Learn the basics of the Innofactor GDPR solution

Manual

April 24, 2018

Innofactor AB
GDPRsolution@innofactor.com
Public

Version History

Responsible Person:

Supervisor: [Manager]

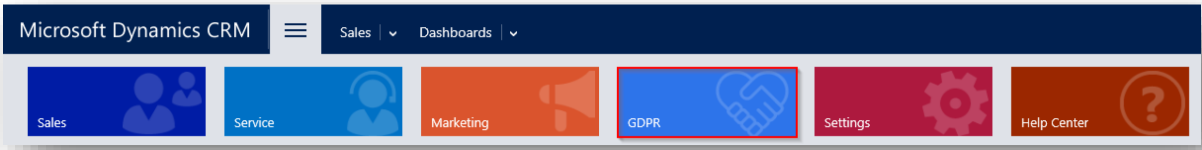
Version	Date	Author	Description	Reviewed by	Approved by
0.1	4.24.2018	EL & MS	Manual	PVa	SEn

Table of Content

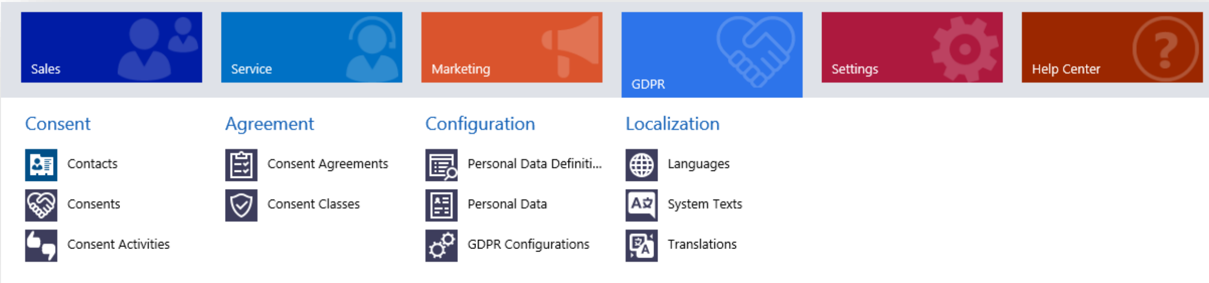
Innofactor AB
Drottninggatan 68, 5tr
111 21 STOCKHOLM
Info.sweden@innofactor.com
www.innofactor.se
tel.: +46 8 20 97 30
fax: +46 8 20 97 33

1 Finding the GDPR solution

1. Sign in to Office 365. From the top menu, select the site map and then select the icon for **GDPR**.



2. This action unfolds the dropdown menu, displaying the various entities included in the GDPR solution.



Innofactor AB
Drottninggatan 68, 5tr
111 21 STOCKHOLM
Info.sweden@innofactor.com
www.innofactor.se
tel.: +46 8 20 97 30
fax: +46 8 20 97 33

2 Understanding the basics

Start here to onboard quickly and learn about the Innofactor GDPR solution, its user interface and how it can improve your business.

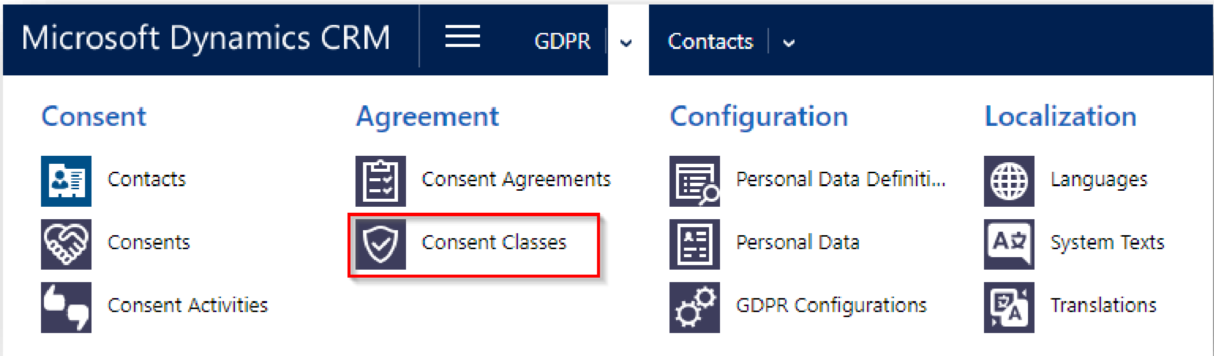
Every day, you will work with different contact records as you manage the different consent agreements available in the system. Here is a breakdown of the different entities available in the solution, and how they relate to each other.

- **What is a Contact?** A Contact is the standard Dynamics 365 Contact, equivalent of the record of a person.
- **What is a Consent?** A Consent is a record associated with a Contact, acting as a container with information regarding the nature of the Consent, status as well as start and end dates.
- **What is a Consent activity?** A Consent activity is the act of approving a Consent or cancelling a previously approved Consent.
- **What is a Consent agreement?** A Consent agreement is a container for general information regarding an agreement, associated with a Consent class. The Consent agreement contains the actual text that a Contact agrees to consent to.
- **What is a Consent class?** A Consent Class is a way of setting up the different types of Consents that are relevant to your business.
- **What is a Personal Data Definition?** A Personal Data Definition is the definition of personal data based on your specific business requirements. In the Innofactor GDPR solution, this is a highly customizable feature.

3 Consents

3.1 Creating a Consent Class

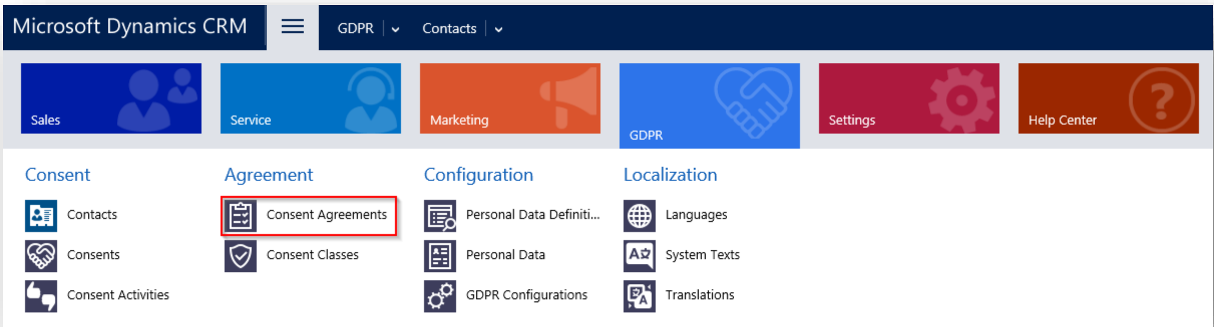
1. Navigate to **GDPR > Agreement > Consent Classes**.



2. Select **+ New** from the command bar. This will open a new record.
   - **Name**: Select a descriptive name for the Consent class, i.e ”Direct Marketing”.
   - **Code**: Select a unique code for the Consent class.
3. To save your changes, on the command bar, select **Save**.
4. The Consent class is now ready to be used when creating a Consent agreement.

3.2 Creating a Consent Agreement

1. Navigate to **GDPR > Agreement > Consent Agreements**.



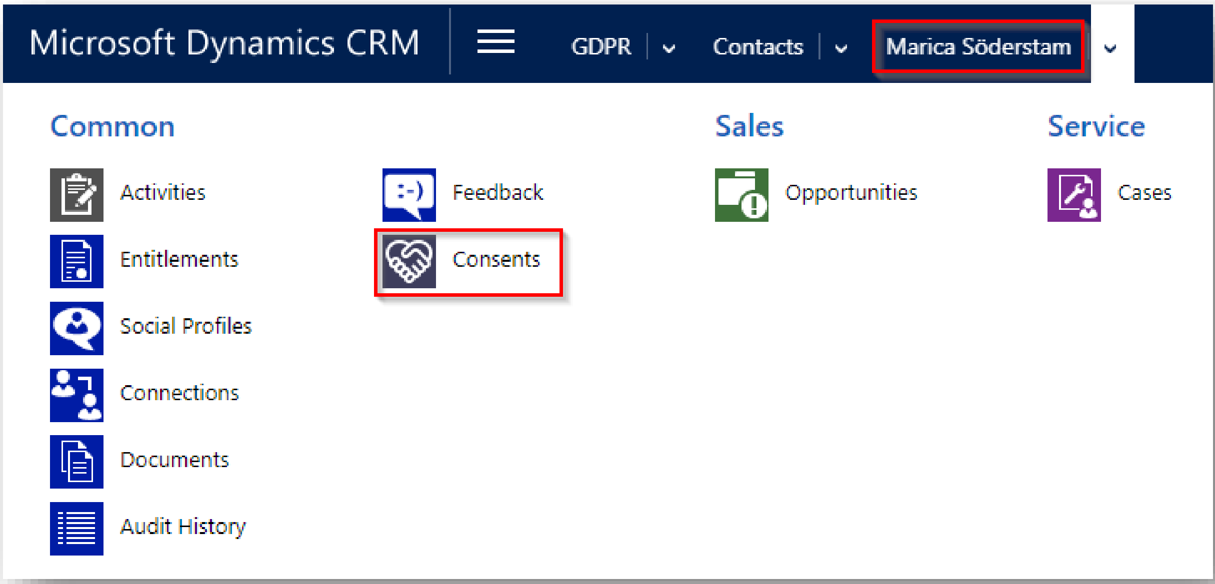
2. Select **+ New** from the command bar. This will open a new record.
3. In the Consent Agreement form, make sure the status reason of the record is set to Draft while editing. **Once the status reason is set to Active, you will not be able to make changes to the Consent text**.
    a. **Consent class**: Select the appropriate Consent class for your Consent Agreement.
    b. **Valid from**: Select the start date of the Consent Agreement.
    c. **Valid until**: Select the end date of the Consent Agreement, if this information is available to you.
    d. **Status Reason**: While working on the Consent Agreement, the status should be Draft to be able to make changes. If the Consent Agreement is in Draft status, the record will not show when adding a Consent Agreement to a new Consent. When you are happy with your changes, set the status reason to Active and save the record.
    e. **Owner**: The user who created the record.
    f. **Notes**: Users can create notes regarding the Consent Agreement.
    g. **Consent Text**: The text that a contact actually consents to. The value of this field can be used in various ways depending on your business requirements. I.e: "I consent to receiving direct marketing".
4. To save your changes, on the command bar, select **Save**.
5. The Consent Agreement is now ready to be used when creating a Consent for a Contact.

