

IGDC & ONETRUST INTEGRATION GUIDE

IBM GUARDIUM DISCOVER AND CLASSIFY

VERSION 4.2.2

TABLE OF CONTENTS

Table of Contents	2
OneTrust Overview	3
Application Flow	3
Prerequisites	4
OneTrust App Installation, Upgrade & Removal	5
Installation	5
Removal	5
OneTrust App Usage	6
Configuration of the project	6
Examples of incident creation	6
DSAR request creation & population	6

ONETRUST OVERVIEW

OneTrust is a solution used to help organizations implement compliance and risk management initiatives in a single platform, across many key stakeholders, to transform compliance and risk reduction into trust, business value, and competitive differentiation. Through a central data model, agile workflows, and value-based reporting, OneTrust helps manage privacy, security, risk, ethics and compliance, legal, data and analytics, marketing, finance, and sustainability.

This integration's purpose is to utilize OneTrust's DSAR requests and communicate with IGDC in order to provide relevant discovered data subject info to the OneTrust system.

Table 1: Use cases for IGDC integration with OneTrust

USE CASE	DESCRIPTION
DSAR request creation & population	Create a DSAR request in OneTrust and use IGDC to populate it with enriched data.

APPLICATION FLOW

1. The user creates a DSAR request in OneTrust.
2. After the request is reviewed and approved, it changes its status to **In Progress**.
3. A subtask in OneTrust's IGDC integration workflow then sends a POST request containing the subtask ID to the integration component at **/process/subtask**.
4. Integration retrieves the subtask ID from the POST request and identifies the DSAR request reference ID in the subtask details.
5. Using the DSAR reference ID, the integration obtains all the necessary info from the DSAR request itself and retrieves the DSAR request enrichment data from IGDC.
6. The Integration then populates the DSAR request with the enriched data and closes the request.

