Oracle Insurance Data Foundation Application Pack

Data Protection Implementation Guide

Release 8.1.x

Mar 2021

ORACLE
Financial Services

ORACLE

Oracle Insurance Data Foundation Application Pack Data Protection Implementation Guide

Document Control

Version Number	Revision Date	Change Log
1.0	September 2020	Created the OIDF Data Protection Implementation Guide for the v8.1.x release.

Table of Contents

1 Preface

This section provides introductory information about the OFSAA Data Foundation Data Protection Implementation in the Oracle Insurance Data Foundation (OIDF) Application Pack.

Topics:

- Audience
- How this Guide is Organized
- Access to Oracle Support
- Related Documents

1.1 Audience

This document is intended to be used by Oracle Financial Services Analytical Applications Data Foundation System Administrator.

The Oracle Insurance Data Foundation (OIDF) Application Pack Data Protection Implementation Guide is intended for System Administrators, who are responsible for installing and maintaining the following:

- OIDF Application Pack components
- OFSAA Architecture
- UNIX Commands
- Database Concepts
- A web server or web application server

1.2 How this Guide is Organized

This document consists of the following sections about the data protection implementation in the OFSAA Data Foundation applications:

- Data Redaction
- Right to be Forgotten
- Data Portability
- Pseudonymization
- Notice and Consent
- Data Archival

1.3   Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support (MOS). For more information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1.4   Related Documents

Oracle strives to keep this and all other related documents updated regularly. Visit the OHC Documentation Library and My Oracle Support (MOS) web pages to download the latest document version available. The list of related documents is as follows:

- OHC Documentation Library for the OIDF Application Pack Release 8.1.x.x.x product documents:
  - Oracle Insurance Data Foundation Application Pack Installation and Configuration Guide
  - Oracle Insurance Data Foundation Application Pack User Guide
  - Oracle Insurance Data Foundation Application Pack Release Notes

- OHC Documentation Library for the OIDF Application Pack Release 8.1.x.x.x other documents:
  - Oracle Financial Services Analytical Applications (OFSAA) Data Model Extension Guidelines Document Release 8.1.x
  - Oracle Financial Services Analytical Applications (OFSAA) Data Model Naming Standards Guide Release 8.1.x
  - Oracle Financial Services Analytical Applications (OFSAA) Data Model Document Generation Release 8.1.x
  - Oracle Insurance Data Foundation Application Pack Security Guide Release 8.1.x
  - Oracle Insurance Data Foundation Application Pack Cloning Reference Guide Release 8.1.x
  - Oracle Insurance Data Foundation Application Pack Cloning Reference Guide Release 8.0.x
  - Oracle Insurance Data Foundation Application Pack Upgrade Guide

- My Oracle Support (MOS) for the OIDF Application Pack Release 8.1.x.x.x technical documents:
  - *Run Chart*
  - *Changelog*
  - *SCD Metadata*
  - *T2T Metadata*
  - *Data Model Difference Reports*

- My Oracle Support (MOS) for the OIDF Application Pack Release 8.1.x.x.x Download Specifications documents

- Oracle Financial Services Analytical Applications (OFSAA) Technology Matrix Release 8.1.x.x.x

- OHC Documentation Library contains the following OFS AAAI Application Pack Release 8.1.x.x.x product documents:
  - Oracle Financial Services Advanced Analytical Applications Infrastructure Installation Guide

- ▪ Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide

- ▪ Oracle Financial Services Advanced Analytical Applications Infrastructure Environment Check Utility Guide Release 8.1.x

- ▪ Oracle Financial Services Advanced Analytical Applications Infrastructure Administration and Configuration Guide Release 8.1.x

- ▪ Oracle Financial Services Analytical Applications Infrastructure Process Modelling Framework Orchestration Guide

- ▪ Oracle Financial Services Analytical Applications (OFSAA) Metadata Browser User Guide

- OHC Documentation Library contains the following OFSAA Release 8.1.x generic documents:

    - ▪ Oracle Financial Services Analytical Applications Infrastructure Security Guide Release 8.1.x

    - ▪ Oracle Financial Services Analytical Applications Infrastructure Cloning Reference Guide Release 8.1.x

- Oracle Financial Services Analytical Applications (OFSAA) Licensing Information User Manual Release 8.1.x.x.x

2 Data Redaction

This section provides information about the Data Redaction feature used in the OFSAA Data Foundation applications.

Topics:

- Overview of Data Redaction in OFSAA

- Accessing PII Table and PII Datasheet

- Data Redaction Batch

- Mapping Roles to User Groups for Data Redaction

- Enabling, Rerunning, and Disabling Data Redaction

- Data Redaction Batch Execution Sample

2.1 Overview of Data Redaction in OFSAA

Data Redaction is one of the features of Data Security that provides protection of data against unauthorized access and data theft.

In OFSAA, these tables are seeded as a part of Data Redaction:

- AAI_DRF_FUNCTION_MASTER

  This table stores the Redaction function definitions. Generic logical functions can be address, email, card number, phone number, and so on.

- AAI_DRF_FUNCTION_COLUMN_MAP

  This table stores the Function- Column mappings Redaction. The PII columns will be redacted according to the Function mapping.