3.3 Creating a Consent

When creating a new Consent, you can choose to do this from a Contact or a Lead record, or you can create one from scratch from the Consents tab in the site map.

3.3.1 Creating a Consent from a Contact

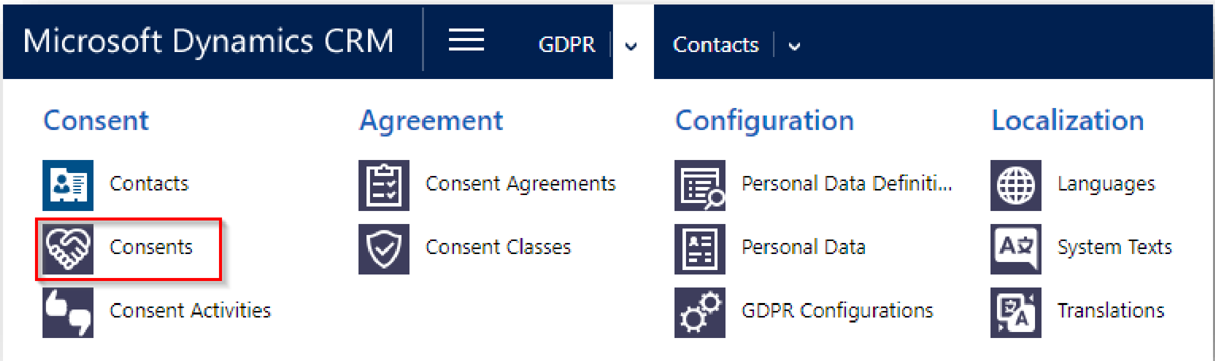
1. Navigate to **GDPR > Consent > Contacts**.
    a. When creating a Consent for a Lead, navigate to **Sales > Leads**. The following steps is the same when creating a Consent for a Contact as creating one for a Lead.
2. Open a Contact record.
3. Select Consents from the sitemap.



4. Select **+ Add New Consent** from the command bar. This will open a new record.

3.3.2 Creating a Consent from the site map

1. Navigate to **GDPR > Consents**



2. Select **+ New** from the command bar. This will open a new record.

3.3.3 Creating the Consent

1. When creating a Consent from a Contact or Lead, the corresponding field is automatically populated with a look up to the chosen Contact or Lead.

2. When creating a new Consent from the sitemap, you have the option to select a Contact or a Lead, depending on your business requirements.
    - **Consent agreement**: Select the appropriate Consent Agreement for your Consent. To do this, click on the looking glass and select a record from the drop down or select Look up more values. This will allow you to search through records.
    - **Consent class**: Saving the record will automatically set this field, based on the value you picked in Consent agreement.
    - **Opt in**: The actual start date when the Consent is agreed to. This locked field is automatically set when managing a Consent activity, see **Creating a Consent Activity**.
    - **Opt out**: The actual end date when the Consent is cancelled. This locked field is automatically set when managing a Consent activity, see **Creating a Consent Activity**.
    - **Status reason**: The status of the Consent agreement is dependent on the associated Consent activities, see **Creating a Consent Activity**.
3. Select **Save** to enable other sections on the form.

3.3.4 Qualifying a Lead – What about the Consents related to the Lead?

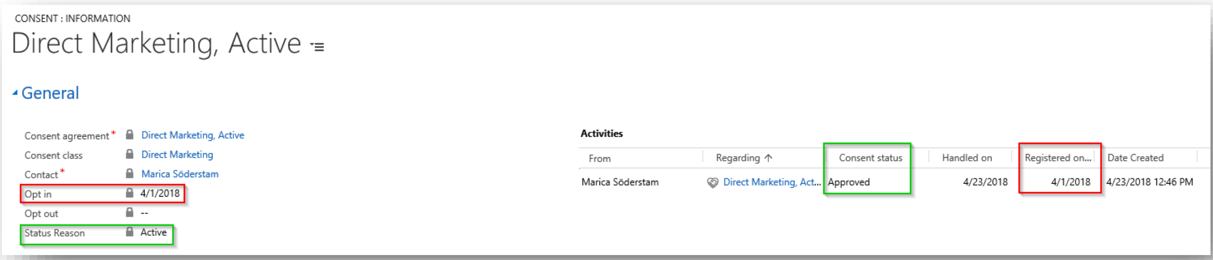
When **qualifying a Lead** all Consents created for the Lead will be **copied** to the created Contact and the Contents related to the originated Lead will be deactivated.

3.4 Creating a Consent Activity

The Consent activity is the actual act of approving (or cancelling) the Consent that you just created. This could have different meaning based on the nature of your business, but in general it means receiving that confirmation from a Contact or a Lead.

1. Add an Activity to the Consent by clicking the **+** by the Activities section. This will open a quick create form to a new record.
2. When creating a Consent activity, the From field is automatically populated with a look up to the Contact or the Lead, inherited from the Consent. The same goes for the Regarding field.
    - **From:** The Contact or Lead that the activity concerns.
    - **Regarding:** Lookup to the Consent agreement that the activity concerns. This name also contains the status of the Consent activity at the time.
    - **Consent status:** The status of the Consent activity, and by extension, the Consent. This field is by default set to Not approved.

        - Not approved means that the status of the Consent is pending.
        - Approved means that confirmation has been received from the Contact or the Lead, that they actually consent to the agreement in question.
        - Cancelled means that the Consent is no longer valid.
    - **Origin:** The origin of the confirmation from the Contact or Lead, i.e phone or email.
    - **Registered on:** The actual date that the Consent activity occurred.
3. Saving the record will return you to the Consent agreement form. Note: You may have to reload this page to see the changes.

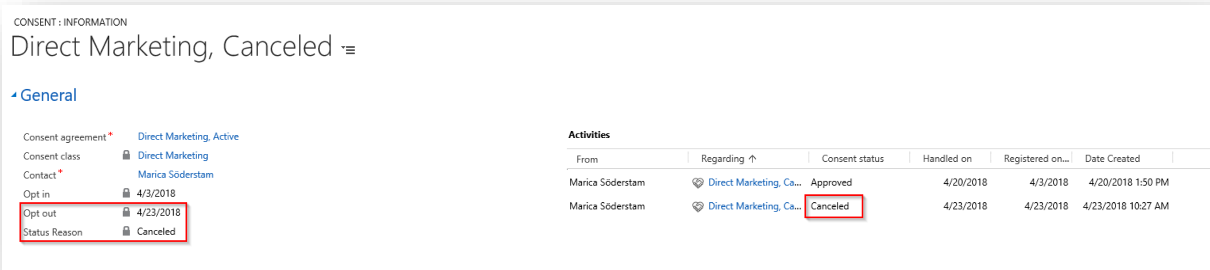


Note that the Handled date from the Consent activity has now been inherited to the Opt in field. Also, **having changed the status of the Consent activity to Active results in locking the form fields of the Consent**.

3.4.1 Cancelling a Consent

In order to cancel an active Consent, we need to create another Consent activity.

1. Add a new Activity to the Consent by clicking the **+** by the Activities section.
2. This time, we **set the Consent status to Cancelled**.
3. Fill out the **Origin** of the cancelation.
4. Set the date that the cancelation was received in the field **Registered on**.
5. Save the record to return to the Consent agreement form. Note: You may have to reload this page to see the changes.



