Infor Distribution SX.e Administration Guide for GDPR Compliancy

Release 11.21.x

Important Notices

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials ("Purpose").

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

Trademark Acknowledgements

Publication Information

Release: Infor Distribution SX.e 11.21.x
Publication Date: June 15, 2021
Document code: sxe_11.21.x_sxgdprag_op_en-us

Contents

About this guide

This document describes the GDPR Compliance functionality in Distribution SX.e. It can be used to help distributors comply with the European Union's General Data Protection Regulation (GDPR). This guide explains the requirements, setup and configuration tasks, and instructions for use.

Intended audience

This guide is intended for system administrators who configure Distribution SX.e and for trained Data Protection specialists.

Only distributors that are subject to the European Union's General Data Protection Regulation should use this function. Data Protection specialists, with correct security, can use GDPR Compliance functionality to help the distributor achieve GDPR compliance.

Required knowledge

To use this functionality, you must understand how to use the Distribution SX.e. You must understand the European Union's General Data Protection Regulation and how that regulation affects your company.

If you are integrated with other Infor applications that use Business Object Documents (BODs), you must understand this information:

- Concepts behind Infor ION and BODs
- How the concepts relate to each of the applications in the integration

See the *Infor Distribution SX.e Configuration Guide for Infor Operating Service* and the *Infor ION Desk User Guide*.

Contacting Infor

If you have questions about Infor products, go to Infor Concierge at https://concierge.infor.com/ and create a support incident.

The latest documentation is available from docs.infor.com or from the Infor Support Portal. To access documentation on the Infor Support Portal, select **Search > Browse Documentation**. We recommend that you check this portal periodically for updated documentation.

If you have comments about Infor documentation, contact documentation@infor.com.

Chapter 1: Overview

This section describes the Global Data Protection Regulation (GDPR) and the Distribution SX.e function, **SA GDPR Compliance Administration**, that is used to comply with GDPR.

Global Data Protection Regulation compliance

The European Union's General Data Protection Regulation (GDPR) became effective on May 25, 2018. The GDPR intends to put EU residents in control of their personal data by regulating how their data is collected, processed, stored, deleted, transferred, and used. Any company, local and international, that does business in Europe or handles the personal data of EU residents should comply with the new rules. Noncompliance can result in financial penalties.

For organizations that have access and control of such data, the regulation obligates the organizations to proactively protect data. An EU citizen or resident has these rights, for example:

- Know what personal data is collected; the right to be informed
- Access to their personal data
- Ask that their data be updated; the right of rectification
- Ask that their data be erased; the right to be forgotten
- Ask that their data be restricted regarding who can process their data; the right to restrict processing
- Ask that their data be provided to them in a machine-readable format; the right to data portability
- Object to how their data is being used
- Request consent or opt out of automated decision-making and profiling

Personal data consists of any information relating to an identified or identifiable individual, entity, or data group. An identifiable person is one who can be identified directly or indirectly, by use of personal data that could be combined with other data that would make an individual reasonably identifiable. This data includes anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or online identifiers, including IP addresses and device IDs.

Infor is committed to ensuring that Infor's products and processes meet or exceed stringent global regulatory requirements, including GDPR.

SA GDPR Compliance Administration

Note: SA GDPR Compliance Administration is available in Distribution SX.e version 11.18.7 and later.

If you are a Data Protection specialist with the correct security, you can use the Distribution SX.e function, **SA GDPR Compliance Administration**, according to your company's established procedures. You can perform searches, generate a portable file, disable an entity, forget an entity, view expiration records, re-enable an entity, and review history records.

The workflow begins when an individual or entity requests one of these actions:

- Access to their personal data
- Disabling of their personal data in the application
- Redaction of their personal data in the application

The first task is to find all identifiable instances of that entity. Use **SA GDPR Compliance Administration** to search for a specific entity. You can use the Search pane or conduct a facet search. The results of the search are displayed in the grid.

