Information Guide: MDG-RFM compliance to Data Privacy and Protection like GDPR and Other Regulations

Applies to

Prometheus Group Solutions for MDG RFM

Summary

Master Data Governance for Retail and Fashion Management (RFM) are applications that provides a workflow-based governance process for article master. Records that are not selected for End of Purpose (EoP) are processed.

Company: Prometheus Group

Created On: November 18, 2020

Version: 1.0

Table of Contents

Introduction....3

Business Context....3

Prerequisite....3

Troubleshooting....3

Error 1: No Policy found for audit area....4

Error 2: Customizing missing for authorization group....6

Registration of MDG Class for EoP check....7

Usability of Sensitive Data on MDG-RFM UI Based on Authorizations....10

Introduction

You can use this document to configure MDG classes to scan through the open Change Requests for the usage of Customer or Vendor while running the report for blocking Customer/Vendor Master data.

In addition, this document explains the settings to help customers to be compliant with data privacy laws like the General Data Protection Regulation (GDPR) with the RFM Solutions by Prometheus Group . This implies that the sensitive data used in MDG Change Requests can only be accessed by user with required authorization.

The following topics are discussed in this document:

- Business Context
- Prerequisite
- Registration of MDG class for EoP check
- Usability of sensitive data on MDG-RFM UI based on authorizations

Business Context

Prometheus Group software products leverage the Standard SAP Framework and the underlying standard features for data protections applies to our products.

For personal data processed in the Master Data Governance (MDG) application, you can use SAP Information Lifecycle Management (ILM) to control the blocking and deletion of personal data.

Also, the personal data accessibility is controlled based on the auditor / non-auditor roles for providing better data protection. The usage of the blocked data is restricted until the same is unblocked.

For more information, see the product assistance for SAP S/4HANA on the SAP Help Portal under Product Assistance > Cross Components > Data Protection.

Prerequisite

Ensure that the relevant ILM business functions are activated to continue with the next steps. You can find the relevant information in ILM Help Chapter on Activating SAP ILM.

https://help.sap.com/erp2005_ehp_08/helpdata/en/99/c05853b2dc7425e10000000a44176d/frameset.htm

Note

Refer section on Troubleshooting if you face errors while running the blocking report CVP_PREPARE_EOP.

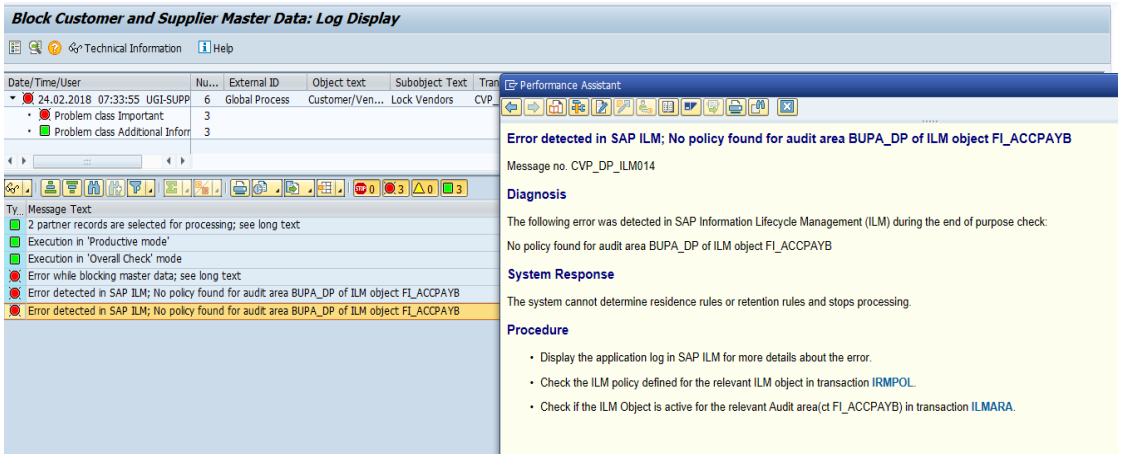
Troubleshooting

Some of the commonly faced errors while running the blocking report and their respective resolutions are provided as below:

- Error 1: No Policy found for audit area
  - Resolution: Define ILM Policy and Rules
- Error 2: Customizing missing for authorization group
  - Resolution: Define Authorization group indicating Blocked Master Data

Error 1: No Policy found for audit area

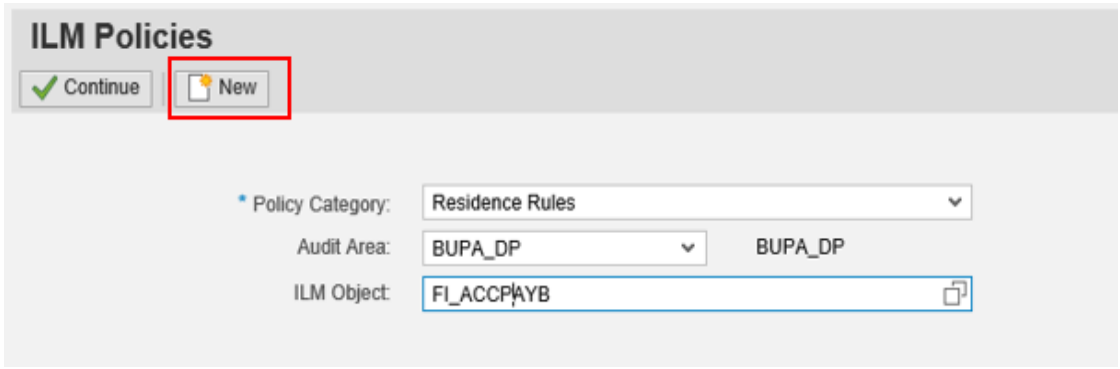
Error message: Error detected in SAP ILM: No Policy found for audit area BUPA DP of ILM object FI ACCPAYB



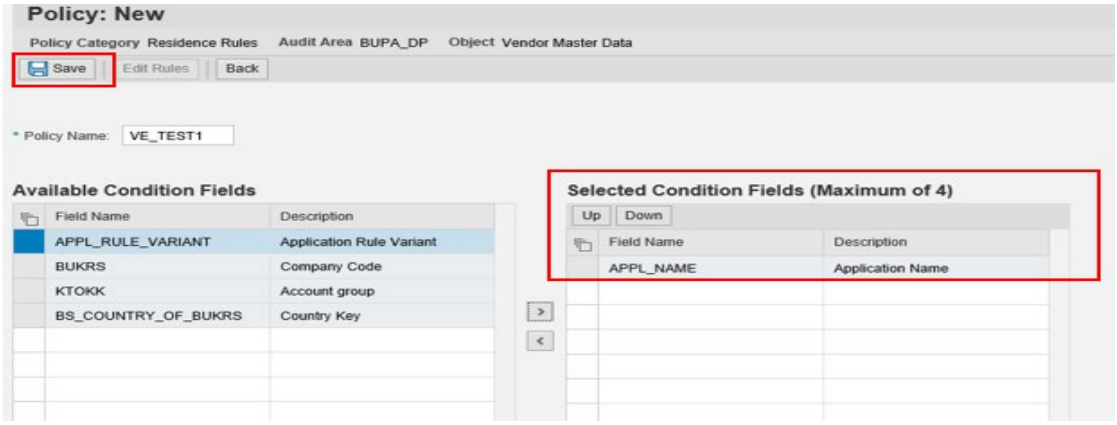
Resolution: Define ILM Policy and Rules

Use the following steps to define the ILM Policy and rules.

1. Navigate to the transaction IRMPOL.
2. Select the following entries:
   - Policy Category – Residence Rules
   - Audit Area – BUPA_DP
   - ILM Object – FI_ACCPAYB (for vendors)
3. Click on “New” button.

