User Guide for Microsoft Dynamics 365 Business Central

Product: SD Data and GDPR Manager

Release: D365 BC V24+

Revision: September 2024

1 Contents

2 Getting Started 4
3 Installing SD Data and GDPR Manager 5
3.1 Security Setup 5
3.2 Choosing the SD Data and GDPR Manager Role 6
3.3 Accessing the SD Data and GDPR Manager Pages 7
3.4 Activating the SD Data and GDPR Manager Licence 8
3.4.1 Activating the SD Data and GDPR Manager Licence with a Free Trial 8
3.4.2 Activating the SD Data and GDPR Manager Licence with a Product Key 10
4 An important note on upgrading versions prior to v3.0.0 of SD Data and GDPR Manager to v3.0.0 or greater 11
5 Setup and Configuration 12
5.1 SD Data and GDPR Manager Assisted Setup 12
6 Understanding SD Data and GDPR Manager Concepts 14
6.1 Rules 14
6.2 Conditions 14
6.3 Validation 14
6.4 GDPR Monitored List 14
6.5 GDPR Requests 14
7 Using SD Data and GDPR Manager 15
7.1 SD Data and GDPR Manager – Setup Card 15
8 Using SD Data and GDPR Manager – Rules 18
8.1 SD Data and GDPR Manager – Rules List 18
8.2 SD Data and GDPR Manager – Rules Card 19
8.3 SD Data and GDPR Manager – Expressions List 23
8.4 SD Data and GDPR Manager – Creating a Rule – Example 1 24
8.5 SD Data and GDPR Manager – Using the Rule – Example 1 28
8.6 SD Data and GDPR Manager – Creating a Rule – Example 2 30
8.7 SD Data and GDPR Manager – Using the Rule – Example 2 33
9 Using SD Data and GDPR Manager – GDPR Requests 34
9.1 SD Data and GDPR Manager – GDPR Monitored Tables List 34
9.2 SD Data and GDPR Manager – GDPR Monitored Table Card 35
9.3 SD Data and GDPR Manager – GDPR Requests 40
9.3.1 Right to Access 44

9.3.2 Right to Information 45
9.3.3 Right to Rectification 46
9.3.4 Right to Portability 47
9.3.5 Right to Erasure 48
9.3.6 Right to Restrict 49
9.3.7 Right to Encryption 50
10 Viewing GDPR Encrypted Fields 51
11 Uninstalling SD Data and GDPR Manager 54

2 Getting Started

The Data Management component of SD Data and GDPR Manager enables you to validate and enforce rules on the data input into your Dynamics 365 Business Central Database without the need to write any code. Creating user-definable rules allows you to validate your data entry and to keep your data clean. Each rule has a condition that must be met before its validation is run.

The GDPR component of SD Data and GDPR Manager enables you to meet your GDPR requirements with the ability to log requests, respond on data held, encrypt fields, and redact information.

You can also set up field level security using SD Data and GDPR Manager.

Note: If upgrading versions prior to v3.0.0 of SD Data and GDPR Manager to v3.0.0 or greater be aware that the method used to generate and store the passphrase key has changed in this version of SD Data and GDPR Manager (v3.0.0. code base Dynamics 365 Business Central v17). Prior versions of SD Data and GDPR Manager generated and stored the passphrase key in a different manner.

This has implications for upgrading from previous versions of SD Data and GDPR Manager. All encrypted data (encrypted by SD Data and GDPR Manager) will have to be decrypted in SD Data and GDPR Manager prior to upgrading to version 3.0.0 or later.

Note: If uninstalling SD Data and GDPR Manager be aware that all encrypted data (encrypted by SD Data and GDPR Manager) will have to be decrypted in SD Data and GDPR Manager prior to uninstalling the product. Otherwise, your encrypted data will no longer be accessible.

3 Installing SD Data and GDPR Manager

SD Data and GDPR Manager is available to download from AppSource or you can install the App from within Business Central using Extension Marketplace.

The **Allow HttpClient Requests** option is automatically enabled on install of SD Data and GDPR Manager. Switching on the **Allow HttpClient Requests** option allows SD Data and GDPR Manager to call an API that sends and returns licence key information to activate the product licence and to call GitHub to import sample data for the product. The **Allow HttpClient Requests** option is automatically enabled on install of SD Data and GDPR Manager.

3.1 Security Setup

We have provided the following permission sets for SD Data and GDPR Manager: SDY UD ADMIN, SDY UD USER and SDY UD VIEW *(Figure 3-1)*.

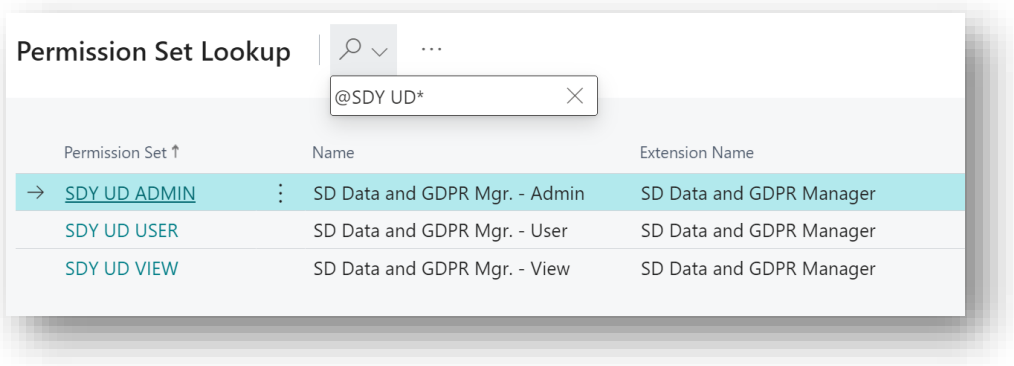


Figure 3-1

We have also created extensions on the following standard Microsoft Dynamics 365 Business Central Permissions:

- Exten. Mgt. - Admin includes SDY UD ADMIN permissions.
- D365 BUS FULL ACCESS includes SDY UD USER permissions.
- D365 BASIC includes SDY UD VIEW permissions.

3.2 Choosing the SD Data and GDPR Manager Role

1. From your Dynamics 365 Business Central Web Client, in the app bar, select the **Settings** icon and then select **My Settings** *(Figure 3-2)*.

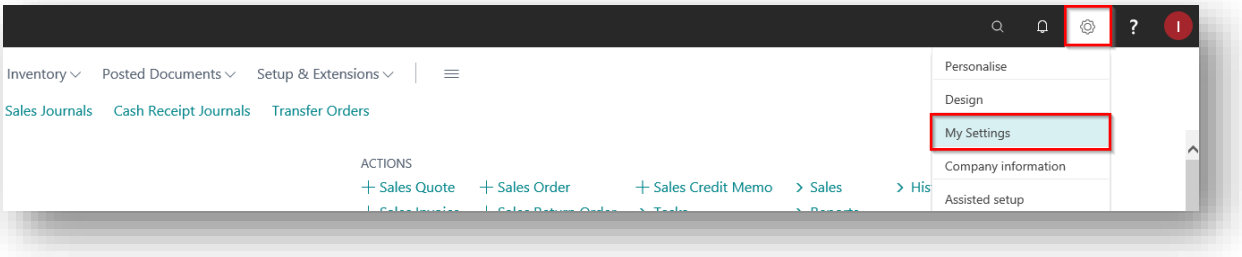


Figure 3-2

2. In the **My Settings** page, on the **Role** field, select the **AssistEdit** icon *(Figure 3-3)*.

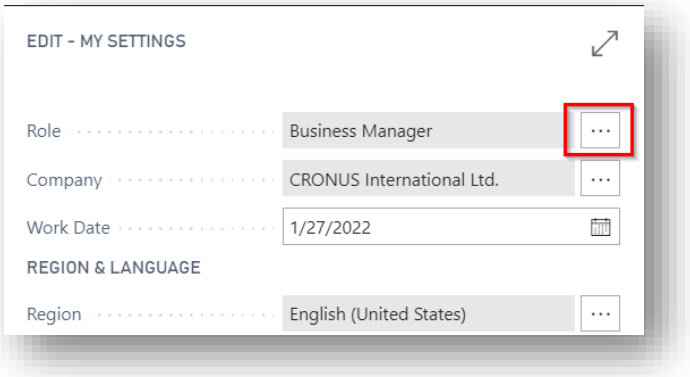


Figure 3-3

3. You should see **SD Data and GDPR Manager** in the list of Roles *(Figure 3-4)*.

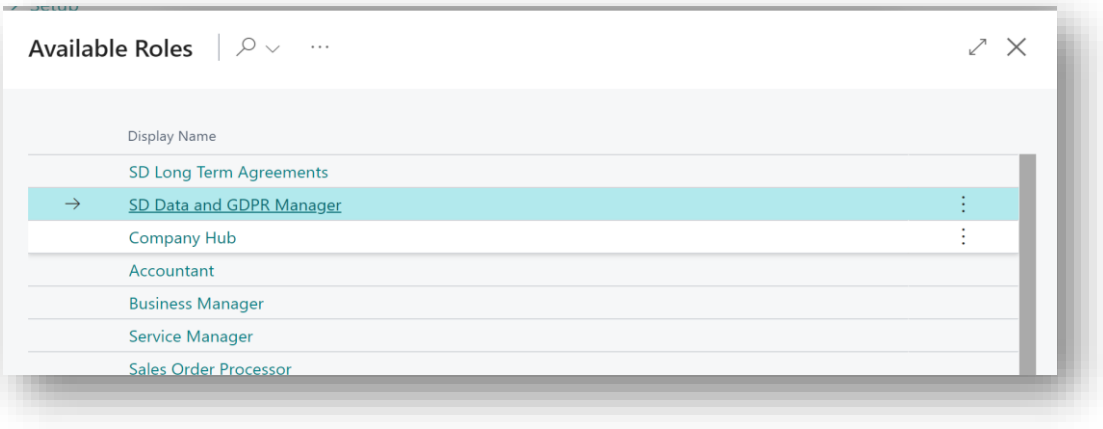


Figure 3-4

4. Choose **SD Data and GDPR Manager** and click **OK**.

5. The **SD Data and GDPR Manager** Role should now be displayed in the **Role** field *(Figure 3-5)*.

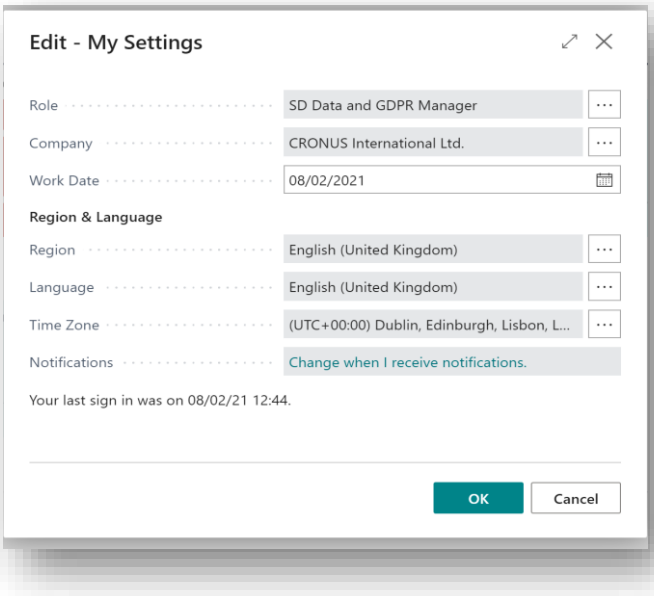


Figure 3-5

3.3 Accessing the SD Data and GDPR Manager Pages

Use the **Tell Me** to search for SD Data and GDPR Manager pages. Begin typing **SD** or **Data** to see a list of the SD Data and GDPR Manager pages *(Figure 3-6)*.

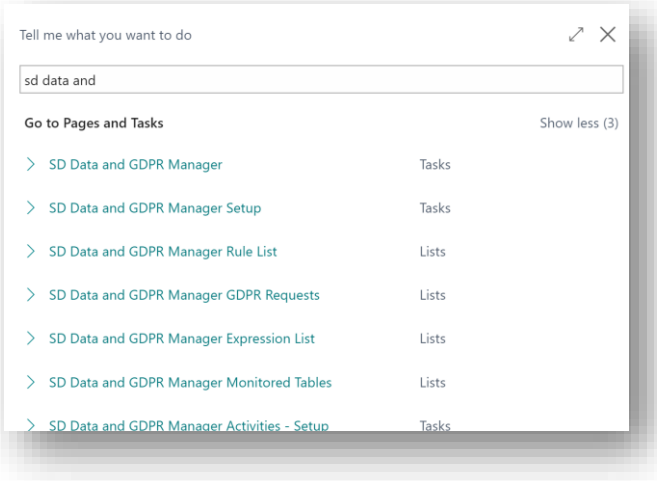


Figure 3-6

3.4 Activating the SD Data and GDPR Manager Licence

To use **SD Data and GDPR Manager**, you must activate the licence.

1. From the **Tell Me**, search for and select the **SD Data and GDPR Manager Setup** card. You will be prompted that "Your SD Data and GDPR Manager license needs to be validated". Choose **Yes** *(Figure 3-7)*.

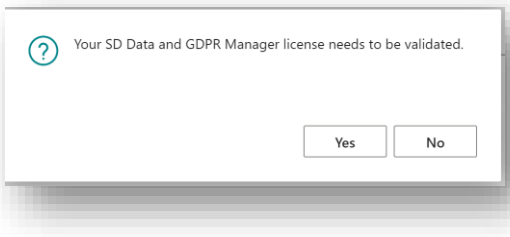


Figure 3-7

2. You will then see the **Activate your product** page.

3.4.1 Activating the SD Data and GDPR Manager Licence with a Free Trial

If you have not received a Product Key from Simply Dynamics Ltd. and want to avail of a free 30 day trial:

1. In the **Activate your Product** page *(Figure 3-8)*
   Enter your company name in **Company Name.**
   Enter your company email in **Email.**
   Choose **Free Trial**

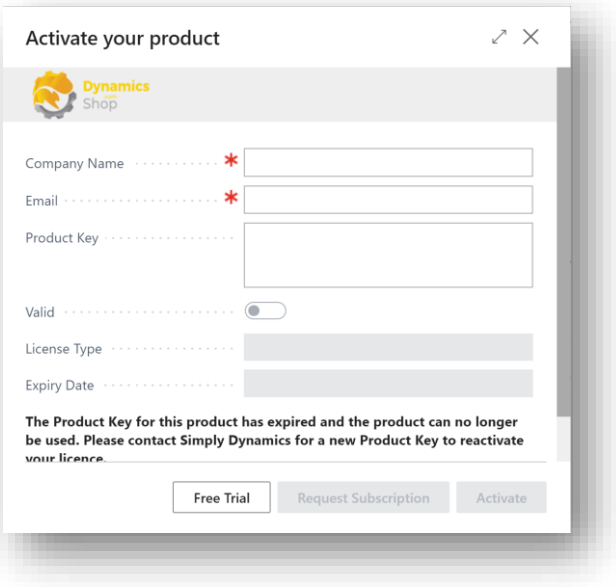


Figure 3-8

2. You are then prompted to choose **Yes** to activate your free trial. Choose **Yes** *(Figure 3-9)*.

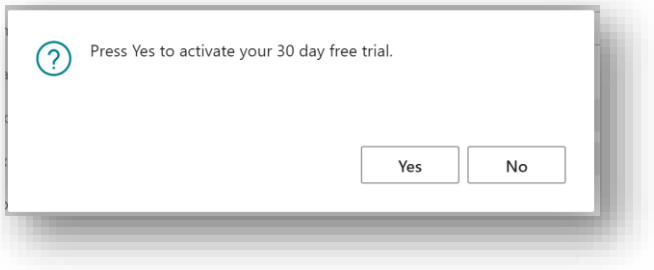


Figure 3-9

3. The **Activate your product page** will update to display a message that the activation was successful. The expiry date will depend on the date that you activated your free trial *(Figure 3-10)*.

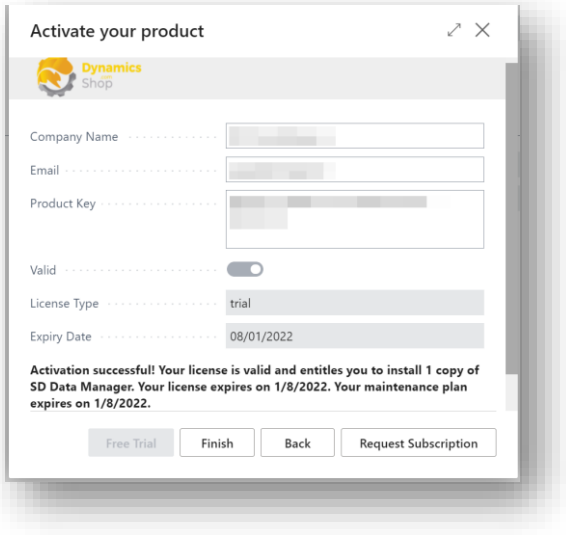


Figure 3-10

4. Choose **Finish** to exit the page.

5. When your Free Trial has expired, choose **Request Subscription** to request a Product Key from Simply Dynamics.

3.4.2 Activating the SD Data and GDPR Manager Licence with a Product Key

Take the following steps if you have received a Product Key from Simply Dynamics Ltd.:

1. In the **Activate your product** page *(Figure 3-11)*:
   Enter your company name in **Company Name**
   Enter your company email in **Email.**
   Paste the supplied product key into the **Product Key** field. **Tab off the Product Key field to validate the contents of the field and to enable the Activate key**. Choose **Activate**.