Figure 1: AAI_DRF_FUNCTION_COLUMN_MAP for DIM_PARTY

V_FUNCTION_CD	V_TABLE_NAME	V_COLUMN_NAME	V_COLUMN_DATATYPE	V_COLUMN_DESC
53 ADDRESS	Dim_Party	v_ADDRESS_city	VARCHAR2(255)	Current / Residence ADDRESS...
54 ADDRESS	Dim_Party	v_ADDRESS_country	VARCHAR2(255)	Current / Residence ADDRESS...
55 ADDRESS	Dim_Party	v_ADDRESS_district	VARCHAR2(255)	Current / Residence ADDRESS...
56 ADDRESS	Dim_Party	v_ADDRESS_line_1	VARCHAR2(255)	Current / Residence ADDRESS...
57 ADDRESS	Dim_Party	v_ADDRESS_line_2	VARCHAR2(255)	Current / Residence ADDRESS...
58 ADDRESS	Dim_Party	v_ADDRESS_line_3	VARCHAR2(255)	Current / Residence ADDRESS...
59 ADDRESS	Dim_Party	v_ADDRESS_off_city	VARCHAR2(255)	Office ADDRESS City
60 ADDRESS	Dim_Party	v_ADDRESS_off_country	VARCHAR2(255)	Office ADDRESS Country
61 ADDRESS	Dim_Party	v_ADDRESS_off_district	VARCHAR2(255)	Office ADDRESS District
62 ADDRESS	Dim_Party	v_ADDRESS_off_line_1	VARCHAR2(255)	Office ADDRESS Line 1
63 ADDRESS	Dim_Party	v_ADDRESS_off_line_2	VARCHAR2(255)	Office ADDRESS Line 2
64 ADDRESS	Dim_Party	v_ADDRESS_off_line_3	VARCHAR2(255)	Office ADDRESS Line 3
65 ADDRESS	Dim_Party	v_ADDRESS_off_state	VARCHAR2(255)	Office ADDRESS State

- AAI_DRF_TABLE_ACCESS_CD_MAP

  This table stores the mapping of tables that contain the columns marked for redaction to the Access codes. These access codes are SMS function codes and are expected to be mapped to the role DATASECURITY. The policy expression will be created based on this role and evaluated to access non-redacted data.

> **NOTE**   The list of PII, on which Data Redaction is applied, is available at
> My Oracle Support (MOS).

2.2   Accessing PII Table and PII Datasheet

AAI_DRF_FUNCTION_COLUMN_MAP is the PII table.

> **NOTE**   The latest version of the PII Datasheet list can be downloaded
> from My Oracle Support (MOS).

2.3   Data Redaction Batch

Execute the Data Redaction seeded Batch `##INFODOM##_DATA_REDACTION` to execute the Data Redaction Utility if it is available as a part of the application common metadata. If the Batch is not available, you must create a new Batch as mentioned in the *Creating Batch for Executing Data Redaction Utility* section in the Oracle Financial Services Advanced Analytical Applications Infrastructure Administration and Configuration Guide Release 8.1.x.

The task in the batch `##INFODOM##_DATA_REDACTION` consists of the following three parameters:

- `dataredaction.sh`
- `true/false`
- OFSAA User ID

For more information, see the *Data Redaction Utility* section in the Oracle Financial Services Advanced Analytical Applications Infrastructure Administration and Configuration Guide Release 8.1.x.

2.4   Mapping Roles to User Groups for Data Redaction

This section provides information about mapping the User Roles to the User Groups for Data Redaction. The details are as follows:

- Data Controller Group is mapped to DATASECURITYADMIN role and the following are the mapping details:
    - Group Code: DATACONTROLLER
    - Group Name: Data Controller Group
    - Group Description: Data Controller Group
    - Role code: DATASECURITYADMIN
    - Role Name: Data Security Admin
    - Role Description: Data security admin role for executing redaction policies
- Map from individual applications to the DATASECURITY role. The following are the mapping details:

- Role code: DATASECURITY

- Role Name: Data Security Viewer

- Role Description: Data Security Viewer role for viewing original (non-redacted) data.

Follow these steps to map the individual applications to the DATASECURITY role:

i. DATASECURITY role must be mapped to those application User groups which hold the privilege to view the data in its original form (un-redacted). Therefore, applications must identify the functions which must be mapped to the DATASECURITY role. These mappings must be sourced as seeded data.

ii. Map the DATASECURITY role to the respective User groups. This mapping must be done manually from individual applications to the DATASECURITY role.

2.5 Enabling, Rerunning, and Disabling Data Redaction

This section provides information about executing the Data Redaction batch for enabling, disabling, and rerunning Data Redaction.

Topics:

- [Enabling Data Redaction](#)
- [Rerunning Data Redaction](#)
- [Disabling Data Redaction](#)

2.5.1 Enabling Data Redaction

To enable Data Redaction, follow these steps:

1. Modify the `OFS_OIDF_SCHEMA_IN.xml` file. For the `DATA_REDACT` parameter, set the value to `TRUE`. For more information, see the *Configure the OFS_OIDF_SCHEMA_IN.XML File* section in the required 8.1.x.x.x release version of the [Oracle Insurance Data Foundation Application Pack Installation and Configuration Guide](#).

   During the upgrade installation, in the `CONFIGURATION` table of the CONFIG schema, update the `IS_DATA_REDACTION_ENABLED` parameter to `Y`.

2. Map the OFSAA user to the Data Redaction role. The OFSAA user who executes the Data Redaction batch requires the following privileges:

   - Users must be mapped to the DATACONTROLLER group.

   - The user group must be mapped to the DATASECURITYADMIN role.