You can review the result instances in the grid and confirm a match. Select one or more result instances and perform actions on those instances. Actions are accessed from buttons on the **GDPR Compliance** view. You can create a portable file, disable, or forget the entity, based on that entity's request.

Print

An entity has a right to access their data. The data must be provided in a portable, readable format. In Distribution SX.e, the portable file is an output of the selected records in a JSON output file. You can select the confirmed instances of personal data and perform a Print action. You can email the JSON file or send the JSON file to a Dropbox.

See the online help for information about enabling report output to Dropbox.

When you create the JSON file, an audit record is created by the system indicating the date, time, and action taken. The audit record can be viewed in the **History** view. The audit records can be used to indicate when certain actions were taken should anyone want to verify GDPR rule compliance.

The top level in the JSON file is the name of the individual or entity for which the search was performed. Below the name are entity sections that equate to a field in a database table that contains the name. Each entity section contains a data section, which lists the personal information stored in the database. An example of the contents of a JSON file may be a series of sections that look like this:

```
!UTF-8!{"pdsGDPRreport": {
  "GDPRname": [
    {
      "Name": "Beth Smith",
      "GDPRentity": [
        {
          "Entity": "VENDOR",
          "Company": "5000",
          "Key1": "600",
```

```
        "Key2": "",
        "Fieldnm": "Name",
        "GDPRdata": [
          {
            "FieldValue": "Beth Smith",
            "Addr1": "2700 University Blvd",
            "Addr2": "Suite 150",
            "Addr3": "Attn: Shipping",
            "City": "NY",
            "State": "NY",
            "PostalCd": "12345",
            "Country": "US",
            "PhoneNumber": "5125551212",
            "FaxNumber": "5125551212",
            "EmailAddress": "beths@exammple.com",
            "EDITradePtnr": "",
            "WebPage": ""
          }
        ]
      },
```


Export to Excel

You can export the contents of the selected records in the grid to a Microsoft Excel .csv file. Select all the confirmed records and select **More > Export to Excel**. Save the `.csv` file to a predetermined directory. You can then email the `.csv` file or send it to a Dropbox.

Disable

You can disable an entity's personal data for a specified time period. Perhaps, an entity is reviewing the personal data you sent in a portable file, or you received a request to disable a suspended sales representative.

To disable, conduct an appropriate search for the entity, select one or more result instances in the grid, and click **Disable**. You are prompted to select an expiration date. Typically, this date reflects when the personal data should be re-enabled or deleted. If the entity has not asked to be re-enabled by that date, you should select those instances and perform a **Forget** action. If you do not specify a date, the instance is not displayed in the **Expiration** view.

When an entity's personal data is disabled, that data is tagged and hidden by the system as much as possible and cannot be accessed in Distribution SX.e functions. The data cannot be used to enter an order or used in future processing. If a Distribution SX.e operator attempts to use disabled personal data, one of these messages is displayed:

- `GDPR Restrictions Exist; Processing Not Allowed With Restricted Data (7087)`

  This message is displayed if the use of personal data in a main record, such as customer or vendor, is being attempted.

- `Warning: Record Contains Data Under GDPR Restrictions (8603)`

  This message is displayed if a main record contains restricted personal data, such as a purchase agent or vendor manager in a **Customer Setup** record.

Data that is received through a Business Object Document (BOD) or through a call to an SX.API program is ignored if the data affects a record that an entity has requested be disabled or forgotten. Likewise, data going out of the system through those venues are blocked if those restrictions are in place.

When you disable personal data, an audit record is created indicating the date, time, and action taken. The audit record is displayed in the **History** view.

Enable

If you disabled an entity's personal data, you can re-enable those instances in **SA GDPR Compliance Administration**. Access the **Expiration** view, select one or more instances in the grid, and perform an **Enable** action.

Disabling personal data does not remove that data from Distribution SX.e. When you search in **SA GDPR Compliance Administration**, you can find all the records for a specific entity, whether those records are enabled or disabled. The **Enable** action removes the tag, unhides the instance, and allows access for entering an order or processing again. It also clears any expiration date that was tagged to the instance so that the instance is not listed as requiring deletion.