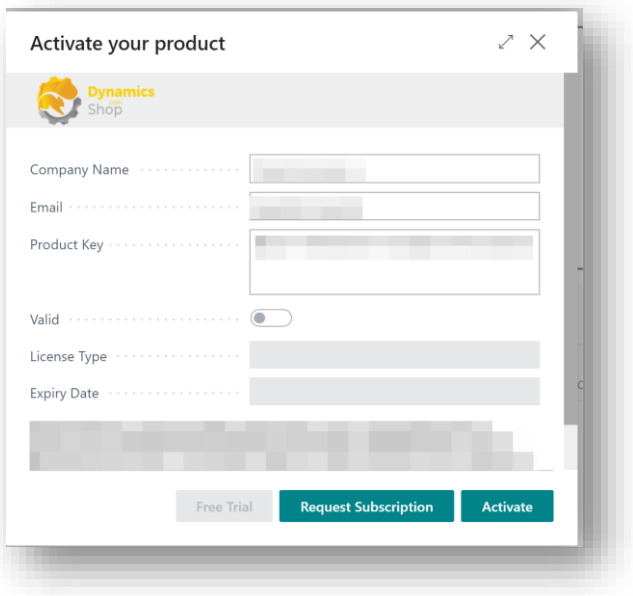


Figure 3-11

2. The **Activate your product** page will update to display a message that the activation was successful. The expiry date will depend on the expiration date of your subscription licence.

3. Choose **Finish** to exit the page.

4 An important note on upgrading versions prior to v3.0.0 of SD Data and GDPR Manager to v3.0.0 or greater

The method used to generate and store the passphrase key has changed in this version of SD Data and GDPR Manager (v3.0.0. code base Dynamics 365 Business Central v17). Prior versions of SD Data and GDPR Manager generated and stored the passphrase key in a different manner.

Note: This has implications for upgrading from previous versions of SD Data and GDPR Manager. All encrypted data (encrypted by SD Data and GDPR Manager) will have to be decrypted in SD Data and GDPR Manager prior to upgrading to version 3.0.0 or later.

5 Setup and Configuration

5.1 SD Data and GDPR Manager Assisted Setup

You can easily import default setup for SD Data and GDPR Manager using the **Assisted Setup** Action on the **SD Data and GDPR Manager Setup** card. The data imported using the Assisted Setup contains sample Rules and Expressions and sample setup for GDPR Monitored Tables.

1. In the **SD Data and GDPR Manager** page, from the menu choose the **Process** group, and then **Assisted Setup** *(Figure 5-1)*.

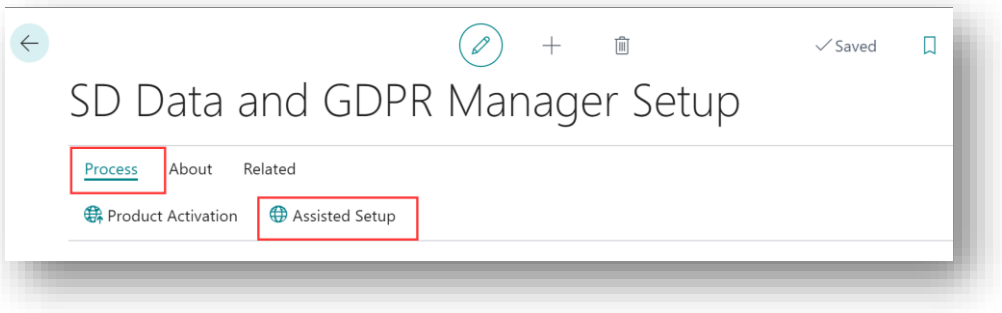


Figure 5-1

2. You are prompted that importing setup will overwrite and modify existing data in SD Data and GDPR Manager. Choose **Yes** if this is your first time to use SD Data and GDPR Manager and you have not already created any setup in SD Data and GDPR Manager *(Figure 5-2)*.

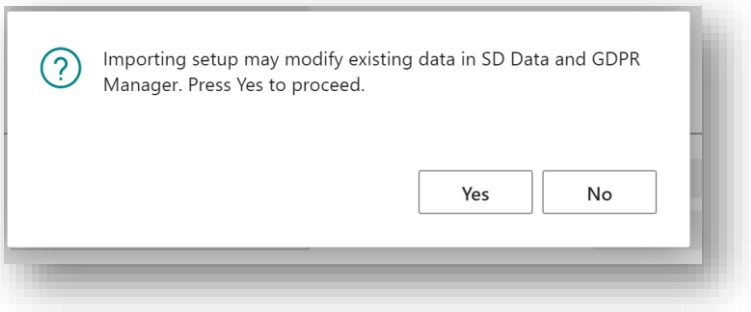


Figure 5-2

3. You are then prompted, “Are you sure?” Choose **Yes** *(Figure 5-3)*.

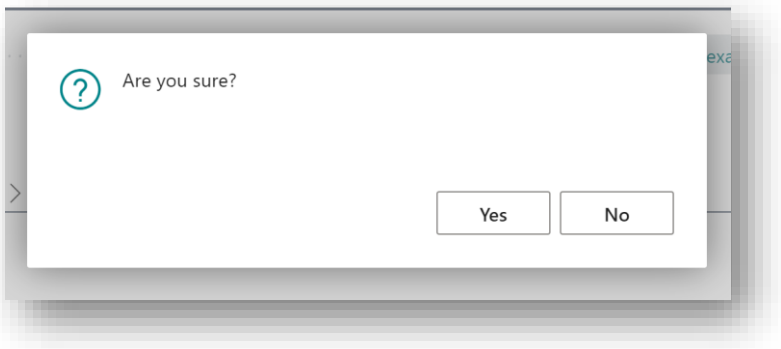


Figure 5-3

4. You will then receive a prompt like the below that the default setup has imported. Choose **OK** *(Figure 5-4)*.

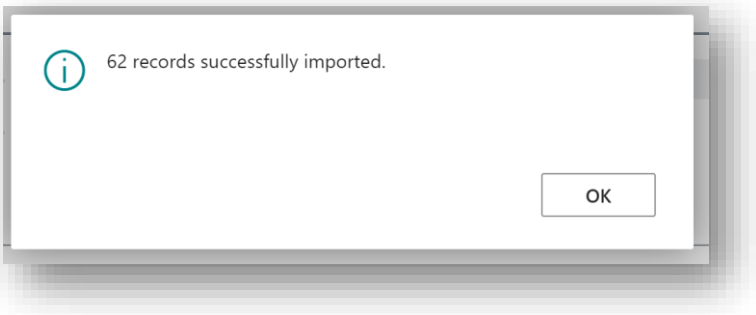


Figure 5-4

6 Understanding SD Data and GDPR Manager Concepts

The Data Management component of SD Data and GDPR Manager allows you to validate and enforce rules on the data entered into your Dynamics 365 Business Central Database by setting up your own user definable rules. These rules are created without the need to write any code and allow you to validate your data entry and to keep your data clean. Each rule has a condition that must be met before its validation is run.

The GDPR component of SD Data and GDPR Manager enables you to meet your GDPR requirements with the ability to log requests, respond on data held, encrypt fields, and redact information.

6.1 Rules

A rule applies to a particular table and is evaluated when a record is either inserted, modified, or deleted.

6.2 Conditions

A condition refers to the list of checks, as defined in the rule, which the record must pass before any validations can take place.

6.3 Validation

Validation refers to the list of checks, as defined in the rule, which the record must pass. Should the validation fail, depending on setup, the user is either notified or an error message is raised.

6.4 GDPR Monitored List

Select any table and any field in Microsoft Dynamics 365 Business Central to add to your GDPR monitored list. You can also easily set up related tables as part of this monitored list.

6.5 GDPR Requests

Once you have set up your GDPR Monitored Tables and Fields, you can then search, report, export, correct, erase, restrict or encrypt this data all within Microsoft Dynamics 365 Business Central.

7 Using SD Data and GDPR Manager

7.1 SD Data and GDPR Manager – Setup Card

The **SD Data and GDPR Manager Setup** card is accessed from the **SD Data and GDPR Manager Role Centre**, by selecting the **Setup** action, or, by searching for the **SD Data and GDPR Manager Setup** page in the **Tell Me**.

In the **SD Data and GDPR Manager** page, expand the **Rules** FastTab. The **Rules** FastTab contains the following fields (*Figure 7-1*):

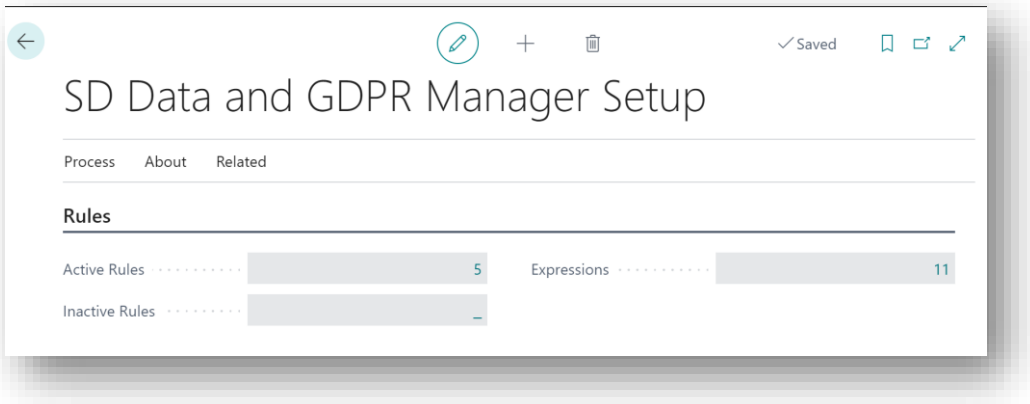


Figure 7-1

- **Active Rules** – A flowfield count of the active user definable rules that have been set up in SD Data and GDPR Manager. These rules allow you to validate and control the data entered in your database. Users can drill through on this flowfield to view the Rule List.

- **Inactive Rules** – A flowfield count of the inactive user definable rules that have been set up in SD Data and GDPR Manager. Users can drill through on this flowfield to view the Rule List.

- **Expressions** – A flowfield count of the expressions that have been set up in SD Data and GDPR Manager. A Regular Expression is a pattern that defines an amount of text. The expressions are used in the conditions and validations of the rules. Users can drill through on this flowfield to view the Expression List.

The **GDPR** FastTab contains the following fields (*Figure 7-2*):

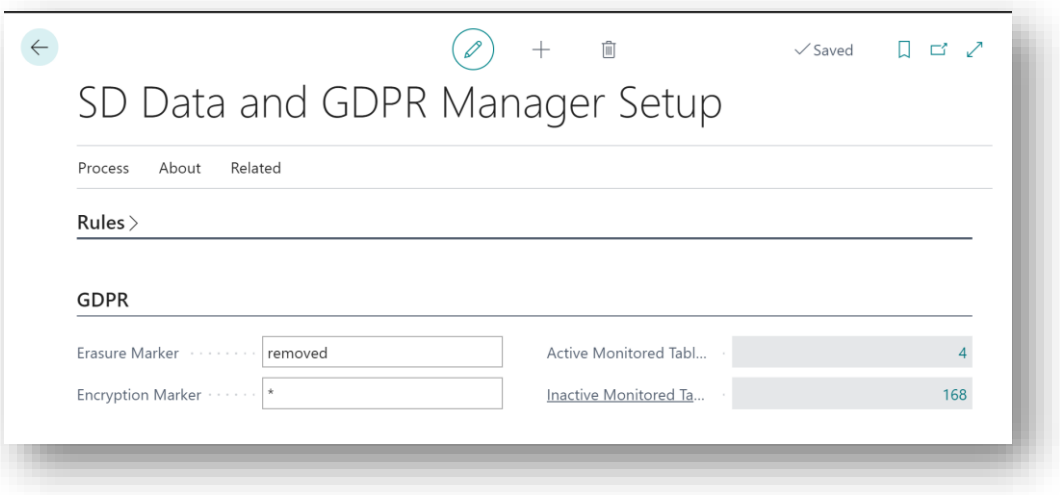


Figure 7-2

- **Erasure Marker** –This field specifies the text to be stamped to a field when data has been erased as part of a GDPR erasure request. Defaults to **removed**.

- **Encryption Marker**– This field allows the user to define the marker to use on a field when data has been encrypted as part of a GDPR encryption request. Defaults to ***.**

  Note: Date fields because of their data type cannot be stamped with an encryption marker otherwise a runtime error would occur. Only fields with a datatype of text or code can be stamped with the encryption marker. Date fields when encrypted will appear as <blank>.

- **Active Monitored Tables** – A flowfield count of the active tables that you have added to your GDPR monitored list. Users can drill through on this flowfield to view the Monitored Tables List.

- **Inactive Monitored Tables** – A flowfield count of the active tables that you have added to your GDPR monitored list. Users can drill through on this flowfield to view the Monitored Tables List.

The following actions are available on the **SD Data and GDPR Manager Setup** card in the **Related** group on the menu (*Figure 7-3*):

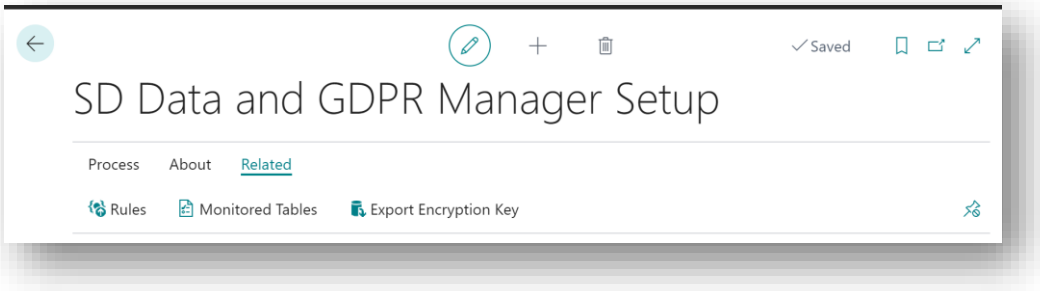


Figure 7-3

- **Rules** – Choose this Action to open the Rule List.

- **Monitored Tables** – Choose this Action to open the GDPR Monitored Tables List.

- **Export Encryption Key** – When the first GDPR Encryption request is run and a passphrase doesn't exist in isolated storage, SD Data and GDPR Manager generates and uses a random 32-character passphrase to encrypt fields and then stores this passphrase in isolated storage to use for subsequent encryption and decryption calls. This Export Encryption Key action allows users with SUPER Permission to extract the passphrase key and store it safely.

  Note: We recommend that you export and store this passphrase key safely.

8 Using SD Data and GDPR Manager – Rules

8.1 SD Data and GDPR Manager – Rules List

The **SD Data Manager Rule List** is accessed from the **Role Centre** by drilling through on the **Active Rules** cue, the **SD Data Manager and GDPR Setup Card** or by searching the **Tell Me** (*Figure 8-1*).

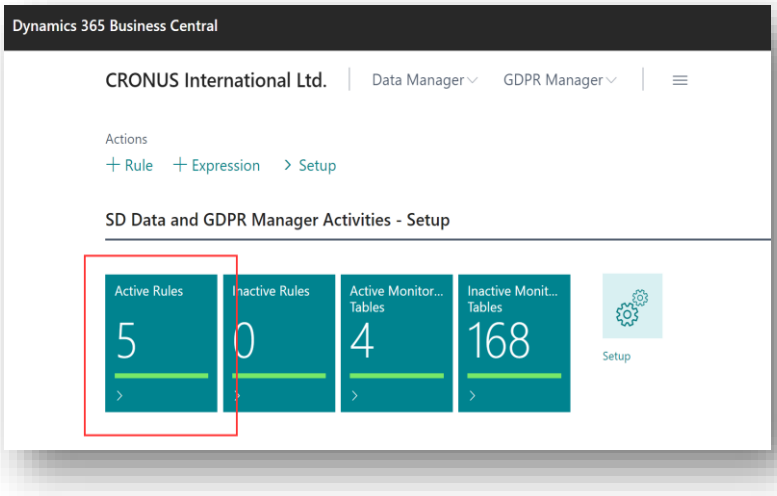


Figure 8-1

A rule in SD Data and GDPR Manager defines the table to apply the data rule to and is evaluated when a record is either inserted, modified, or deleted. The rules also define the conditions that the record must pass before any validations can take place on the record. Should the validation fail then the user can be notified, or an error raised. If you chose to import the **Assisted Setup**, several sample rules will have been created in SD Data and GDPR Manager.

To create a new rule, from the menu, choose **+New**. To view or edit an existing rule from the **Manage** group choose **Edit** or **View** (*Figure 8-2*).

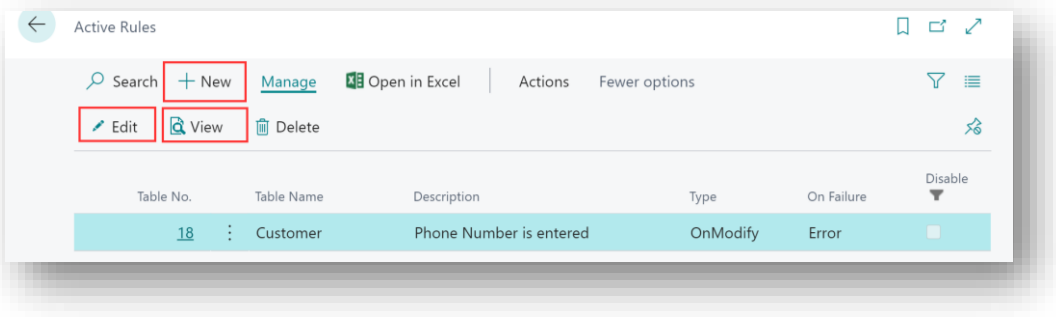


Figure 8-2

8.2 SD Data and GDPR Manager – Rules Card

The SD Data and GDPR Manager Rule Card contains the following fields in the **General** FastTab (*Figure 9-3*):

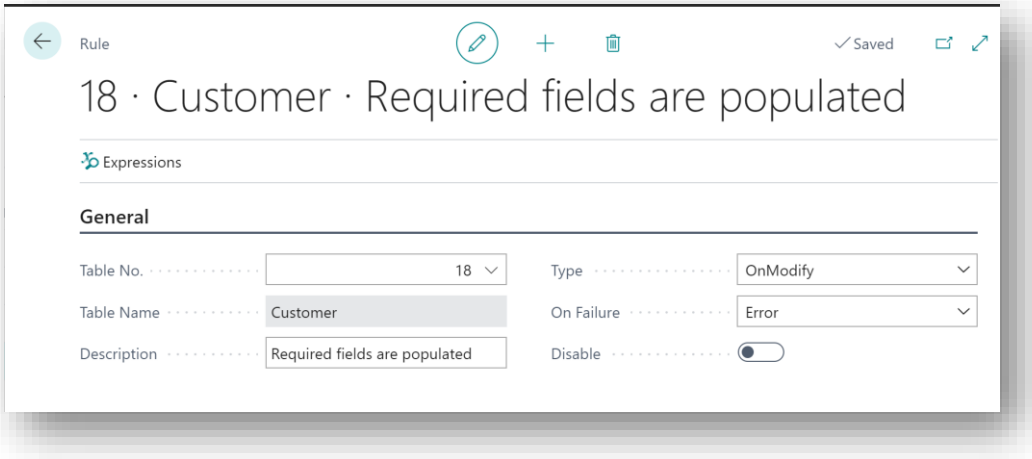


Figure 8-3

- **Table No.** – Specifies the number of the Dynamics 365 Business Central Table to which the rule is to apply.