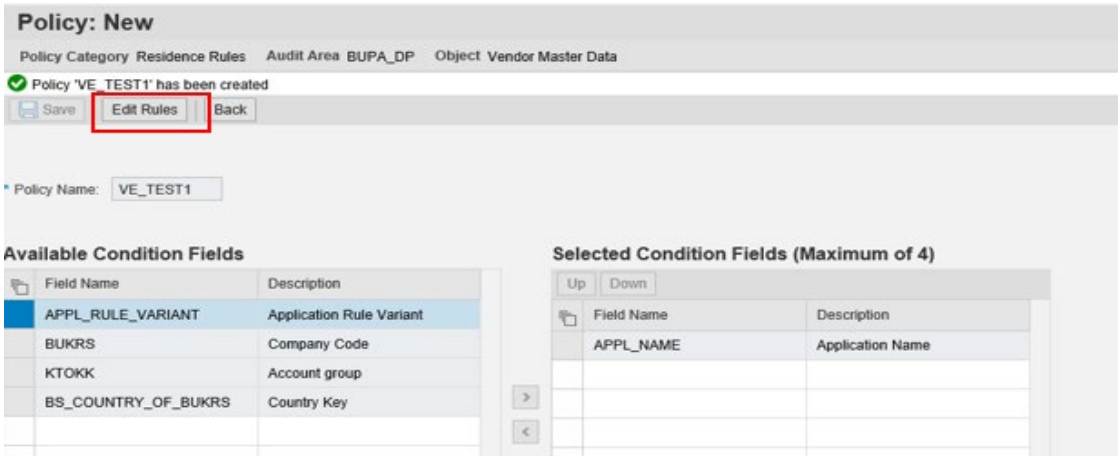


4. Select the “Application Name” from the ‘Available Condition Fields” and include in the selection criteria.



5. Click on “Save” button.

   A success message is displayed as ‘Policy VE_TEST1 has been created’.



6. Click on ‘Edit Rules’.
7. Navigate to the heading ‘Rules for Policy VE_TEST1’ and define a rule. Make the following selections for residence period 0.
   - Application Name: ERP_VEND
   - Residence period: 0
   - Residence time unit: days
   - Time ref: Start of retention period

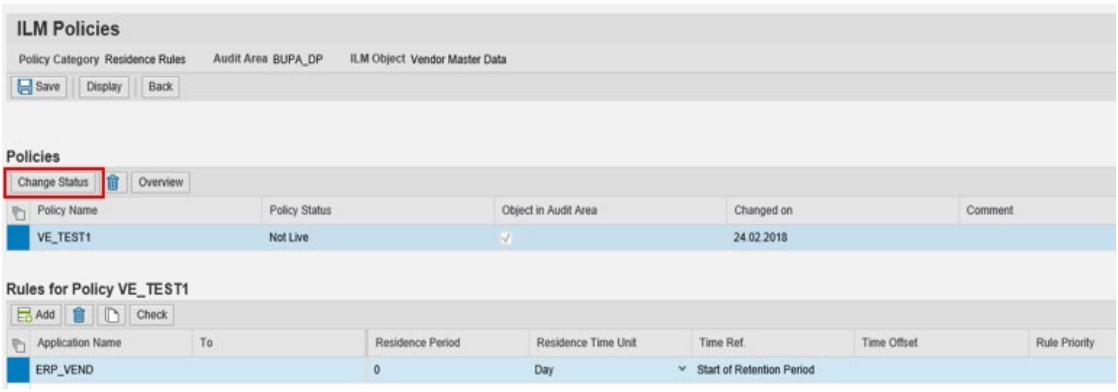
Note

The Residence period decides the time span since the last change/create date after which the newly created vendor/customer can be blocked. Blocking is possible only if the end of retention date is less than current date. This is checked against all the company codes defined for that vendor based on the customizing.

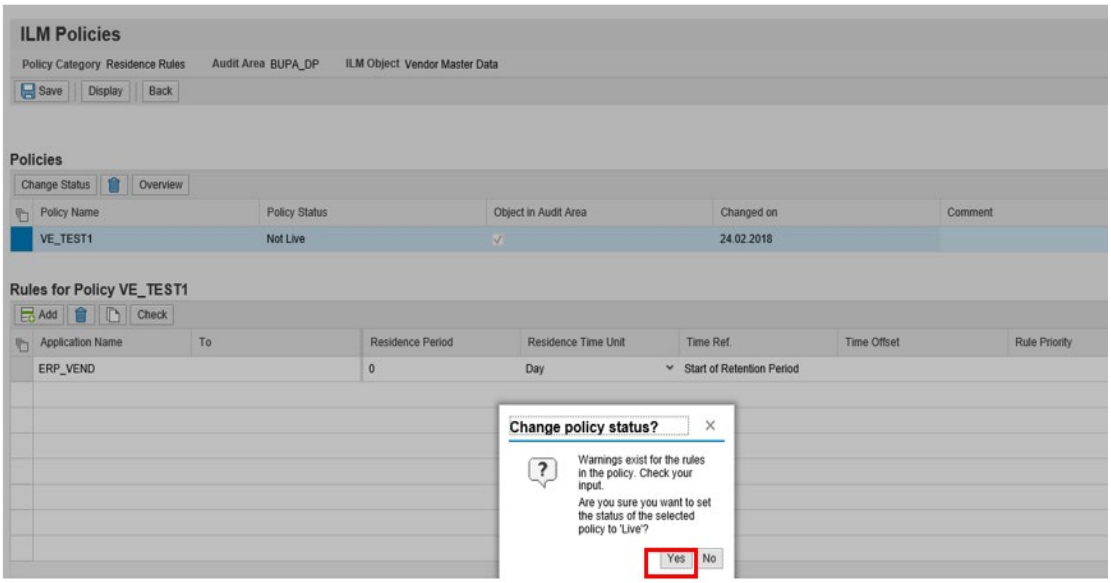
Also, if the end of retention period lies in future, it flags the vendor/customer with ‘Ongoing business’ and hence the vendor cannot be blocked.

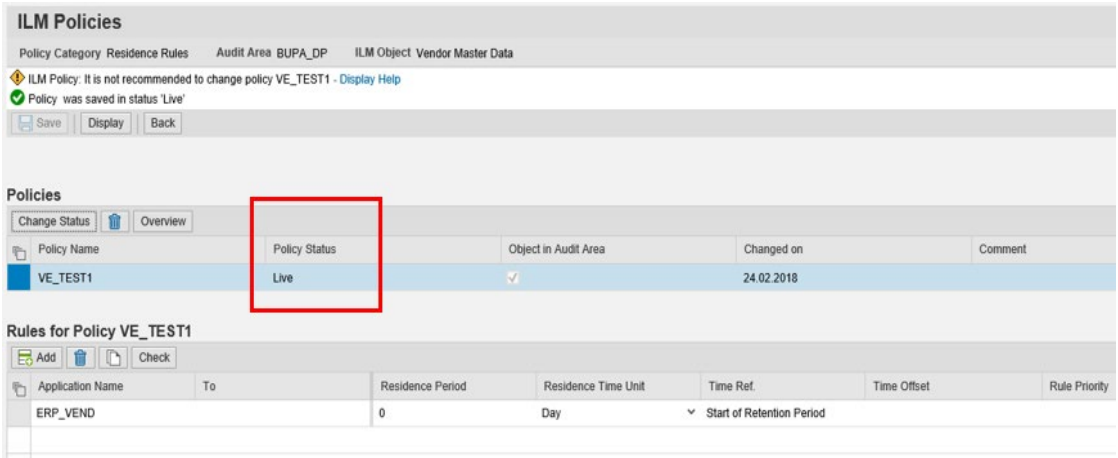
8. Click on “Save” button.
9. Click on “Change Status” button.

   A popup appears to confirm to set the policy live.



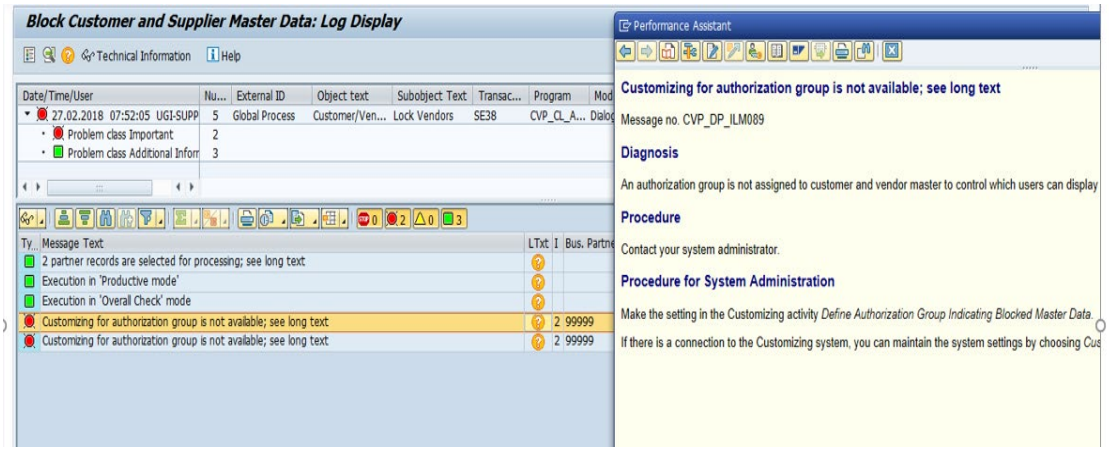
10. Click on “Yes” button on the pop up.
    A success message appears ‘Policy was saved in status Live’.