Note: Since the status of the latest Activity is now Cancelled, the status reason of the Consent has also been set to Cancelled. Also, the date that we input in the field Registered on has now been inherited to the opt out field.

4 The definition of Personal Data

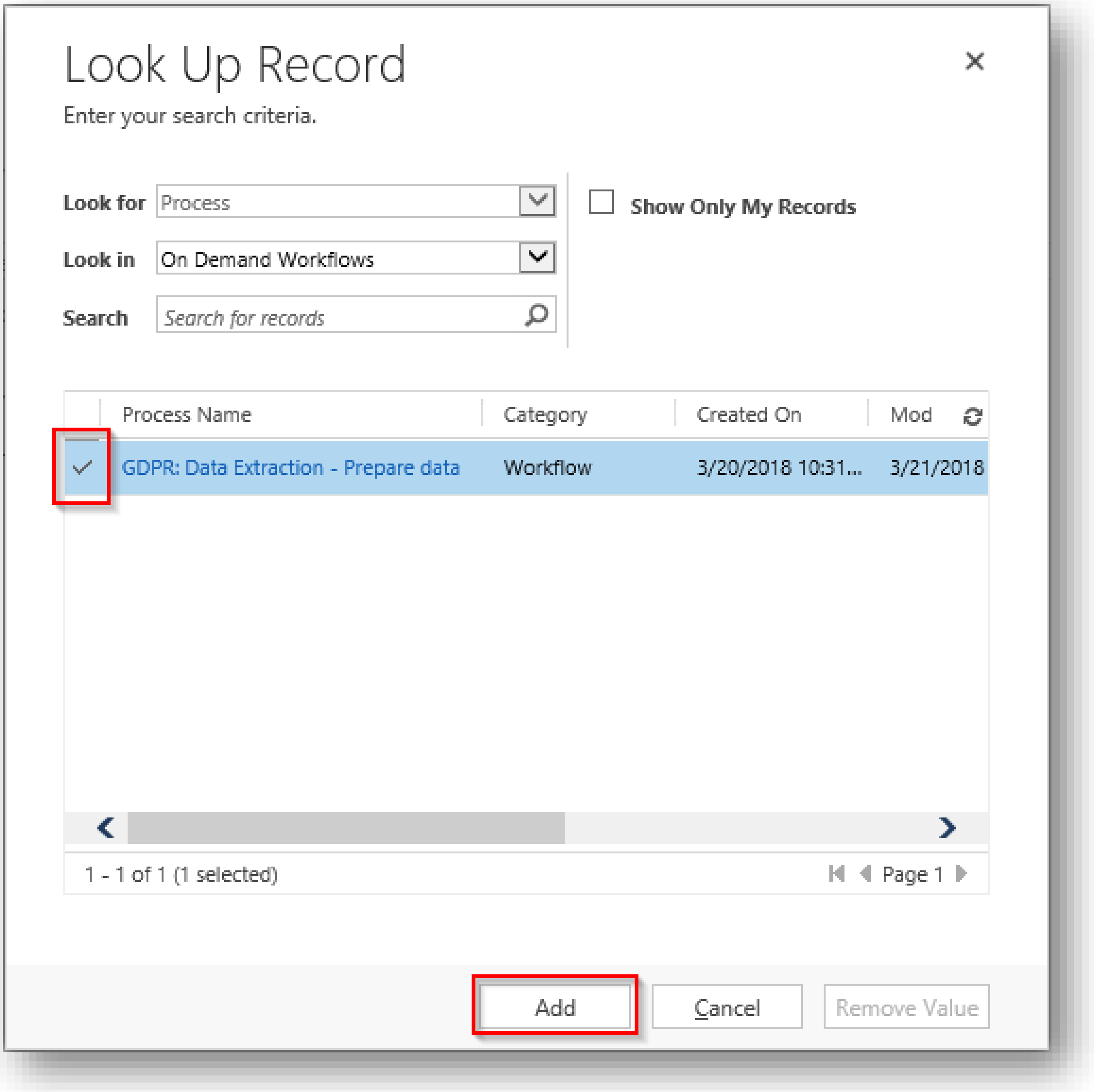
The Innofactor GDPR Solution makes it possible for you to customize the way that you work with personal information and tailor the definition of Personal data based on your business requirements.
The Personal data definitions will be used when extracting data by request of a person in your system, or for the use of data portability when transferring personal data to other external systems.

1. Navigate to **GDPR > Configuration > Personal Data Definitions**
2. Select **+ New** from the command bar. This will open a new record.
3. You will want to create a record of Personal data definition for each entity that contains information that your business values as Personal data.
   - **Name:** The name that you want for this section in the data report.
   - **Sort order:** The sort order of the section in the data report.
   - **Entity:** The name of the entity from which we want to extract the personal data.
   - **Name Attribute:** The main attribute that you want to display as a heading in the data report.
   - **Scope:** This defines which GDPR-related features the data will be used for.
     - **Data Extraction** means that the data can be used in the Data Extraction Report.
     - **Data Portability** means that the data can be used to transfer to other external systems.
   - **List Documents:** If selected, the extraction will include Sharepoint documents related to the record in question.
   - **Delete Documents:** If selected, the Sharepoint documents related to the record will be deleted when the record is deleted.
   - **FetchXML:** The specific attributes that make out the Personal Data Definition. This fetchXML need to contain a filter with the Contact ID.
4. **Save** the record.

5 Personal Data Extraction

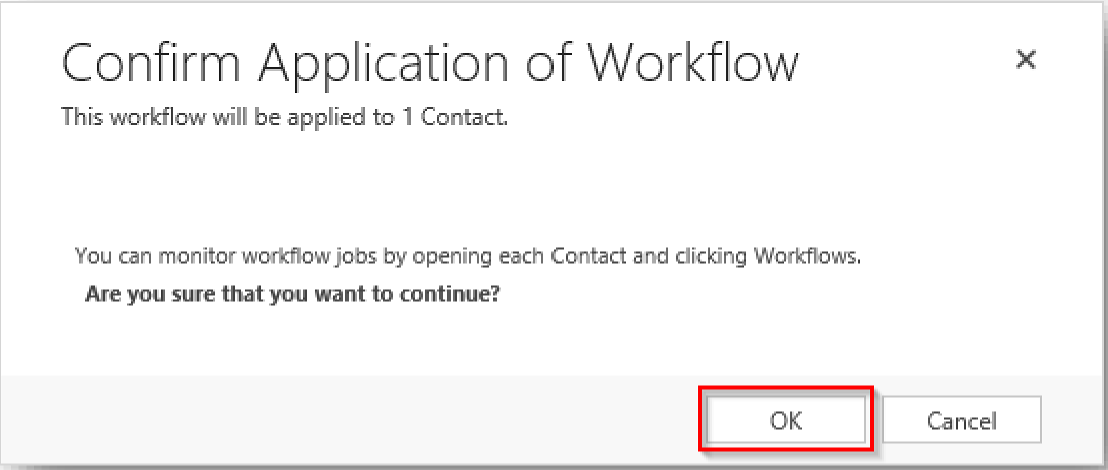
5.1.1 Preparing the personal data

1. Navigate to **GDPR > Consent > Contacts.**
2. Open a Contact record that your wish to run a data extraction report on.
3. In the command bar, select **"…"** and choose **Run workflow**.
4. In the look up record dialogue frame, select the workflow named **GDPR: Data Extraction – Prepare data** and click **Add**. This will immediately start the work-flow that prepares the data for the data extraction report.



5. Click **OK** in the following dialogue box.

Innofactor AB
Drottninggatan 68, 5tr
111 21 STOCKHOLM
Info.sweden@innofactor.com
www.innofactor.se
tel.: +46 8 20 97 30
fax: +46 8 20 97 33



Note: After running the GDPR data extraction workflow, you can view the personal data records that the workflow has prepared by navigating to **GDPR > Configuration > Personal Data**. These Personal data records are available for viewing in the system for up to one hour after running the workflow. After one hour they are automatically deleted, giving the user enough time to run the actual data extraction report that use these temporary personal data records.

5.1.2 Running the report

1. Navigate to **GDPR > Consent > Contacts.**
2. Open the same Contact record for which you prepared personal data.
3. In the command bar, select **"…"** and choose **Run report > GDPR – Data Extraction**.

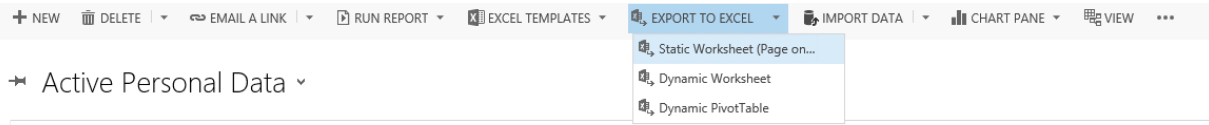
This will generate the **GDPR Data Extraction Report** based on the personal data records that was prepared by the workflow. Note that only data based on Personal data definitions with **Scope** set to **Data Extraction** (or **Extraction and Portability**) will be included in the Data Extraction report.