- **Table Name** – Displays the name of the table specified in the **Table No.** field.

- **Description** – Enter a user defined description for the rule.

- **Type** – This field specifies which table action the rule is triggered on. Options are **OnInsert**, **OnModify**, **OnDelete**.

  OnInsert – The rule is triggered when a record is first created.

  OnModify - The rule is triggered when record changes are saved to the database.

  OnDelete - The rule is triggered when a record is deleted.

- **On Failure** – Select the action taken should one or more of the validations fail. Options are **Error**, **Notify First**, **Notify All**, **Ignore**.

  Error - Raise an error on the field that fails validation.

  Notify First - Inform the user of only the first failure. The changes are saved to the record.

Notify All - Inform the user of all failures. The changes are saved to the record.

Expand the **Condition** FastTab *(Figure 8-4*):

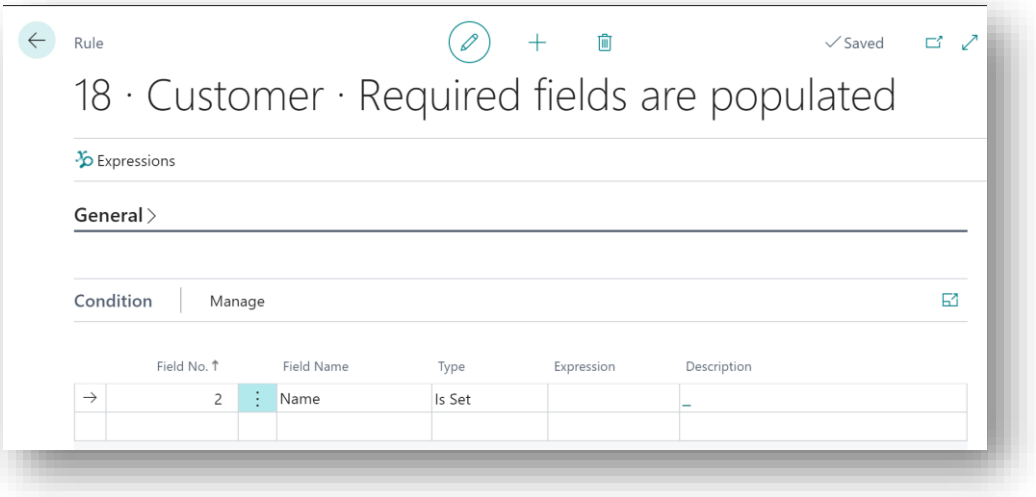


Figure 8-4

- **Field No.** – Enter the number of the field on which to run the condition.
- **Field Name** – Displays the name of the chosen **Field No.**
- **Type** – Select the type of check to perform on the field. Options are **Is Set, Is Not Set, Matches Expression.**

  Is Set - The field is not empty or has a value other than the default.

  Is Not Set - The field is empty or has a value of the default value.

  Matches Expression - The value in the field matches that specified in the **Expression** field.

- **Expression** – Select the expression to use when the **Type** is set to **Matches Expression**.
- **Description** – Displays the description of the expression chosen in **Expression**.

Expand the **Validation** FastTab *(Figure 8-5*):

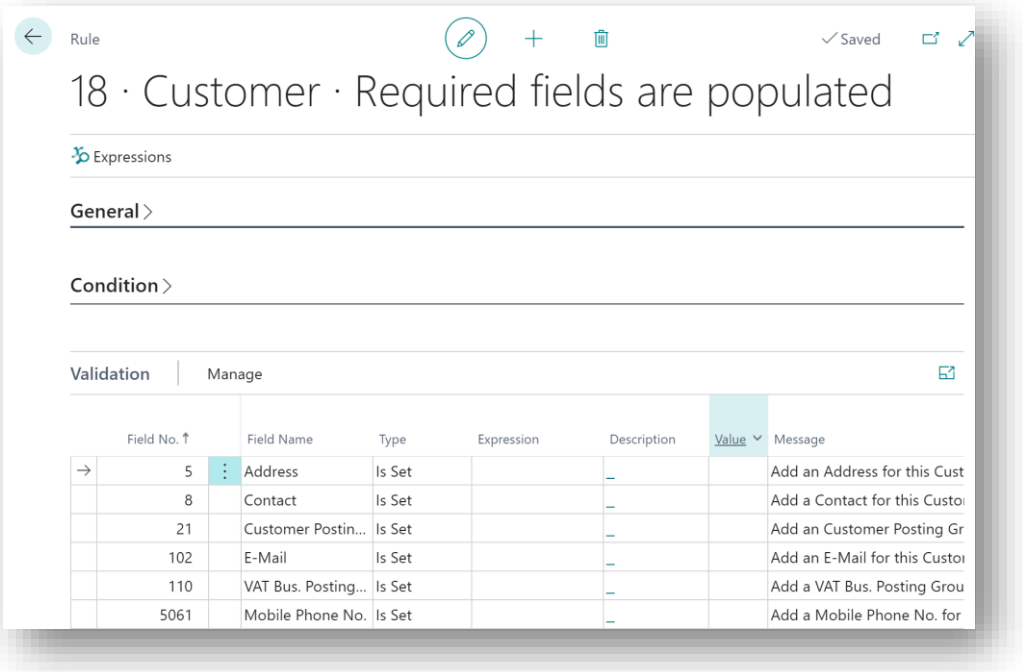


Figure 8-5

- **Field No.** – Enter the number of the field on which to run the validation.
- **Field Name** – Displays the name of the chosen **Field No.**
- **Type** – Select the type of validation to perform on the field. Options are **Is Set, Is Not Set, Matches Expression, Set to Value, Security.**

  Is Set – Checks that the field is not empty or has a value other than the field's default value.

  Is Not Set - The field is empty or has a value of the field's default value.

  Matches Expression - The value in the field matches that entered in the **Expression** field.

  Set to Value - This sets the value of the field to that entered in the **Value** field.

  Security – This enforces field level security on the field. The field cannot be modified.

- **Expression** – Applicable when **Type** is **Matches Expression**. Select which expression to use from the list of regular expressions.

- **Value** – Applicable when **Type** is **Set to Value.** Enter the value that you want to set the field to. The contents of **Value** must be convertible to the selected field's data type.

- **Message** – Specify the message to display to the user if the validation fails.

Expand the **Bypass rule for users** FastTab *(Figure 8-6*):

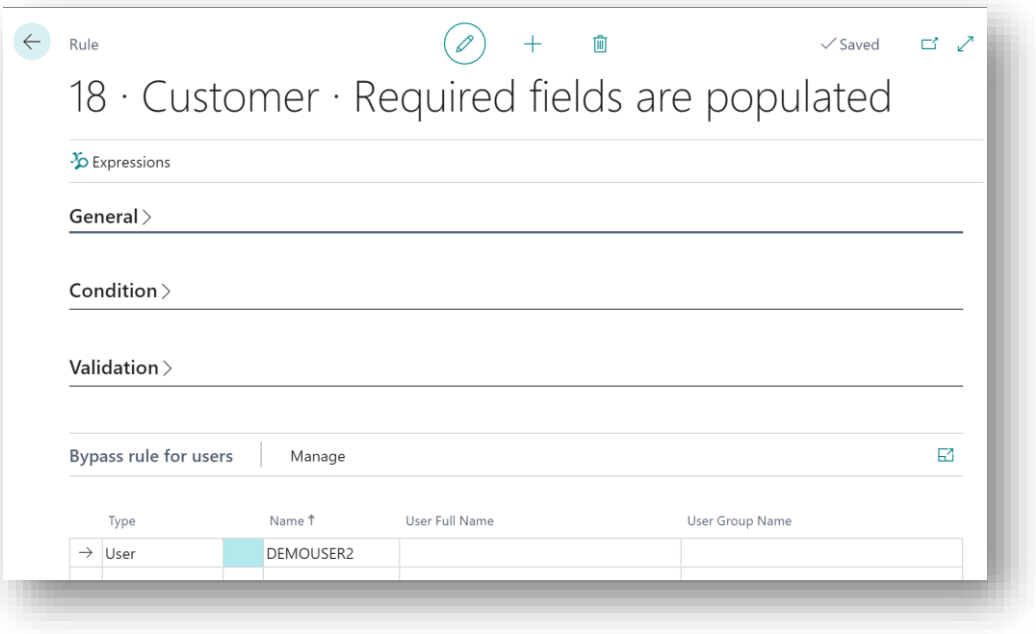


Figure 8-6

- **Type** - Enter the Type. Options are **User**, **Security Group**.

- **Name** - Depending on the **Type** chosen, enter the User(s) or Security Group(s) you want to allow bypass the rules you set up. Select from a list of existing Users or Security Groups from your Dynamics 365 Business Central Database.

- **User Full Name** - If Type is **User**, displays the Name of the User. If Type is **Security Group**, displays the Name of the Security Group.

8.3 SD Data and GDPR Manager – Expressions List

The SD Data and GDPR Manager **Expression List** Page, is accessed from the **Data Manager Rule** card by selecting the **Expressions** action *(Figure 8-7)*.

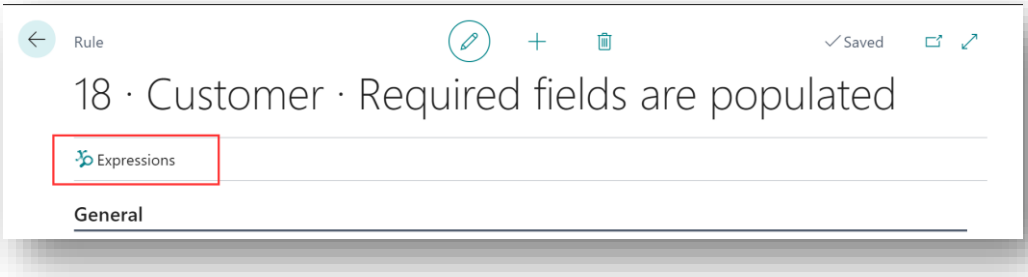


Figure 8-7

A regular expression is a pattern that defines an amount of text. The Expression List page defines the expressions used in the conditions and validations of the rules. Using the regular expressions, SD Data and GDPR Manager uses the defined pattern to search on and/or match the data in a field.

If you chose to load the **Assisted Setup**, some sample expressions have been imported into SD Data and GDPR Manager *(Figure 8-8)*.

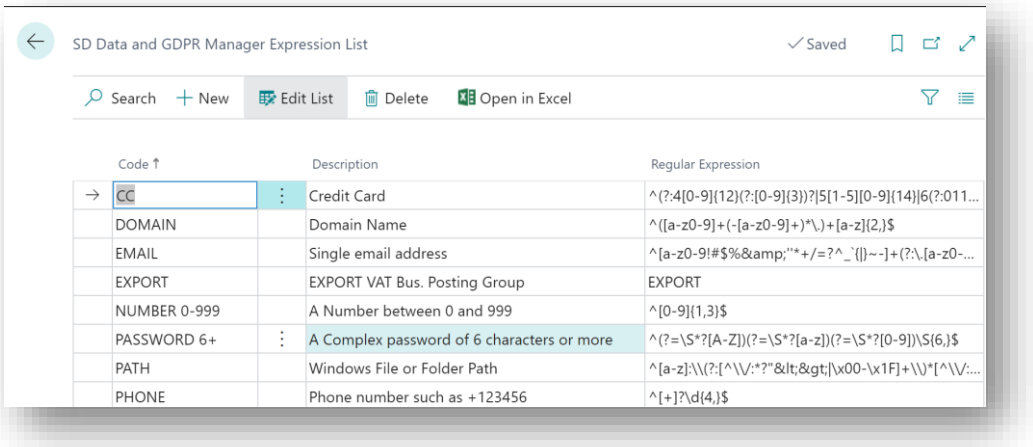


Figure 8-8

- **Code** – Enter a unique code to identify the Expression.
- **Description** – Specify a user defined description of the Expression.
- **Regular Expression** – Defines the Regular Expression to be used when matching against field data in the condition and validation section of rules.

8.4 SD Data and GDPR Manager – Creating a Rule – Example 1

If, for example, you wanted to set a rule on the Customer Table that for those Customers whose VAT. Bus. Posting Group is set to EXPORT, then the VAT Registration No. for that Customer should not be blank, you would set up the following rule in the Rule card *(Figure 8-9)*.

1. Navigate to the **SD Data and GDPR Manager Rules** List. Form the **Home** tab, on the **New** group, choose **New**.

2. In the **General** FastTab the fields would be set as follows *(Figure 8-9)*:

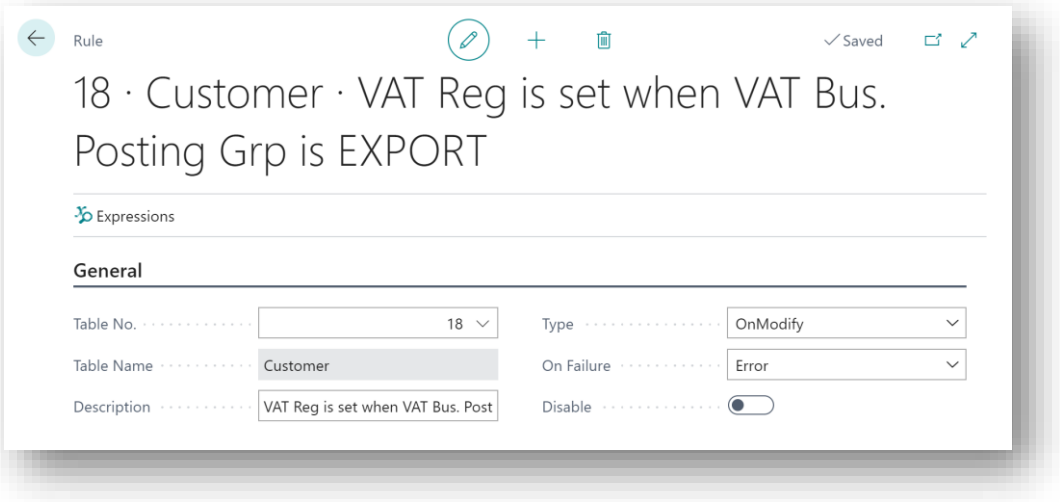


Figure 8-9

- **Table No.** – For this example, set this field to **18**, to apply the rule to table 18, the Customer Table.

- **Table Name** – The table name displays as **Customer**.

- **Description** –Enter a description to identify the rule.

- **Type** –We will specify the rule to trigger on the **OnModify** table action.

- **On Failure** – In this example, we will set this field to **Error** to raise an error on the field that fails its validation.

3. In the **Condition** FastTab the fields would be set as follows *(Figure 8-10)*:

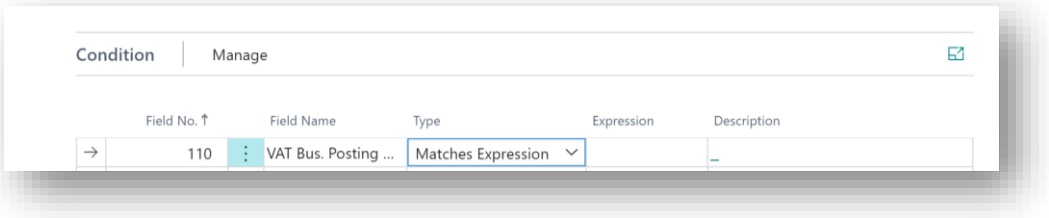


Figure 8-10

- **Field No.** – Enter the number of the field on which to run the condition. For this example, enter a value of **110**, for the VAT Bus. Posting Group field.

- **Field Name** – This will display **VAT Bus. Posting Group**, the Field Name of the chosen Field No.

- **Type** – For this example we will perform a **Matches Expression** check on the VAT Bus. Posting Group field.

- **Expression** – To select which expression to use when the Type is set to Matches Expression, we will add a new entry to our list of Expressions by selecting **New** on the drop-down list on the **Expression** field *(Figure 8-11)*.