In the **Expiration** view, the instances in the grid do not show the entity name or value because the entity is restricted. Typically, only the various instances from one entity are displayed. In lieu of the name, clues to the entity are the primary and secondary keys, company number, type of record, name of the restricted field, and expiration date. For example, for the TWLOCM function, **TWL Carrier Master Setup**, if the record is a carrier, the primary key might be **UPS**, and the secondary key would be the warehouse. If the record is a federal tax setup for a vendor, the primary key is the tax year.

When you enable personal data, an audit record is created by the system indicating the date, time, and action taken. The audit record is displayed in the **History** view.

Forget

If the entity requests that their personal data be forgotten, search and confirm matching instances of the entity's personal data, select one or more instances, and perform the **Forget** action. This action redacts the personal data so that the data is not recoverable.

The personal data is redacted by overwriting the content with one of two characters, depending on field value. The '**X**' character is used to fill the length of the field if the field is alphanumeric. The '**9**' character is used to fill the length of the field if the field is numeric. For example, the field contains **XXXXXXXXXX** or **999999999**.

Any record where the personal data is 'forgotten' is not available for use in the application. This data cannot be restored. If personal data is forgotten by mistake, you must create new records and instances.

When performing a **Forget** action, you are able to specify an expiration date to indicate when the record containing the instance of personal data should be deleted. Because the record is not usable after the personal data has been overwritten, the record should be deleted from the application as soon as possible. You should delete the affected instances by navigating to the appropriate function in the application, selecting the record, and deleting the record from the function.

If your company uses CenPOS for credit card payment or electronic AP payment remittance, specific procedures should be followed when forgetting and deleting personal data in **Customer Credit Card Setup** and **Vendor Setup-eCommerce**. Certain personal data cannot be edited or restored. You should coordinate your procedural tasks with CenPOS.

Some personal data, such as a credit manager, a vendor manager, or a bank contact, does not require that an entire record be deleted. In those cases, you would open a related customer record and delete the value in the **Credit Manager** field.

In the **Expiration** view, the instances in the grid do not show the entity name or value because the entity is restricted. Typically, only the various instances from one entity are displayed. In lieu of the name, clues to the entity are the primary and secondary keys, company number, type of record, name of the restricted field, and expiration date. For example, if the record is a carrier, the primary key might be **`UPS`**, and the secondary key would be the warehouse. If the record is a federal tax setup for a vendor, the primary key is the tax year.

When you **Forget** personal data, an audit record is created indicating the date, time, and action taken. The audit record is displayed in the **History** view.

Expiration view

Instances of personal data that have had actions performed on them are displayed in the **Expiration** view. Use the fields in the Search pane to filter instances based on the Expires, Action, or Data Source values

For instances in the grid with a status of **`Disable`**, select one or more instances and click **Enable**. This action enables you to access and restore or take other GDPR action on the record. The **Enable** action removes the tag, unhides the instance, and allows access for processing.

For instances with a status of **`Forget`**, select one or more instances and click **Enable**. This action enables you to access and delete the record. For example, if a customer has been forgotten, that customer record is no longer displayed in the lookup and cannot be accessed in **Customer Setup** to delete or maintain. You must re-enable the customer, so the record is accessible in **Customer Setup**, and then you can delete the customer record. Enabling does not restore the forgotten personal data. That data is still redacted and cannot be retrieved. When you enable an instance, that instance is omitted from the **Expiration** view.

History view

Use the **History** view to view records that detail all the actions that have been taken in **SA GDPR Compliance Administration**. Use the **Action** field in the Search pane to filter instances based on action. The **History** view only shows what kind of action and when a specific action was taken. The view does not show the specific instances of personal data on which the action was taken.

Chapter 2: Setup and configuration

This section describes the planning efforts required before you implement GDPR compliancy and how to enable GDPR compliance functionality.

