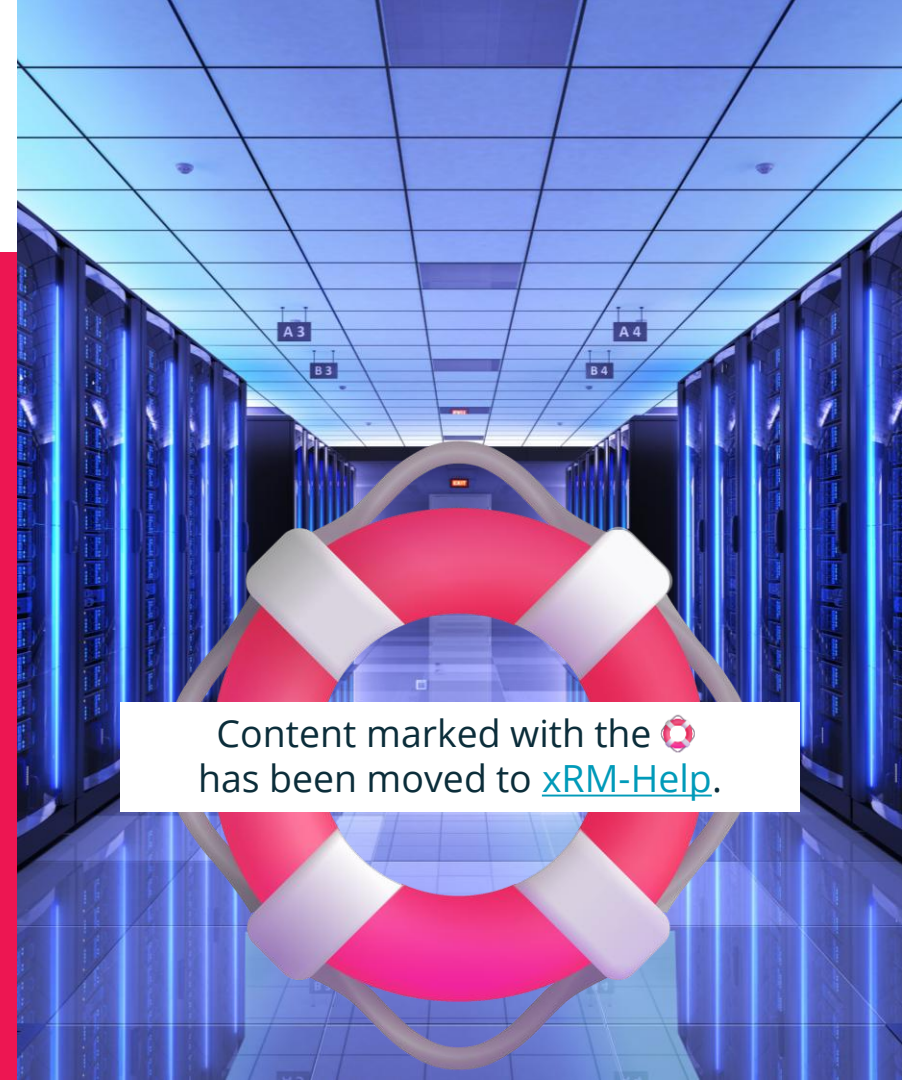




Data protection in the contact person

ADITO Software GmbH

From Version xRM 2026.4.1 | June 2026



Content marked with the 
has been moved to [xRM-Help](#).



Screenshots

The UX design of ADITO is continuously optimized for you. There may therefore be deviations in the screenshots.



Agenda – 1/2

Data protection in the contact person

- [Introduction](#)
-  Data protection for contacts
 -  Collecting privacy-related info
 -  Overview
 -  Record legal basis, intended use, and period of validity
 - [Data protection relevant attributes](#)
 - [Mark attribute as “GDPR relevant”](#)
 -  Record “GDPR relevant” attributes for the contact
-  Documentation of the privacy policy
 -  Upload privacy policy
 -  Update privacy policy
- [Issuance of GDPR-relevant reports](#)
 -  Information report
 - [Disclosure report](#)
 -  CSV export

Agenda – 2/2

Data protection in the contact person

- Delete data
 - Manage deletion indicator
 - Access authorization for the “Data protection administration” Context
 - Create deletion indicator
 - Edit deletion indicator
 - Delete deletion indicator
 - Mark data for deletion
 -  Manually set deletion indicator for contacts
 - Set deletion indicator through a process
 -  Information – who set which deletion indicator and when
 - Delete deletion indicator for contacts
 - Delete/anonymize data
 - Define deletion delay
 - Number of records marked for deletion
 - Deletion/anonymization processes
 - Execute deletion process manually
 - Data to be deleted/anonymized
 - Deletion/anonymization of employee data
 - Overview: Data in the deletion process
 - Search/filter for data “marked for deletion”
 - Search/filter for anonymized data
- System parameters
 - Advertising settings



Introduction

Introduction

Data protection in the contact person

The European Union's General Data Protection Regulation (GDPR) regulates the processing of personal data by private companies and public bodies to ensure the protection of personal data. This regulation has been in force since May 25, 2018, and it is therefore necessary for companies to transparently demonstrate the legal basis on which personal data has been stored, for what purpose, and for how long.



The information contained herein does not constitute a legal opinion under the GDPR and is therefore not legally binding as templates and specifications from ADITO. Please consult the data protection officer responsible for your company if you are planning to use the functionality in your system.

ADITO's data protection features serve

- **data protection compliance** to ensure adherence to internal and legal data protection requirements.
- **efficient data management** to avoid data clutter through automatic link deletion.

In order to be able to automatically delete/anonymize data in compliance with data protection regulations, a deletion flag can be set on the respective data record in ADITO, which is then subjected to a deletion/anonymization process.



The functions can be customized.

Introduction



Data protection in the contact person

Data protection functions that the **user** needs/uses:

- The user can enter the legal basis, the purpose of use, and the period of validity for the data protection-relevant information.
- The user can save the privacy notice as a document in the contact.
- The user can generate reports relevant to data protection regarding the contact.
- The user can manually set a delete flag to mark the dataset for deletion or anonymization processes.
- The user can delete the delete flags after checking to keep the contact in the system.
- Advertising settings can be mapped to different channels.



Introduction



Data protection in the contact person

Data protection functions required/used by the **data protection officer**:

- The data protection officer can configure deletion flags for various conditions, which are set by the system on the respective data records.
- The deletion/anonymization process can run at fixed intervals or be triggered manually by the data protection officer.



Data protection relevant attributes

Data protection relevant attributes



Information that is mapped to the contact using attribute can also be classified as relevant to data protection.

This requires special labeling:

- Attributes that are classified as “relevant to data protection” are first entered into the system as attributes by the specialist administrator.
- They are then labeled as “relevant to data protection” by the data protection officer.

The user enters such an attribute for the contact and receives a note to enter the data protection information for it in the “Data protection” tab in the next step.