Error 2: Customizing missing for authorization group

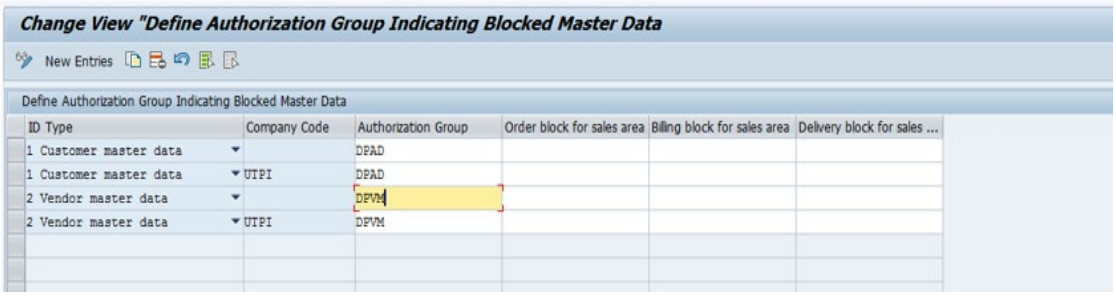
Error message: Customizing for the authorization group is not available; see long text



Resolution: Define Authorization group indicating Blocked Master Data

Navigate to the following path and maintain the authorization group for blocked master data.

Logistics – General-> Business Partner-> Deletion of Customer and Supplier Master Data-> Define Authorization Group Indicating Blocked Master Data



Note

Refer the following link for more information on ILM configuration:

https://help.sap.com/saphelp_crm700_ehp03/helpdata/en/f4/e6642b7f5542d8a7b7c7a037cba46f/frameset.htm

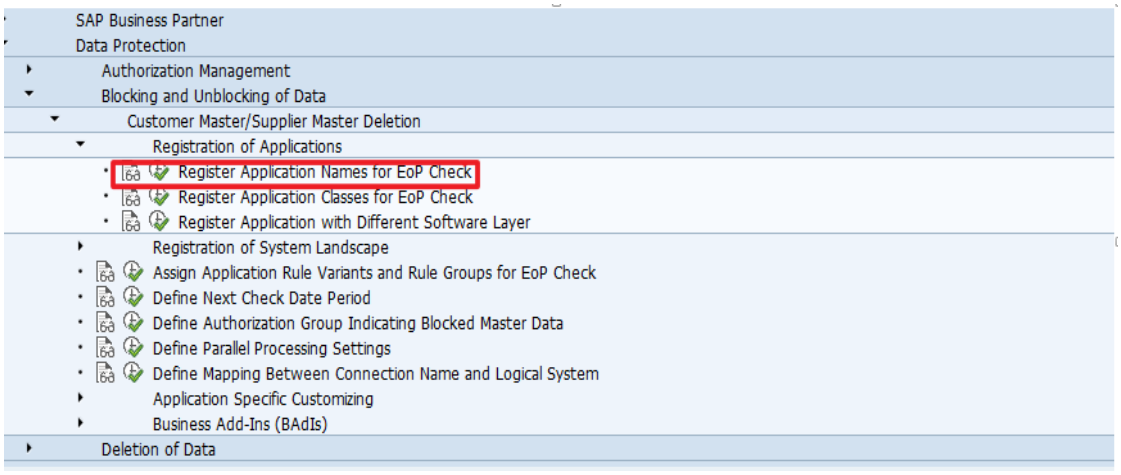
Registration of MDG Class for EoP check

To scan for the usage of Customer/Vendor in the MDG open Change Requests, you need to register the following application and classes.

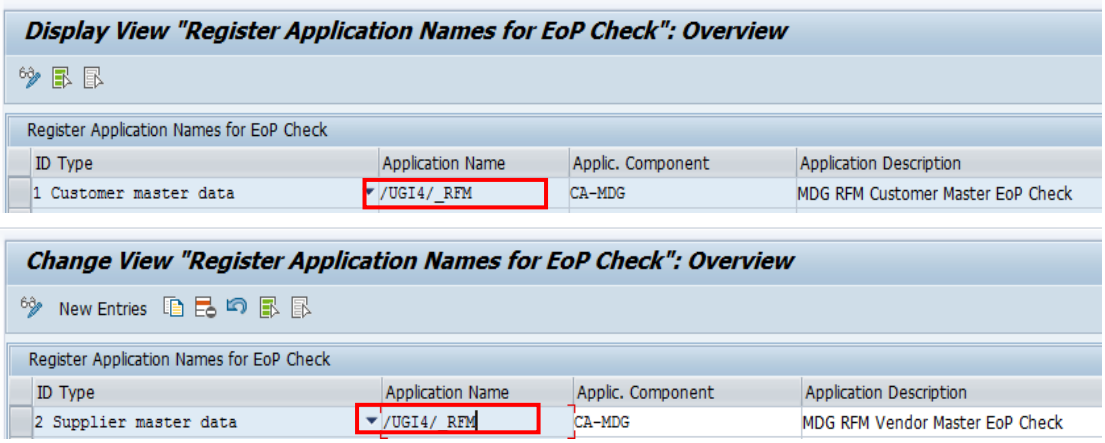
Note

You should ensure that the following steps of the configuration are completed. If you have not configured use the following steps to register MDG Class for End of Purpose (EoP) check:

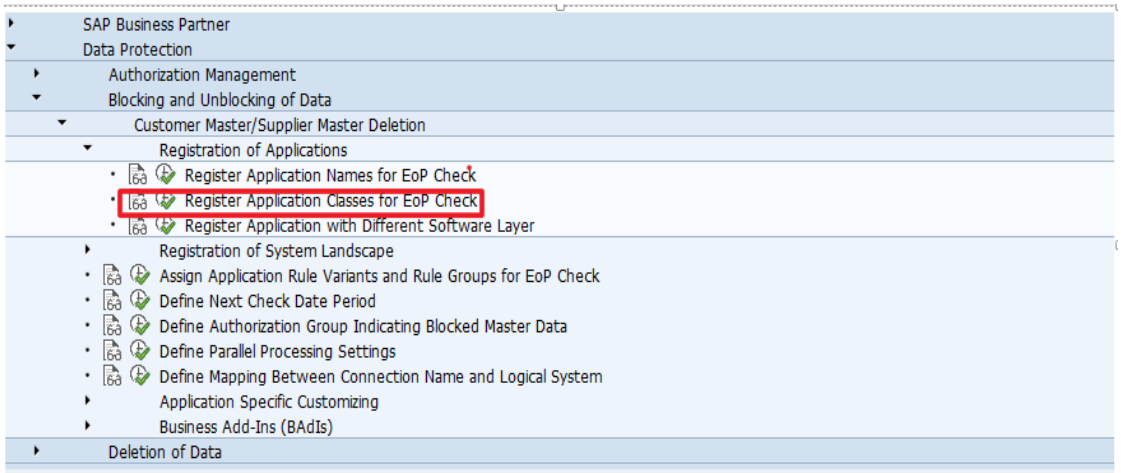
1. Navigate to SPRO > Cross-Application Components > Data protection > Blocking and Unblocking of Data > Registration of Applications > Register Application Names for EoP Check.