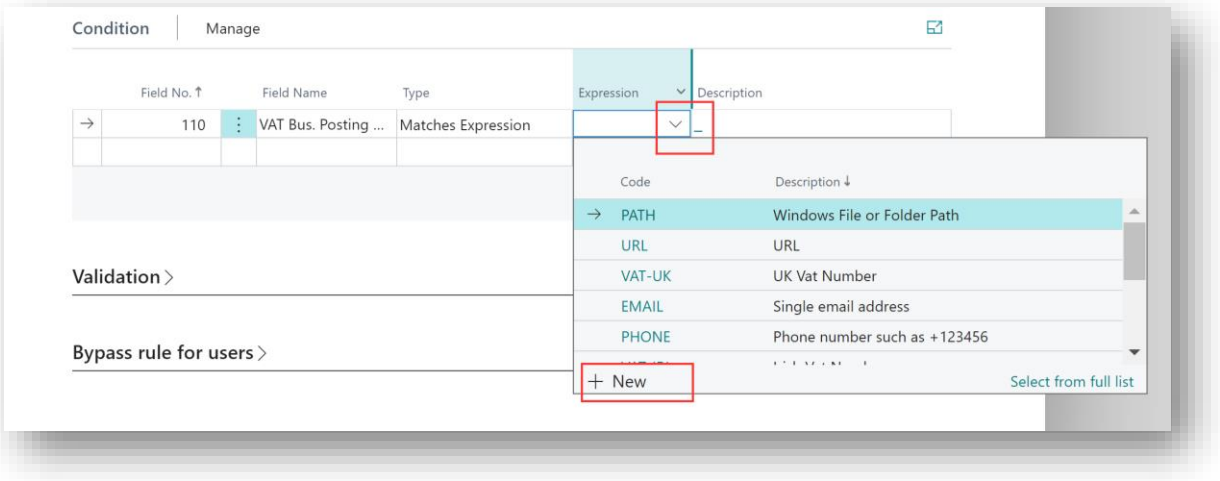


Figure 8-11

4. We will enter a **New** record in the Expression List in SD Data and GDPR Manager as follows *(Figure 8-12)*:

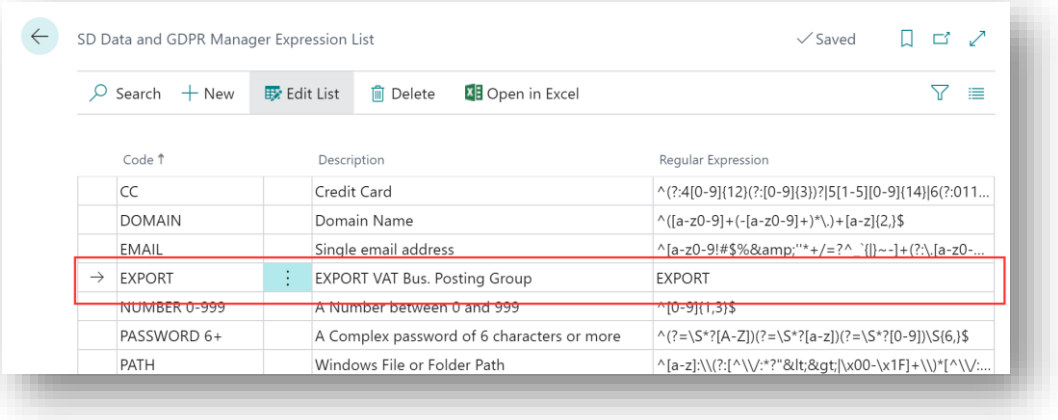


Figure 8-12

- **Code** – Enter a unique code to identify the new expression.
- **Description** – Enter a user defined description.
- **Regular Expression** – Set the regular expression to EXPORT

5. After selecting this new expression, the fields in the record are set as follows *(Figure 8-13)*:

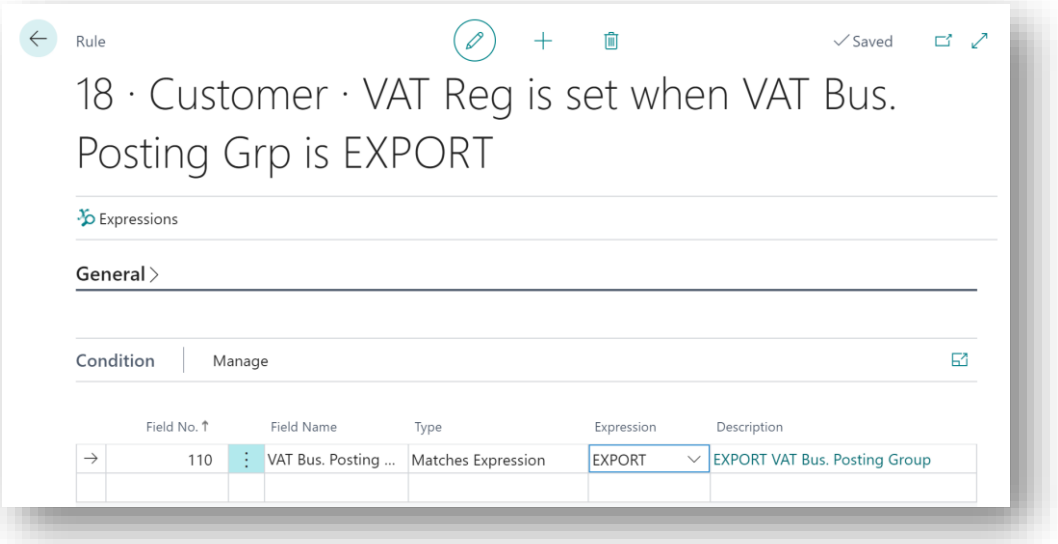


Figure 8-13

6. In the **Validation** FastTab, set the fields as per below *(Figure 8-14)*:

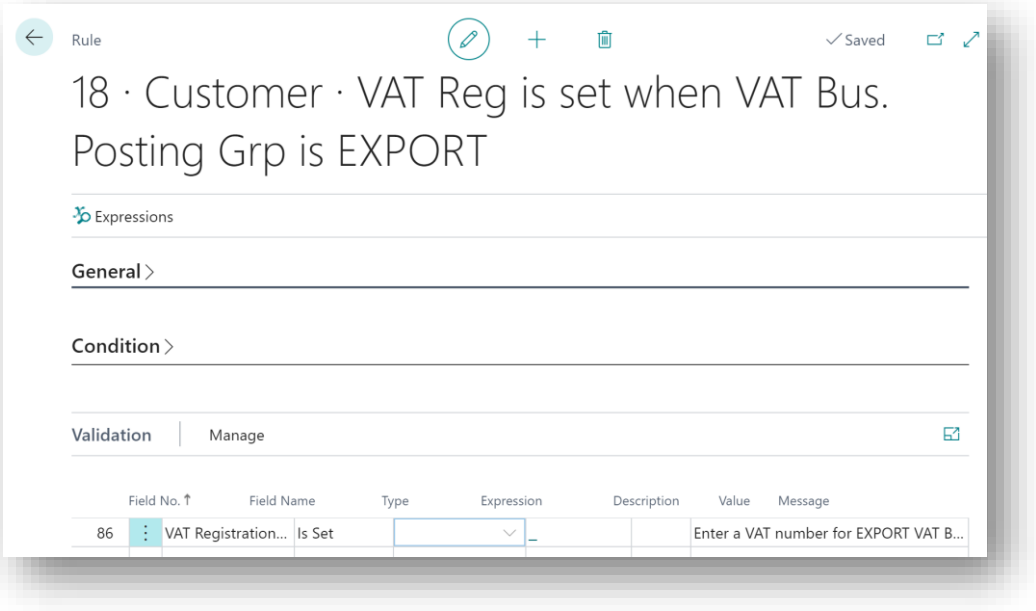


Figure 8-14

- **Field No.** – Enter **86**, for the VAT Registration No. field, the number of the field on which to run the Condition.

- **Field Name** – Displays **VAT Registration No.**, the Field Name of the chosen Field No.
- **Type** – Select **Is Set** as the type of validation to perform on the field. SD Data and GDPR Manger will validate that the VAT Registration No. field on the Customer Table is not empty or has a value other than the default.

- **Message** – Enter a custom message to display to the user if validation of the rule fails.

8.5 SD Data and GDPR Manager – Using the Rule – Example 1

To use the rule which we defined in the previous section of this document, **SD Data and GDPR Manager – Creating a Rule – Example 1**, that on the Customer Table for those customers whose VAT. Bus. Posting Group is set to EXPORT, then the VAT Registration No. for that Customer should not be blank, i.e., the VAT Registration No. for that Customer should have a value:

1. Navigate to the **Customer Card** in the **Cronus** Company, taking Customer No. 27090917, Zanlan Corp. as our example.

2. Modify this record by adding a Phone No., a Mobile Phone No., and an Email to the record *(Figure 8-15*).

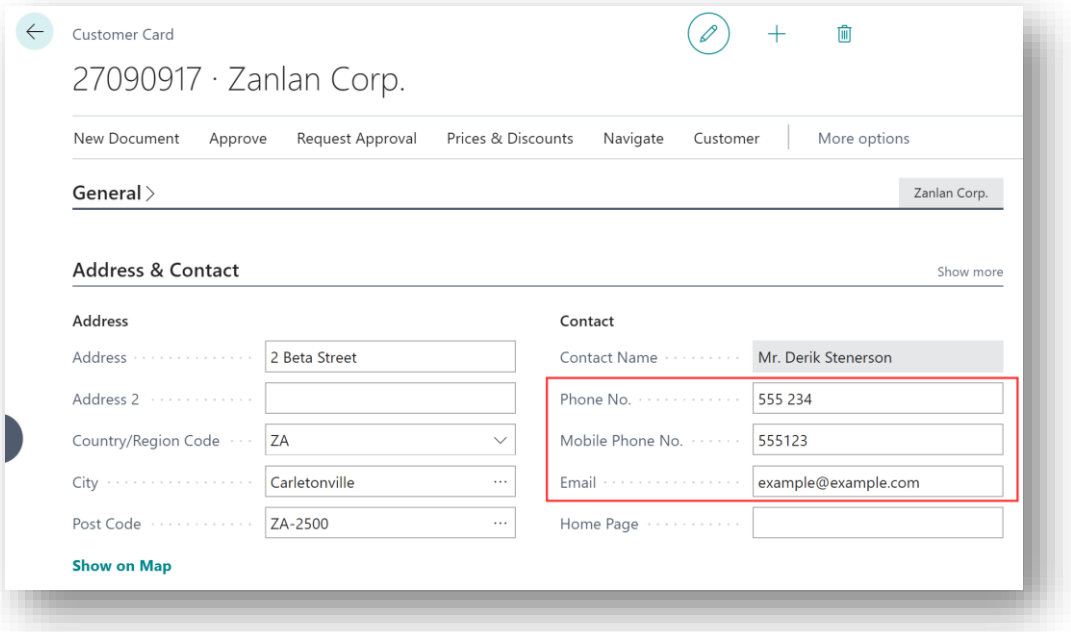


Figure 8-15

3. Navigate off the record. The SD Data and GDPR Manager rule is triggered on the On Modify Record Trigger, the condition is checked, and the validation as specified in SD Data and GDPR Manger is performed. As validation has failed, SD Data and GDPR Manger raises the error as specified in the related rule *(Figure 8-16*).

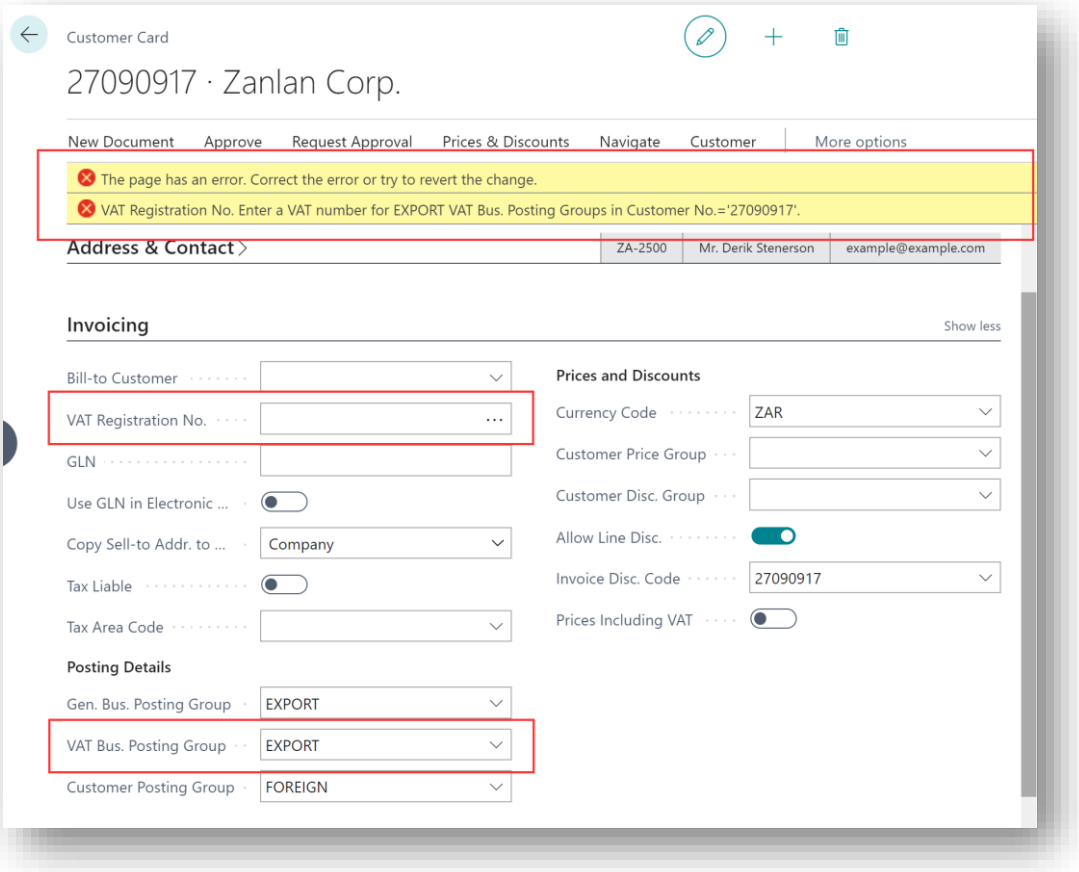


Figure 8-16

8.6 SD Data and GDPR Manager – Creating a Rule – Example 2

If, for example, you wanted to set a rule on the Customer Table that for those customers who have a phone number entered then the phone number must match a specific format, you could set up the following Rule in the SD Data and GDPR Manager Rule Card:

1. Navigate to the **SD Data and GDPR Manager Rules** List. Form the **Home** tab, on the **New** group, choose **New**.

2. In the **General** FastTab the fields would be set as follows *(Figure 8-17*):

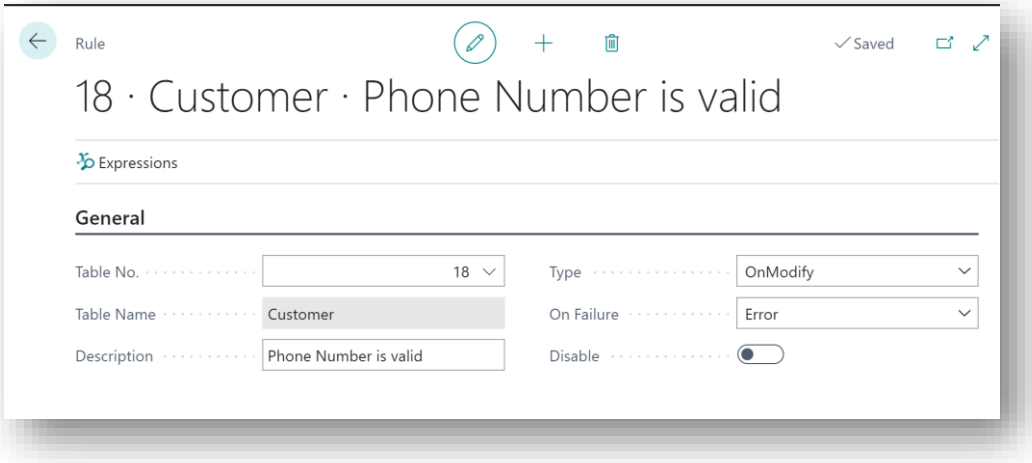


Figure 8-17

- **Table No.** – For this example, set this field to 18, to apply the rule to Table No. 18, the Customer Table.

- **Table Name** – The table name displays as Customer.

- **Description** – Enter a description to identify the rule.

- **Type** –We will specify the rule to trigger on the OnModify table action.

- **On Failure** – In this example, we will set this field to **Error** to raise an error on the field that fails the validation.

3. In the **Condition** FastTab the fields would be set as follows *(Figure 8-18*):

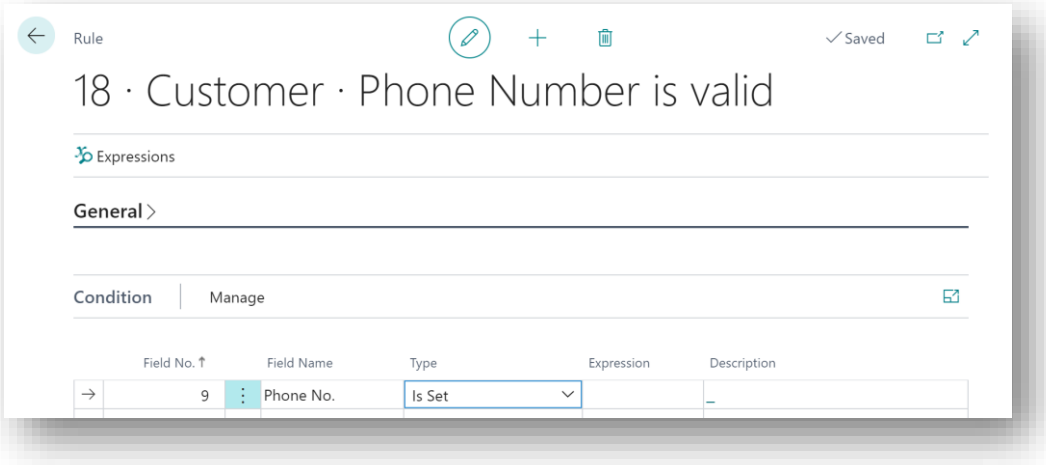


Figure 8-18

- **Field No.** – Enter the number of the field on which to run the condition. For this example, enter a value of 9, for the phone no. field.