Data protection relevant attributes

Mark attribute as “GDPR relevant”

As a data protection officer, you are authorized to mark attribute values recorded for the contact as “relevant for data protection”:

1. In the “Data protection administration” Context, open the “Relevant Attributes” tab. [1]
2. All attributes recorded in the system for the “Contact” Context are displayed.
3. Select an attribute [2] and click on the “Change GDPR Relevance” button [3].

1

Change GDPR Relevance

3

2

Name	is GDPR Relevant
▼ Conditions	No
Bank name	No
VAT-ID	No
Delivery term	No
IBAN	No
Payment term	No
BIC	No
Departments	No
▶ Assessment	No
▶ Operation planning	No

Data protection relevant attributes

Mark attribute as “GDPR relevant”

The Context „Data protection administration" contains an overview of all attributes, which can be entered in a contact.

- With the action **"Change GDPR Relevance"**, the **attribute** can then be **adjusted to "is GDPR Relevant"**. Therefore, the attribute is listed in table in the tab "Data Privacy", when added to the contact. This means that when saving after creating or changing this property, the user is informed that it is necessary to enter the information in the Data Privacy tab.
- If the indicator is set for a superordinate attribute, this is adapted for the subordinate attribute.
- Which attributes are relevant to the GDPR must be defined individually.

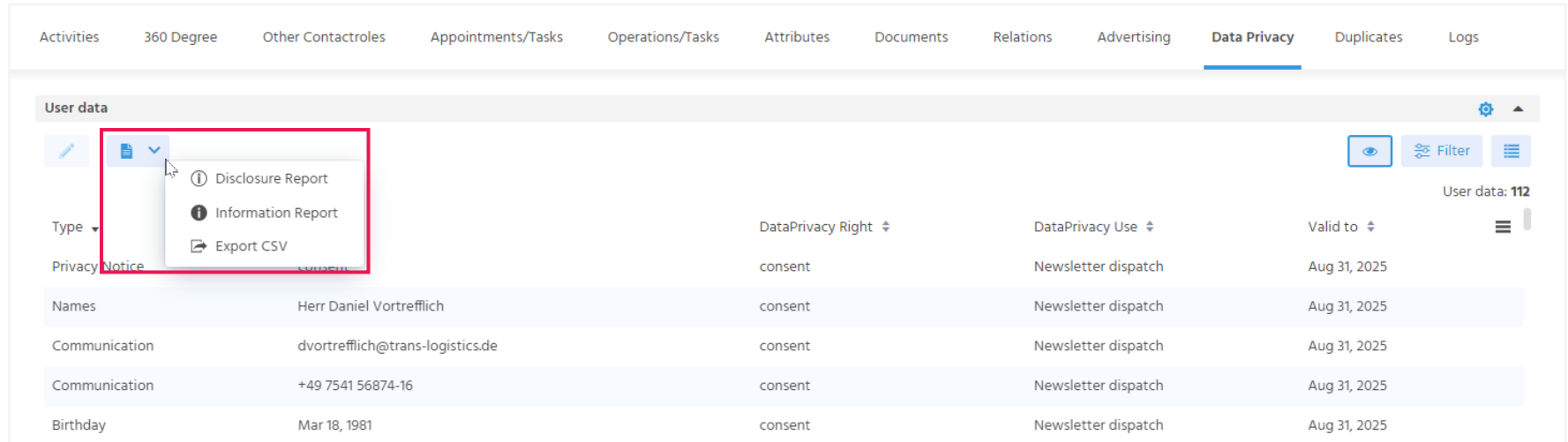


In the attribute dataset, an attribute relevant to data protection is mentioned for the usage in the contact.
The use "Data Privacy" can be set either in the Context "Data protection administration" with the action "Change GDPR Relevance", or directly in the Context "Attribute".

Issuance of GDPR-relevant reports

Issuance of GDPR-relevant reports

The possibility to issue different reports can be found in the tab "Data Privacy".



The screenshot displays the 'Data Privacy' tab in the ADITO application. The 'User data' section is highlighted with a red box, showing a dropdown menu with options: 'Disclosure Report', 'Information Report', and 'Export CSV'. The table below shows user data for 'Herr Daniel Vortrefflich' with columns for Type, Privacy Notice, DataPrivacy Right, DataPrivacy Use, and Valid to.

Type	Privacy Notice	DataPrivacy Right	DataPrivacy Use	Valid to
Names	Herr Daniel Vortrefflich	consent	Newsletter dispatch	Aug 31, 2025
Communication	dvortrefflich@trans-logistics.de	consent	Newsletter dispatch	Aug 31, 2025
Communication	+49 7541 56874-16	consent	Newsletter dispatch	Aug 31, 2025
Birthday	Mar 18, 1981	consent	Newsletter dispatch	Aug 31, 2025

Issuance of GDPR-relevant reports



Disclosure report

The GDPR disclosure report shows all relevant data of a contact person for information in accordance with Article 15 of the GDPR.

If a private individual approaches your company and wants to know what data you have stored, create a GDPR disclosure report that includes the following data:

- Salutation, first and last name
- Addresses
- Contact data (telephone numbers, email addresses, etc.)
- Additional information, such as date of birth
- Assigned attributes, which are classified as „GDPR-relevant“



Issuance of GDPR-relevant reports

Disclosure report

Before the report is created, the following data is requested via a dialogue box:

- **Transmission** to record whether a transfer to third parties has taken place
 - None
 - Recipients from inland
 - Recipients from a foreign country
- **Recipient** (mandatory field if data has been passed on to third parties from inland or a foreign country)
- **Guarantees** (mandatory field if data has been passed on to third parties from a foreign country)
- **External Datasource** to record the origin of the data (mandatory field if data was not collected from the person concerned)
- **Date of request** (mandatory field)
- **Deadline** (mandatory field):
 - On time
 - Extend – complexity
 - Extend – request count
- **Extension letter date** (date, mandatory field if "Extend – complexity" or "Extend – request count" was selected).

The report is output as a PDF and can be sent by email.



The screenshot shows a web form for a disclosure report. At the top is the 'meineFirma' logo and address: 'meineFirma | Wilhelm-Str. 2 | DE 80807 München'. Below this is the contact information for Herr Daniel Vortrefflich at Fallenbrunnen 3, DE - 88045 Friedrichshafen. The subject is 'Betreff: Erteilung der Auskunft nach Art 15 DSGVO'. The form body contains a letter addressed to Herr Vortrefflich, explaining that his request for information under Art 15 DSGVO has been processed and that the data is being provided. It also states that the company complies with the request within the statutory period of one month. A table follows, detailing the data processing for various purposes. The table has five columns: Art, Wert, Rechtsgrundlage, Verwendungszweck, and gültig bis. The data is then transmitted to the recipient, Herr Daniel Vortrefflich, at Transatlantik Logistics GmbH. The form concludes with a statement that the data is saved until 09.06.2025 and a reminder of the rights under the GDPR.