6 Data Portability

The Personal Data that is generated using the workflow GDPR: Data Extraction can also be used for Data Portability purposes.

There is a view for Personal Data named **Personal Data for Data Portability**. This view displays records tagged with Data Portability (i.e. Data Portability is checked on the records.). The idea is to start with that view and then get a comma separated file by using the standard functionality **Export to Excel** and **Save Excel** as a **comma separated** (.csv) file.

Go to the above described view and choose Export to Excel.



Save the Excel document. Open it and then choose to Save As -> *(.csv). Please note that there are a few extra columns in the Excel file other than those in the view. (Standard Dynamics 365 uses these in the case where data is re-imported.).

Innofactor AB
Drottninggatan 68, 5tr
111 21 STOCKHOLM
Info.sweden@innofactor.com
www.innofactor.se
tel.: +46 8 20 97 30
fax: +46 8 20 97 33

7 Right to be forgotten

We have two functions connected to “Right to be forgotten” or data minimizing that is based on that we view Dynamics 365 for Customer Engagement to function as a right now system that holds the actual and relevant data for the users to be able to do their job most efficiently. Based on that we’ve included two fields on the contact to mark who should be deleted and when to minimize the amount of information in the system that is not current.

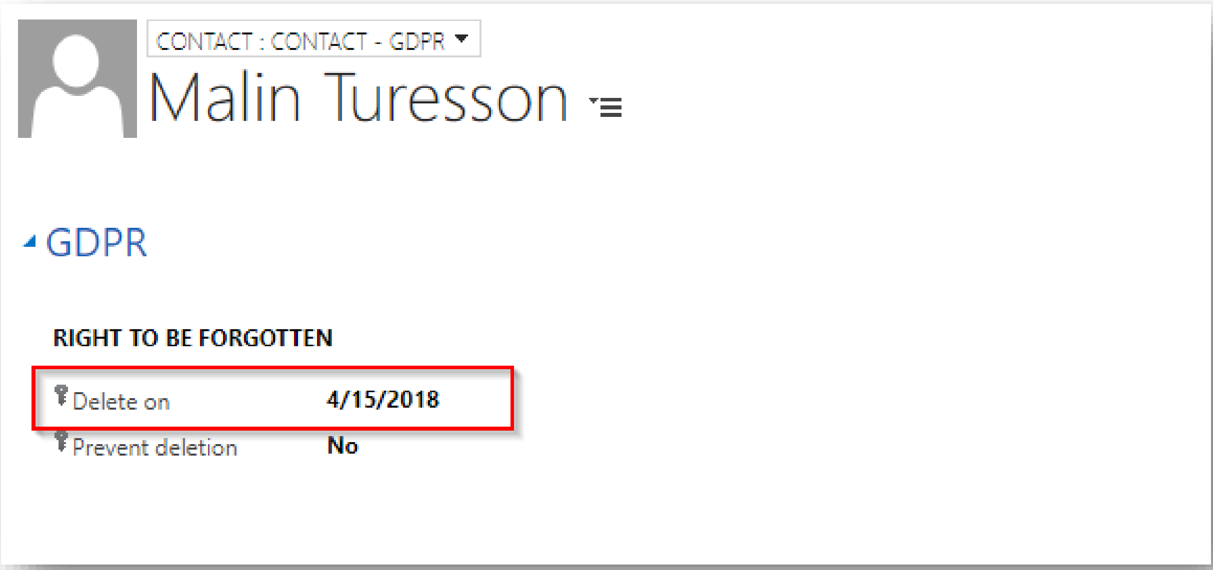
7.1.1 What gets deleted?

If you use the functionality of deleting a contact from the system following the steps below these records will be deleted:

- The **Contact.**
- All related information/entity that in Dynamics 365 CE has a relationship of type **Parental** from 1:N viewed from the **Contact.**
- All related information/entity that has **Cascade All** on the **Delete** section of the relationship.
- Potential SharePoint Sites if you have configured to use SharePoint.

7.1.2 Delete on

1. Navigate to **GDPR > Consent > Contacts.**
2. Open a Contact record that you want to mark for deletion.
3. Switch form to **Contact – GDPR.**
4. Enter a future date for when the contact should be removed in the field **Delete on.**



7.1.3 Prevent Delete

1. Navigate **GDPR > Consent > Contacts.**
2. Open a Contact record that you want to mark for deletion.
3. Switch form to **Contact – GDPR.**
4. In the field **Prevent delete** enter either **Yes** or **No.**
    - **Yes:** The contact should be kept in the system.
        - If you set Prevent delete to **Yes**, then you cannot enter a date for when the contact should be deleted.
    - **No:** The contact can be removed.

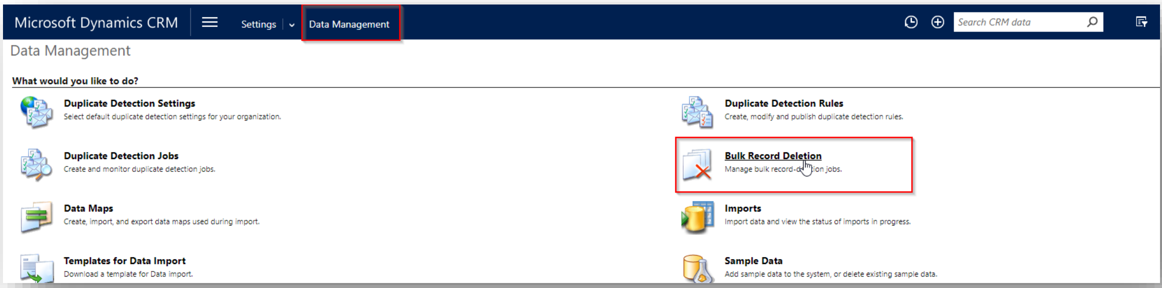
7.1.4 Recommended work process

We recommend that you create a dashboard containing possible contacts that from a data minimizing view should be deleted. Then you set up a process where you systematically either mark them for deletion or mark that you need to keep them in the system. That way you always ensure that you have actual and relevant data in your system. It is also possible to bulk change these values or that you trigger on a certain event in the system to set the fields. However, a more manual process is recommended in the first stage.

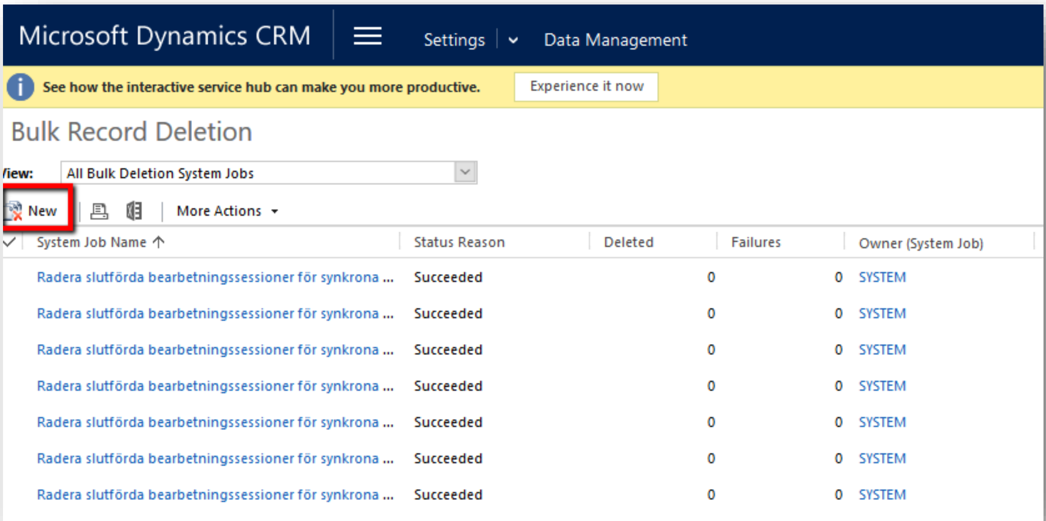
7.2 Deletion of contacts

7.2.1 Bulk Deletion Job

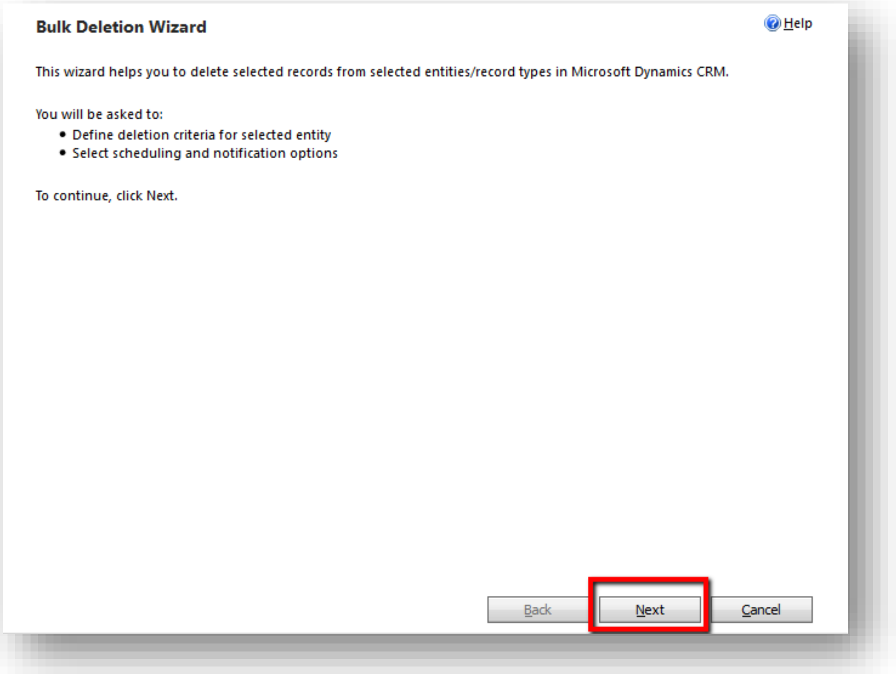
1. Go to **Settings > Data Management > Bulk Record Deletion.**