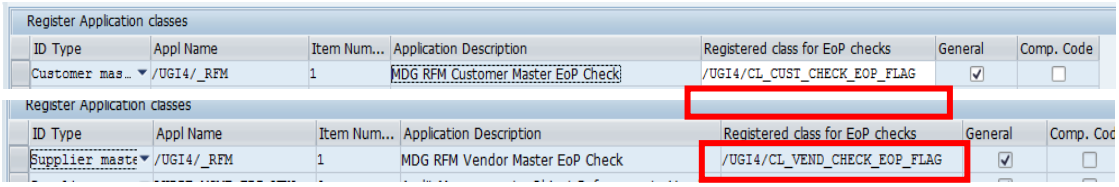
2. Make an entry for /UGI/_RFM application.



3. Navigate to SPRO > Cross-Application Components > Data protection > Blocking and Unblocking of Data > Registration of Applications > Register Application Classes for EoP Check.



4. Make the following entries for registering the MDG Class for checking Customer/Vendor usage in open Change Requests.
   - Customer - /UGI4/CL_CUST_CHECK_EOP_FLAG
   - Vendor - /UGI4/CL_VEND_CHECK_EOP_FLAG



5. Use transaction code (t-code) SM30 to maintain the entities and the MDG attributes to be scanned while running the blocking report in the maintenance view /UGI4/EOP_CHECK. If customers have extended the data model with any sensitive data fields and wants to implement the MDG RFM EoP check for the fields, the field should be added to the following table.

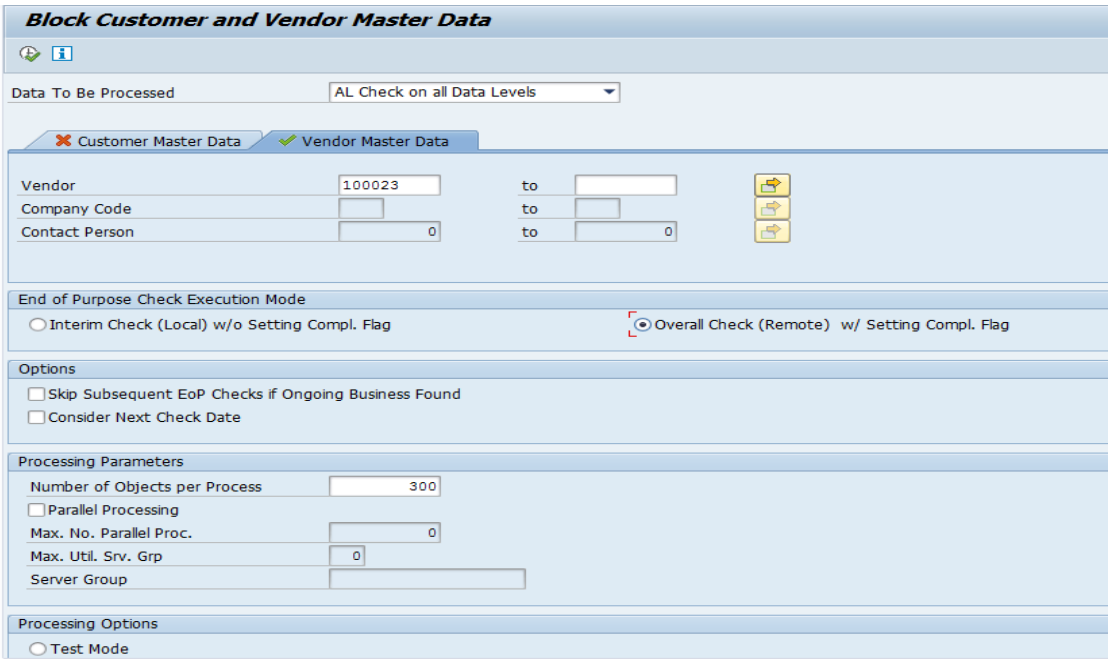
Object	Entity Type	Attribute	ObTy.
MARA	PIR_NOTE	LIFNR	Vendor
MARA	PURCHEINA	KOLIF	Vendor
MARA	PURCHEINA	LIFNR	Vendor
MARA	PURCHEINA	MFRNR	Vendor
MARA	PURCHINFO	LIFNR	Vendor
MARA	WYT2	LIFNR	Vendor
MARA	MEAN_GTIN	LIFNR	Vendor

6. Run t-code CVP_PRE_EOP in ECC. This report can be used to block data related to customers and vendors. The report checks with the dependent applications if business is complete and the residence period is over and then blocks the customer and vendor master data.

   You can no longer display, edit, create business objects or conduct follow-up activities with the blocked data. The blocked data can be displayed only by users having the appropriate permissions. You can use this report if the authorization object B_BUP_PCPT is set with ACTVT 05.

   Refer to the following url for more information:
   https://help.sap.com/saphelp_banking90loc/helpdata/en/fe/125953c91eff4fe10000000a44176d/frameset.htm

7. Select “Overall Check” as Execution Mode and “Production Mode” as Processing Options.

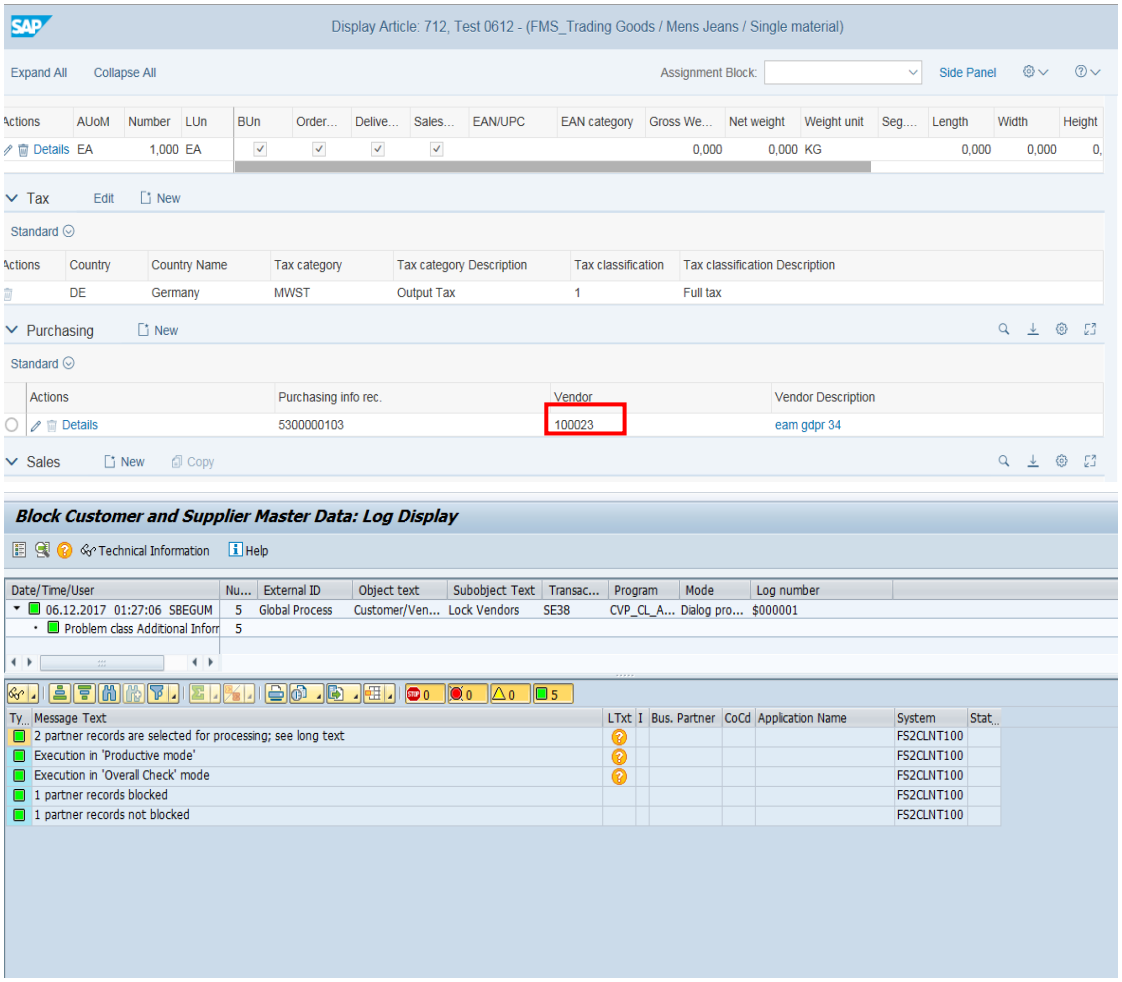


8. Click the “Execute” button.

Note

In case the Vendor/Customer is used in any of the open Change Request in MDG, blocking of the same is stopped as displayed in the following screens.

