Genesys Security Deployment Guide

Genesys Info Mart Support for GDPR

5/5/2025

Genesys Info Mart Support for GDPR

Overview of Genesys Info Mart support for GDPR compliance

Starting with the initial 8.5.010 release, Genesys Info Mart processes input JSON files that customers provide to comply with Right of Access ("export") or Right of Erasure ("forget") requests from their customers (*consumers*). Starting with release 8.5.010.16, Genesys Info Mart also processes GDPR requests that customers provide from their employees, who are contact center agents and supervisors.

Genesys Info Mart uses the JSON files customers place in configured, tenant-specific locations (see Input file location). The JSON files identify the consumers or employees who have made GDPR requests to either "export" or "forget" their personally identifiable information (PII). The Info Mart database potentially stores requesting consumers' and employees' PII.

The daily Info Mart database maintenance job, Job_MaintainGIM, processes any "export" or "forget" JSON files that have been added or modified since the last processed JSON file. To execute the requests, the maintenance job uses a SQL script, **gdpr.sql** or **gdpr_partitioned.sql**, located in the **sql_scripts** folder in the installation directory.

- For "export" requests, the applicable PII is reported in a database table, CTL_GDPR_HISTORY.
- For "forget" requests, the data is redacted in Info Mart tables (primarily fact tables), and the PII that was searched for (in other words, the data prior to redaction) is reported in the CTL_GDPR_HISTORY table.

The PII is stored in the CTL_GDPR_HISTORY table for a configurable amount of time (maximum 30 days). You can query the CTL_GDPR_HISTORY table to obtain:

- PII data to satisfy an "export" request (see Example: SQL for export)
- A detailed audit trail of all the fields that were interrogated to satisfy the GDPR requests (see Example: SQL for audit)

To query the CTL_GDPR_HISTORY table, you must have read-only privileges for the Info Mart schema.

> ### Important
> No special configuration is required on the Genesys Info Mart side to enable support for GDPR. Equally, no special actions are required as long as the maintenance job runs regularly. Genesys recommends that you do not disable the run-maintain option, which enables the maintenance job to run on an automatic schedule.

Data retention policies

A number of configuration options control how long data is retained in the Info Mart database. The following table summarizes the applicability of GDPR to different types of Info Mart data. For more information about the categories of data in the Info Mart database, see the "Genesys Info Mart Database Schema" page in the *Genesys Info Mart Physical Data Model* for your RDBMS.

Important

Genesys Info Mart support for GDPR compliance is based on default configuration settings and typical application usage. For example, given the recommended values of the **days-to-keep-*** options, fact data in GIDB tables and logs is short-lived (ephemeral) data that is automatically deleted within a short period of time, and Genesys Info Mart does not redact this data outside of the automated deletion.

Particularly in multimedia deployments with long-living interactions, Genesys recommends that you reduce the values of certain options that affect purge behavior. See Recommendations for purge-related options for multimedia for more information.

Configuration option	Controls what type of data?	Contains PII?	Included in GDPR processing?
Never deleted—not configurable	Configuration object data	Yes, for employees	Yes (starting with release 8.5.010.16)
gim-etl section			
days-to-keep-gim-facts	Fact data in the dimensional model	Yes	Yes. **Note:** Dimension tables in the dimensional model are never purged. Dimensions store low-cardinality data that does not contain PII.
days-to-keep-active-facts	Active multimedia interaction data in the dimensional model, GIDB, and Staging tables	Yes	Active interaction data in dimensional model fact tables is processed. Active interaction data in GIDB and Staging tables is short-lived and is not processed.
days-to-keep-gidb-facts	Fact data in GIDB	Yes	No. See Important note, above.
days-to-keep-gdpr-history (introduced to support GDPR)	The CTL_GDPR_HISTORY table	Yes	Not considered for GDPR reprocessing, because the data is short-lived (maximum 30 days).
days-to-keep-cfg-facts	Deleted configuration fact data	No consumer- or employee-related PII	No