3. As a SYSADMIN, do the following tasks:

   a. Modify the Data Redaction batch as follows:

   `##INFODOM##_DATA_REDACTION` to `dataredaction.sh,false,`*<USER that is mapped to DATACONTROLLER and FSADMIN groups>*

   b. Give access to the OFSAA user mentioned in the previous step.

4. To redact data in the columns, execute the Data Redaction batch `##INFODOM##_DATA_REDACTION`.

5. Validate the AAI_DRF_FUNCTION_COLUMN_MAP table, and verify if all the redacted columns and policies are created in the table.

2.5.2   Rerunning Data Redaction

To rerun the Data Redaction batch, follow these steps:

1. In the `CONFIGURATION` table of the CONFIG schema, update the `IS_DATA_REDACTION_ENABLED` parameter to `N`.

2. Rerun the Data Redaction batch `##INFODOM##_DATA_REDACTION`.

3. Perform steps mentioned in the <u>Enabling Data Redaction</u> section.

2.5.3   Disabling Data Redaction

To disable Data Redaction, follow these steps:

1. In the `CONFIGURATION` table of the CONFIG schema, update the `IS_DATA_REDACTION_ENABLED` parameter to `N`.

2. Rerun the Data Redaction batch `##INFODOM##_DATA_REDACTION`.

2.6   Data Redaction Batch Execution Sample

This is a sample of data before executing the Data Redaction Batch.

Figure 2: Sample data before executing the Data Redaction batch

Row 1	Fields	
▶ N_ACCT_SKEY	6	
V_ACCOUNT_NUMBER	BC1007	⋯
V_ACCOUNT_DESC	data redaction desc	⋯
V_ACCOUNT_MANAGER_CODE	drmc1	⋯
V_ORIGINAL_ACCOUNT_NUMBER	data redaction original account numb	⋯

This is a sample of data after executing the Data Redaction batch:

Figure 3: Sample data after executing the Data Redaction batch

Row 1	Fields	
▶ N_ACCT_SKEY	6	
V_ACCOUNT_NUMBER	BC1007	⋯
V_ACCOUNT_DESC		⋯
V_ACCOUNT_MANAGER_CODE		⋯
V_ORIGINAL_ACCOUNT_NUMBER		⋯

3 Right to be Forgotten

This section provides information about the Right to be Forgotten feature used in the OFSAA Data Foundation applications.

Topics:

- Introduction to Right to be Forgotten
- Implementation of Right to be Forgotten by OFSAA

3.1 Introduction to Right to be Forgotten

Right to be Forgotten is the task of dropping PII (Personally Identifiable Information) of a Data Subject for the given Party. The financial institution can drop PII for those Data Subjects who have exercised the Right to be Forgotten functionality.

The Data Subjects may have made significant financial transactions, and (or) financial information may be required for regulatory or compliance reporting. Deleting the complete record that consists of PII may lead to issues in data reconciliation. In OFSAA, the PII data is replaced with randomized values, and therefore, the complete Data Subject record is retained. As a result, financial information is retained; however, the associated Party PII is removed permanently.

3.2 Implementation of Right to be Forgotten by OFSAA

To implement Right to be Forgotten, follow these steps:

1. Use the FSI_PARTY_RIGHT_TO_FORGET table to collect the input list of Party IDs for which PII must be removed from the system. The financial institution must source this Party ID list into the FSI_PARTY_RIGHT_TO_FORGET table, and then call the batch (`<<INFODOM>>_RightToForget`) or schedule it.

> **NOTE**   For the sample query, see the Sample Query For The FSI_PARTY_RIGHT_TO_FORGET Table section.

2. Use the AAI table AAI_DRF_FUNCTION_COLUMN_MAP to store the PII attribute list. During the Right to Forget batch execution, the AAI_DRF_FUNCTION_COLUMN_MAP table is referred to as randomize the PII values. See the *Data Redaction* section in Oracle Financial Services Advanced Analytical Applications Infrastructure Administration and Configuration Guide Release 8.1.x.

3. Use the AAI table AAI_DRF_QUERY_METADATA to store the query metadata, which is used during the `<<INFODOM>>_RightToForget` batch execution. This is the query metadata table that can lead to the following two types of queries:

   a. When the table consists of Party Identifier as an attribute, a simple record is required in the metadata query table.

   For example:

   ```
   Select v_party_id from Dim_Party where v_party_id='10'
   ```

b. When the table does not consist of Party Identifier as an attribute, an interrelated set of records is required in the metadata query table AAI_DRF_QUERY_METADATA. Compose these set of records in a systematic way such that, for the selected Party Identifier, the table join procedure can be performed and traversed to reach the required PII attribute.

To see more information about the table in the above image, see the Table Definition for AAI_DRF_QUERY_METADATA section.

For example:

DIM_CLAIM table does not consist of N_CLAIM_SKEY (N_CLAIM_SKEY is the required Primary Key for the PII Attribute N_DRIVER_SKEY). Therefore, perform the table join procedure similar to the following query:

```
Dim_driver.n_driver_skey from dim_driver dim_driver,
fct_driver_details fct_driver_details, Fct_Claim_Driver_Vehicle_Map
Fct_Claim_Driver_Vehicle_Map, Dim_Claim Dim_Claim where
dim_driver.n_driver_skey=fct_driver_details.n_driver_skey and
fct_driver_details.n_driver_skey=Fct_Claim_Driver_Vehicle_Map.n_driv
er_skey and
Fct_Claim_Driver_Vehicle_Map.n_claim_skey=Dim_Claim.n_claim_skey and
v_claim_id='GDPR'
```

In the preceding scenario, DIM_CLAIM.N_CLAIM_SKEY is a Number Datatype.