The following screen displays the specific Customer is locked in a Change Request.



Usability of Sensitive Data on MDG-RFM UI Based on Authorizations

Partner, Vendor and Customer data are available in the following MDG-RFM screens.

- Purchasing > Vendor, Vendor description
- Purchasing > Vendor > Area of validity vendor
- General Data for each Vendor > Vendor Data > Prior Supplier, Manufacturer etc.
- Purchasing > Info record note.
- Purchasing > Purchase Order Text
- Units of Measure > Additional GTIN (with vendor)

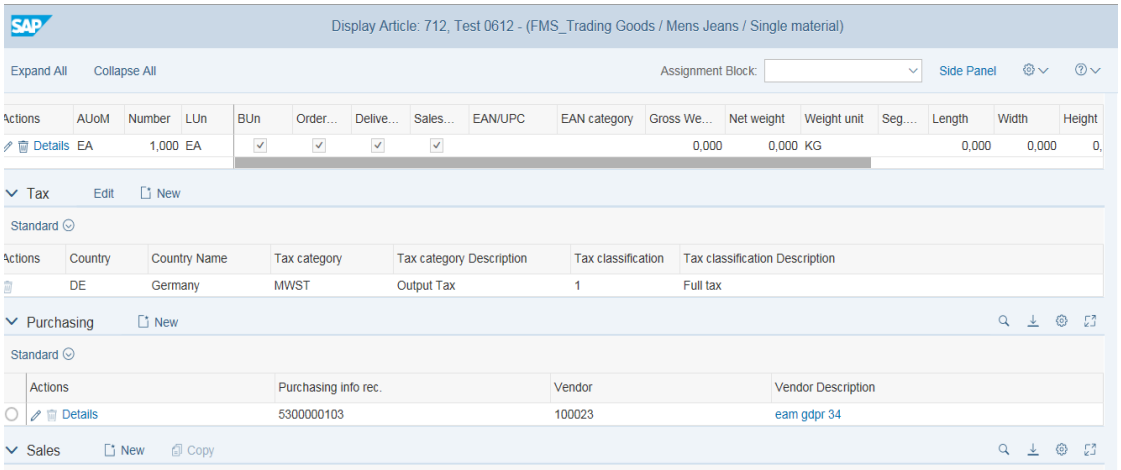
Use the following steps to check the accessibility of sensitive data on MDG-RFM based on authorizations:

1. Open the existing RFM Change Request containing Customer/Vendor marked with EoP flag.

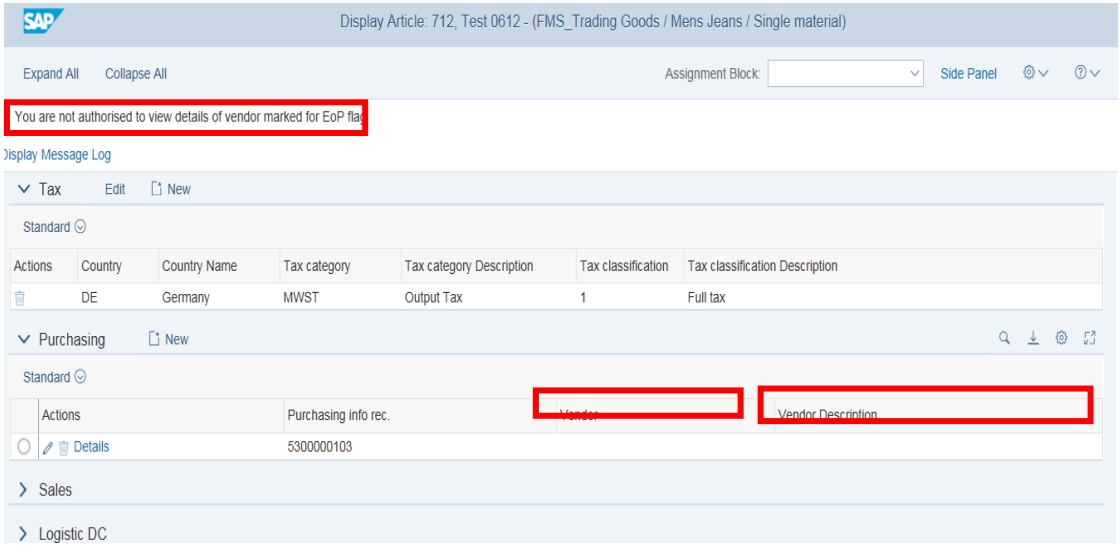
   Note

In case of limited authorizations, the same is not visible/blank. Deletion/Changing of the same is not allowed with limited authorizations.

The following screen displays the existing Change Request with all visible data to a user who has full authorization.

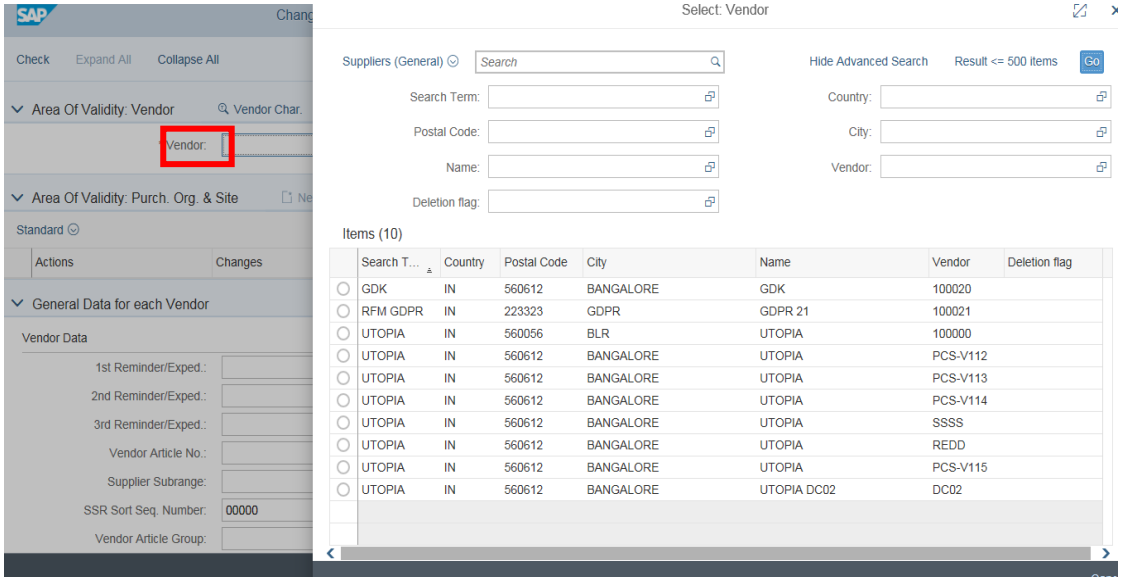


The following screen displays the Change Request with blanked out sensitive data for the user with limited authorization. An information message is displayed to convey the same.