Configuration option	Controls what type of data?	Contains PII?	Included in GDPR processing?
days-to-keep-discards-and-job-history	Discard tables, and audit and history tables	No	No
gim-export section			
days-to-keep-output-files	Files generated by Job_ExportGIM to provide Info Mart data to customers who use Genesys Info Mart's Data Export feature	Yes	No. See Important note, above. **Note:** Customers are responsible for implementing adequate processes to ensure that any PII in their imported data is handled in accordance with GDPR requirements, including using suitable retention periods or redacting data to comply with "forget" requests.
log4j section			
max-backup-index	Log files	Yes	No. See Important note, above.

Recommendations for purge-related options for multimedia

Particularly in multimedia deployments with long-living interactions, ensure that the **days-to-keep-*** options that control retention policies for short-lived data that is not included in GDPR processing provide a sufficient buffer for unexpected delays—for example, if a database purge was not executed because the maintenance job was interrupted. In deployments where the Info Mart database is partitioned, you must also factor in partition sizes, since a partition is not purged until all the data it contains is eligible to be purged.

Genesys recommends that you base option settings on the following calculations:

- **days-to-keep-active-facts** = 30 – <buffer> – "partitioning-interval-size-gidb-mm"/24/3600
- **days-to-keep-gidb-facts** = 30 – <buffer> – max("partitioning-interval-size-gidb", “partitioning-interval-size-gidb-mm”, “partitioning-interval-size-gidb-ocs”)/24/3600

Example

If the partition size for multimedia interactions in GIDB has been increased to the nondefault value of one week (`partitioning-interval-size-gidb-mm=604800`), the partition size for Outbound Contact–related data in GIDB has been increased to the nondefault value of ten days (`partitioning-interval-size-gidb-ocs=864000`), and you want to allow a buffer of three days for unexpected delays, set:

- `days-to-keep-active-facts = 30 – 3 – 604800/24/3600 = 20`
- `days-to-keep-gidb-facts = 30 – 3 – 864000/24/3600 = 17`

Input file location

You specify the location for each tenant's JSON files in the **[gdpr].gdpr-directory** option on the Annex tab of the Tenant configuration object. Genesys has no special requirements for the location of the directory. The **gdpr-directory** option must simply specify a valid path that both Genesys and you can get to.

All Genesys products use the same tenant-specific directory for the input and, if the product provides them (Genesys Info Mart does not), output files for that tenant. You are responsible for maintaining this directory.

JSON input files

There are separate input files for Right of Erasure and Right of Access requests:

- forget-<DDMMYYYY>-<any optional content>.json
- export-<DDMMYYYY>-<any optional content>.json

The date part of the file name (<DDMMYYYY>) indicates the date the file was created, to maintain file uniqueness. Using timestamps in the file system, Genesys Info Mart processes any files added or modified for that tenant since the last time Genesys Info Mart processed GDPR requests.

It is your responsibility to ensure that the request does not conflict with other regulatory or legal obligations.

File specification

The JSON specification for the forget and export files for GDPR requests is identical.

- "caseid" — (Optional) Holds customer case numbers, for possible use by Customer Care to supplement customer self-service.
- "consumers" — (Required for consumer requests) Holds an array of individual "consumer" elements, so that GDPR requests from multiple consumers can be processed at the same time.
  - "consumer" — (Required) An individual consumer for whom a GDPR request is being submitted. Each consumer may be identified by one or more of the following attributes, specified in an array:
    - "phone" — Phone number, without separators
    - "email" — Email address
    - "fbid" — Facebook ID
    - "twid" — Twitter handle
    - "wcid" — WeChat ID
    - "name" — Given name
    - "ipaddr" — IP address