2. Here you will see a view with existing Bulk Record Deletion jobs. Click **New** to create a new job.

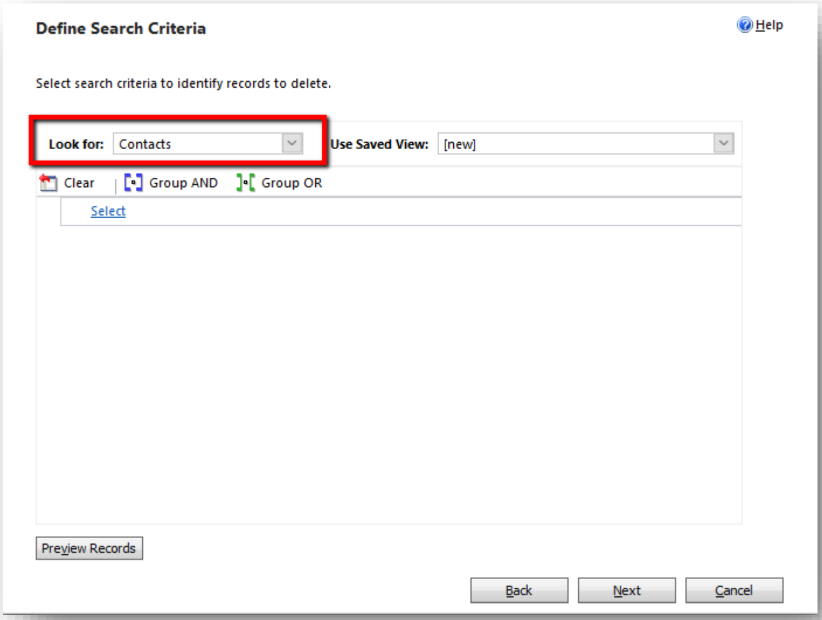


3. This will open the Bulk Deletion Wizard. Click **Next.**

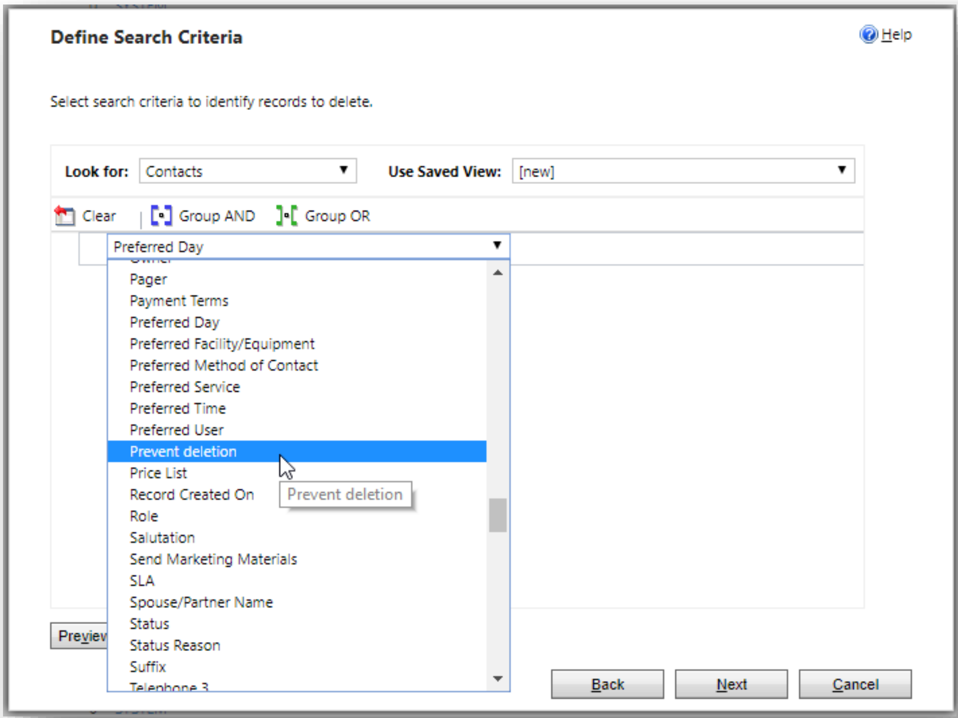


4. Here we have a view similar to Advanced Find, and we will be setting up a search criteria that gets all Contacts where **Prevent Delete = No** and **Delete on** is **"On or Before" Today's date**.

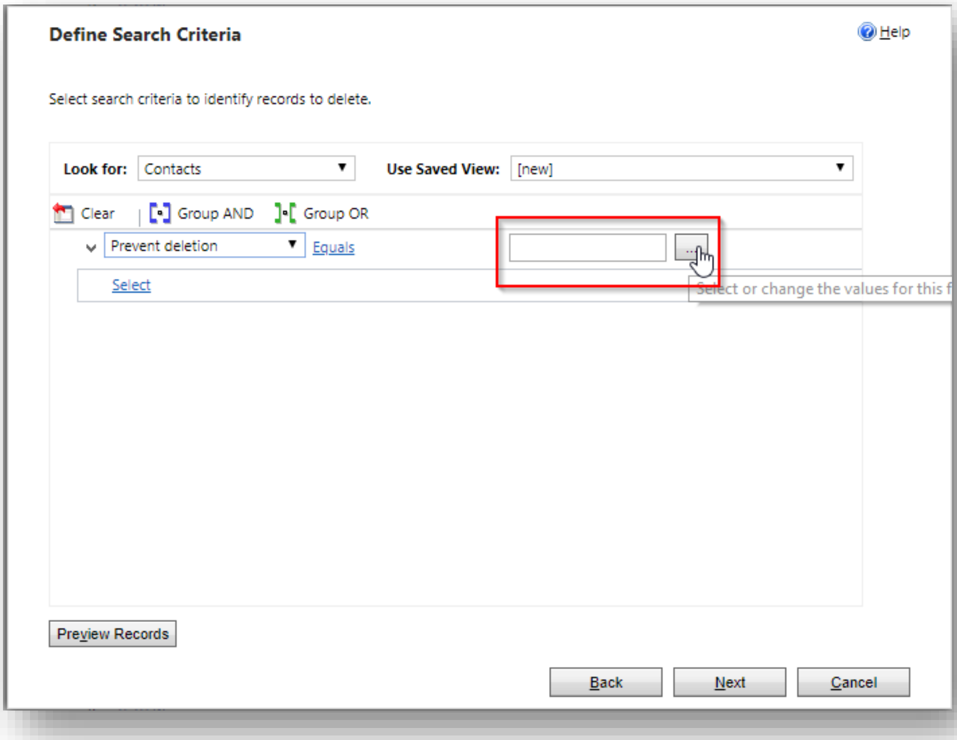
5. Search for contacts.



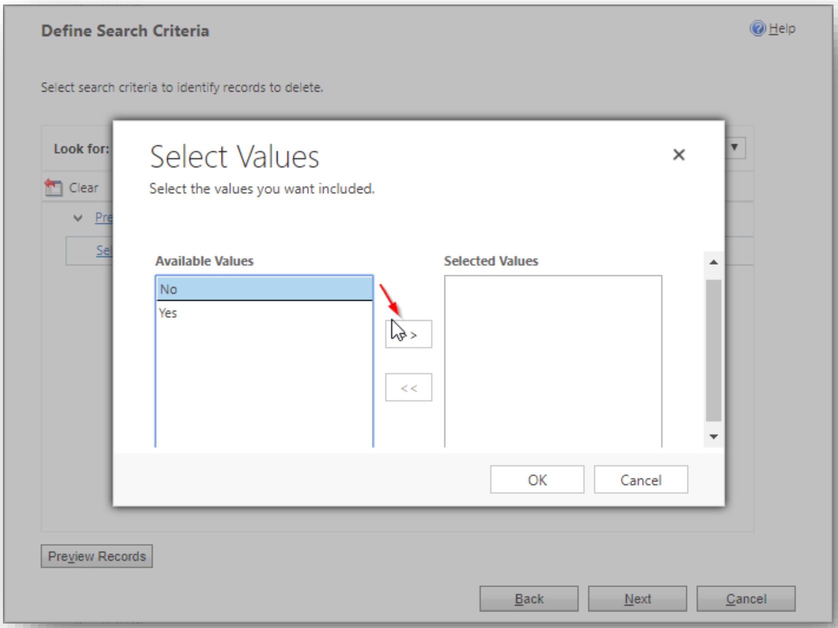
6. Next, select **"Prevent Delete"** field from the dropdown.