Planning

Planning and coordination are required before implementing GDPR compliancy. You should modify your workflow so your procedural tasks reflect how you will use **SA GDPR Compliance Administration**. Because of the importance of compliance activities affecting data, the more effort you put into planning, the more successful you will be in effectively using this functionality. In addition to having procedures in place to use **SA GDPR Compliance Administration**, we recommend that your company have an overall General Data Protection Regulation (GDPR) policy in place.

Before defining compliancy procedures, we recommend that you first conduct an assessment. For example, consider what type of individuals or entities you have in your system, such as customers, ship tos, operators, buyers, users, and expediters. Determine what personal data for each entity must comply with GDPR regulations. This kind of assessment helps to conduct a more efficient and effective search with appropriate criteria when you receive GDPR requests.

Consider how you will respond to GDPR requests: email, phone, text, mail? Who should receive, analyze, and respond to requests? Will you have a predefined form for a call taker to take notes about the request? Consider how you will process GDPR requests. Is this a request for a portable file of instances of an individual or entity's personal data? Is this a request for you to disable an entity? Is this a request for you to forget an entity? How often will you process requests? As needed, weekly, monthly? Can you negotiate with the entity to determine what data should be forgotten and when?

Under what kind of scenarios are you most likely to receive GDPR requests? For example, a vendor calls you and requests a report of all instances of their name with the application. Or, a sales representative has violated company rules and has been suspended. Their manager wants to know all instances of that sales representative throughout the application. Or, a customer is in a legal dispute with the distributor and requests all instances of their name be forgotten within the application.

Consider how you will assess and complete processing on sales or purchase orders associated with an entity. Are there open orders? Outstanding balances? Are there orders that have been invoiced, but not paid? Are there orders that have been shipped, but not invoiced? Are there credit card setup records that are affected? You should complete all stages of an order before you disable or forget an entity.

Are there ancillary procedures that you must establish before re-enabling an entity? The action of "forgetting an entity" redacts the associated data. For example, you have disabled a bank contact in **Customer Setup**. The customer assures you that they will provide a new contact name. Do you want to complete the forgetting process, or modify the field in edit mode? Another example might be that you are deleting **Customer Setup** records. When is the most convenient time for that task to be completed?

Are you running more than one environment, such as a test and production environment? Are there special considerations for disabling or forgetting instances of personal data in those environments?

Because of the importance of compliance activities affecting data, we also recommend you designate one, or a limited number of Data Protection specialists. For example, you may decide to have a Data Protection specialist for each business unit, each company, and each warehouse. You may decide to have a Data Protection specialist for initiating requests, and another for executing the requests. Enable **SA GDPR Compliance Administration** for Data Protection specialists only.

Integrations

If you are integrated with other Infor applications, contact your Infor representative to determine this information:

- GDPR compliance timelines that relate to that application
- Whether additional tools are available
- Whether additional planning and procedures are required

If you are integrated with third-party applications, contact your third-party representative for information about achieving GDPR compliance. For example, if your company uses CenPOS for credit card payment or electronic AP payment remittance, you should coordinate your procedural tasks with CenPOS.

If an integration uses Business Object Documents (BODs), be prepared to address the shared personal data between the systems. When you use **SA GDPR Compliance Administration** to disable an entity, forget an entity, and re-enable an entity, personal data contained in BODs and shared between systems is affected.

These outbound BODs are affected by GDPR Compliance:

- ContactMaster
- CustomerPartyMaster
- Person
- ShipFromPartyMaster
- ShipToPartyMaster
- SupplierPartyMaster

Limitations

The scope of **SA GDPR Compliance Administration** is broad and targets prime impact points, but some limitations exist. The limitations may be due to these considerations:

- Audit commitments

  For example, the ship to address is required to calculate and audit taxes and cannot be redacted.
- The feasibility to redact personal data on multiple past transactions