- **Field Name** – This will display Phone No., the name of the chosen **Field No**.

- **Type** – For this example we will perform a **Is Set** conditional check on the phone no. field. SD Data and GDPR Manger will check for this rule if the phone no. field is not empty or if it has a value other than the default value.

- **Message** – Enter a custom message to display to the user if validation of the rule fails.

4. In the **Validation** FastTab the fields would be set as follows *Figure 9-19*):

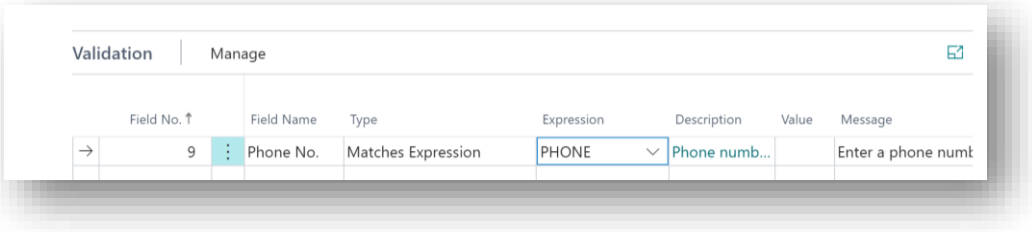


Figure 8-19

- **Field No.** – Enter 9, for the Phone No. field, the number of the field on which to run the condition.

- **Field Name** – Displays Phone No., the name of the chosen **Field No**.

- **Type** – Select **Matches Expression** as the type of validation to perform on the field. SD Data and GDPR Manger will validate that the phone no. field on the Customer Table value in the field matches the selected regular expression.

- **Expression** – If you have imported the Cronus Demo Setup when installing **SD Data and GDPR Manager**, select the PHONE Expression.

8.7 SD Data and GDPR Manager – Using the Rule – Example 2

To use the rule that we defined in the previous section of this document, **SD Data and GDPR Manager – Creating a Rule – Example 2**, that on the Customer Table, for those customers who have a Phone No. entered, the phone number must match a specific format as defined by the regular expression PHONE:

1. Navigate to the **Customer Card** in **Cronus**, again, taking Customer No. 20000, Selangorian Ltd. as our example.

2. Modify this record by adding a phone no to the record with a space entered in the field between some of the numbers.

3. Navigate off the record. The SD Data and GDPR Manager Rule is triggered on the On Modify Record Trigger, the condition is checked, and the validation as specified in the rule is performed. As validation has failed, SD Data and GDPR Manager raises the error as specified in the related rule *(Figure 8-20*).

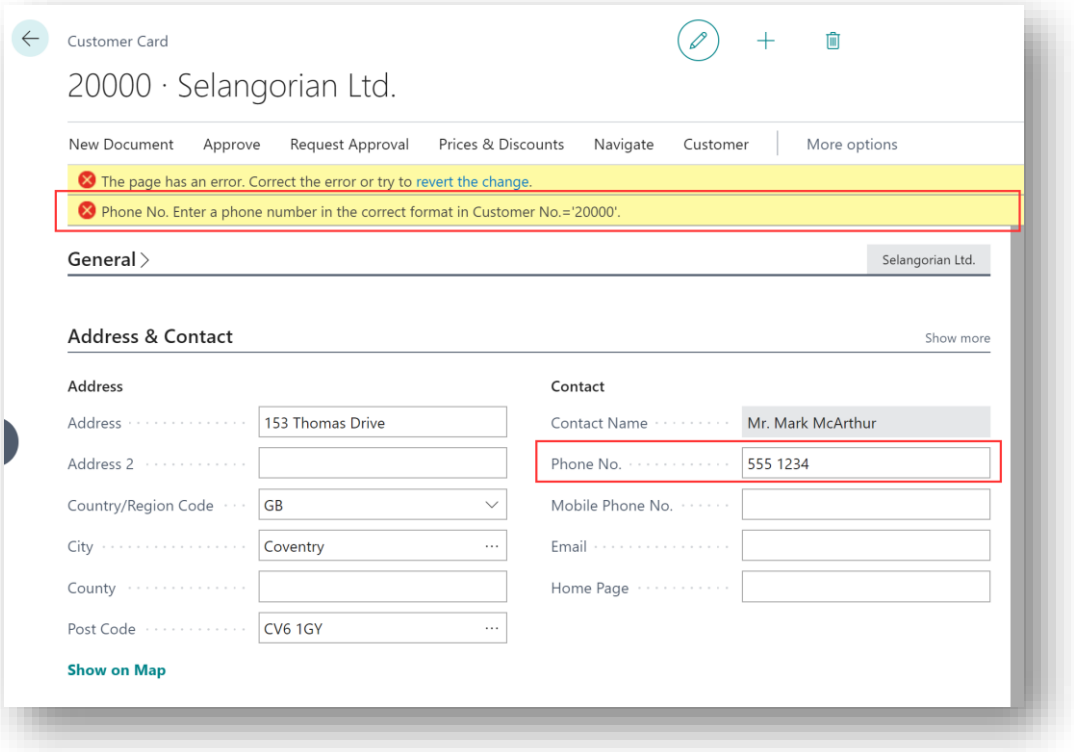


Figure 8-20

9 Using SD Data and GDPR Manager – GDPR Requests

9.1 SD Data and GDPR Manager – GDPR Monitored Tables List

The **SD Data and GDPR Manager Monitored Tables List** is accessed from the **Role Centre** by drilling through on the **Active Monitored Tables** cue, the **SD Data Manager and GDPR Setup Card** or by searching the **Tell Me** *(Figure 9-1)*.

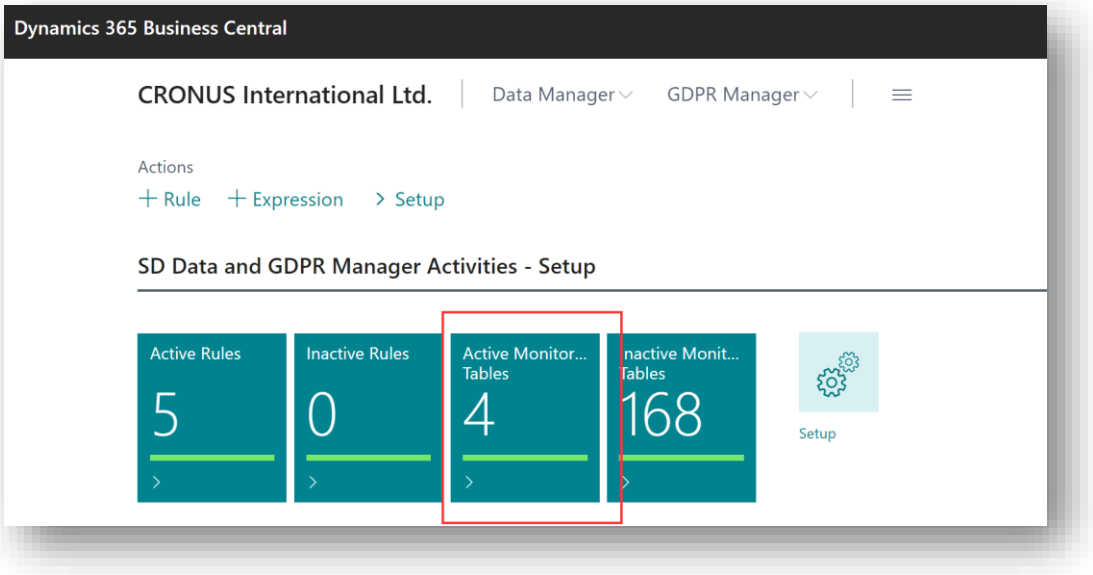


Figure 9-1

The **SD Data Manager GDPR Monitored Tables Card**, accessed from this list, defines the table and fields that you add to your GDPR monitored list.

If you chose to import the **Assisted Setup**, some sample records will have been created in SD Data and GDPR Manager. To add a table to the GDPR Monitored Table list, from the menu, choose **+New**. To view or edit a record for an existing GDPR Monitored Table from the **Manage** group choose **Edit** or **View** *(Figure 9-2)*.

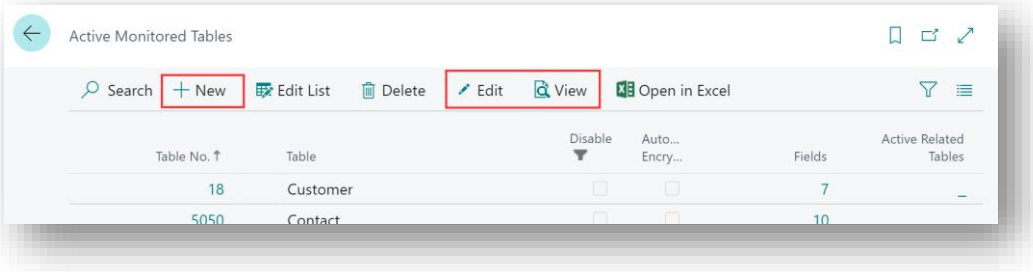


Figure 9-2

9.2 SD Data and GDPR Manager – GDPR Monitored Table Card

The **SD Data and GDPR Manager Monitored Table** card displays the following fields in the **General** FastTab *(Figure 9-3)*:

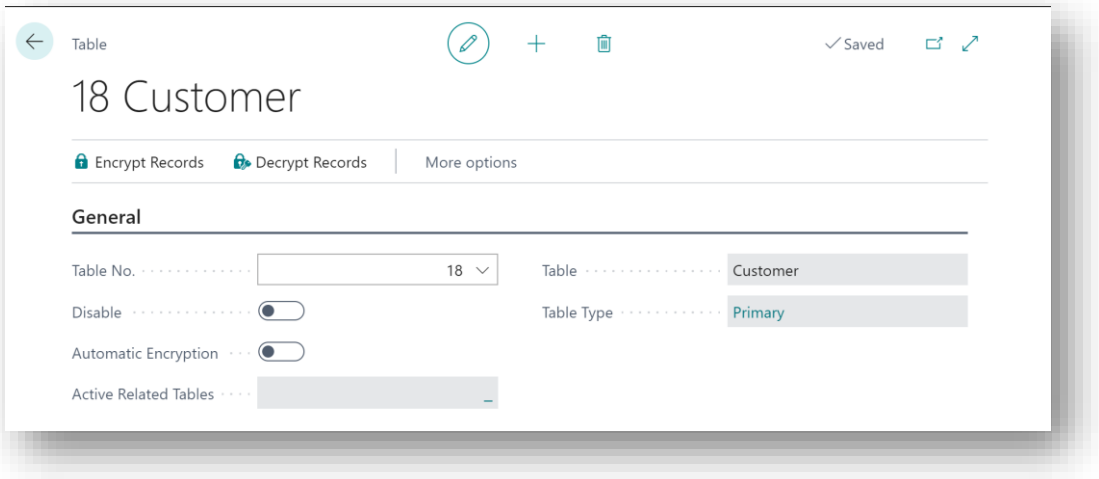


Figure 9-3

- **Table No.** – Specifies the number of the Microsoft Dynamics 365 Business Central Table that has been added to the GDPR monitored list.

- **Table** – Displays the name of the table specified in the **Table No.** field.

- **Disable** - Select this checkbox to exclude the table from GDPR Monitoring and GDPR Requests.

- **Automatic Encryption** - Select this checkbox to automatically encrypt the fields on the table which are marked to be encrypted whenever a new record is added to this table or when the existing record is modified.

- **Active Related Tables** –A flowfield Count of the enabled tables, related to this current table, that have been added to your GDPR monitored list of tables.

- **Table Type** - Defines the table type of the monitored table. Options are **Primary**, **Related**.

Expand the **Fields** FastTab *(Figure 9-4)*:

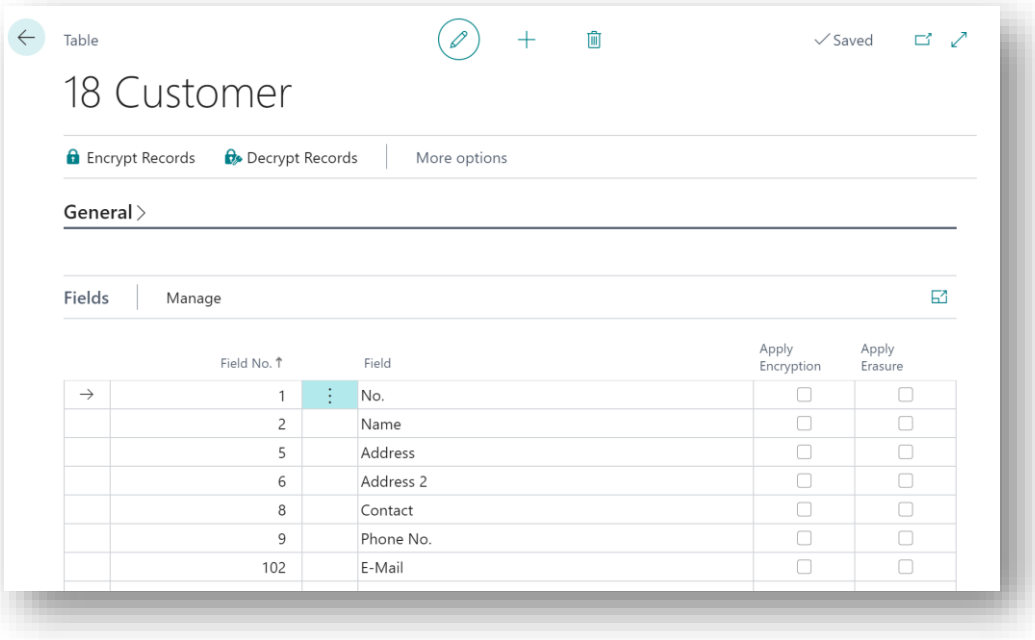


Figure 9-4

- **Field No.** – Enter the number of the field, from a list of the fields in **Table No.** to add to your GDPR monitored list of fields.

- **Field Name** – Displays the name of the field chosen in **Field No.**

- **Apply Encryption** - Select this checkbox to allow this field to be encrypted when a Right to Encryption Request is logged and the user chooses the **Encrypt Action** in the **Related Records FastTab** of the **Request Card**.

- **Apply Erasure** - Select this checkbox to allow this field to be erased when a Right to Erasure Request is logged and the user chooses the **Forget Action** in the **Related Records FastTab** of the **Request Card**.

Expand the **Restricted Field Values** FastTab *(Figure 9-5)*:

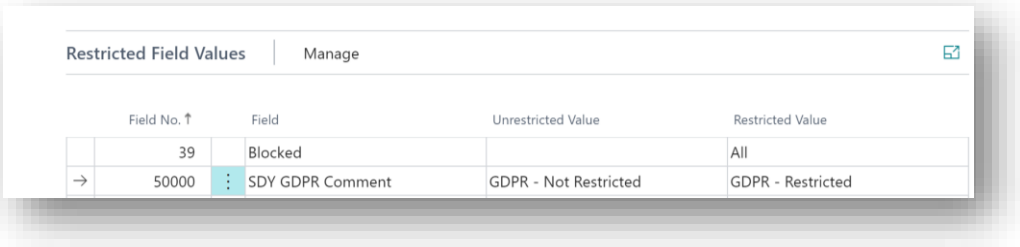


Figure 9-5

- **Field No.** – Enter the number of the field from a list of fields in **Table No.** on which to define an Unrestricted Value and/or a Restricted Value.

- **Field Name** – Displays the Name of the field chosen in **Field No.**

- **Unrestricted Value** - Enter the value that the field will be set to when a Restrict Request is logged, and the user chooses the **UnRestrict Action** in the **Related Records FastTab** of the **Request Card**.

- **Restricted Value** - Enter the value that the field will be set to when a Restrict Request is logged, and the user chooses the **Restrict Action** in the **Related Records FastTab** of the **Request Card**.

Expand the **Related Tables** FastTab *(Figure 9-6)*:

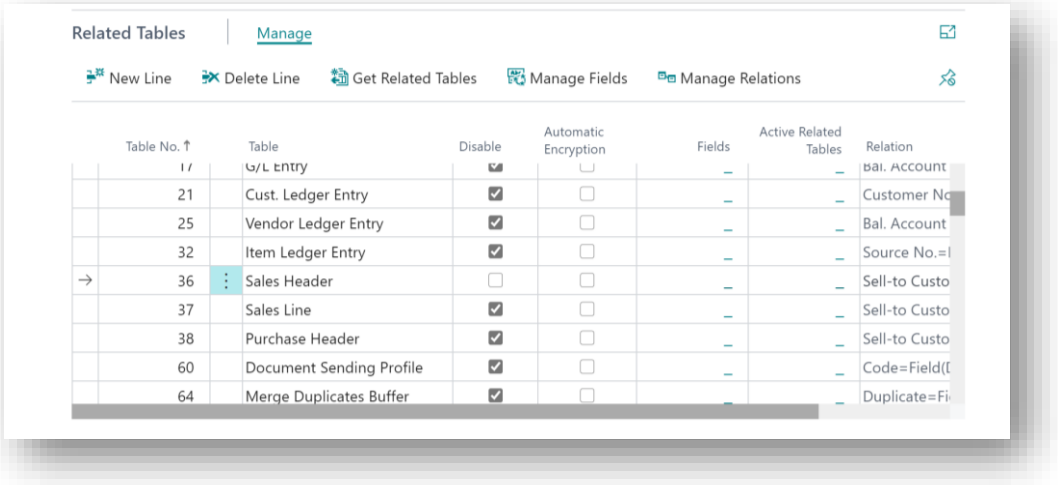


Figure 9-6

- **Table No.** - Select a Table No. from a list of tables in your Microsoft Dynamics 365 Business Central database, related to the **Table No.** in the **General FastTab**, to add to your GDPR monitored list of tables.