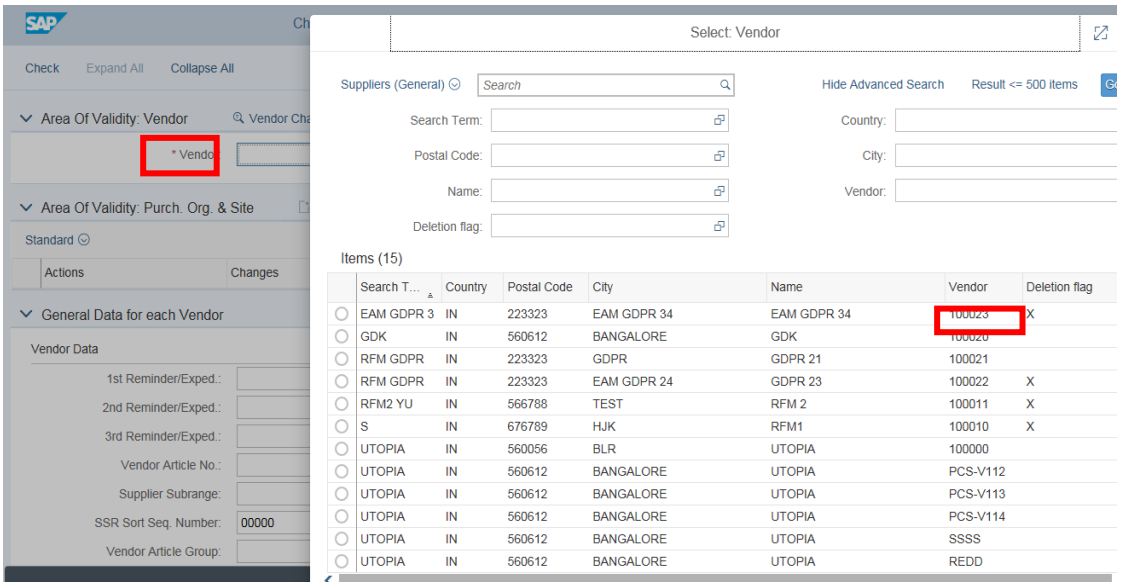


2. Run a Create/Change flow on an RFM object. F4 Help is restricted for Customer/Vendor marked with EoP with respect to authorizations.

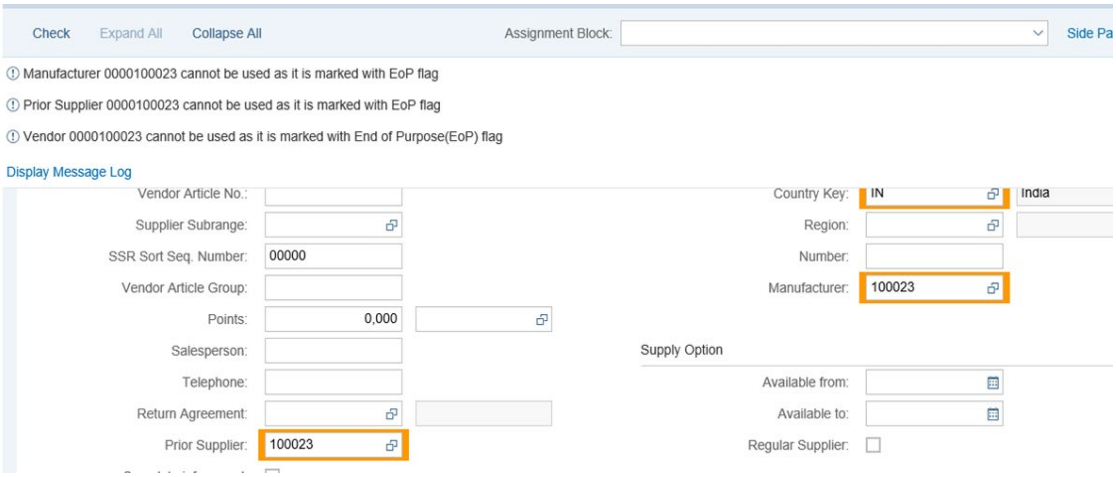
   The following screen displays that Vendors with EoP are not available for selection with limited authorizations.



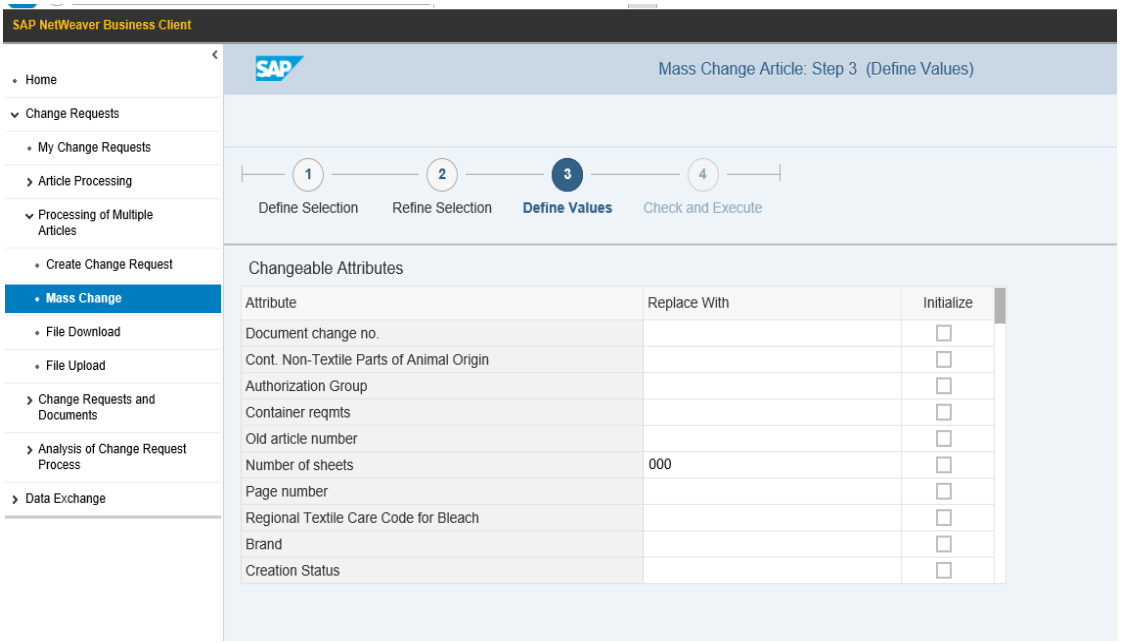
The following screen displays that vendor with EoP are available for selection with complete authorizations.



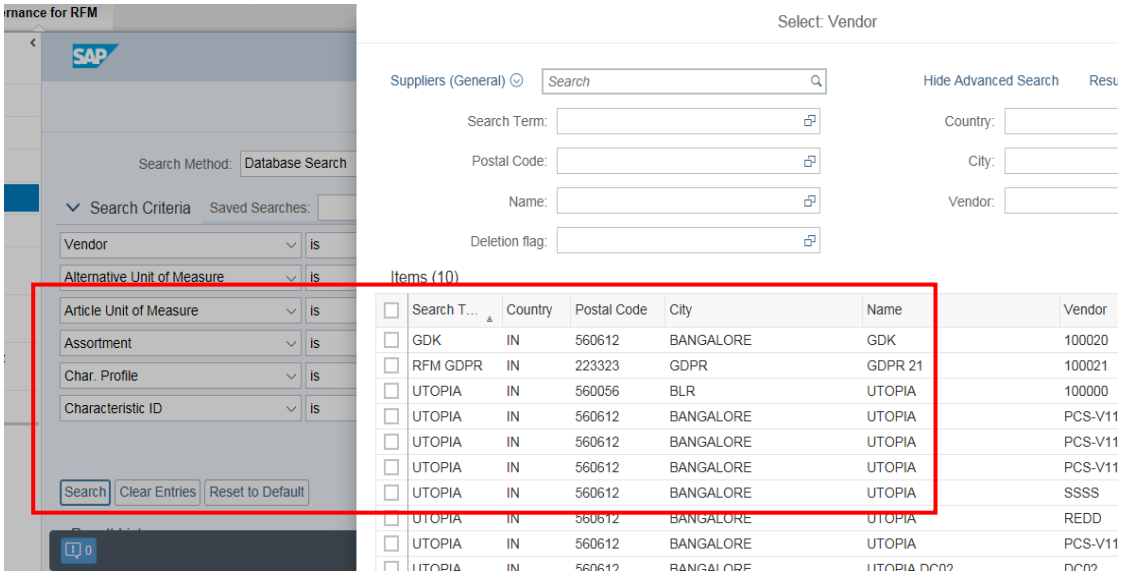
3. Run a Create/Change flow on an RFM object. For example, Vendors in Article Master > Purchasing tab. In case a vendor with EoP flag is assigned, error message is displayed to stop the assignment of blocked Customer/Vendor in Change Request.



4. Run Mass Change scenario for an RFM object. The sensitive fields such as Vendor/Customer/Contact Person data should not be available on the Mass Change UI for selection.