  SA GDPR Compliance Administration does not review data on existing documents, such as sales orders, purchase orders, warehouse transfers, kit product work orders, value-add orders. With such orders, it is probable that the personal information on a transactional document has been shared with an external entity. So, for example, three years of transactional records that are associated with an individual is not displayed in the **SA GDPR Compliance Administration** grid.
- Maintaining a balance of search time with likelihood of the existence of entity data

  Manual address data that is entered in functions such as **Vendor Invoice Center Entry** cannot be reviewed, disabled, or forgotten. You cannot review this data:
  - Notes and comments
  - Captured signatures
  - Data stored in User fields
  - Text entered by a user in reference or instructions fields
  - Data sent or received in Business Object Documents (BODs)

Log files and debug files created and updated from the application You can also run these reports to include use the **Sales Order Register Report** to provide a list of all the sales orders for a particular customer. You can use the **Purchase Order Register Report** to obtain a list of all purchase orders for a particular vendor. If you are generating a portable file for an entity, you can include the report output, along with the output from **SA GDPR Compliance Administration**, in the file.

Enabling GDPR compliance functionality

To enable the GDPR compliance functionality, you must grant functional security to your Data Protection specialists in **SA Operator Setup**. Only grant access to functions that operators require to perform their jobs. If you grant access to functions that operators do not use, you compromise the validity of your data.

1. Select **System Administrator > Setup > Operator**.
2. Specify operator criteria, and then click **Search**.
3. Select the operator record to maintain and click **Edit**.
4. Click **Function Security**.
5. Specify **`web`** in the **Menu Set** field.
6. Specify **`*saag`** in the **Name** field.
7. Click **Search**.
8. Select the **`SAAG`** function.

9 Click **Set Function Security**.

10 Select **`5-Full Security`**, and then click **OK**.

11 Security for the entire function, including sub functions, is set. Click **Save**.

12 Sign out of Distribution SX.e and then sign back in to activate this setting.

Chapter 3: Using SA GDPR Compliance Administration

If you are a Data Protection specialist with the correct security, use **SA GDPR Compliance Administration** according to your company's established procedures. Use **SA GDPR Compliance Administration** to perform searches, generate a portable file, disable an entity, forget an entity, view expiration records, re-enable an entity, and review history records.

Performing a search

Use **SA GDPR Compliance Administration** to search for a specific entity. You can use the Search pane and then conduct a facet search. The results of the search are displayed in the grid.

1. Select **System Administrator > Administration > GDPR Compliance**.
2. In the Search pane, specify the name of the entity.

   This query searches for an exact match of the value in the **Name** field. You may be required to search for and confirm variations of an entity's name. For example, **`Beth Smith`**, **`Elizabeth Smith`**, **`Liz Smith`**.
3. In the **Data Source** field, retain the default **`All`**, or select one or more sources. You can filter the results, based on these groupings of database sources:
   - **`Accounts Receivable`** includes customer-related setup functions
   - **`Accounts Payable`** includes vendor-related setup functions
   - **`Employees`** includes operator, buyer, sales representative setup functions
   - **`Contacts`**, as specified in the Contacts context application
   - **`Prospects`**, as specified in **Sales Prospect Setup**
   - **`Warehouse Logistics`** includes Total Warehouse Logistics carrier, employee, master, vendor records
4. Click **Search**.
5. Optionally, click **Show More** to conduct a facet search.

   A facet search to narrows your initial search results. You can conduct a subsequent facet search to narrow the results of a previous facet search.

   Note: If you use the Contacts context application, how a contact is set up may affect data in the Compliance grid. For example, the Function column shows contacts and the Value column contains a name, but the phone and address are missing. It is likely that the **`Primary`** option was not selected for the phone and address in the Contacts setup.

Generating a portable file

With the GDPR regulation, an entity has a right to access their data. The data must be provided in a portable, readable format. In Distribution SX.e, the portable file is an output of the selected records in a JSON output file.

The top level in the JSON file is the name of the individual or entity for which the search was performed. Below the name are entity sections that equate to a field in a database table that contains the name. Each entity section contains a data section, which lists the personal information stored in the database.