- "employees" — (Required for employee requests) Holds an array of individual "employee" elements, so that GDPR requests from multiple employees can be processed at the same time.
  - "employee" — (Required) An individual employee for whom a GDPR request is being submitted. Each employee may be identified by one or more of the following attributes, specified in an array:
    - "username" — (Required) Username of the person object in Configuration Server and/or Outbound Engagement configuration
    - "employeeid" — Employee ID of the person object in Configuration Server
    - "name" — Given name
- "gim-attached-data" — (Optional) Used by Genesys Info Mart to target custom user data attached to interactions and custom Outbound Contact Server (OCS) fields used in Outbound Contact campaigns. Custom user data and custom fields contain data for which customers configured customized storage in the Info Mart database.
  - "kvlist" — Holds an array of the custom user data KVPs and custom OCS fields that might contain PII.

Example

```
{
   "caseid":"123456789",
   "consumers":[
      {"consumer":
         [
            {"name":"John Doe"},
            {"name": "John Q. Doe"},
            {"phone":"555551212"}
         ]
      },
      {"consumer":
         [
            {"name":"Dan Akroyd"},
            {"phone":"555556161"},
            {"phone":"555556162"},
            {"email":"danny@hollywood.com"},
            {"email":"funnyguy@comedy.org"},
            {"fbid":"Dan Akroyd"}
         ]
      }],
    "gim-attached-data":
         {"kvlist": ["AcctNum", "SSN"]
         },
   "employees":[
      {"employee":
         [
            {"username":"SueSmith"},
            {"name": "Sue Smith"},
            {"employeeid":"RR11243"}
         ]
      }]
 }
```

Right of Access ("export") requests

Genesys Info Mart uses the GDPR input files named **export-<DDMMYYYY>-<any optional**

content>.json as the input for "export" processing. See Input files for details about the JSON file requirements. The PII that Genesys Info Mart will report is specified in the input JSON files in:

- The phone and email attributes that identify the requesting consumer
- The username attribute that identifies the requesting employee
- Custom user data KVPs and custom Outbound Contact Server (OCS) fields customers might specify in the "gim-attached-data" element

While custom KVPs and fields are included in the GDPR output, Genesys Info Mart searches only on the phone or email address in order to find fact table records associated with the requesting consumers. Similarly for employee requests, while employee ID, name, and other attributes in the configuration record (for example, email address) are included in the GDPR output, Genesys Info Mart searches only on the username in order to find configuration object and fact table records associated with the requesting employees. For details about the specific tables and fields that are searched, see the description of the CTL_GDPR_HISTORY table in the *Genesys Info Mart Physical Data Model* for your RDBMS.

In the initial implementation, Genesys Info Mart does not provide an output JSON file. Instead, the PII data is reported in the CTL_GDPR_HISTORY table.

Example: SQL query for "export"

The following is an example of SQL you can use to retrieve PII for export. The example returns distinct occurrences of consumer PII data for phone number 5551212. The same query specifying `CONSUMER_ID = 'jsmith'` will return distinct occurrences of employee PII data for the agent with username *jsmith*.

```
SELECT TENANT_KEY,
       FORGET,
       CONSUMER_ID,
       TABLE_NAME,
       COLUMN_NAME,
       KEY_VALUE
FROM CTL_GDPR_HISTORY
WHERE TENANT_KEY = <tenant>
AND FORGET = 0
AND CONSUMER_ID = '5551212'
AND KEY_VALUE IS NOT NULL
AND CREATED_TS BETWEEN <TS_1> AND <TS_2>
GROUP BY TENANT_KEY, FORGET, CONSUMER_ID, TABLE_NAME, COLUMN_NAME, KEY_VALUE
ORDER BY TENANT_KEY, FORGET, CONSUMER_ID, TABLE_NAME, COLUMN_NAME, KEY_VALUE
```

Right of Erasure ("forget") requests

Genesys Info Mart uses the GDPR input files named **forget-<DDMMYYYY>-<any optional content>.json** as the input for "forget" processing. See Input files for details about the JSON file requirements. Genesys Info Mart processing of "forget" requests parallels "export" requests, except that any PII that is found is redacted in the applicable Info Mart database tables, with the PII that was searched for (in other words, the data prior to redaction) recorded in the CTL_GDPR_HISTORY table.