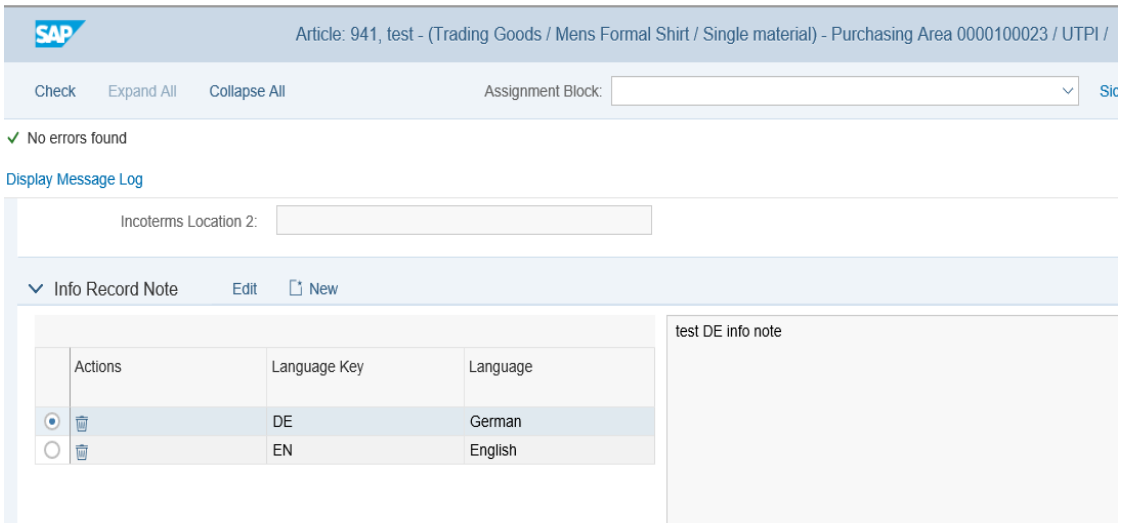


5. Run Database Search on the sensitive fields. F4 Help is restricted based on authorization for the EoP marked Customer/Vendor.

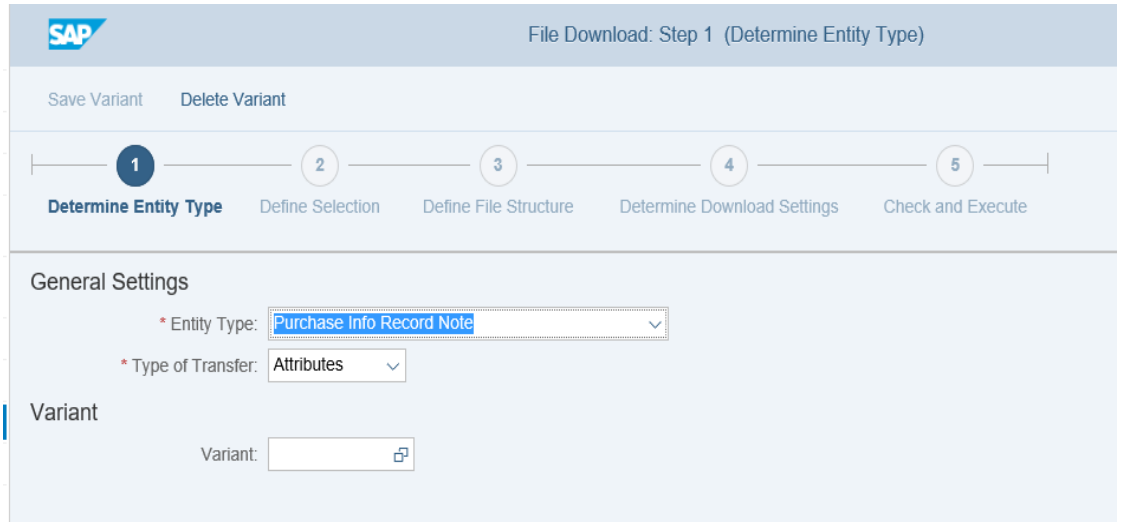


6. File Download does not display sensitive data for unauthorized users.

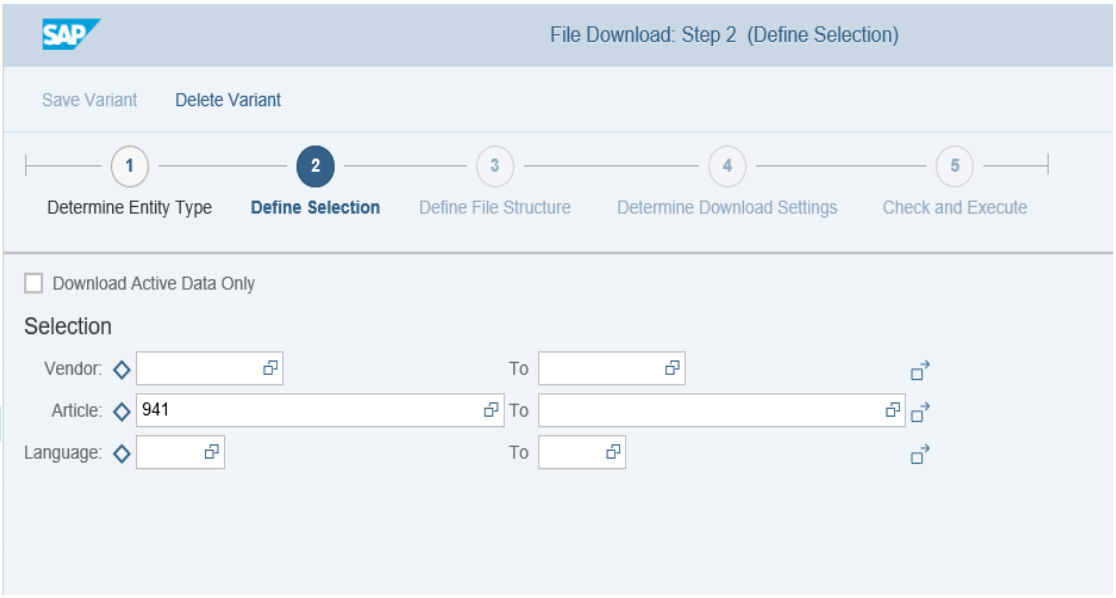
   The following screen depicts article 941 has the info record note text maintained for vendor 100023.



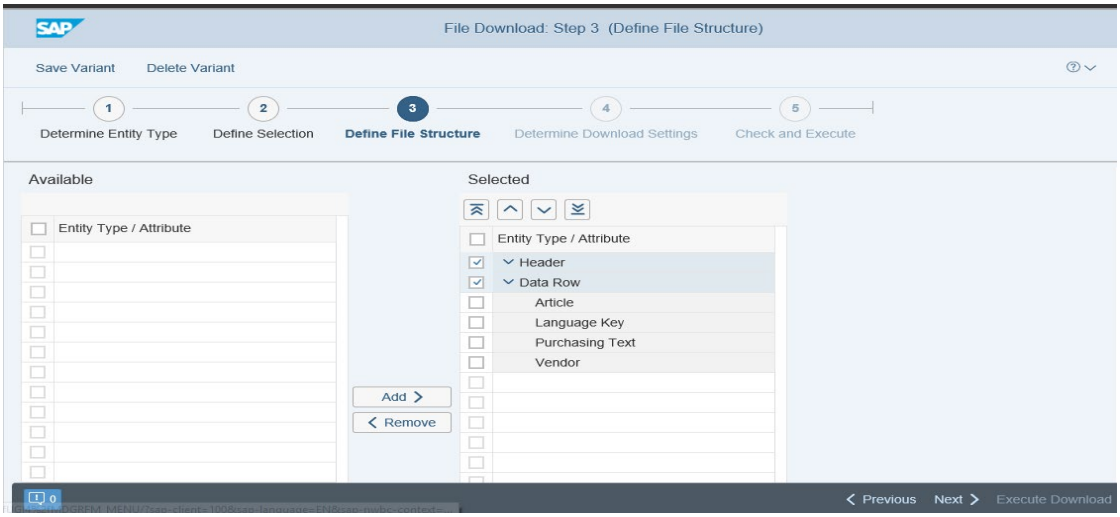
   a. "Entity Type" is selected as Purchase Info Record Note.