NOTE	• To arrive at the above-mentioned query, see the Steps to Perform the Table Join Procedure section. • For a pictorial representation of the above query, see the Pictorial Representation of Query Formed from the AAI_DRF_QUERY_METADATA Table section. • For more sample queries generated using the query metadata table, see Sample Queries Using the AAI_DRF_QUERY_METADATA Table section.

c. You must arrive at the SKey or equivalent column in the table, which consists of the required PII attributes. Then the <<INFODOM>>_RightToForget batch uses this key to filter records (For example DIM_DRIVER) and randomize all the PIIs listed in the AAI_DRF_FUNCTION_COLUMN_MAP for that table.

4. Now, PII attributes can be queried and the values are randomized.

4 Data Portability

This section provides information about the Data Portability feature used in the OFSAA Data Foundation applications.

Topics:

- Overview of Data Portability in OFSAA
- Data Portability Scenario

4.1 Overview of Data Portability in OFSAA

According to the Data Protection guidelines, a scenario may occur with a customer in which a Data Subject requests the financial institution to share the PII of that Data Subject stored in the application. To cater to such a scenario, the customer may use T2F (Table to File) functionality provided by AAI. This T2F functionality enables the customer to query the data warehouse and save the attributes to a file.

4.2 Data Portability Scenario

This is a sample scenario to apply Data Portability:

1. The DIM_PARTY table consists of a set of PIIs for multiple Data Subjects.

   Figure 4: Sample of the DIM_PARTY table

V_PARTY_NAME	V_PAN_CARD_ID	D_DATE_OF_BIRTH	D_DATE_OF_BIRTH_1	V_ADDRESS_TELE_PH_NO	V_ADDRESS_STATE
1 Aditya Sharma	HSWNJ8291T	09-JAN-93	09-JAN-93	8801283098	Himachal Pradesh
2 Maria Victor	PCLDS7413N	15-SEP-84	15-SEP-84	9024372784	Karnataka
3 Abdul Mohammed	AHJNS8384F	04-DEC-73	04-DEC-73	9852198762	Orissa
4 Vibha Rao	RQSAA7190L	13-MAY-78	13-MAY-78	8962735610	Maharashtra
5 Sharanya Gupta	EMHPL5167K	29-JAN-90	29-JAN-90	9901838919	Punjab

   A Data Subject requests the financial institution to share a copy of the PII data of that Data Subject stored by the financial institution. For illustration, the Data Subject with V_PAN_CARD_ID EMHPL5167K is used.

2. To make a file copy of the PII requested by the Data Subject, the User (financial institution) must perform T2F data mapping. Follow the Data Mapping procedure in the *Defining Data Mapping to File (T2F, H2F)* section in the required 8.1.x.x.x release version of the Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide to perform the following steps:

a. Create a T2F definition for the scenario mentioned in the preceding step. Map the column V_PAN_CARD_ID to V_PARTY_ID in the DIM_PARTY table.

Figure 5: Map the columns selected for the T2F definition creation in the Entity Selection page
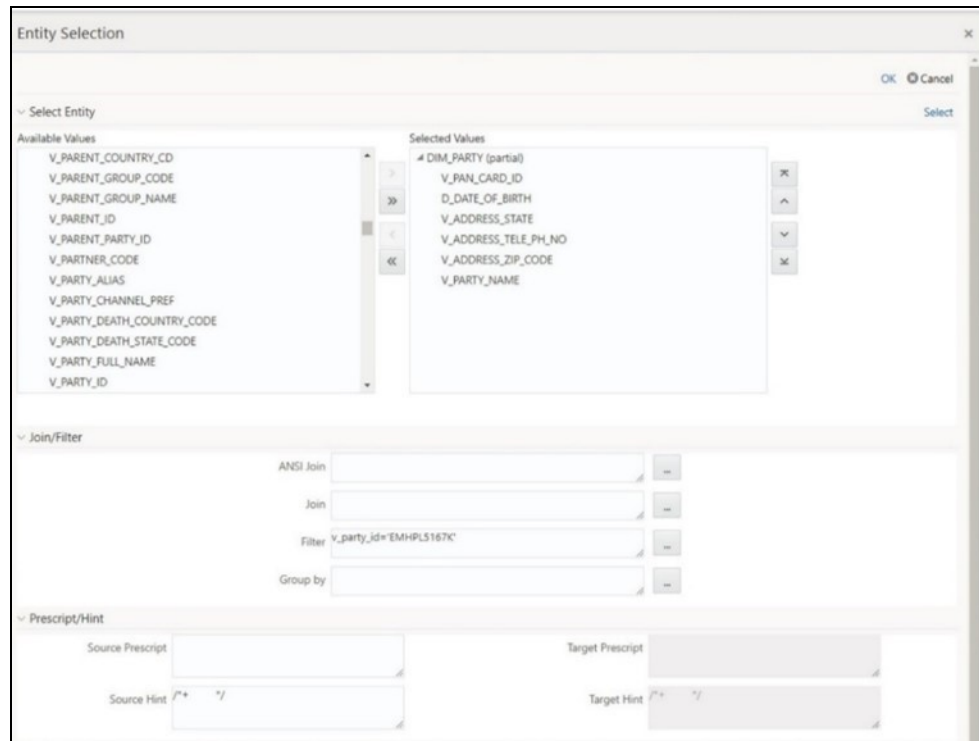
b. Create a Batch to run the T2F.