Art	Wert	Rechtsgrundlage	Verwendungszweck	gültig bis
Birthday	12/25/1980	consent	Newsletter dispatch	06/09/2025
Communication	dvortrefflich@trans-logistics.de	consent	Newsletter dispatch	06/09/2025
Names	Herr Daniel Vortrefflich	consent	Newsletter dispatch	06/09/2025
Communication	+49 7541 56874-16	consent	Newsletter dispatch	06/09/2025
Privacy Notice	consent pending	consent	Newsletter dispatch	06/09/2025

The background of the slide is a dark blue field filled with glowing, semi-transparent binary code (0s and 1s) and a faint grid pattern. A solid red vertical bar runs along the right edge of the slide.

Delete data

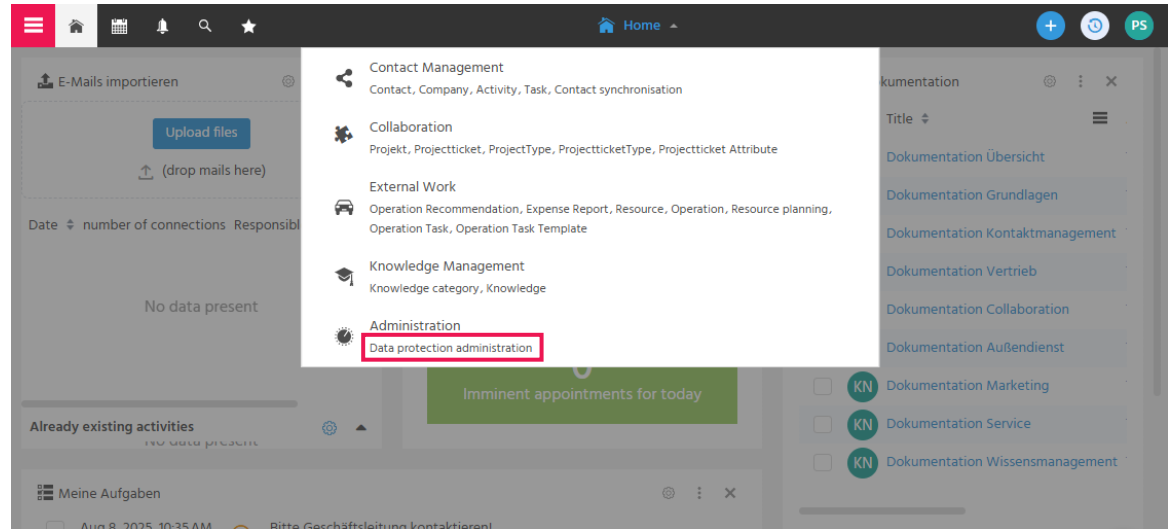
Manage deletion indicator

Manage deletion indicator

Access authorization for the “Data protection administration” Context

With the role „Data privacy agent,, (PROJECT_DSGVO), the Context „Data protection administration" is only displayed for authorized users in the Globale Menu in the Menu Group "Administration".

This means that, e.g. specialist administrators or data privacy agents may be authorized.

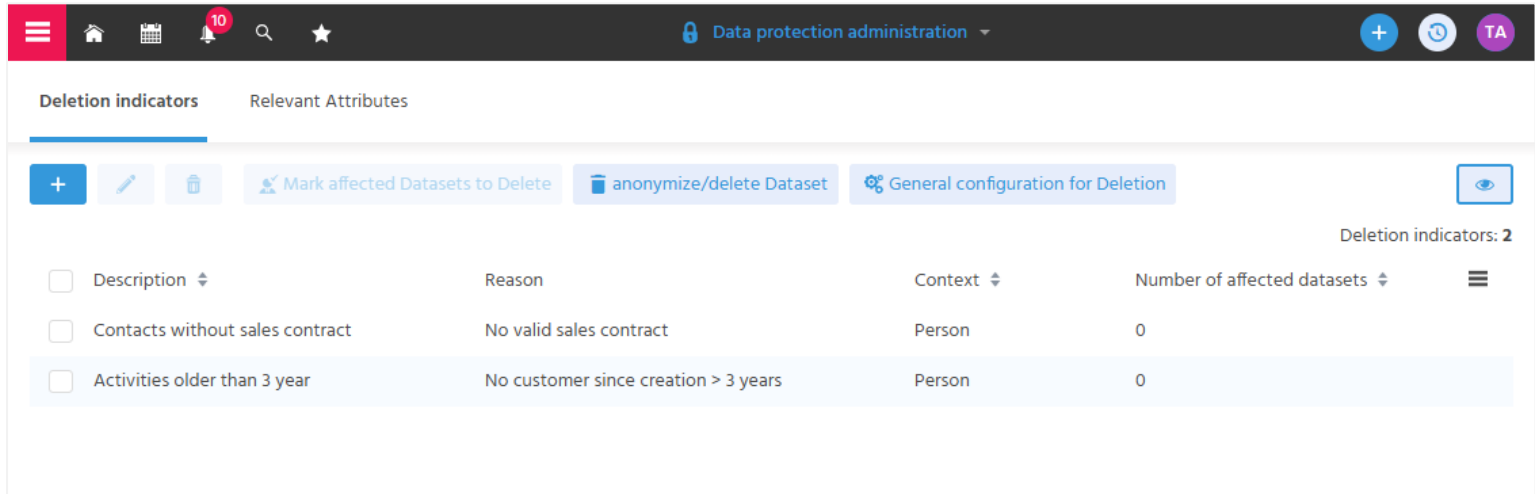


Manage deletion indicator

Access authorization for the “Data protection administration” Context

The “Data protection administration” Context contains the functions for managing

- the deletion indicators and
- the attributes relevant to data protection.



The screenshot displays the 'Data protection administration' interface. At the top, there is a navigation bar with a menu icon, home, calendar, notifications (10), search, and star icons. The main header shows 'Data protection administration' with a lock icon and a dropdown arrow. On the right, there are three circular icons: a plus sign, a clock, and a purple circle with 'TA'.

Below the header, there are two tabs: 'Deletion indicators' (active) and 'Relevant Attributes'. Under the 'Deletion indicators' tab, there is a toolbar with a plus icon, an edit icon, a trash icon, and three buttons: 'Mark affected Datasets to Delete', 'anonymize/delete Dataset', and 'General configuration for Deletion'. A toggle icon is on the far right.

Below the toolbar, there is a table with the following columns: 'Description', 'Reason', 'Context', and 'Number of affected datasets'. The table contains two rows of data:

Description	Reason	Context	Number of affected datasets
Contacts without sales contract	No valid sales contract	Person	0
Activities older than 3 year	No customer since creation > 3 years	Person	0

At the bottom right of the table area, it says 'Deletion indicators: 2'.