- **Table** - Displays the name of the table chosen in **Table No.**

- **Disable** - Displays whether the table in **Table No**. has been included or excluded from your GDPR Monitoring and GDPR Requests.

- **Automatic Encryption** - Select this checkbox to automatically encrypt fields on the table that are set to be encrypted when a record is added to this table or when the record is modified.

- **Fields -** A flowfield count of the fields on the table that have been added to your GDPR monitored list of fields.

- **Active Related Tables** –A flowfield count of the enabled tables related to this table that have been added to your GDPR monitored list of tables.

- **Relation -** The relation that links the table in **Table No**. to the Primary Table No. on the card.

There are several **Actions** available on the **Related Tables FastTab** *(Figure 9-7*):

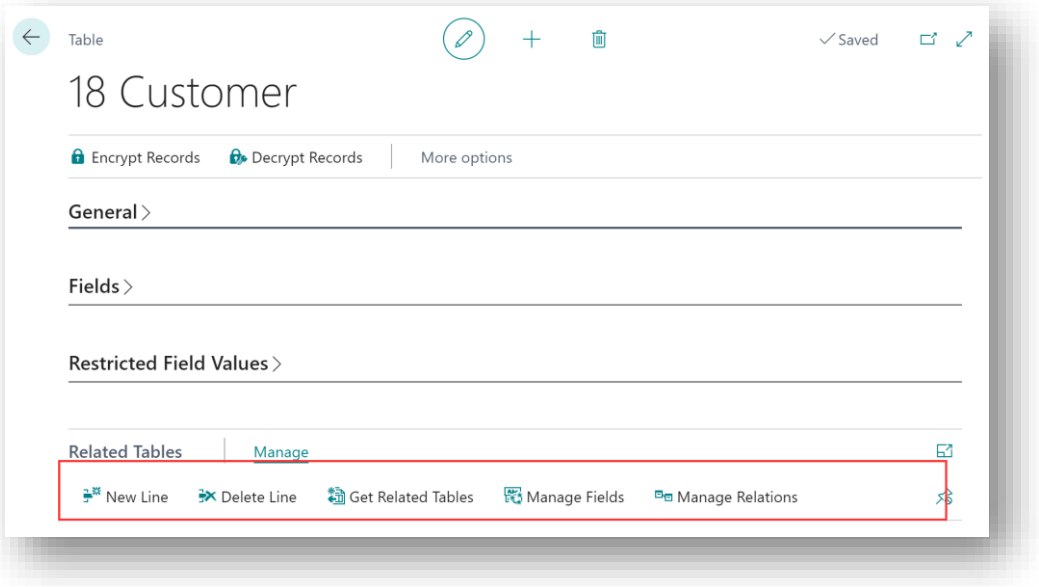


Figure 9-7

- **New Line**- choose this action to add a new record to the Related Tables.

- **Get Related Tables** - Choose this action to allow SD Data and GDPR Manager to automatically search through the related tables and create the list of tables related to the primary table.

- **Manage Fields** - Choose this action to open the SD Data and GDPR Manager Monitored Table Card for the selected Related table from where you can add fields from the Related table to your GDPR monitored list.

- **Manage Relations** - Choose this action to manage the relationships between the parent (primary) and child (secondary) table.

The following **Actions** are available on the **Actions** tab of **SD Data and GDPR Manager Monitored Table Card** *(Figure 9-8)*:

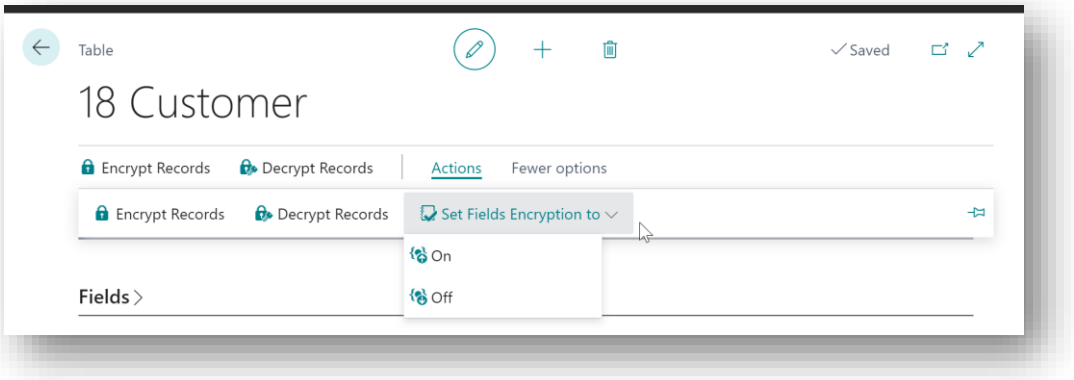


Figure 9-8

- **Encrypt Records** - Choose this action to encrypt those fields that have the **Apply Encryption** checkbox selected for all records on the table.

- **Decrypt Records** - Choose this action to decrypt those fields that have the **Apply Encryption** checkbox selected for all records on the table.

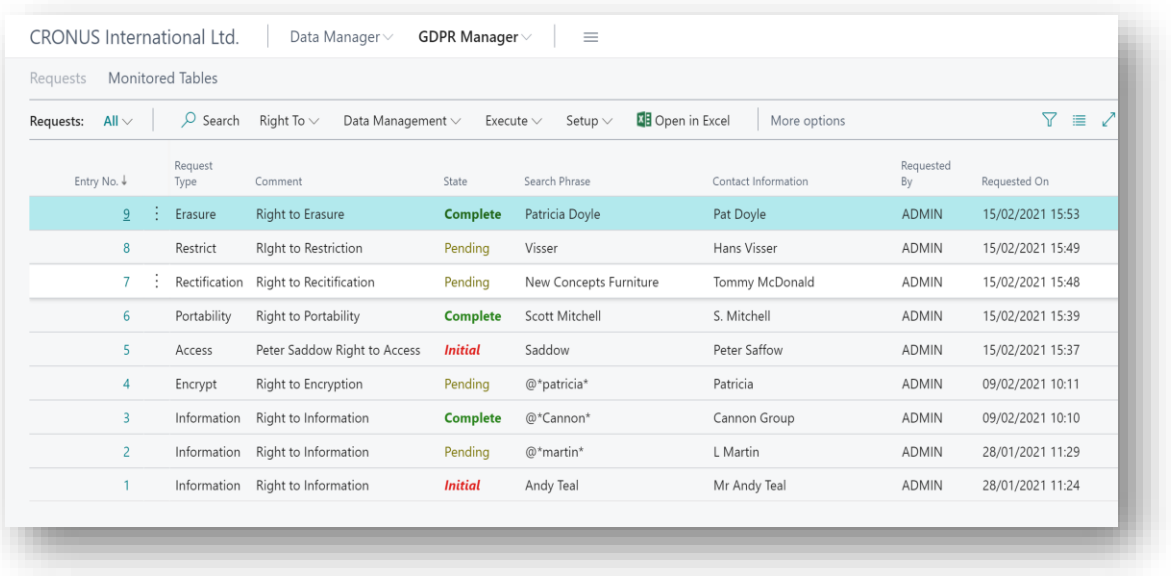
- **Set Fields Encryption to On** - Choose this Action to set the **Apply Encryption** checkbox to yes for all fields that have been added to the **Fields** FastTab for this table.

- **Set Fields Encryption to Off** - Choose this Action to set the **Apply Encryption** checkbox to no for all fields that have been added to the **Fields** FastTab for this table.

9.3 SD Data and GDPR Manager – GDPR Requests

Once you have set up your GDPR Monitored Tables and Fields, you can then search, report, export, correct, erase, restrict or encrypt this data all within Microsoft Dynamics 365 Business Central.

The **SD Data and GDPR Manager GDPR Requests List** Page, displays the GDPR Requests that have been made and allows users to log and action GDPR Requests *(Figure 9-9*):



Entry No.	Request Type	Comment	State	Search Phrase	Contact Information	Requested By	Requested On
9	Erasure	Right to Erasure	Complete	Patricia Doyle	Pat Doyle	ADMIN	15/02/2021 15:53
8	Restrict	RIght to Restriction	Pending	Visser	Hans Visser	ADMIN	15/02/2021 15:49
7	Rectification	Right to Recitification	Pending	New Concepts Furniture	Tommy McDonald	ADMIN	15/02/2021 15:48
6	Portability	Right to Portability	Complete	Scott Mitchell	S. Mitchell	ADMIN	15/02/2021 15:39
5	Access	Peter Saddow Right to Access	Initial	Saddow	Peter Saffow	ADMIN	15/02/2021 15:37
4	Encrypt	Right to Encryption	Pending	@*patricia*	Patricia	ADMIN	09/02/2021 10:11
3	Information	Right to Information	Complete	@*Cannon*	Cannon Group	ADMIN	09/02/2021 10:10
2	Information	Right to Information	Pending	@*martin*	L Martin	ADMIN	28/01/2021 11:29
1	Information	Right to Information	Initial	Andy Teal	Mr Andy Teal	ADMIN	28/01/2021 11:24

Figure 9-9

- **Entry No. -** A unique integer to identify the request.
- **Request Type** - Displays the Request Type that was logged and performed on your GDPR Monitored Tables and Fields. Options are **Access**, **Rectification**, **Erasure**, **Information**, **Portability**, **Restrict**, or **Encrypt**.
- **Comment** - Displays the comment entered by the Dynamics 365 Business Central user who logged the GDPR request.
- **State** - Displays the state of the request. Options are **Initial**, **Pending**, or **Complete**.
- **Search Phrase** - Displays the search phrase entered by the Dynamics 365 Business Central user who made the GDPR request.

- **Contact Information** - Displays the contact information of the person who made the GDPR request.

- **Requested By** - Displays the USERID of the Dynamics 365 Business Central user who logged the request.

- **Requested On** - Displays the date and time that the request was logged.

- **Records** - A flowfield count of the records returned from your GDPR monitored list of tables whose monitored field(s) contained the value entered in the **Search Phrase**.

To **View** or **Edit** an existing GDPR Request, choose the **View** or **Edit** Action in the **Manage** group or drill down on the Entry No. field *(Figure 9-10*).

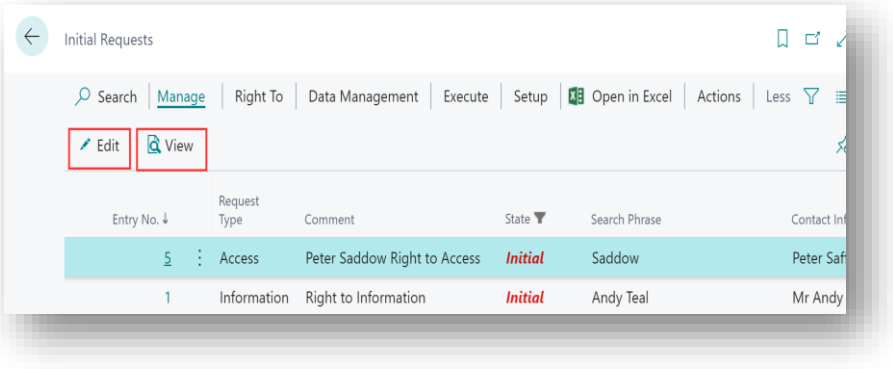


Figure 9-10

For each type of GDPR request logged, the GDPR Request Card contains the fields as described below *(Figure 9-11*).

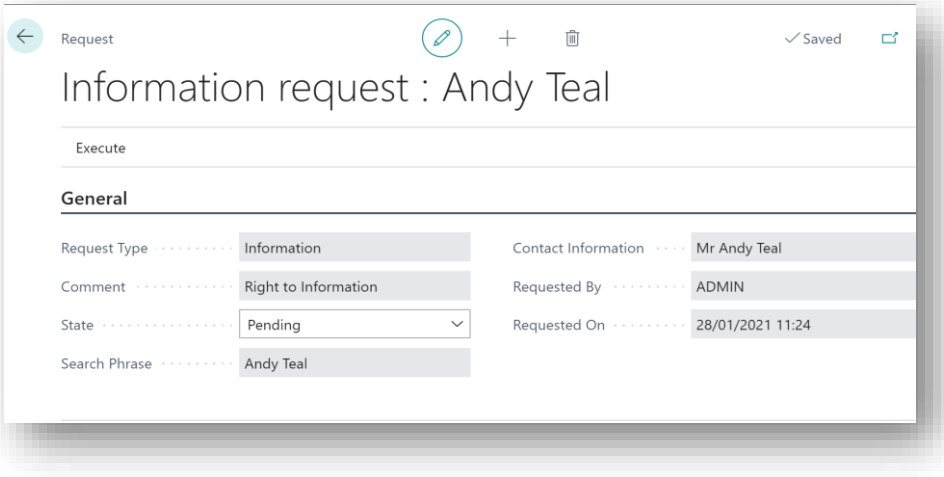


Figure 9-11

- **Request Type** - Displays the type of GDPR request that was logged and performed on your GDPR Monitored Tables and Fields. Options are **Access**, **Rectification**, **Erasure**, **Information**, **Portability**, **Restrict**, or **Encrypt**.

  Note: For SD Data and GDPR Manager to determine if a record has been accessed (viewed), the record must be encrypted.

- **Comment** - Displays the comment entered by the Dynamics 365 Business Central user who logged the GDPR request.

- **State** - Displays the state of the request. Options are **Initial**, **Pending**, or **Complete**.

- **Search Phrase** - Displays the search phrase entered by the Dynamics 365 Business Central user who made the GDPR request.

- **Contact Information** - Displays the contact information of the person who made the GDPR request.

- **Requested By** - Displays the USERID of the Dynamics 365 Business Central user who logged the request.

- **Requested On** - Displays the date and time that the request was logged.

In the **Related Records** FastTab *(Figure 9-12*):

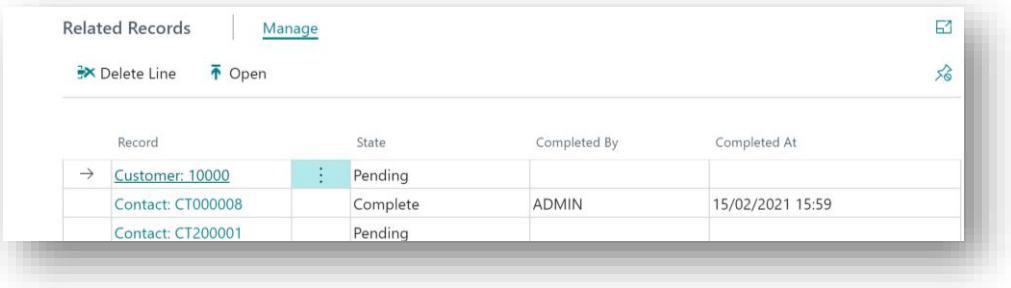


Figure 9-12

- **Record** - Displays the Table Name and primary key value of the record returned from your GDPR monitored list of tables whose monitored field(s) contained the value entered in the Search Phrase.

- **State** - Displays the state of the request. Options are **Initial**, **Pending**, or **Complete**.

- **Completed By** - Displays the USERID of the Dynamics 365 Business Central user who Completed the request.

- **Completed At** - Displays the date and time that the GDPR request was completed.

The **Actions** available on the **Right To** and **Data Management** groups of the **SD Data and GDPR Manager GDPR Requests List** allow you log and action on various GDPR Requests *(Figure 9-13*):

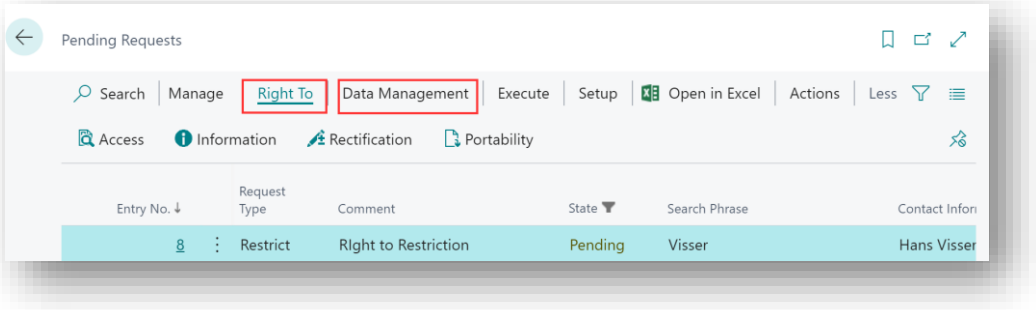


Figure 9-13

Note: Certain standard Microsoft Dynamics 365 Business Central "Archived" tables can be modified using the GDPR functionality when using a Customer Licence.

These tables are:

- Sales Shipment Header (T 110),
- Sales Invoice Header (T 112),
- Return Receipt Header (T 6660),
- Sales Cr.Memo Header (T 114),
- Purch. Rcpt. Header (T 120),
- Purch. Inv. Header (T 122),
- Purch. Cr. Memo Hdr. (T 124).

9.3.1 Right to Access

Choosing this action allows the user to log a **Right to Access Request**. **Note: To determine if a record has been accessed (viewed), the record must first be encrypted.** When this action is chosen, the page below opens, where the user can enter a **Comment**, a **Search Phrase**, and **Contact Information**. The **GDPR Request Card** then displays those records from your GDPR monitored list of tables whose monitored field(s) contain the value entered in the **Search Phrase**. You can remove any record(s) from the **Related Records** list by selecting the record(s), right-clicking on the record(s), and choosing **Delete Line**.

Users can **Open** the Related Records and **Print** or **Preview** the **Access Report** *(Figure 9-14)*. When the report is printed and the request has been completed, the **State** of the GDPR request can be set to **Complete**.

