandleOnModifyAndPermissionIsMissing(VAR RecRef : RecordRef)
RecRef.MODIFY;

```

In the standard functions for deleting and changing records, the system checks whether the license or code unit contains the corresponding authorizations for the respective table. If this right is missing, these functions are called and the deletion and modification are moved to this object. The corresponding permissions must then be assigned here or forwarded to separate objects.

Note: In this code unit only limited permissions can be assigned (number of tables is technically limited). The assignment of permissions is only possible with a corresponding developer license.