Manage deletion indicator

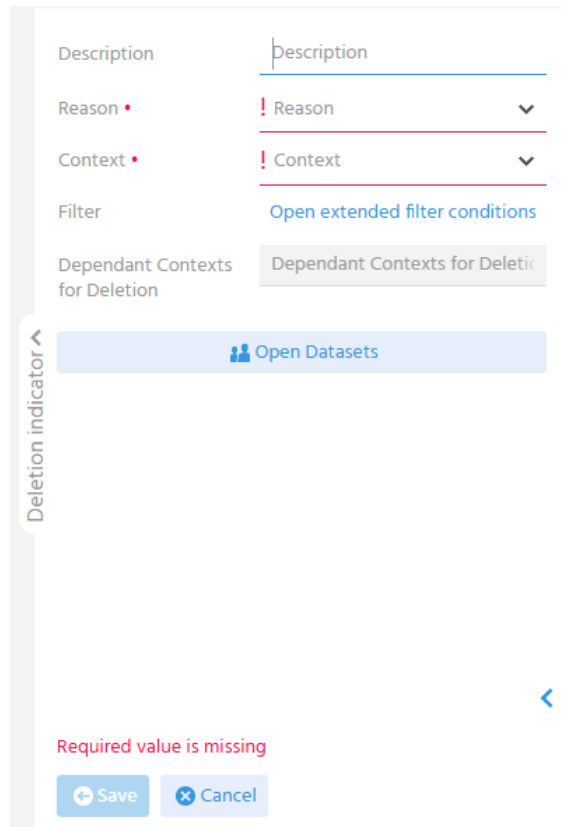
Create deletion indicator (1/4)

When creating a new deletion indicator,

- the description (info field for the data protection officer),
 - the reason (see next slides),
 - the Context* and
 - the filter (see next slides) are recorded.
- Once the context has been selected, the “Dependent contexts to be deleted”* field shows which contexts will also be deleted.



* In xRM, the “Contact” Context is supplied with the dependent contexts “Activity, Task, Service Ticket, and Advertising Material.” The selection of contexts and dependent contexts can be expanded via customizing.



The screenshot shows the 'Create deletion indicator' form in the ADITO system. The form is titled 'Deletion indicator' on the left side. It contains several fields: 'Description' with a text input field containing 'Description'; 'Reason' with a dropdown menu showing 'Reason' and a red exclamation mark icon; 'Context' with a dropdown menu showing 'Context' and a red exclamation mark icon; 'Filter' with a link 'Open extended filter conditions'; and 'Dependant Contexts for Deletion' with a button 'Dependant Contexts for Deletion'. Below these fields is a blue button 'Open Datasets'. At the bottom, there is a red error message 'Required value is missing' and two buttons: 'Save' and 'Cancel'.

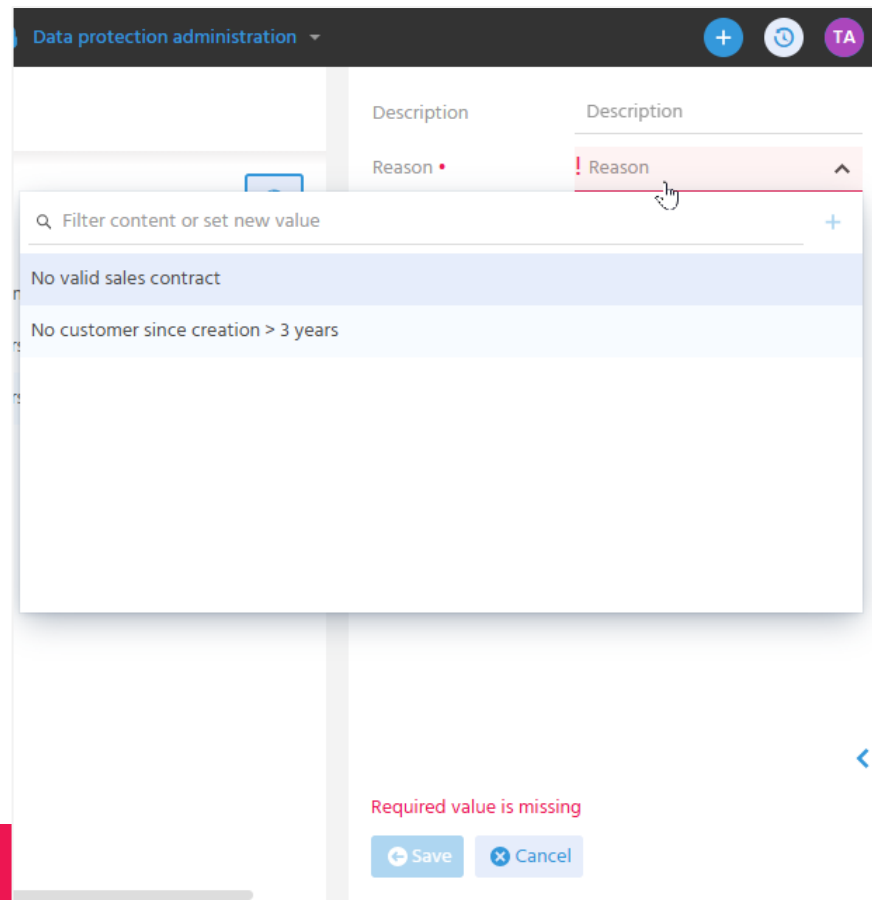
Manage deletion indicator

Create deletion indicator (2/4)

Reason: From a technical point of view, the reason why a delete indicator should be set is indicated here, e.g., "Purchase contract expired."

To enter the reason here,

- you can use the selection (which can be customized via the keyword category "DSGVOREASON" if further reasons are required) or
- you can enter a reason manually (which may only be required once) (enter the term and apply the value with the plus button).



The screenshot shows the 'Data protection administration' interface. A dropdown menu is open for the 'Reason' field, displaying two options: 'No valid sales contract' and 'No customer since creation > 3 years'. A search bar at the top of the dropdown says 'Filter content or set new value'. At the bottom of the interface, a red error message states 'Required value is missing', and there are 'Save' and 'Cancel' buttons.

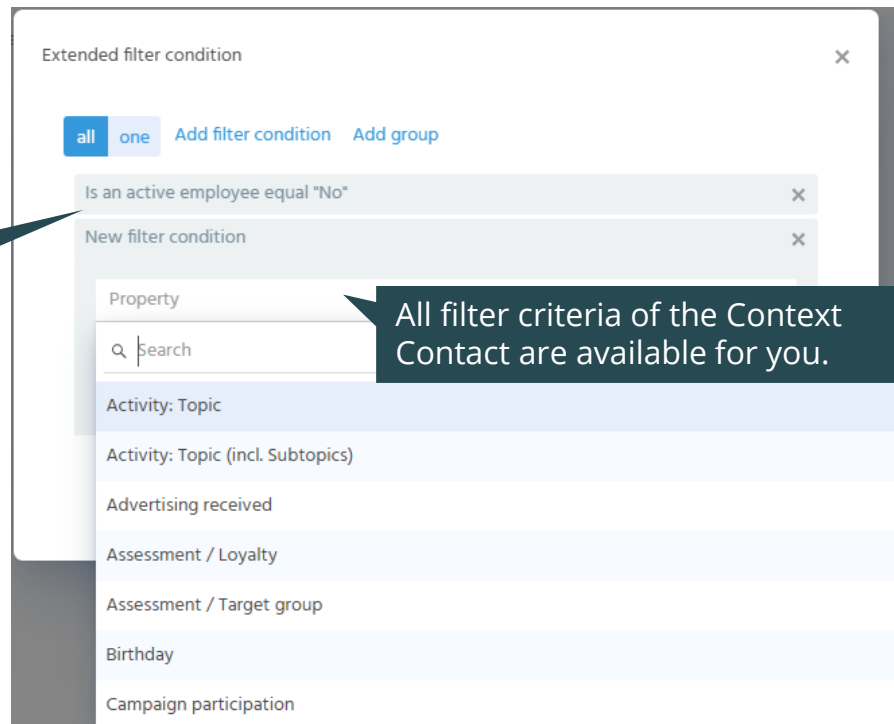
Manage deletion indicator

Create deletion indicator (3/4)

Filter: Here, you define a filter with conditions that determine the datasets for which there is a valid reason to mark the data for deletion.