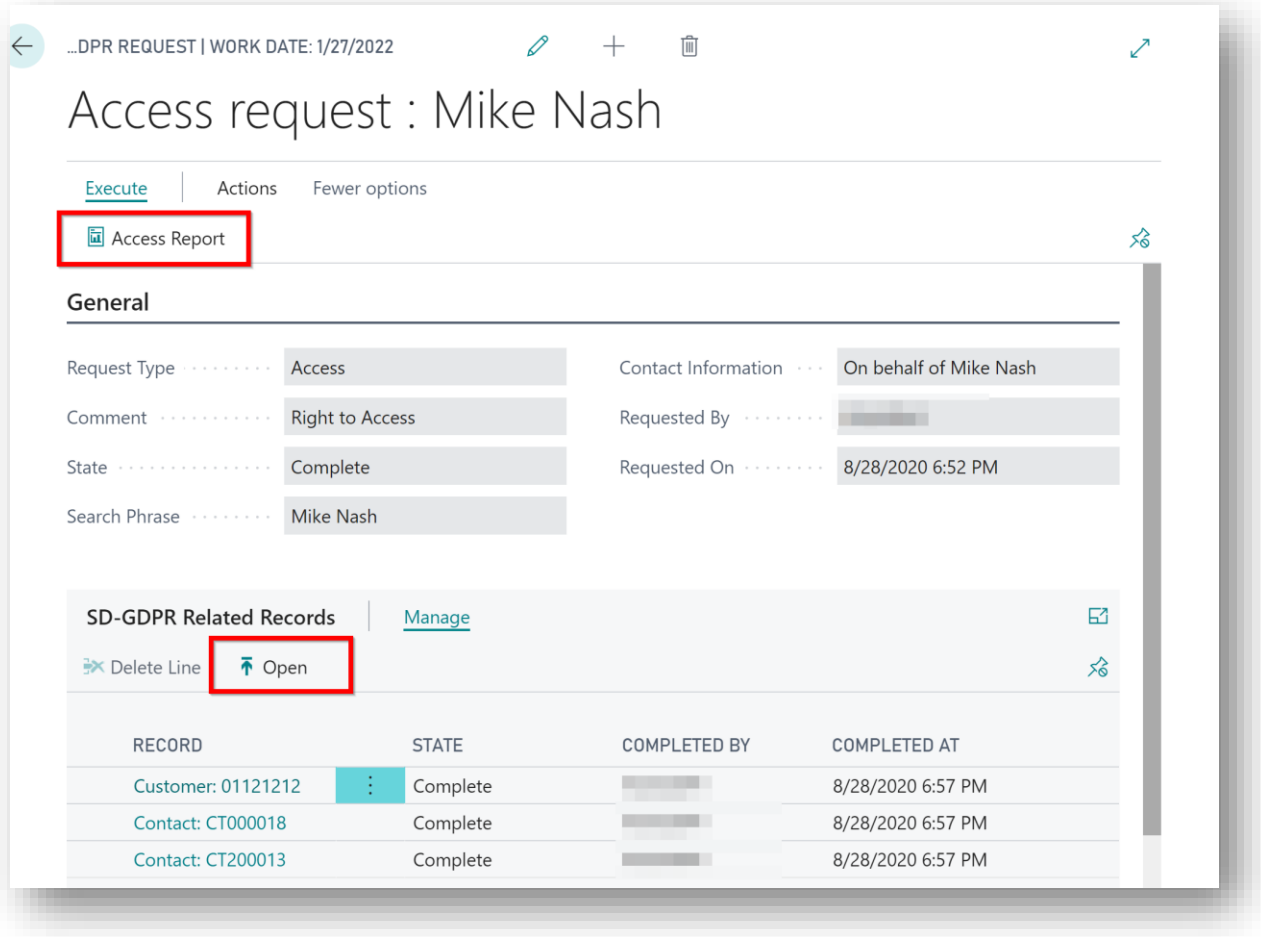


Figure 9-14

9.3.2 Right to Information

Choosing this action allows the user to log a **Right to Information Request**. When this action is chosen, the page below opens, where the user can enter a **Comment**, a **Search Phrase**, and **Contact Information**. The **GDPR Request Card** then displays those records from your GDPR monitored list of tables whose monitored field(s) contain the value entered in the **Search Phrase**. You can remove any record(s) from the **Related Records** list by selecting the record(s), right-clicking on the record(s), and choosing **Delete Line**.

Users can **Open** the Related Records and print or preview the **Information Report** *(Figure 9-15*). When the report is printed and the request has been completed, the **State** of the GDPR request can be set to **Complete**.

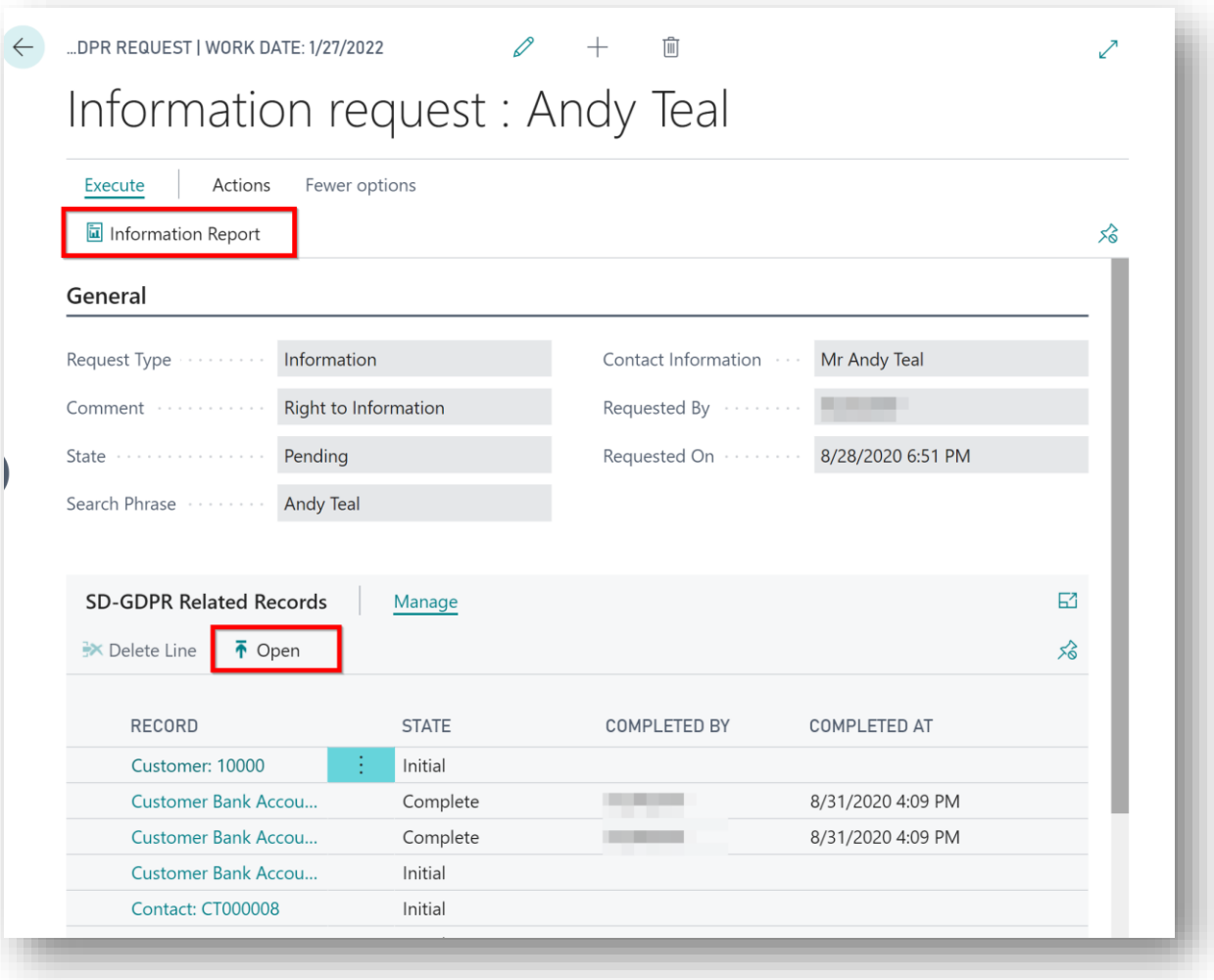


Figure 9-15

9.3.3 Right to Rectification

Choosing this action allows the user to log a Right to **Rectification Request**. When this action is chosen, the page below opens, where the user can enter a **Comment**, a **Search Phrase**, and **Contact Information**. The **GDPR Request Card** then displays those records from your GDPR monitored list of tables whose monitored field(s) contain the value entered in the **Search Phrase**. You can remove any record(s) from the **Related Records** list by selecting the record(s), right-clicking on the record(s), and choosing **Delete Line**.

Users can **Open** the Related Records to manually rectify the fields *(Figure 9-16)*. When the fields are rectified, the **State** of the GDPR request can be set to **Complete**.

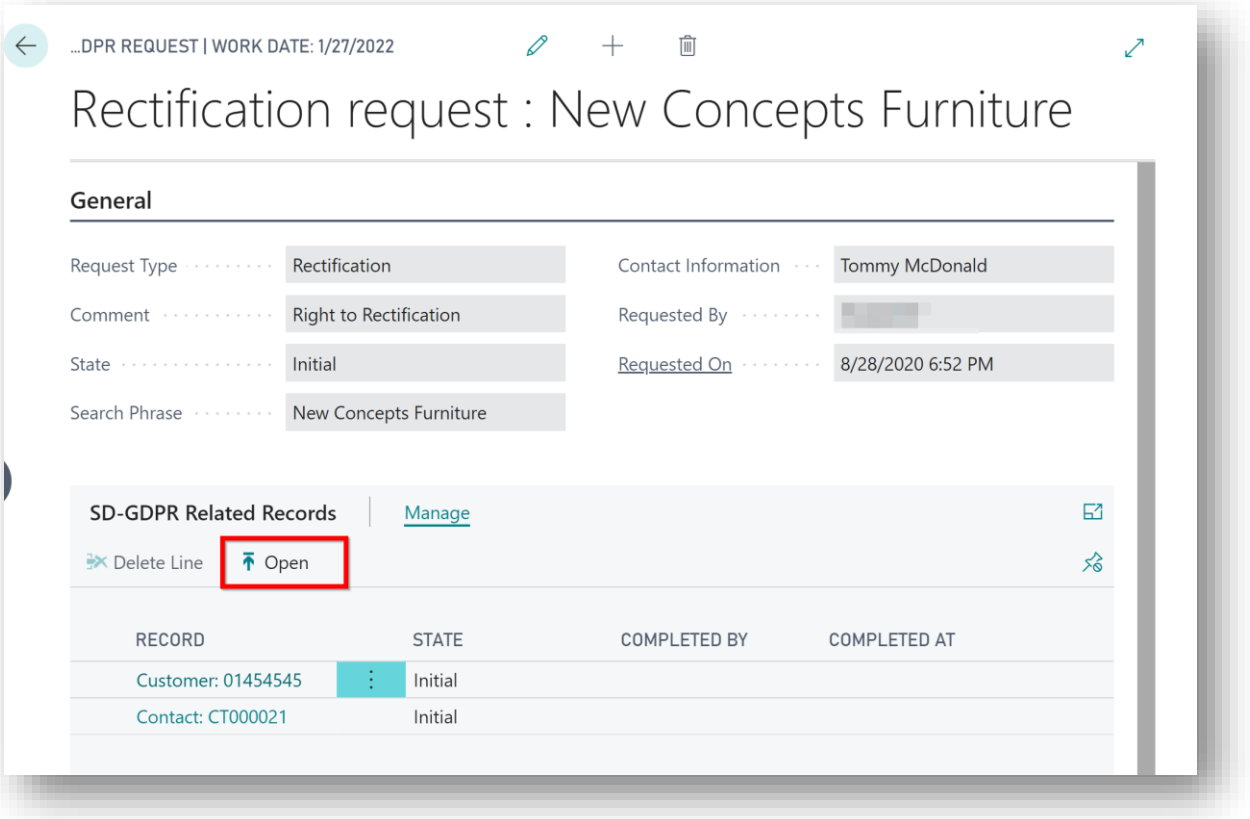


Figure 9-16

9.3.4 Right to Portability

Choosing this action allows the user to log a **Right to Portability Request**. When this action is chosen, the page below opens, where the user can enter a **Comment**, a **Search Phrase**, and **Contact Information**. The **GDPR Request Card** then displays those records from your GDPR monitored list of tables whose monitored field(s) contain the value entered in the **Search Phrase**. You can remove any record(s) from the **Related Records** list by selecting the record(s), right-clicking on the record(s), and choosing **Delete Line**.

Users can **Open** the Related Records and **Export** the GDPR monitored fields to a file *(Figure 9-17*). When the records have been exported to a file and the request has been completed, the **State** of the GDPR request can be set to **Complete**.

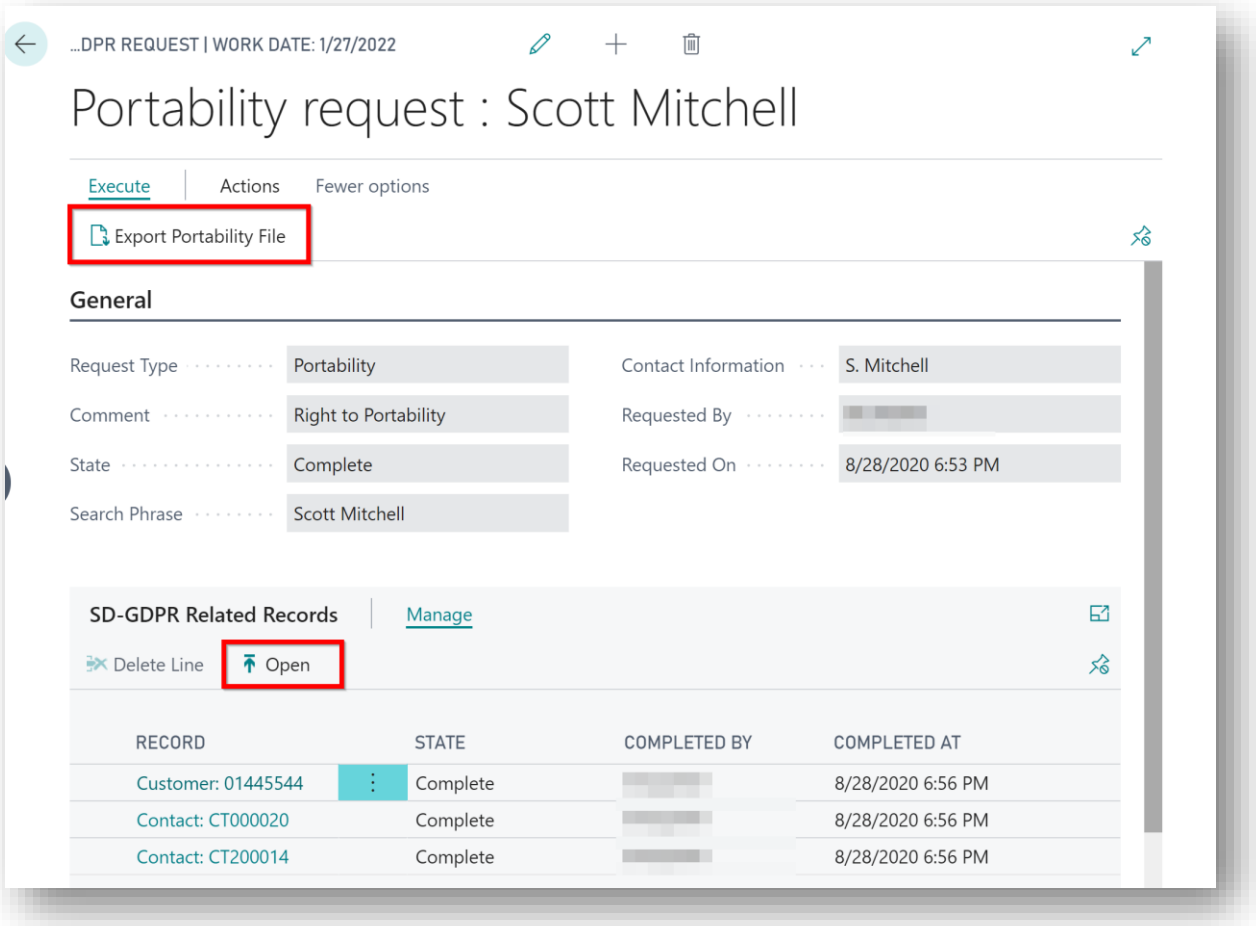


Figure 9-17

9.3.5 Right to Erasure

Choosing this action allows the user to log a Right to Erasure Request. When this action is chosen, the page below opens, where the user can enter a **Comment**, a **Search Phrase**, and **Contact Information**. The **GDPR Request Card** then displays those records from your GDPR monitored list of tables whose monitored field(s) contain the value entered in the **Search Phrase**. You can remove any record(s) from the **Related Records** list by selecting the record(s), right-clicking on the record(s), and choosing **Delete Line**.

Users can **Open** the Related Records and **Forget** (erase/remove) the GDPR monitored fields from the database *(Figure 9-18*). When the records have been removed, and the request has been completed, the **State** of the GDPR request can be set to **Complete**.