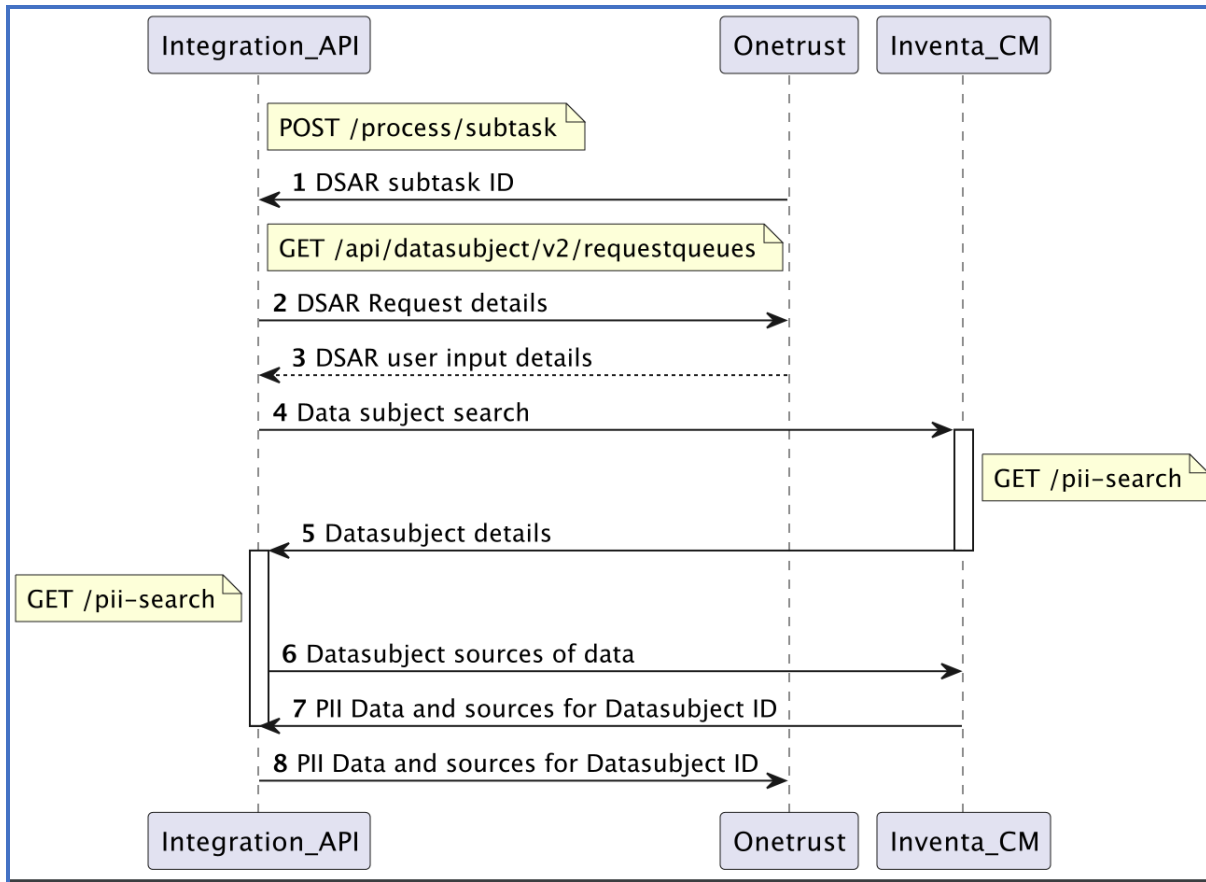


Figure 2: Integration flow

PREREQUISITES

1. IGDC version 3.7.0+ secured with a trusted CA certificate.
2. 8001 port open for outbound connections.
3. ClientID/ClientSecret API credentials available.
4. DSAR_READ, DSAR_WRITE, ATTACHMENTS, INTEGRATIONS scopes are attached to the API credentials.

ONETRUST APP INSTALLATION, UPGRADE & REMOVAL

INSTALLATION

Integration package is provided on demand. It can be installed on your VM, local machine, or cluster node. To deploy the project, perform the following steps:

1. Configure all variables above in docker-compose.yml file and run below commands to start the app.

```
docker-compose build --no-cache
docker-compose up
```

Once launched the application will monitor the incoming tasks in incidents in the background.

REMOVAL

1. To delete the application, stop the containers from the directory with deployment files:

```
docker-compose down
```

2. Remove the docker volumes created for the project. Volumes can be listed using command:

```
docker volume ls
docker volume rm <s-now related volumes>
```

ONETRUST APP USAGE

CONFIGURATION OF THE PROJECT

The following environment variables are used to configure the integration.

Table 1: Environment variables

VARIABLE	DESCRIPTION
INVENTA_BASE_URL	URL of IGDCinstance
INVENTA_USERNAME	Username used for logging in to the IGDCinstance
INVENTA_PASSWORD	Password used for logging in to IGDC
INVENTA_KEYCLOAK_PORT	Instance port used by IGDC keycloak. Should be used only in cases when the keycloak port is relevant (applicable to some older IGDC instances), otherwise should omitted completely.
ONETRUST_BASE_URL	OneTrust instance URL
ONETRUST_CLIENT_ID	ClientID used for logging in to OneTrust
ONETRUST_CLIENT_SECRET	ClientSecret used for logging in to OneTrust
ONETRUST_COLLECTION_POINT	URL of a data collection point within OneTrust (optional)
ONETRUST_WORKING_STATUS	Working status of a subtask
LAUNCH_TIMEOUT_SECONDS	Timeout in seconds between scanning the OneTrust instances for relevant requests

EXAMPLES OF INCIDENT CREATION

DSAR REQUEST CREATION & POPULATION

Create a DSAR request in OneTrust and communicate with IGDC in order to provide the relevant discovered data subject info to the OneTrust system.

For example, the user makes a DSAR request of Company A via OneTrust. OneTrust communicates with IGDC. IGDC then executes a data subject search to gather additional information and sends this data back to OneTrust to populate the DSAR report. The report is then provided to the user via OneTrust.

IBM, the IBM logo, and IBM Guardium Discover and Classify are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.