Figure 6: Create a batch to Run the T2F

c. Create a Task in the Batch.

Figure 7: Create a task in the T2F batch

d. Execute the Batch. Verify the progress of batch execution in the **Batch Monitor** page.

Figure 8: Execute the T2F batch

3. The output file path is as follows:

```
/scratch/ofsaaapp1/ftpshare/OIDFINFO/dmt/def/<T2F_name>/<Batch_name>/<b
atch_run_id>/<information_date>/<T2Fname>.dat
```

For example:

```
/scratch/ofsaaapp1/ftpshare/OIDFINFO/dmt/def/T2F_DIM_PARTY/OIDFINFO_T2F
_DIM_PARTY_20180504_1_Task1/20180504/T2F_DIM_PARTY.dat
```

> **NOTE** This extracted file consists of PII of a Data Subject that must be encrypted. See the *Data Mapping* section in the *Data Management Tools* section in the required 8.1.x.x.x release version of the Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide.
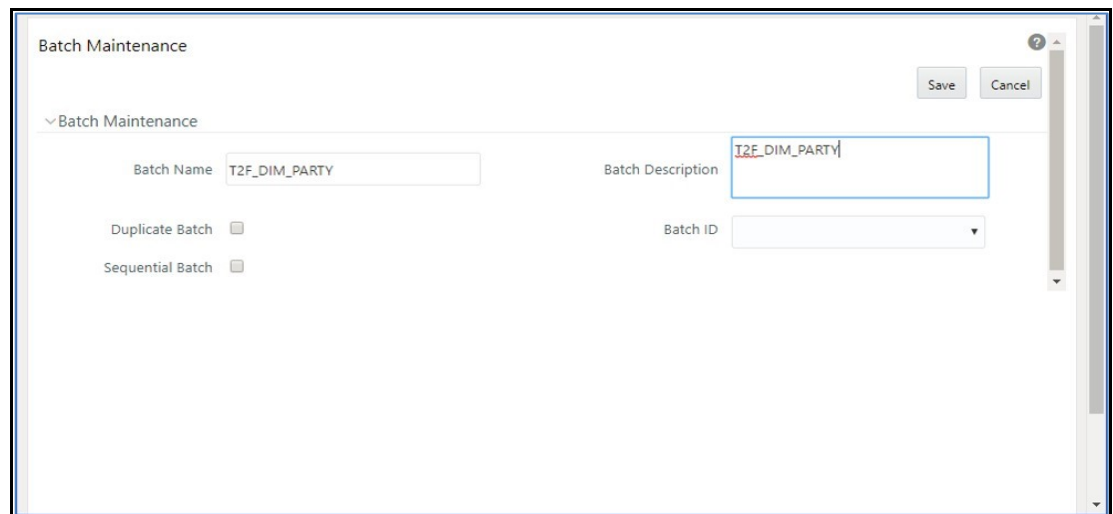
4. This is a sample T2F output file with the PII details requested by the Data Subject.

Figure 9: A sample of the T2F output file
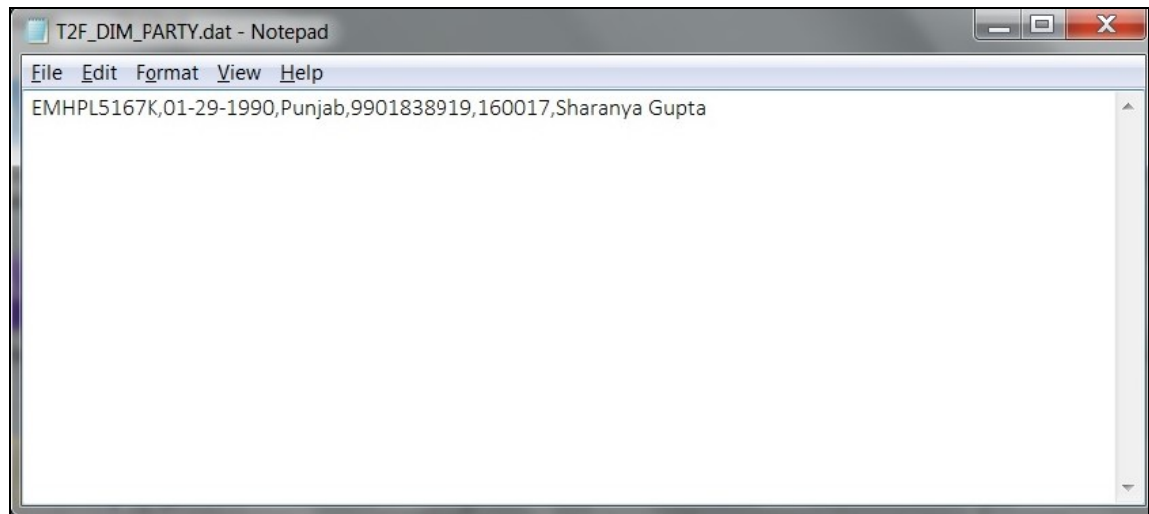
5   Pseudonymization

This section provides information about the Pseudonymization feature used in the OFSAA Data Foundation applications.