For example, use the filter criteria "No activity" to filter contacts, where no activities have been added in a specific time period.

With the predefined filter "Is an active employee equal No", all employees are excluded from the automated setting of the deletion maps.



Extended filter condition

all one Add filter condition Add group

Is an active employee equal "No" x

New filter condition x

Property

q Search

Activity: Topic

Activity: Topic (incl. Subtopics)

Advertising received

Assessment / Loyalty

Assessment / Target group

Birthday

Campaign participation

All filter criteria of the Context Contact are available for you.

Manage deletion indicator

Create deletion indicator (4/4)

Actions „Open Datasets“

This action opens the "Live View" of all datasets, which would be listed as result of the set filter condition

Deletion indicator ^

Description

Contacts without sales contract

Reason •

No valid sales contract ▼

Context •

Person ▼

Filter

Open extended filter conditions

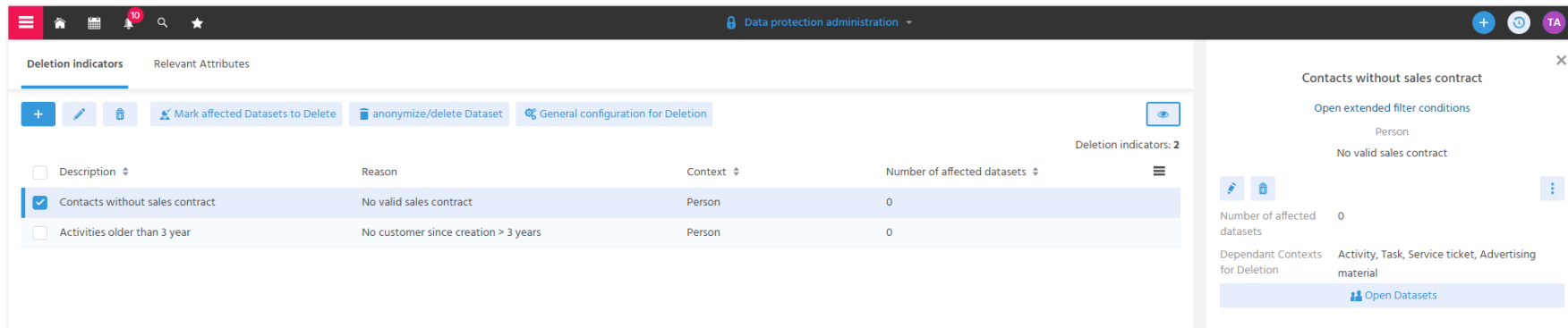
Dependant Contexts
for Deletion

Activity, Task, Service ticket, Ac

Open Datasets

Manage deletion indicator

Edit deletion indicator



The screenshot displays the 'Data protection administration' interface. The main section, 'Deletion indicators', shows a table with two indicators. The first indicator, 'Contacts without sales contract', is selected and has a reason of 'No valid sales contract'. The second indicator, 'Activities older than 3 year', has a reason of 'No customer since creation > 3 years'. Both indicators have a context of 'Person' and 0 affected datasets. A right-hand panel provides details for the selected indicator, including 'Open extended filter conditions' (Person, No valid sales contract), 'Number of affected datasets' (0), and 'Dependant Contexts for Deletion' (Activity, Task, Service ticket, Advertising material). An 'Open Datasets' button is also present.

Description	Reason	Context	Number of affected datasets
☒ Contacts without sales contract	No valid sales contract	Person	0
☐ Activities older than 3 year	No customer since creation > 3 years	Person	0

- **As long as a deletion indicator has not yet been set on the contact records**, all fields can be edited retrospectively.
- If a **deletion indicator has already been set for contact data**, the reason can no longer be changed. In this case, the reason is not deleted from the contacts for which it was already set when the action "Mark affected Datasets to Delete" is executed again, but a second deletion indicator with the new reason is set. However, if a change to the reason is necessary in such a case, the deletion indicator must first be deleted and then recreated in order to remove it from the contacts.

Manage deletion indicator



Delete deletion indicator

If a defined deletion flag is no longer required, it can be removed in the Context "GDPR configuration" by using the delete button.

This delete flag is then removed from all contact datasets in which it was set.



In the "Logs" tab of the contact, you can see why the status of the contact has changed and which delete flags have been removed.

Mark data for deletion

Mark data for deletion

Set deletion indicator using process

The **process sets a deletion indicator** at the defined times or as soon as it has been manually triggered for one or more conditions using the “Mark affected Datasets to Delete” action.

Here, the system checks whether the defined filters for these deletion indicators are met. As soon as this is the case, the deletion indicator with this condition is set on the data record. The user sees the corresponding entry in the “Data protection” tab (in the lower table) and can see which condition was set at what time.



The process for setting the deletion indicators
DSGVOSetDeleteFlags_serverProcess is usually executed at fixed times.
This setting can be customized in ADITO Manager.

Mark data for deletion



Set deletion indicator using process – Manually trigger the process

The **“Mark affected Datasets to Delete” action** manually initiates the process of setting the deletion indicator.

You can use this function to respond to changes in the records.

When the action is executed, a query is first opened to specify whether the deletion indicator for this reason should be removed or added to all data records in the first step. If the contact still meets the filter condition, the deletion indicator is set again with this reason.

Once the action “Mark affected Datasets to Delete” has been executed, the user will find the deletion indicator in the contact in the “Data protection” tab. They can see the reason why it was set and when.

Example: You have a deletion indicator that checks when the last activity within a certain category was recorded within a certain period of time. Now you first delete all deletion indicators set so far from this condition and set them again. If a new activity of the category in question has been added to a contact since the deletion indicator was last set, it no longer meets the conditions of the filter. This means that the deletion indicator is no longer set for this contact and the contact is not deleted.



Mark data for deletion

Delete deletion indicator

As a user, I would like to delete a deletion indicator that was set manually or by the system if I have reasons that speak against deleting the contact.