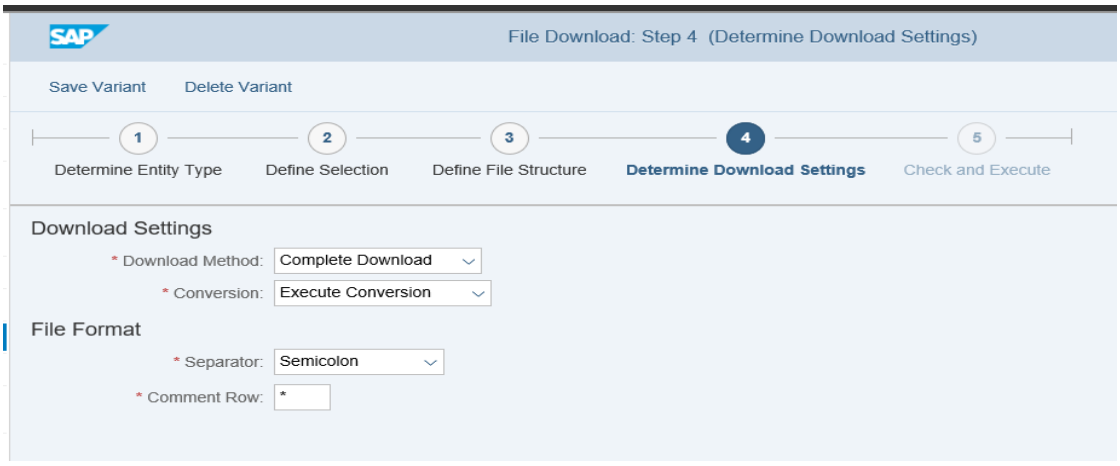
b. Enter the Article number in Selection criteria.



c. Define the File Structure as displayed in the following screen.

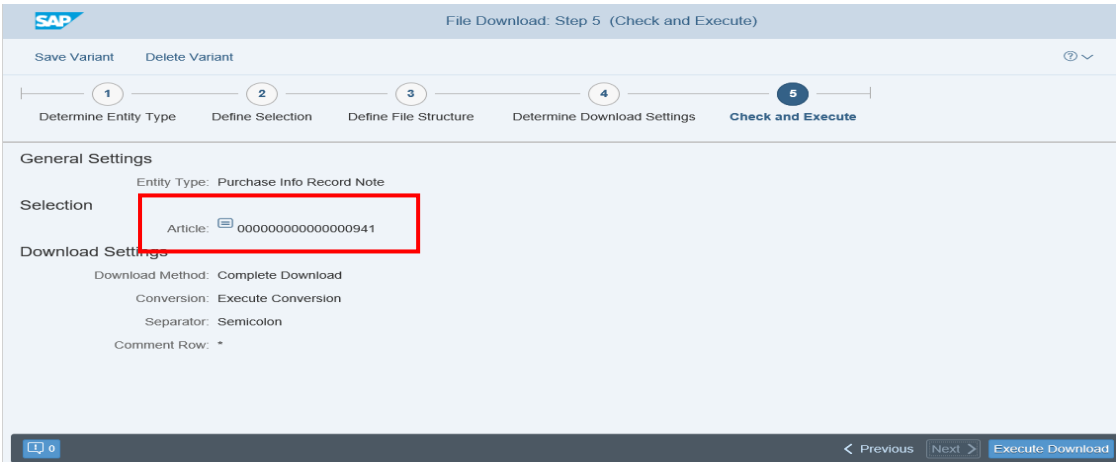


d. Select the Download Settings from the drop-down list as displayed in the following screen.

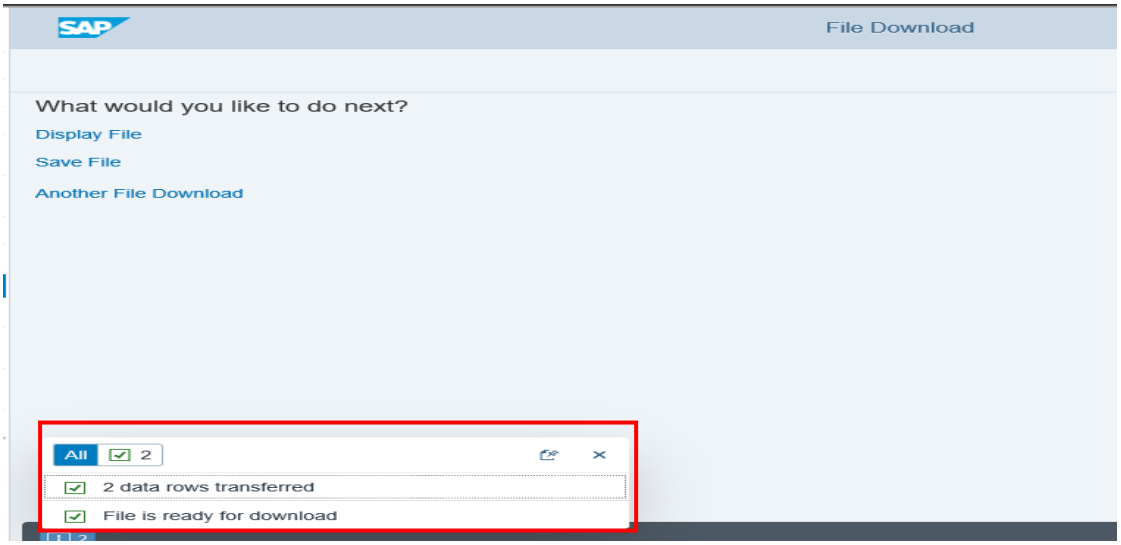


e. Click “Next”.

f. Click “Execute Download” button.

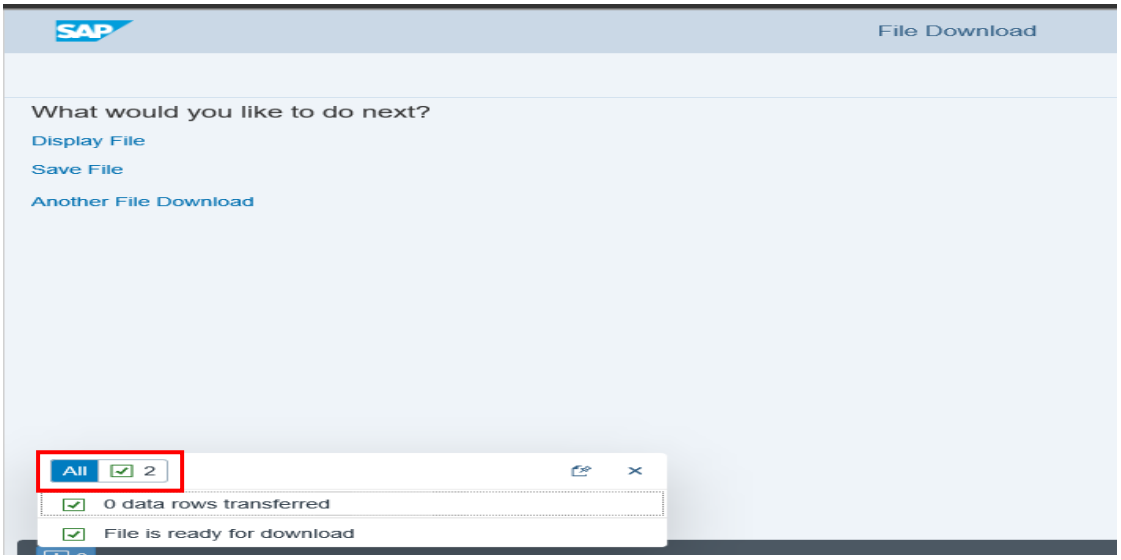


File Download performed for user with required authorization.
Both the data rows appear in the downloaded file with vendor field (key) populated.




```
* Download
* Data Model: AR
* Entity Type: PIR_NOTE
* Variant:
* User: [redacted]
* Date: 20171226 / Time: 062358
* Selection:
* MARA EQ | 941 |
*MARA;SPRAS;TXTPIRNOT;LIFNR
941;DE;test DE info note;100023;
941;EN;test English info record;100023;
```

File download result for user with limited authorization
Sensitive data does not appear in the downloaded file.




```
* Download
* Data Model: AR
* Entity Type: PIR_NOTE
* Variant:
* User: DPP_DEMOUSER
* Date: 20171226 / Time: 062728
* Selection:
* MARA EQ | 941 |
```