Topics:

- [Overview of Pseudonymization](#)
- [Implementation of Pseudonymization by OFSAA](#)

5.1   Overview of Pseudonymization

Pseudonymization is a process by which PII fields of a record are replaced by one or more artificial identifiers or pseudonyms. There can be a single pseudonym for a collection of replaced fields or one pseudonym for each replaced field. Therefore, Pseudonymization is a method to substitute PII data with a reversible and consistent value. This decreases the linking ability of a data set with the original identity of a data subject and acts as a Data Security mechanism.

The mapping of pseudonyms to those PIIs that are required for lookups, to retrieve the data subject information, must be stored away from the data warehouse in a secure location. This involves highly restricted access controls and security mechanisms that are defined in the customer environment to suit customer data security needs.

5.2   Implementation of Pseudonymization by OFSAA

OIDF data model enables its customers to implement the Pseudonymization process such that the PII data is separated from transaction data, and this PII data is referenced only by a pseudonym. For a wide range of analytical processes, access to PII data is not necessary.

1. Customers can employ Pseudonymization and load the Pseudonymized data into OIDF.

2. When analytical or modeling condition requires the availability of PII data, then care must be taken by the customer to load PII data into those columns that consist of additional data security controls such as Redaction. When the required attributes are not part of the seeded PII list, then the customer must:

   - Extend the PII list

   - Verify the completeness of the extensions

   - Verify that Redaction is enabled on the extended PII fields prior to loading sensitive data attributes

   To know more about Data Redaction, see [Oracle Financial Services Advanced Analytical Applications Infrastructure Administration and Configuration Guide Release 8.1.x](#).

NOTE	It is recommended that the PII values must not be added in the account dimension, party dimension, and customer dimension columns where redaction is not applied. For example, PII values must not be added in the V_ACCOUNT_NUMBER, V_PARTY_ID, and V_CUST_ID columns. Instead, they must be loaded in the V_ORIGINAL_ACCOUNT_NUMBER, V_ORIG_PARTY_ID and V_ORIG_CUST_REF_CODE columns respectively, where redaction is applied.

6 Notice and Consent

This section provides information about the Notice and Consent feature used in the OFSAA Data Foundation applications.

Topics:

- Introduction to Notice and Consent
- Populate Consent Purpose Dimension and Fact Party Consent Tables

6.1 Introduction to Notice and Consent

According to the Data Protection guidelines, a clear, legal-based, and accessible Notice must be provided to the Party regarding the Personally Identifiable Information (PII), which is collected from the Party during the onboarding process or during any stage of the workflow where PII of the Data Subject is captured.

After providing a Notice, clear Consent must be obtained from the Party regarding the usage and handling of PII by the financial institutions. This Consent must be given by the Party and must be presented to them as their choice with the option of withdrawal from providing Consent at any time. After the Party gives their Consent, their PII can be used in the workflow.

6.2 Populate Consent Purpose Dimension and Fact Party Consent Tables

OFSAA is a back-office product and does not have direct interaction with the end-user of the financial institution. Therefore, Notice, and Consent User Interfaces are not applicable. However, the Data Model of Data Foundation is enhanced to hold Notice and Consent information as a download from source systems. The financial institution may further use this feature for the task of processing or reporting.

6.2.1 Procedure to Populate Consent Purpose Dimension and Fact Party Consent

This section provides information about the Consent Purpose Dimension Population and Party Consent Population processes in the Oracle Insurance Data Foundation application.

Topics:

- Overview of the Consent Purpose Dimension and Fact Party Consent Tables
- Execute the Consent Purpose Dimension and Party Consent T2T
- Error Messages
- Check the Execution Status of the Party Consent Table
- Retrieve T2T Definition as an Excel File

6.2.1.1 Overview of Consent Purpose Dimension and Fact Party Consent Tables

This section provides information about the overview of the Consent Purpose Dimension and Fact Party Consent tables.

Topics:

- Overview of Consent Purpose Dimension Table
- Overview of Fact Party Consent Table

6.2.1.1.1 Overview of Consent Purpose Dimension Table

In the Consent Purpose Dimension table (DIM_CONSENT_PURPOSE), Consent content is stored. This table can be populated from Stage Consent Purpose Master Entity (STG_CONSENT_PURPOSE_MASTER) using the SCD-468 packaged in OIDF.

6.2.1.1.2 Overview of Fact Party Consent Table

Fact Party Consent is the table where the Consent of the Party is stored. Table to Table seeded definitions are provided for loading data into the target table Fact Party Consent (FCT_PARTY_CONSENT):

Table 1: Party Consent T2T mapping details

Source Table Name	Target Table Name	T2T Name
STG_PARTY_CONSENT	FCT_PARTY_CONSENT	T2T_FCT_PARTY_CONSENT

6.2.1.2 Execute Consent Purpose Dimension and Party Consent T2T

This section provides information about the execution of the Consent Purpose Dimension and Party Consent T2T.

- Execute the Consent Purpose Dimension through Batch
- Execute the Party Consent T2T Process in PMF

6.2.1.2.1 Execute the Consent Purpose Dimension through Batch

From Consent Party Master, execute the Consent Purpose Dimension SCD by executing tasks present in the SCD batch <INFODOM>_DATA_FOUNDATION_SCD.

Follow these steps to execute the batch:

1. Navigate to the **Batch Execution** page.
2. Select the seeded batch <INFODOM>_DATA_FOUNDATION_SCD for Consent Purpose Dimension.
3. Select the AS_OF_DATE for which source customer information is required to be loaded into the table.
4. Click **Execute Batch**.
5. Monitor the status of the batch in the **Batch Monitor** page of OFSAAI.