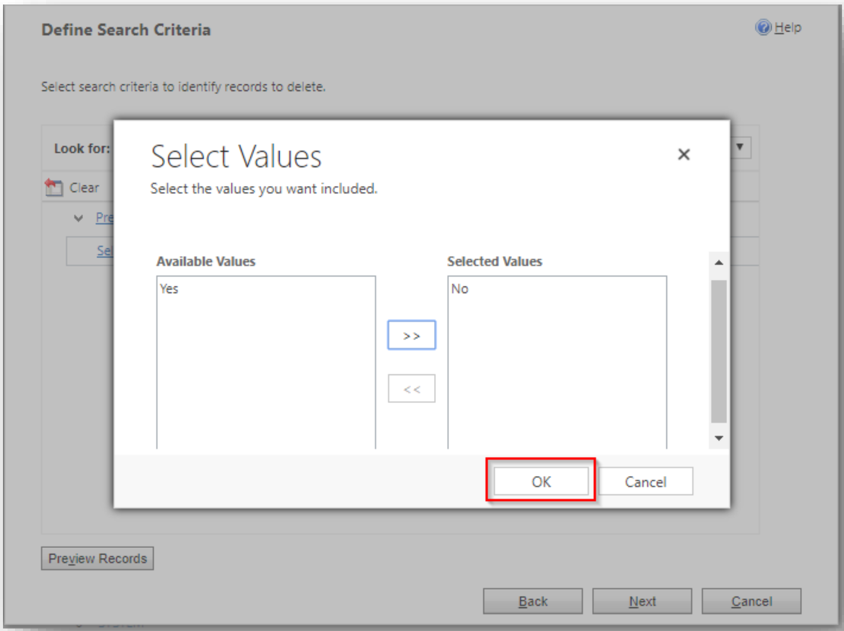
7. Click the "**...**" button

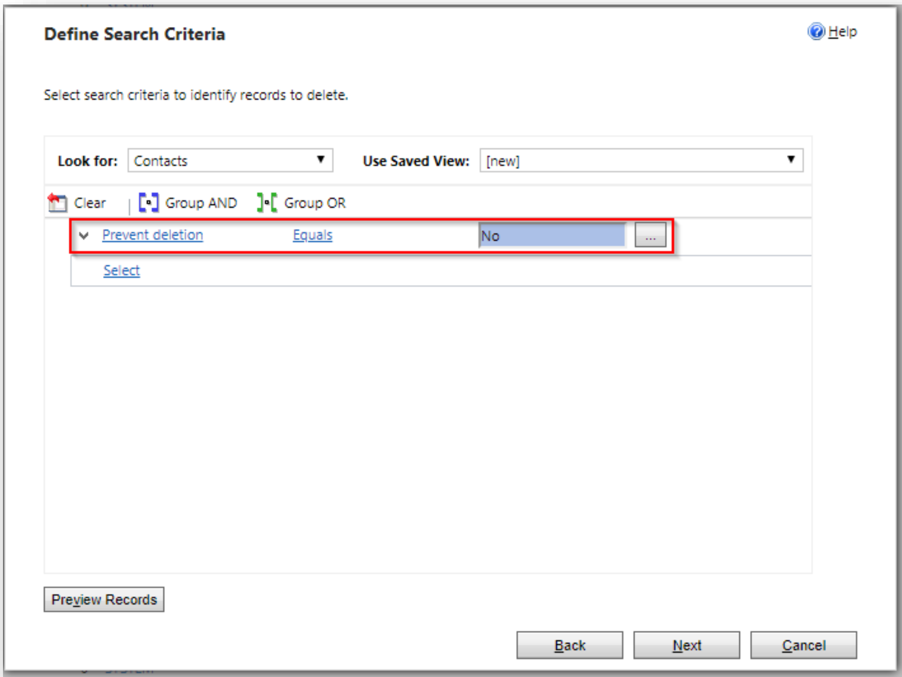


8. Select **No** and click the "**>>**" button to add it to the Selected Values.

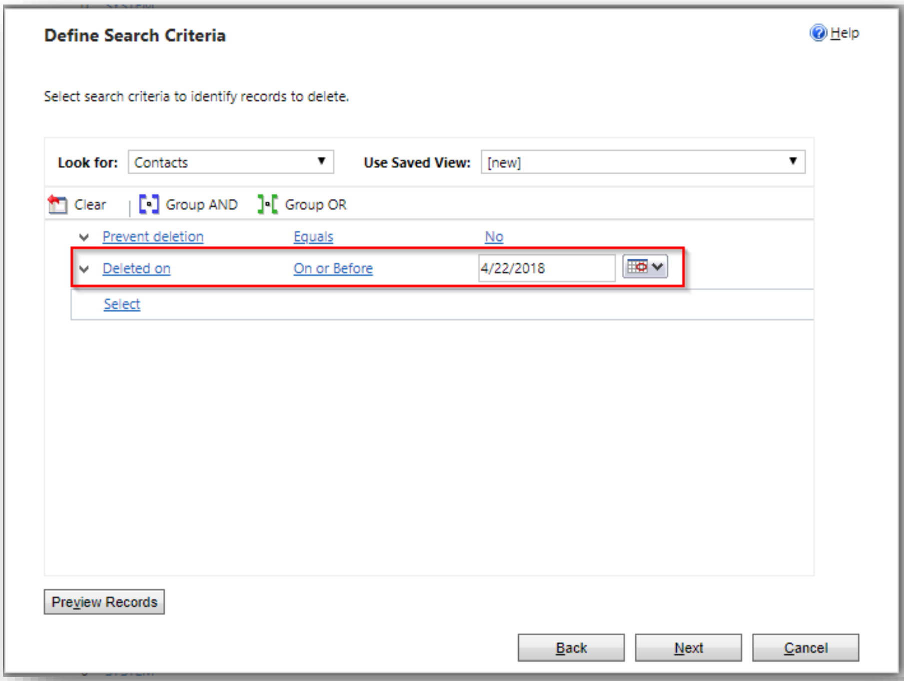


9. Click **OK**.

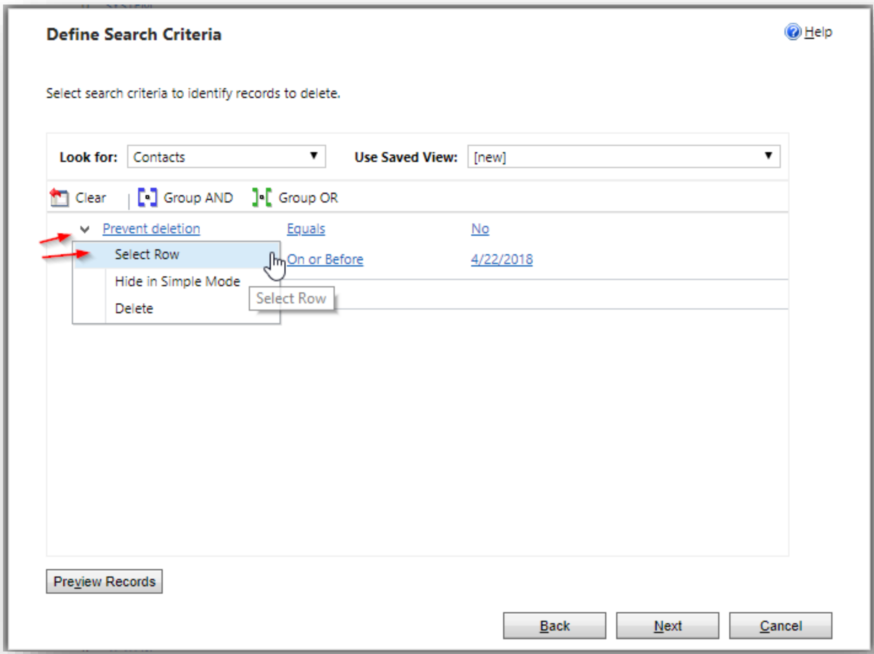

Define Search Criteria
Help
Select search criteria to identify records to delete.
Look for:
Clear
Select Values
Select the values you want included.
Available Values
Yes
Selected Values
No
> >
< <
OK
Cancel
Preview Records
Back
Next
Cancel