- All deletion indicators must be removed in the “Data protection” tab (Delete button), then the status is set back to “active”. Both manually set deletion indicators and process-set deletion indicators can be removed from the contact again with the Delete button.



The setting and removal of deletion flags is logged directly in the contact in the “Logs” tab.

Delete/anonymize data

Delete/anonymize data

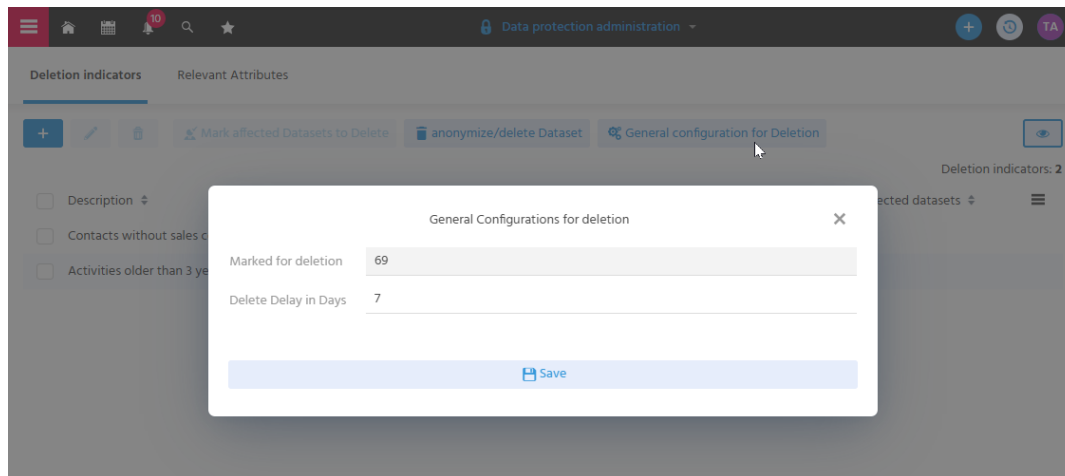
Define deletion delay

The number of days that a deletion indicator must be set before the deletion process is executed and a data record can actually be deleted is adjusted in the “Data protection administration” Context in the “Deletion indicators” tab under the **“General configuration for Deletion” action**.

Click on this action to open the dialog box where you can see the current setting. To change the value, enter the desired value here and exit the dialog box by clicking Save.



The number of days is set to 7 by default. This setting can be customized for each customer.



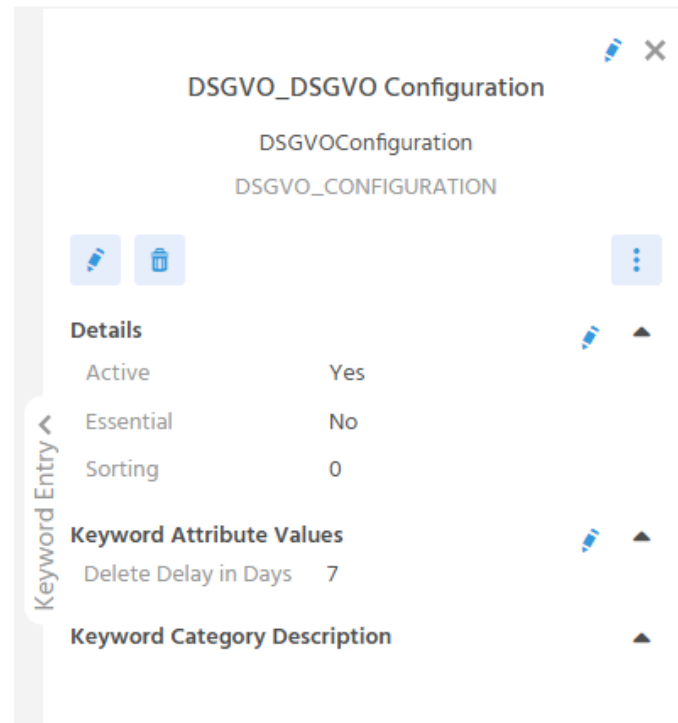
Delete/anonymize data

Define deletion delay – alternative procedure:

The value “Delete delay in days” is maintained in the keyword “DSGVOConfiguration”.

The number of days is specified in the keyword property **“Delete Delay in Days”** in the keyword entry.

To adjust the number of days, open the preview of the keyword “DSGVOConfiguration” in the “Keyword Entry” Context and edit the value for “Delete Delay in Days” in the “Keyword Attribute Values” area.



The screenshot shows a configuration window for the keyword "DSGVO_CONFIGURATION". The window has a title bar with a pencil icon and a close button. Below the title, the keyword name "DSGVO_CONFIGURATION" is displayed. There are two icons (pencil and trash) and a three-dot menu icon. The main content area is divided into sections: "Details" with a table of attributes, "Keyword Attribute Values" with a table of values, and "Keyword Category Description". A vertical label "Keyword Entry" is on the left side of the main content area.

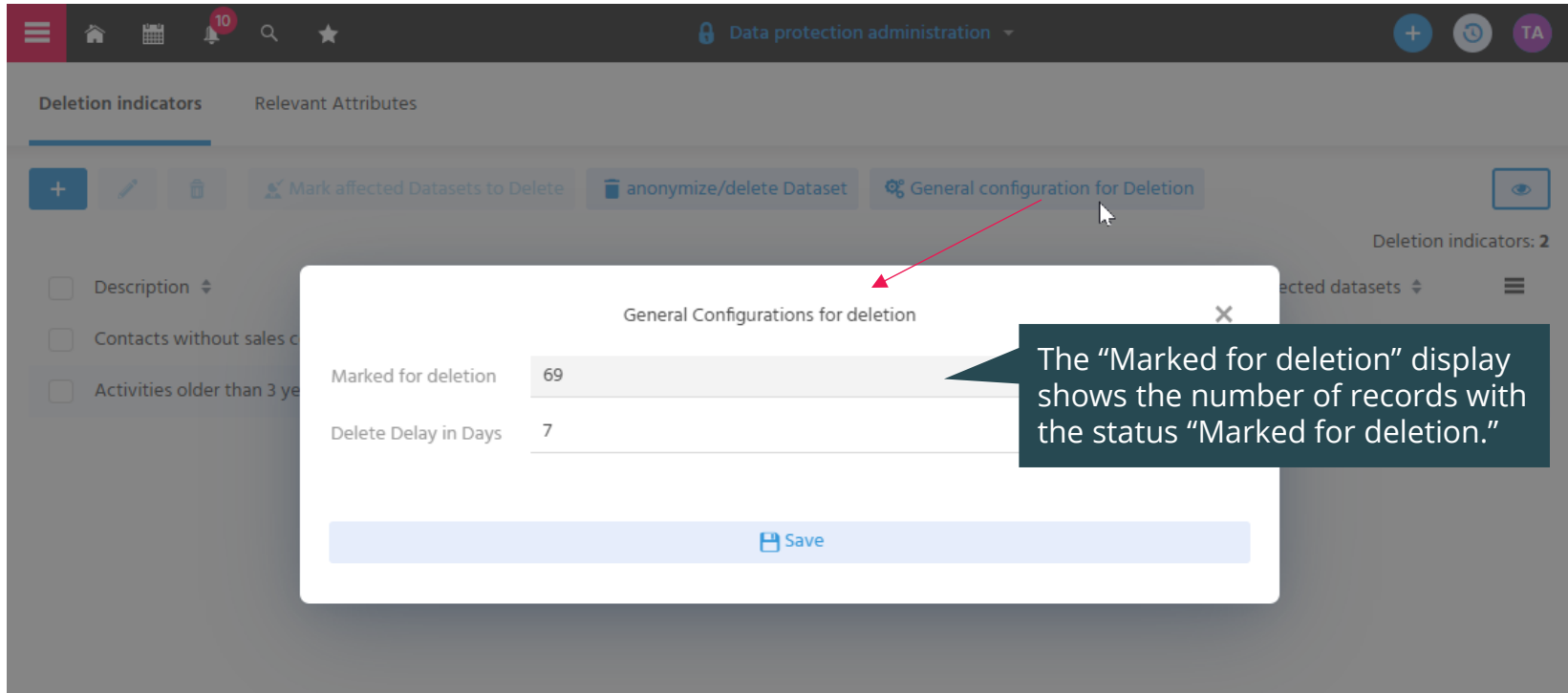
Details	
Active	Yes
Essential	No
Sorting	0