For information about the SCD batch execution, see the *Slowly Changing Dimension (SCD) Process* section in the required 8.1.x.x.x release version of the Oracle Insurance Data Foundation Application Pack User Guide.

6.2.1.2.2 Execute the Party Consent T2T Process in PMF

Execute the T2T_FCT_PARTY_CONSENT using the Process Modelling Framework (PMF). For information about how to execute the T2T process, see the *Table to Table (T2T) Loading Process* section in the required 8.1.x.x.x release version of the Oracle Insurance Data Foundation Application Pack User Guide.

6.2.1.3 Error Messages

You can check the log file in the following directories to check the error messages, if any:

- `ftpshare/logs/<Run_Date>/<infodom>/RUN EXECUTABLE` directory for `DIM_CONSENT_PURPOSE`.

- `ftpshare/logs/<Run_Date>/<infodom>/LOAD DATA` directory for `T2T_FCT_PARTY_CONSENT`.

The most common error message is as follows:

Unique Constraint Violation

This occurs when attempting to re-load or when loading existing records for the already executed AS_OF_DATE.

6.2.1.4 Check the Execution Status of the Party Consent Table

For SCD, monitor the execution status in the **Batch Monitor** page.

> **NOTE**   For more comprehensive coverage of the configuration and execution of a batch, see the required 8.1.x.x.x release version of the Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide.

For T2T, check the status of the Run execution in the **Process Monitor** page of the Process Modelling Framework (PMF).

6.2.1.5 Retrieve T2T Definition as an Excel File

T2T definition can be retrieved as an excel document for reference from the metadata browser of the Unified Metadata Manager (UMM) component of OFSAAI.

7   Data Archival

This section provides information about the Data Archival feature used in the OFSAA Data Foundation applications.

Topics:

7.1   Synopsis for Data Archival

The OFSAA data model, along with the active data stores Personally Identifiable Information (PII) of Data Subjects who are no longer actively using the financial services, which is a liability.

7.2   Implementation of Data Archival by OFSAA

To implement this invisibility of data at the row level, Oracle Database 12c has introduced a new feature called Row Archival.

- The Row Archival feature is simple and effective to use as opposed to the traditional approach, which requires storage and maintenance of historical tables.

- This feature enables to archive records based on given criteria within the account table. The criteria can be, for example, the Account Close Date of the Data Subject.

- This archived data can be viewed or made hidden by setting a session parameter.

7.2.1   A Criteria for Data Archival

To archive Party records, which are closed for more than seven years, follow these steps:

1. To enable Row Archival on the DIM_PARTY table, run the following command:

   ```
   ALTER TABLE DIM_PARTY ROW ARCHIVAL
   ```

2. Run the Row Archival Update statement periodically, to search for the account Party records which are closed for more than seven years. Run the following command:

   ```
   UPDATE DIM_PARTY SET ora_archive_state='1' where
   trunc(months_between(SYSDATE, d_closed_date)/12)>7
   ```

   In the above query, the details are as follows:

   - `ora_archive_state` is a hidden column that is created after the ROW ARCHIVAL is set on the table.

   - `SET ora_archive_state='1'` is part of the query archives the records which meet the criteria of seven years of account closure.

   - Hidden rows are available for the `Select/Update` queries only after the `ora_archive_state` column is disabled.

7.2.1.1 Viewing Archived Rows

To make hidden rows visible for a session, run the following command:

```
ALTER SESSION SET ROW ARCHIVAL VISIBILITY=ALL;
```

To make the rows invisible, run the following command:

```
ALTER SESSION SET ROW ARCHIVAL VISIBILITY=ACTIVE;
```

8   Additional Information for Right to be Forgotten

This section provides additional information for the Right to be Forgotten functionality.

Topics:

- [Table Definition for AAI_DRF_QUERY_METADATA](#)
- [Pictorial Representation Of The Query Formed From The AAI_DRF_QUERY_METADATA Table](#)
- [Steps to Perform the Table Join Procedure](#)
- [Sample Queries Using the AAI_DRF_QUERY_METADATA Table](#)
- [Sample Query for The FSI_PARTY_RIGHT_TO_FORGET Table](#)

8.1   Table Definition for AAI_DRF_QUERY_METADATA

This is the Table Definition for the AAI_DRF_QUERY_METADATA.

Table 2: Table Definition for the AAI_DRF_QUERY_METADATA

Colum Name	Column Type	Description
ID	Number	This is the Primary Key field. You must enter a numerical value.
V_TABLE_NAME	Varchar	This is the source table name.
V_COLUMN_NAME	Varchar	This is the source column name.
V_CHILD_TABLE_NAME	Varchar	This is the table name, which must be linked to the V_TABLE_NAME. If the same table name is repeated with the same column name V_COLUMN_NAME, then the AND condition is formed with V_CHILD_TABLE_NAME. V_CHILD_TABLE_NAME
V_CHILD_COLUMN_NAME	Varchar	This the column name, which must be linked to the V_COLUMN_NAME.
F_QUERY_FLAG	Varchar	Enter Y or N, which is case sensitive. If the value is Y, then you must form a query from V_TABLE_NAME .V_COLUMN_NAME
V_COLUMN_DATA_TYPE	Varchar	Mention the Data Type of the V_COLUMN_NAME. This is required only if F_QUERY_FLAG = Y.
V_TARGET_COLUMN_NAME	Varchar	Mention the PARTY_ID column name, which is required only if F_QUERY_FLAG = Y.
V_QUERY_NAME	Varchar	Mention the same query for a set of joining tables and columns. The set of tables and columns under the join query are grouped together using the same query name.