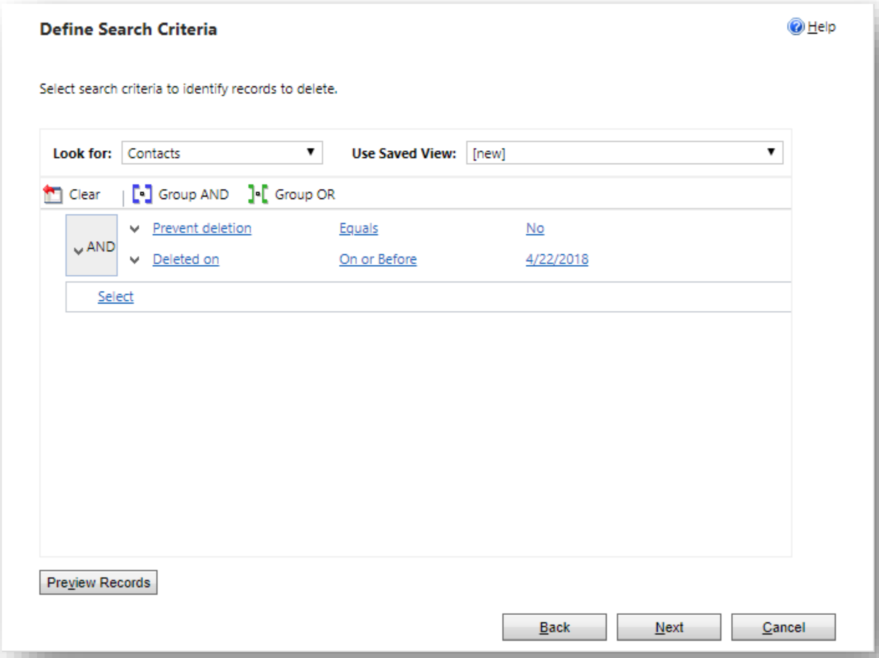

Define Search Criteria
Help
Select search criteria to identify records to delete.
Look for:
Contacts
Use Saved View:
[new]
Clear
Group AND
Group OR
Prevent deletion
Equals
No
Select
Preview Records
Back
Next
Cancel

10. Similarly, select “**Delete on**” from the dropdown of fields, select “On or Before” and select yesterday’s date.

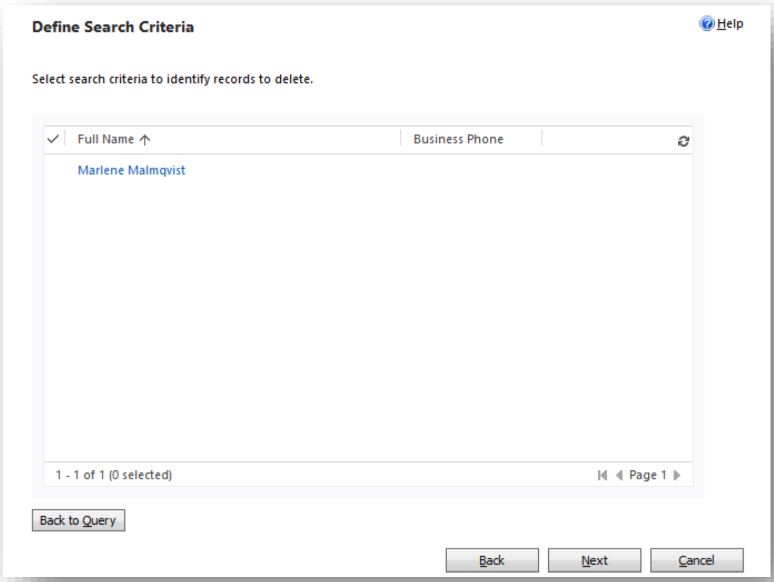


11. Select both rows by clicking on the left corner and **Select Row** on both conditions. Then click on **Group AND**. Click on **Preview Records button**.

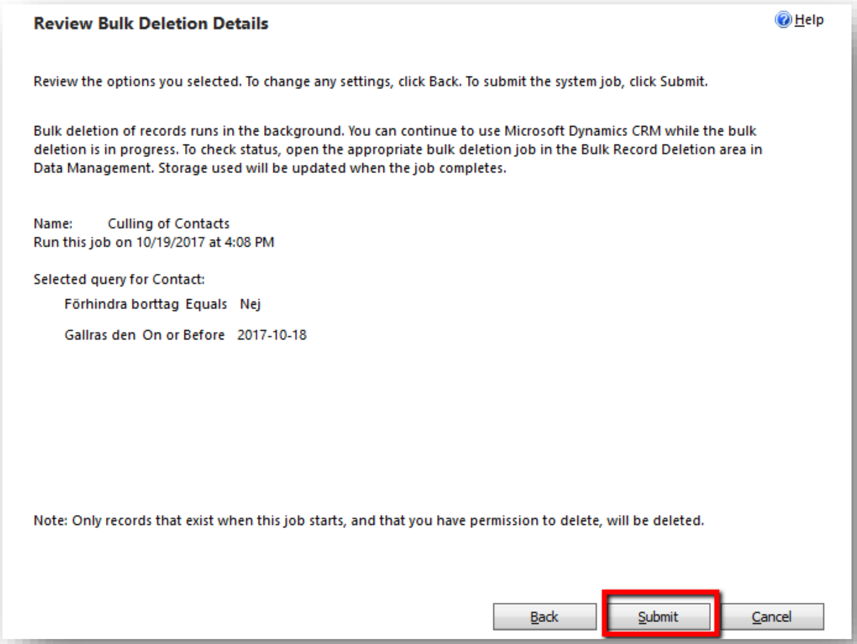


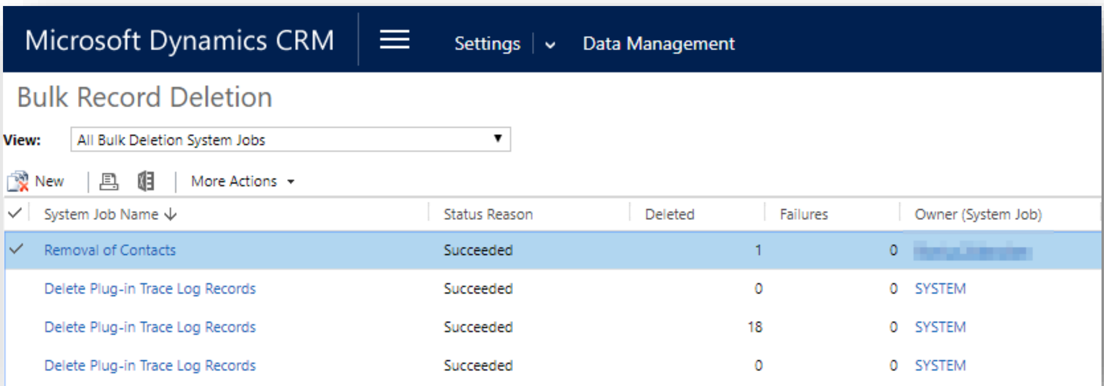


12. Click **Next.**

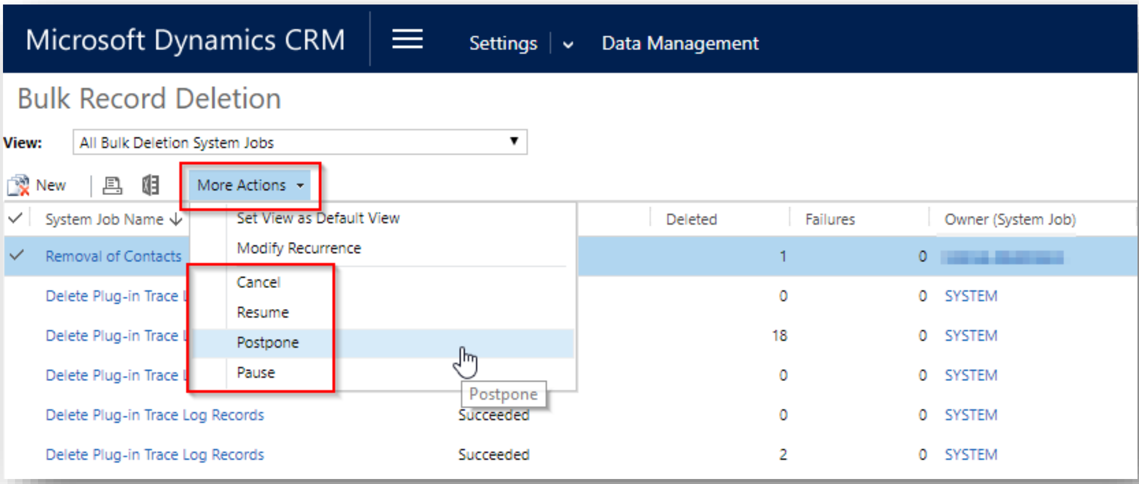


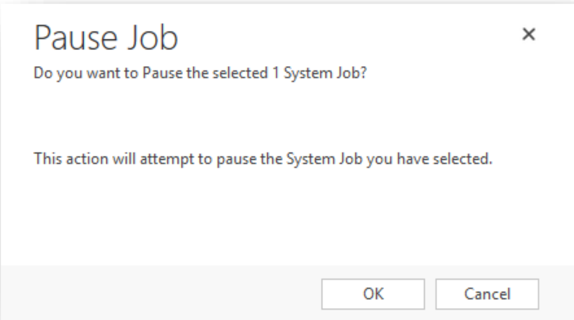
13. Click **Submit**.