Keyword Attribute Values	
Delete Delay in Days	7

Keyword Category Description

Delete/anonymize data

Marked for deletion – Number of marked records



The screenshot displays the ADITO Data protection administration interface. A modal dialog titled "General Configurations for deletion" is open, showing the following configuration:

Configuration Item	Value
Marked for deletion	69
Delete Delay in Days	7

A red arrow points from the "General configuration for Deletion" button in the top navigation bar to the dialog box. A dark blue callout box points to the "Marked for deletion" value, containing the text: "The 'Marked for deletion' display shows the number of records with the status 'Marked for deletion.'"

The background interface shows the "Deletion indicators" tab selected, with a list of indicators including "Description", "Contacts without sales c", and "Activities older than 3 ye". The top navigation bar includes icons for home, calendar, notifications (10), search, and star, along with the "Data protection administration" title and user profile icons (+, TA).

Delete/anonymize data

Deletion/anonymization processes

The processes for deletion or anonymization of the data is usually carried out at predefined times.



Depending on the amount of data, the process can, for example, be executed daily or weekly at 02:00. These settings can be customized in the ADITO Manager for the DSGVOAnonymize_serverProcess based on the customer's needs.

The deletion/anonymization is only carried out in the process on the **condition** that the **delete flag** must have been **set for X days**.

The number of days for this **deletion delay** will be determined administratively. This time period is necessary to establish a **check period for automatically set delete flags**. This enables the user to respond within the deletion delay time of X days and to a delete flag that may have been set incorrectly, whether automatically or manually.

The process can also be **triggered manually** using the "anonymize/delete Dataset" action (for further information, check the ["Manual triggering of the process for setting delete flags"](#) chapter).

The process **anonymizes** data ([data to be anonymized](#)) and **deletes** data ([data to be deleted](#)). In addition, the contact is assigned to the **"GDPR Anonymization"** company ([Assignment of inactive anonymized contacts to the "GDPR anonymization" company](#)). Duplicates are no longer displayed. The delete flag with reason remains recorded and the status is set to "inactive". This makes it possible to understand why this dataset was deleted/anonymized. Finally, the contact dataset is removed from the index.

Information, such as the affiliation to a campaign, remains anonymous so that it is still possible to see how many contacts a campaign includes.

Delete/anonymize data



Manual initiation of the deletion/anonymization process

You can manually initiate the deletion/anonymization process using the "anonymize persons" action. In this case, the system also checks whether the delete flags have been set for X days.

Before the "anonymize persons" action starts the process, a confirmation is required.

The screenshot displays the ADITO Data protection administration interface. The top navigation bar includes a menu icon, home, calendar, notifications (10), search, and star icons. The main header shows "Data protection administration" with a lock icon and user avatars (+, TA).

The interface is divided into two main sections. The left section, titled "Deletion indicators", contains a table with columns: Description, Reason, Context, and Number of affected datasets. The right section, titled "Relevant Attributes", shows a confirmation dialog for the selected indicator.

Description	Reason	Context	Number of affected datasets
☐ Contacts without sales contract	No valid sales contract	Person	0
☒ Activities older than 3 year	No customer since creation > 3 years	Person	69

Deletion indicators: 2

Activities older than 3 year

Open extended filter conditions

Person

No customer since creation > 3 years

Number of affected datasets: 69

Dependant Contexts for Deletion: Activity, Task, Service ticket, Advertising material

Open Datasets



Delete/anonymize data



Data to be anonymized

Data, which has to be anonymized, is the **first** and **last name**.

Here, the original entries are replaced with an anonymization string *********.

Delete/anonymize data

Data to be deleted

All data, which is not required for calculations in further processes, belong to the data, which should be deleted. This includes:

- **Log entries**
- **Activities:** here, all corresponding connections, documents, attributes and log entries of the activities will be deleted. Activities, which are connected with several contacts, are also completely deleted, as soon as a contact is affected by the deletion process. Therefore, the activity of the remaining contacts is also deleted.
- **Tasks**
- **Communication media**
- **Date of birth**
- **Addresses** (the addresses directly on the contact, not the company address)
- **Documents**
- **Attributes**
- **Relations**
- **Servicetickets** (if the contact was registered as a requester)
- **Advertising material**
- **Entries in the data protection table:** the entries of the type "Name" containing anonymized content and the type "Privacy Notice" with the reset status "consent pending" remain here.

Delete/anonymize data

Deletion/anonymization of employee data

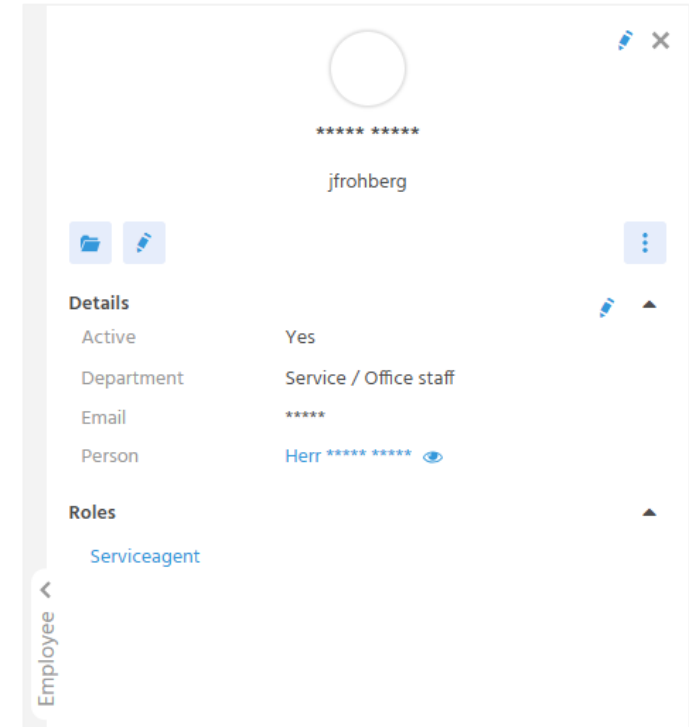
If an employee's contact record is deleted/anonymized, the employee record is also included in this process.