As is the case for "export" requests, the PII that Genesys Info Mart will redact is specified in the input

JSON files in:

- The phone and email attributes that identify the requesting consumer
- The username attribute that identifies the requesting employee
- Custom user data KVPs and custom Outbound Contact Server (OCS) fields customers might specify in the "gim-attached-data" element

While custom KVPs and fields are redacted, Genesys Info Mart searches only on the phone or email address in order to find fact table records associated with the requesting consumers. Similarly for employee requests, while employee ID, name, and other attributes in the configuration record (for example, email address) are redacted, Genesys Info Mart searches only on the username in order to find configuration object and fact table records associated with the requesting employees. For details about the specific tables and fields that are searched, see the description of the CTL_GDPR_HISTORY table in the *Genesys Info Mart Physical Data Model* for your RDBMS.

Warning

Usage of Genesys products requires processing of employees' Personal Data (user's name, work phone number, and work email) for proper functioning of the Genesys solution. Without storing this Personal Data associated with an employee, Genesys Info Mart could stop performing its function. Thus, for current employees, the processing of their Personal Data is necessary for the purposes of the legitimate interests pursued by the customer. Further, the customer may be required to keep employee interaction records in order to meet other regulatory requirements. Based on the lawfulness of this processing and the design of Genesys products, Genesys does not recommend erasing Personal Data associated with an ongoing user.

Audit and tracking

The Genesys Info Mart log tracks the progress of GDPR processing.

Sample Genesys Info Mart log (click to enlarge)

In addition, there are two log events that report the status of GDPR request processing, by tenant: STANDARD-level log messages 55-20172 (GIM_ETL_GDPR_ERROR) and 55-20173 (GIM_ETL_GDPR_SUCCESS). (In Genesys Info Mart releases earlier than 8.5.011.18, GIM_ETL_GDPR_SUCCESS was a TRACE-level message, 55-31406.) Genesys recommends setting an alarm on message 55-20172, to alert you to problems that are preventing completion of GDPR processing. You can use log message 55-20173 (or 55-31406 in pre-8.5.011.18 releases) to cancel the alarm.

The CTL_GDPR_HISTORY table as audit report

Genesys Info Mart does not provide an execution report in the form of an output file. Instead, the CTL_GDPR_HISTORY table provides details about the PII data associated with “export” or “forget” requests. The table also provides a detailed audit trail of all the fields that were interrogated to satisfy a particular GDPR request. NULL values indicate that the field was evaluated for a particular instance of PII and was found to be empty.

Consider the following example:

- An input JSON file for a specific tenant indicates that the consumer with phone number 5551212 wishes to see PII data related to that phone number. The input JSON file also specifies custom user data keys, which, based on business practices in the customer's environment, might be associated with PII data.
- To satisfy this request, Genesys Info Mart interrogates interactions to or from 5551212, as well as related facts, such as user data related to those interactions. CTL_GDPR_HISTORY would have a row for each table/column searched.
- Say there were no interactions to or from 5551212. In this case, the row for each table searched for this phone number would have a NULL FACT_ID and a NULL KEY_VALUE.
- Say there were interactions to or from 5551212. However, in an associated record, a field populated by one of the keys specified in the JSON file is empty. In this case, the row for that table and column would have a NULL KEY_VALUE.

Example: SQL query for audit

The following is an example of SQL you can use to see the PII data for phone number 5551212, along with a full audit trail of the search for this PII, showing both the presence and the absence of this instance of PII data in tables and columns included in the search.

```
SELECT * FROM CTL_GDPR_HISTORY
WHERE TENANT_KEY = <tenant>
AND CONSUMER_ID = '5551212'
AND CREATED_TS BETWEEN <TS_1> AND <TS_2>
ORDER BY TABLE_NAME, COLUMN_NAME, FACT_ID
```