The JSON data is exported to a file in the print directory specified in **SA Company Setup-Required-Directories**. You can then distribute it, based on the user's instructions.

When you create the JSON file, an audit record is created indicating the date, time, and action taken. The audit record is displayed in the **History** view. The audit records can be used to indicate when certain actions were taken should anyone want to verify GDPR rules compliance.

You can email the JSON file or send it to Dropbox.

See the online help for information about enabling report output to Dropbox.

1. Select **System Administrator > Administration > GDPR Compliance**.
2. Perform a search for the subject entity.
3. In the grid, select the confirmed instances of personal data and click **Print**.
4. If the **Output Type** field is available, select an output type. The **Output Type** field is available if you are set up to use Dropbox.
5. If appropriate, specify the email address of the entity that requested the file.
6. Specify a name for the file. We recommend that the file name be recognizable as a GDPR-related file. For example, prefix the file name with **`GDPR`**.

Disabling an entity

You may be asked to disable an entity's personal data for a specified time period. Perhaps an entity is reviewing the personal data that you sent in a portable file, or you received a request to disable a suspended sales representative.

When an entity's personal data is disabled, that data is tagged and hidden by the system as much as possible and cannot be accessed in Distribution SX.e functions. An audit record is created indicating the date, time, and action taken. The audit record is displayed in the **History** view.

1. Select **System Administrator > Administration > GDPR Compliance**.
2. Perform a search for the subject entity.
3. In the grid, select the confirmed instances of personal data and click **Disable**.
4. Specify an expiration date. Typically, this date should reflect when the personal data should be re-enabled or deleted.
5. Click **OK**.

Forgetting an entity

If an entity requests that their personal data be forgotten, you will perform the **Forget** action. This action redacts the personal data so that the data is not recoverable. The personal data is redacted by overwriting the content with one of two characters, depending upon field value. The '**x**' character is used to fill the length of the field if the field is alphanumeric. The '**9**' character is used to fill the length of the field if the field if the field is numeric. Like the **Disable** function, any record where the personal data is 'forgotten' is not available for use in the application.

Note: Because the record is not usable after the personal data has been overwritten, the record should be deleted from the application as soon as possible. You should delete the affected instances by navigating to the appropriate function in the application, selecting the record, and deleting the record from the function..

If your company uses CenPOS for credit card payment or electronic AP payment remittance, specific procedures should be followed when forgetting and deleting personal data in **Customer Credit Card Setup** and **Vendor Setup-eCommerce**. Certain personal data cannot be edited or restored. You should coordinate these tasks with CenPOS.

Some personal data, such as for a credit manager, a vendor manager, or a bank contact, does not require that an entire record be deleted. In those cases, you would open a related customer record and delete the value in the **Credit Manager** field.

1. Select **System Administrator > Administration > GDPR Compliance**.
2. Perform a search for the subject entity.
3. In the grid, select the confirmed instances of personal data and click **Forget**.
4. Specify an expiration date. Typically, this date should reflect when the personal data should be deleted.
5. Click **OK**. The audit record is displayed in the **History** view.
6. Monitor the expiration date. On that date, you must re-enable the entity. This action allows you to access and delete the record.

   See Re-enabling an entity on page 20.

Viewing records due to expire

Instances of personal data that have had actions performed on them are displayed in the **Expiration** view. In the **Expiration** view, the instances in the grid do not show the entity name or value because the entity is restricted. Typically, only the various instances from one entity are displayed.

In lieu of the name, clues to the entity are the primary and secondary keys, company number, type of record, name of the restricted field, and expiration date. For example, if the record is a carrier, the primary key might be **UPS**, and the secondary key would be the warehouse. If the record is a federal tax setup for a vendor, the primary key is the tax year.