More actions menu item can be used to Cancel, Resume, Postpone or Pause the existing job.


Microsoft Dynamics CRM
Settings
Data Management
Bulk Record Deletion
View:
All Bulk Deletion System Jobs
New
More Actions
Set View as Default View
Modify Recurrence
Cancel
Resume
Postpone
Pause
Postpone
System Job Name
Deleted
Failures
Owner (System Job)
Removal of Contacts
Delete Plug-in Trace Log Records
Succeeded
SYSTEM


Pause Job
Do you want to Pause the selected 1 System Job?
This action will attempt to pause the System Job you have selected.
OK
Cancel

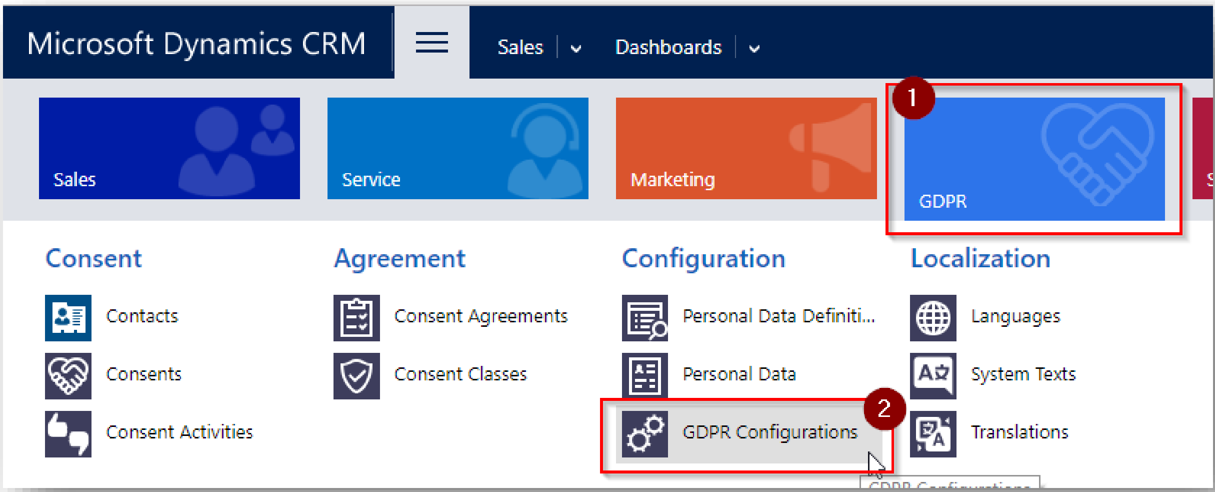
8 How to set up SharePoint-support in the solution

In the Innofactor GDPR solution we have included support for handling your documents when either removing a contact or when you want to extract personal data from the system.

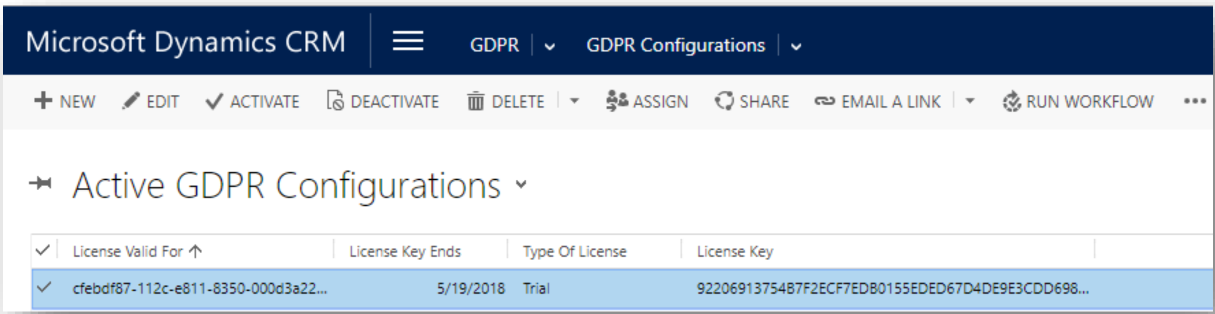
Note that this instruction only describes how you set up the integration for this solution and not the standard integration between Dynamics CE and SharePoint. For more information on that, see: https://msdn.microsoft.com/en-us/library/gg334768.aspx

You need to have System administrator privileges in the Dynamics organization that you want to set up.

1. Navigate to **GDPR > Configuration > GDPR Configuration.**

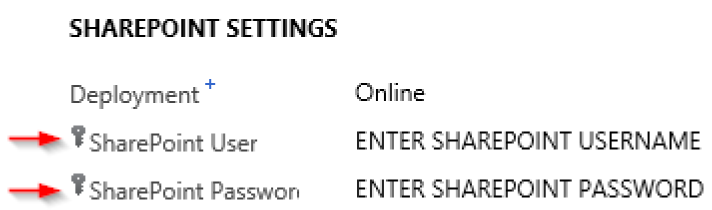


2. Open the configuration that contains your license key.



3. Proceed to define the following:

  - **Deployment:** Here you enter if you want to integrate towards an On-Premise SharePoint or an Online SharePoint.
  - **SharePoint User:** Enter the credentials of the SharePoint user that should function as an integration user.
  - **SharePoint Password:** Enter the Password for the user that you entered as a user.



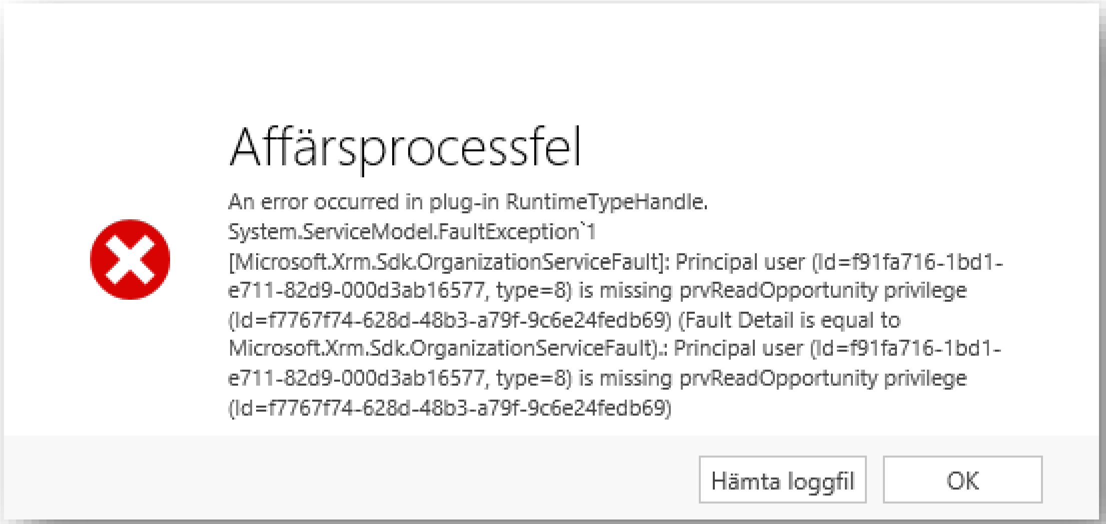
Note: Currently the Innofactor GDPR solution only supports SharePoint Online.

Note: The Innofactor GDPR solution allows the user to delete contacts and its related documents from the system (see chapter 6). However, sometimes your business may not allow documents to be deleted even if the contact is deleted. This can be customized in your system using the settings on **Personal Data Definitions** (see chapter 4, section about **Delete Documents**).

Note: In order for documents to be deleted from SharePoint when a Contact is deleted the user that deletes the Contact needs to have access to the GDPR configuration and the **SP settings** (username and password). However, you may not want the users to access that information. Instead you can set the plugin steps for plugin **ContactRemoveDocuments** to run as a specific user and then please make sure that specific user has access to the SP settings on the GDPR configuration. This step can be accomplished using the **XrmToolBox** and **Plugin Registration**.

9 Troubleshooting

To perform a Personal Data Extraction, the user who triggers the workflow “GDPR: Data Extraction – Prepare data” must have read access to the entities that are included in the FetchXML of the Personal Data Defintions. If the user has insufficient privileges, the following error will appear when “GDPR: Data Extraction – Prepare data” is triggered.



The issue is resolved by giving the user or Security Role read access to the entities that appear in the error message. In the example above, the user lacks read privileges on the Opportunity entity.