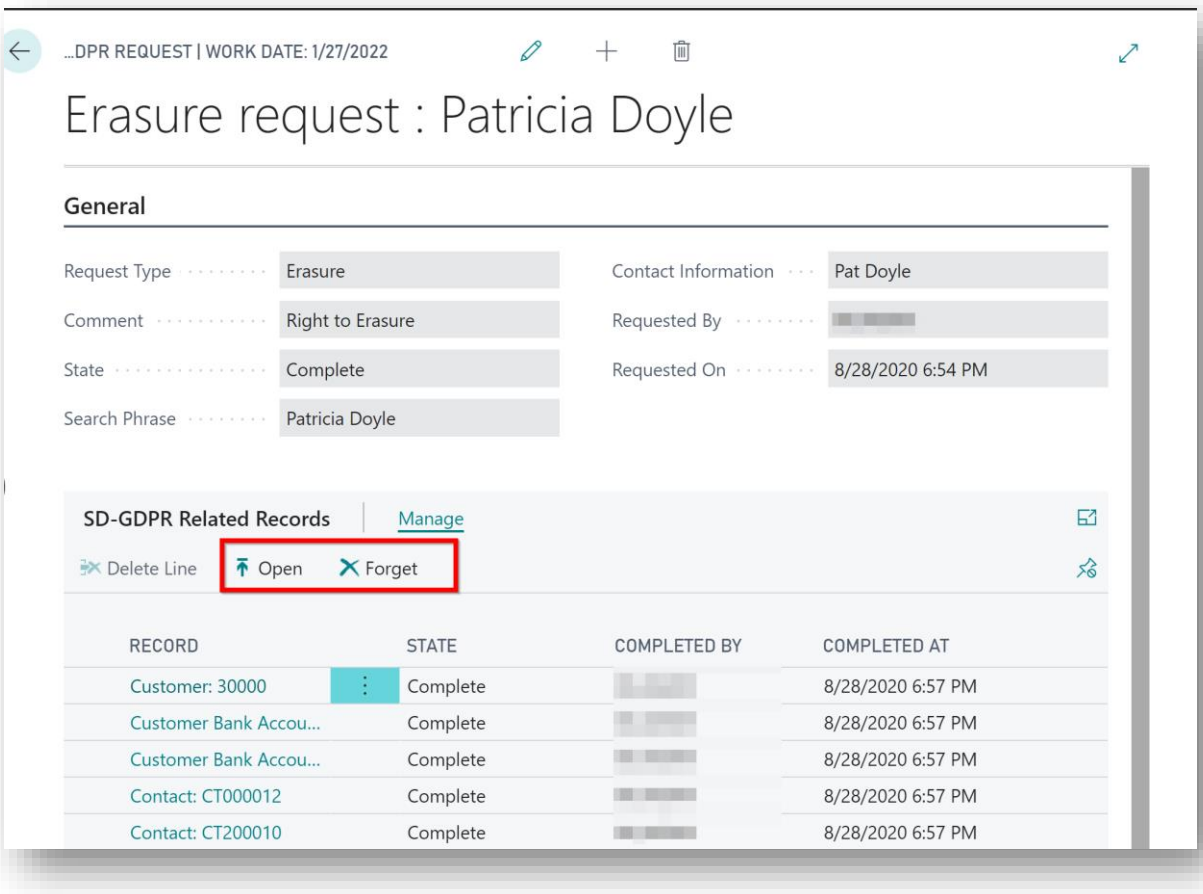


Figure 9-18

9.3.6 Right to Restrict

Choosing this action allows the user to log a Right to Restrict Request. When this action is chosen, the page below opens, where the user can enter a **Comment**, a **Search Phrase**, and **Contact Information**. The **GDPR Request Card** then displays those records from your GDPR monitored list of tables whose monitored field(s) contain the value entered in the **Search Phrase**. You can remove any record(s) from the **Related Records** list by selecting the record(s), right-clicking on the record(s), and choosing **Delete Line**.

Users can **Open** the Related Records and **Restrict** or **Unrestrict** the GDPR monitored fields on the returned records *(Figure 9-19)*. When the request has been completed, the **State** of the GDPR request can be set to **Complete**.

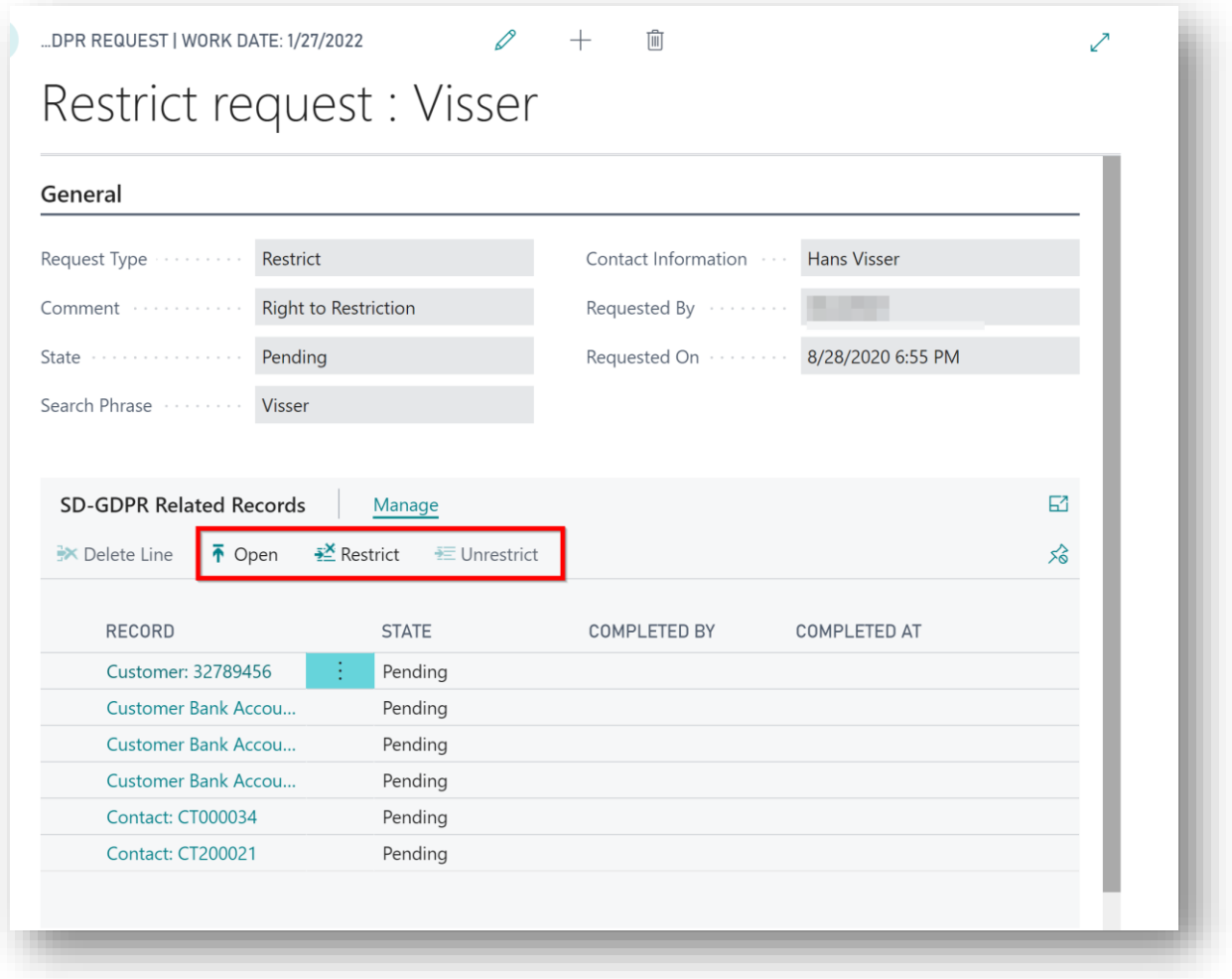


Figure 9-19

9.3.7 Right to Encryption

Choosing this action allows the user to log a Right to Encryption Request. When this action is chosen, the page below opens, where the user can enter a **Comment**, a **Search Phrase**, and **Contact Information**. The **GDPR Request Card** then displays those records from your GDPR monitored list of tables whose monitored field(s) contain the value entered in the **Search Phrase**. You can remove any record(s) from the **Related Records** list by selecting the record(s), right-clicking on the record(s), and choosing **Delete Line**.

Users can **Open** the Related Records and **Encrypt** or **Decrypt** the GDPR monitored fields on the returned records *(Figure 9-20*). When the request has been completed, the **State** of the GDPR request can be set to **Complete**.

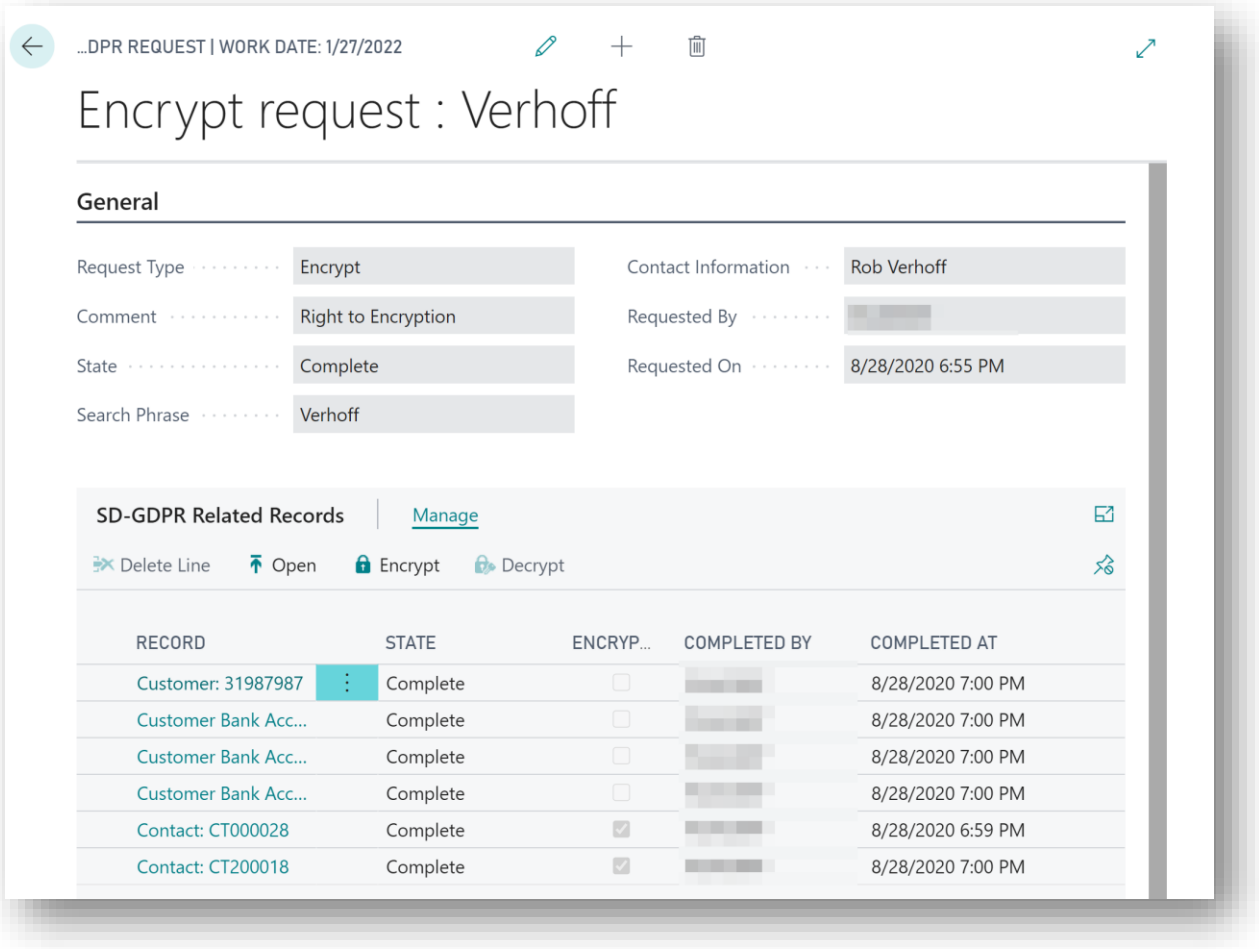


Figure 9-20

10 Viewing GDPR Encrypted Fields

To view the content of fields encrypted by SD Data and GDPR Manager we have included a **GDPR Demo Customer List** Page which demos how to call two functions to view the content of the fields.

GetFieldValue() allows you to pass the record and the field no. to the function and return the contents of the encrypted field.

GetFieldValueByName() allows you to pass the record and the field name to the function and return the contents of the encrypted field.

To do this firstly create a dependency to the version of SD Data and GDPR Manager that you currently have installed.

```
"dependencies": [
  {
    "id": "89616861-ed08-4907-b52a-488c1c10f779",
    "name": "SD Data and GDPR Manager",
    "publisher": "Simply Dynamics Ltd",
    "version": "3.0.0.0"
  }
 ],
```

Then add code similar to the below to your existing Customer List extension:

```
pageextension 50000 "Customer List Extension" extends "Customer List"
{

  layout
  {

    modify("Name")
    {
      Visible = false;
    }
```

```
modify("Phone No.")
{
   Visible = false;
}
modify("Contact")
{
   Visible = false;
}
modify("Search Name")
{
   Visible = false;
}


addafter("No.")
{
   field("Name Extended"; gSDYUDGDPRManager.GetFieldValue(Rec, Rec.FieldNo(Rec.Name)))
   {
      ApplicationArea = All;
      Caption = 'Name';
      ToolTip = 'Name';
   }
}
addafter("Country/Region Code")
{

   field("Phone No. Extended"; gSDYUDGDPRManager.GetFieldValueByName(Rec, Rec.FieldName(Rec."Phone No.")))
   {
      ApplicationArea = All;
      Caption = 'Phone No.';
      ToolTip = 'Phone No.';
   }
}

addafter("IC Partner Code")
{
```

```
        field("Contact Extended"; gSDYUDGDPRManager.GetFieldValue(Rec, Rec.FieldNo(Rec.Contact)))
        {
          ApplicationArea = All;
          Caption = 'Contact';
          ToolTip = 'Contact';
        }
      }

      addafter("Language Code")
      {
        field("Search Name Extended"; gSDYUDGDPRManager.GetFieldValueByName(Rec, Rec.FieldName(Rec."Search Name")))
        {
          ApplicationArea = All;
          Caption = 'Search Name';
          ToolTip = 'Search Name';
        }
      }
    }


    var
      gSDYUDGDPRManager: Codeunit "SDY UD GDPR Manager";
}
```

11 Uninstalling SD Data and GDPR Manager

Note: All encrypted data (encrypted by SD Data and GDPR Manager) will have to be decrypted in SD Data and GDPR Manager prior to uninstalling the product. Otherwise, your encrypted data will no longer be accessible.

You can uninstall **SD Data and GDPR Manager** using the Web Client:

1. Open your Dynamics 365 Business Central Web Client and use the **Tell Me** to search for **Extension Management** *(Figure 5-1)*.

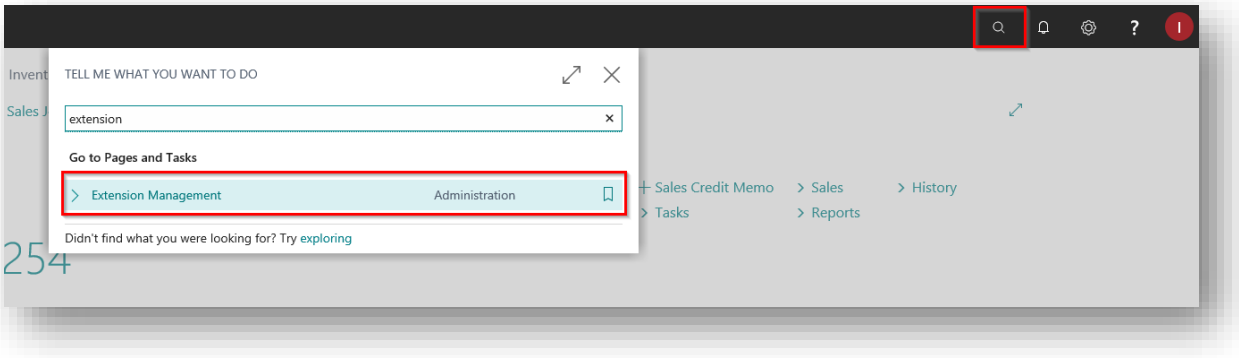


Figure 11-1

2. In **Extension Management**, you should see the **SD Data and GDPR Manager** App installed.

3. Select the **SD Data and GDPR Manager** App and choose the **Uninstall** Action (*Figure 5-2*).

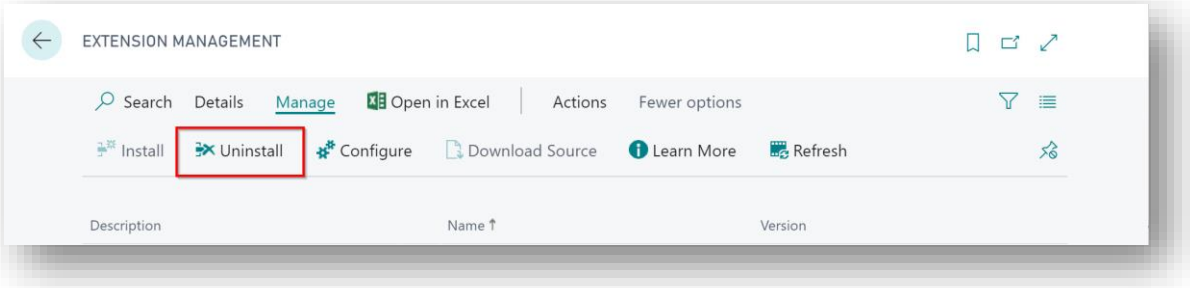


Figure 11-2

Dynamics Shop

IT Simply Makes Business Sense with Microsoft Dynamics 365

Simply Dynamics has been delivering complex and custom Dynamics 365 Projects and Support since 2007. Now servicing clients in over 18 countries.

DynamicsShop delivers Dynamics 365 enhancements through App's and as SAAS solutions to bring next level automation to your Dynamics 365 Solution.

DynAzure delivers cloud only, low cost & standardised model rapid deployment Dynamics 365 Projects and support utilising standard features and enhanced Apps.

Dublin Location

Unit 4, 4075 Kingswood Rd,
Citywest Business Campus,
Dublin, D24 H972, Ireland
Get Directions

+353 1 687 6600

info@simplyd.ie