1. Select **System Administrator > Administration > GDPR Compliance**.
2. Click **Expiration**.

3 Select one of these values from the **Expires** field:
   - **Today**
   - **This Week**
   - **This Month**
   - **All Dates**

   The grid shows instances the dates that are associated with this value and any previous dates.
4 Select **Disable** or **Forget** in the **Action** field.
5 Retain the default **All**, or select one or more sources, in the **Data Source** field.
6 Click **Search**.
7 In the grid, select the confirmed instances of personal data and click **Enable**.
   See Re-enabling an entity on page 20.

Re-enabling an entity

If you have set an entity's personal data to Disable or Forget, you can re-enable those instances in **SA GDPR Compliance Administration**.

If you re-enable an instance with a status of **Disable**, you can then access and restore or take other GDPR action on the record. The **Enable** action removes the tag, unhides the instance, and allows access for processing.

If you re-enable an instance with a status of **Forget**, you can then access and delete the record. For example, if a customer has been forgotten, that customer record is no longer displayed in the lookup and cannot be accessed in **Customer Setup** to delete. You must re-enable the customer, so the record is accessible in **Customer Setup**, and then you can delete the customer record. Enabling does not restore the forgotten personal data. That data is still redacted and cannot be retrieved. When you enable an instance, that instance is omitted from the **Expiration** view.

When you enable personal data, an audit record is created by the system indicating the date, time, and action taken. The audit record is displayed in the **History** view.

1 Select **System Administrator > Administration > GDPR Compliance**.
2 Click **Expiration**.
3 Select one of these values from the **Expires** field:
   - **Today**
   - **This Week**
   - **This Month**
   - **All Dates**

   The grid displays instances with dates that are associated with this value and any previous dates.
4 Select **Disable** or **Forget** in the **Action** field.
5 Retain the default **All**, or select one or more sources, in the **Data Source** field.
6 Click **Search**.

7 In the grid, select the confirmed instances of personal data and click **Enable**. The instances are no longer displayed in the grid.

Viewing history records

Use the **History** view to view records that detail all the actions that have been taken in the **SA GDPR Compliance Administration**. The **History** view only shows what kind of action and when a specific action was taken. The view does not show the specific instances of personal data on which the action was taken.

1 Select **System Administrator > Administration > GDPR Compliance**.
2 Click **History**.
3 Select one of these values in the **Action** field:
   - **Print**
   - **Enable**
   - **Disable**
   - **Forget**
4 Click **Search**.

Appendix A: Workflow examples

As the Data Protection specialist, you will use **SA GDPR Compliance Administration** differently depending upon the request made. Some workflow examples are provided in this section.

Note: Depending on how your company has set up their procedural tasks, and how they have structured Data Protection specialist tasks, the person handling the workflow may vary.

Customer has requested to be forgotten

A customer is in a legal dispute with the distribution company and requests that all instances of their name be forgotten within the application. Because this action destroys data on the customer record that cannot be recovered, you must perform certain tasks before taking the GDPR action on this customer.

A review of all orders for the customer must be performed. You must have a policy for handling these scenarios:

- Orders that have been entered, but not shipped
- Orders that have been shipped, but not invoiced
- Invoices sent but not paid

After the customer is forgotten, your company can no longer work with the sales orders for that customer.

Perform a review all transactions and balances for the customer. You must have a policy to address open transactions and non-zero balances in the most expedient way possible.

After you review and update data related to the customer and the use of that customer record throughout the application, begin processing the request. In **SA GDPR Compliance Administration**, perform an initial search on the name that was provided. Based on the number of results returned, you can use the facet search to add additional search criteria to reduce the number of results.

Select all the confirmed records and click the **Forget** button. Specify an expiration date that reflects how long the forgotten records can remain in the system before they are required to be removed. When you click **OK**, the processing to redact the personal data begins in the system.

After the redaction process is complete, that customer record and any ship to records for that customer cannot be edited. The records are not visible in the customer or ship to lookups. No sales orders for the customer can be created or maintained. In other functions, such as **Product Warehouse Description**

Setup where the **Customer** field is associated with a warehouse, that customer number cannot be specified.