This means that the following information is also deleted/anonymized from the employee record:

- Name,
- email address and
- picture, if available.



For technical reasons, the **username is not anonymized.**



The image shows a screenshot of an employee record interface. At the top, there is a circular profile picture placeholder with the text '*****' below it, and the username 'jfrohberg' below that. To the right of the profile picture is a pencil icon and a close icon. Below the profile picture are two icons: a folder and a pencil. To the right of these icons is a three-dot menu icon. The 'Details' section is expanded, showing the following information: 'Active' with the value 'Yes', 'Department' with the value 'Service / Office staff', 'Email' with the value '*****', and 'Person' with the value 'Herr *****' followed by an eye icon. The 'Roles' section is also expanded, showing the role 'Serviceagent'. On the left side of the interface, there is a vertical tab labeled 'Employee' with a chevron icon.

Overview: Data in the deletion process

Overview: Data in the deletion process



Filtering contacts marked for deletion

The “Status” filter criterion can be used to filter for the value “To Delete” to filter all contacts with this status.

This provides an overview of these contacts and, if necessary, the deletion indicators of a contact can be deleted again if it is professionally required.

The screenshot displays the ADITO interface for managing contacts. The main area shows a table of contacts with columns for Picture, Salutation, Title, Firstname, Lastname, Company, E-Mail, Phone, and Address. Two contacts are listed: Herr Markus Altinger (Skyscraper Bau GmbH) and Monsieur Bernard Bertin (Hamel Collin SAS). The right sidebar shows the filter configuration, with the 'Status' filter set to 'To Delete'. The 'Grouping' section is also visible, showing 'Group by' and 'Condition' options.

Picture	Salutation	Title	Firstname	Lastname	Company	E-Mail	Phone	Address
	Herr		Markus	Altinger	Skyscraper Bau GmbH	maltinger@skyscraper-bau.de		Rathausallee 50 - DE 22846 Norderstedt
	Monsieur		Bernard	Bertin	Hamel Collin SAS	bertin@hamel.fr		Passage de l'Hôtel de Ville 6 - FR 68100 Mulhouse

Contacts: 2

Filter content...

Grouping

Group by

Condition

Join conditions by: all one

Status equal "To Delete"

Status equal To Delete

+ Add filter condition

Open extended filter conditions

Saved filters

Last filters



Overview: Data in the deletion process



Filtering inactive anonymized contacts

If contacts are anonymized/deleted, the status of the contact will finally be set to "inactive".

To distinguish between **inactive anonymized** contacts and **inactive non-anonymized** contacts of a company when filtering, the inactive anonymized contacts are assigned to the "GDPR anonymization" company.

Persons for whom only one additional function has been deleted/anonymized are also listed as anonymized contacts under the company "GDPR anonymization"; the remaining additional functions are retained in the system in their entirety and no longer have any connection to the deleted data record.

This means that the original company now only contains active and inactive, non-anonymized contacts.

Inactive anonymized contacts can be clearly filtered via the company "GDPR anonymization."





**Activate data
protection
functions in the
system**

Activate data protecting functions in the system



Your system administrator will take care of the setting described here.

To display the functions related to data protection for the user in your system, it is necessary to activate the system option (`dsgvo.aktiv` under `_____PREFERENCES_PROJECT:Custom`) in your system:

- If you set "**GDPR active**" to **TRUE**, the "**Data Privacy**" tab **will be displayed** in the Context "Contact". The user will receive a note ([Note for new creations or changes](#)) when saving data protection-relevant information ([information relevant to data protection](#)) that they must document the legal basis and purpose of use for this in the "Data Privacy" tab.
- Set "GDPR active" to FALSE to hide the tab and the notification functionality accordingly.



Advertising settings

Advertising settings

To document which data may or may not be used for advertising purposes, advertising settings can be specified. For this purpose, you will find the "Advertising" tab (the short name for Advertising settings), where you can enter advertising indicators. Documented here are the advertising consents with the status "Allowed", as well as the rejections with the status "Rejected".

The advertising indicators can be displayed for the "Email," "Telephone," and "Letter" channels. To document advertising consent or a revocation depending on the channel, the status can take the following values: "Pending," "Allowed," or "Rejected." Information is also recorded regarding the entry.

In the Preview of the contact, a note (in red font) is displayed indicating which advertising indicator has the status "Rejected."

Additionally to the advertising indicators, the interest areas of a contact are recorded in this tab as well. Define the interest areas to categorize the serial mails. The interest areas to which individuals subscribed are entered directly in the contact.



Further information about the use of interests in connection with an interest area-dependent dispatch control can be found in the marketing-specific documentation.

Advertising settings



Query advertising indicator

For use in email marketing, the query of the advertising indicators begins with the DOI. If, for example, the contact registers for the newsletter via the homepage, their status is set to "Pending," and an email is sent to them. If they click on the link contained in the email, they confirm their registration (DOI) and their status is changed to "Allowed." The "Pending" status provides an overview of the newsletter subscriptions that have not yet been finally confirmed.

If a newsletter recipient no longer wishes to receive a newsletter, they can withdraw their consent and the status of the advertising indicator will be set to "Rejected".

The documentation of the advertising indicators for logging in or signing out takes place in the tab "Advertising" in the contact.

The registration and signing-out processes are mapped using "Workflow" and can be customized. The advertising indicators for letters, telephone, etc. can be entered manually.

When designing the unsubscribe link, it is important to consider what interest it may address.



Advertising settings



Use of advertising indicators

As soon as advertising indicators are available, these must be taken into account. For this reason, the sending of emails, for example, is prevented in the channels for which a corresponding advertising indicator with a contradiction exists.

Contacts for whom an objection has been stored can no longer be added as recipients of a serial mail, taking the interest into account.

Regarding recipient management in serial mails, this means that recipients who have received this mail to date and have now revoked their serial mail subscription are excluded from sending. To make this fact immediately visible to the user, these recipients are marked with a red warning symbol in the recipient list.

Using the button "Remove recipients with advertising ban", recipients can be removed from the recipient list, if they have a revocation. This can, for example, be used to remove recipients from a longer recipients list so that the sending process is not slowed down unnecessarily.

The behavior is similar when dealing with serial letters.

This document is subject to copyright protection. Therefore all contents may only be used, saved or duplicated for designated purposes such as for ADITO workshops or ADITO projects. It is mandatory to consult ADITO first before changing, publishing or passing on contents to a third party, as well as any other possible purposes.



Einzigartige Beziehungen