8.2 Pictorial Representation of the Query Formed from the AAI_DRF_QUERY_METADATA Table

This is the pictorial representation of the query formed from the AAI_DRF_QUERY_METADATA table.

Figure 10: Pictorial representation of query formed from the AAI_DRF_QUERY_METADATA table
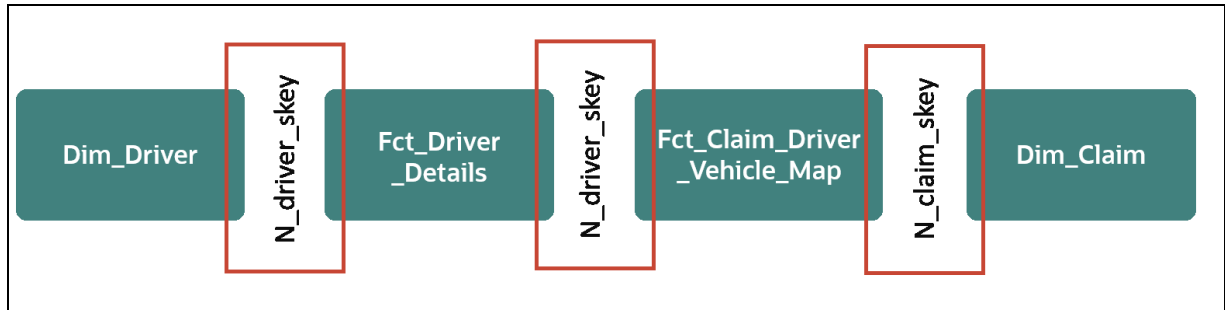
8.3 Steps to Perform the Table Join Procedure

For illustration, the required table Dim_Cards_Master does not consist of Party Identifier. Therefore, perform the table join procedure using the AND condition at the table level.

To perform the table join procedure, follow these steps:

1. Search for a table, which consists of the Party Identifier field. In this query, we have searched for the table DIM_CLAIM with a unique identifier N_CLAIM_SKEY field. This table must be joined with the required table DIM_DRIVER.

2. However, the tables DIM_CLAIM and DIM_DRIVER do not consist of any common column name to perform the table join operation. Therefore, search for one more table FCT_DRIVER_DETAILS. This table (FCT_DRIVER_DETAILS) consists of a common column name (N_DRIVER_SKEY) between the DIM_DRIVER table and itself.

3. Join the FCT_DRIVER_DETAILS table, which consists of a common column name (N_DRIVER_SKEY) with another table FCT_CLAIM_DRIVER_VEHICLE_MAP.

4. Join the FCT_CLAIM_DRIVER_VEHICLE_MAP table, which consists of a common column name (N_CLAIM_SKEY) with the final table DIM_CLAIM.

5. Now, the DIM_DRIVER table is joined with the DIM_CLAIM table.

8.4 Sample Queries Using the AAI_DRF_QUERY_METADATA Table

The sample queries generated using the AAI_DRF_QUERY_METADATA table are as follows:

Example 1:

```
select DIM_MANAGEMENT.n_manager_skey from DIM_MANAGEMENT DIM_MANAGEMENT,
FCT_CUSTOMER FCT_CUSTOMER, DIM_CUSTOMER DIM_CUSTOMER where
DIM_MANAGEMENT.n_manager_skey=FCT_CUSTOMER.n_manager_skey and
FCT_CUSTOMER.n_cust_skey=DIM_CUSTOMER.n_cust_skey and
DIM_CUSTOMER.v_d_cust_ref_code in(?,?)
```

Example 2:

```
select DIM_EMAIL.n_email_skey from DIM_EMAIL DIM_EMAIL, FCT_PARTY_EMAIL_MAP
FCT_PARTY_EMAIL_MAP, DIM_PARTY DIM_PARTY where
DIM_EMAIL.n_email_skey=FCT_PARTY_EMAIL_MAP.n_email_skey and
FCT_PARTY_EMAIL_MAP.n_party_skey=DIM_PARTY.n_party_skey and
DIM_PARTY.v_party_id in(?,?)
```

Example 3:

```
select STG_CLAIM_DETAILS.v_claim_id from STG_CLAIM_DETAILS
STG_CLAIM_DETAILS, STG_CLAIM_CLAIMANT STG_CLAIM_CLAIMANT where
STG_CLAIM_DETAILS.v_claim_id=STG_CLAIM_CLAIMANT.v_claim_id and
STG_CLAIM_CLAIMANT.v_cust_ref_code in(?,?)
```

8.5 Sample Query for the FSI_PARTY_RIGHT_TO_FORGET Table

This is the sample entry for the FSI_PARTY_RIGHT_TO_FORGET table:

```
Insert into FSI_PARTY_RIGHT_TO_FORGET values (SYSDATE,
<<PARTY_ID_FROM_Ur_ENV>>, 'Testing Right2Forget');
```

OFSAA Support

Raise a Service Request (SR) in [My Oracle Support (MOS)](#) for queries related to OFSAA applications.

Send Us Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?

- Is the information clearly presented?

- Do you need more information? If so, where?

- Are the examples correct? Do you need more examples?

- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site that has all the revised/recently released documents.