Use the **Expiration** view in **SA GDPR Compliance Administration** to keep track of forgotten records that are approaching the specified expiration date. You are responsible for ensuring that the records are deleted. When you are ready to delete the customer record, you must select the instances in the **Expiration** view and re-enable the instances so the record can be accessed and deleted.

Monitor the time between the enablement and the deletion. The time frame must be as small as possible so that the records with the destroyed data are not used anywhere in the application. If a different Data Protection specialist deletes the **Customer Setup** and **Customer Ship To Setup** records, you must coordinate to ensure a short time frame.

Vendor requests a report of instances

One of your company's vendors calls their representative and requests a report of all instances of their name within the application. The representative notes the name of the individual, the vendor number, and any information needed to send the report to that individual. The request and the notes are sent to you.

In **SA GDPR Compliance Administration**, perform an initial search on the name that was provided. Based on the number of results returned, you can use the facet search to add additional search criteria to reduce the number of results.

Select all the confirmed records and click **Print**. is displayed. Specify the email address provided in the request notes and a file name on the **Print Options** window. When you click **OK**, the processing to generate the JSON document and email that document to the individual begins.

You can also run these reports to locate instances of the vendor in Distribution SX.e:

- **Purchase Order Register Report**

  Use this report to find all open purchase orders for the vendor.
- **Vendor Transaction Activity Report**

  Use this report to determine if your company owes the vendor. This information is useful if the vender asks to be disabled or forgotten.

Sales representative has been suspended

One of your company's sales representatives has violated company rules and is temporarily suspended. The sales manager requests a report of all instances of that sales representative throughout the application. The sales manager sends you an email noting the name of the individual.

In **SA GDPR Compliance Administration**, perform an initial search on the name that was provided. Based on the number of results returned, you can use the facet search to add additional search criteria to reduce the number of results.

Select all the confirmed records and select **More > Export to Excel**. Save the `.csv` file to a predetermined directory. In the `.csv` file, review the data if necessary. Email the spreadsheet to the sales manager for evaluation.

The sales manager can search the application to find customers associated with this sales representative. The sales manager can run the **Sales Order Register Report** to find orders where the sales representative is assigned as the Sales Rep In or Sales Rep Out. The sales manager can run the **SM Commission Report** to determine what commissions are due to the sales representative.

Note: The sales manager can change the sales representative on sales orders so that the restricted sales representative does not collect commissions or get credit for the sale. We recommend that the sales manager perform that action.

If, after evaluating the `.csv` file and the output from other reports, the sales manager decides that the sales representative personal data must be disabled, the sales manager notifies you, requests a Disable action, and provides the date when the suspension is over.

In **SA GDPR Compliance Administration**, perform a search on the sales representative. Select all the confirmed records and click **Disable**. When prompted, specify the end date for the suspension in the **Expiration Date** field. When you click **OK**, the processing to disable the personal data begins.

During the disabled period, data on the sales representative record is not changed. During the time the sales representative personal data is disabled, that sales representative record cannot be edited. The name is not visible in the sales representative lookup. In functions with an associated **Sales Rep In** or **Sales Rep Out** field, the sales representative cannot be specified.

Use the **Expiration** view track the disabled sales representative personal data that is approaching the specified expiration date. You should notify the sales manager that a decision must be made with regard to the status of the sales representative.

If management removes the sales rep from suspension, you can re-enable the sales representative's personal data. In **SA GDPR Compliance Administration**, perform a search on the sales representative. Select all the confirmed records and click **Enable**. The Enable action removes the tag, unhides the instance, and allows access for processing.

If the sales manager decides to dismiss the sales representative, you can remove the personal data from the application. In **SA GDPR Compliance Administration**, perform a search on the sales representative. Select all the confirmed records and click **Enable**. The Enable action removes the tag, unhides the instance, and allows access to remove the personal data.

The sales manager should use **Sales Rep Setup** to delete the sales representative and assign a new sales representative.