Collibra

Collibra Data Intelligence Cloud

Collibra Data Privacy

Version 2022.07

Collibra

Collibra Data Intelligence Cloud - Collibra Data Privacy

Release date: Thursday, July 7, 2022

Revision date: Thu Jul 07, 2022

You can find the most up-to-date technical documentation on our Documentation Center at

https://productresources.collibra.com/docs/collibra/latest/Content/to_data-privacy.htm

Contents

Introduction to Data Privacy

In response to data protection and privacy regulations, we developed Collibra Data Privacy, which is used in conjunction with Collibra Data Intelligence Cloud. The purpose of Collibra Data Privacy is to provide you with:

- A solid foundation and framework, to help you with the implementation of your privacy and data protection programs.
- A holistic overview of your sensitive enterprise information, including the processes that use the data and where the data stored.

All configurations in Collibra Data Privacy are carried out using Collibra's default functionality, and do not require the involvement of your development department for significant product extension.

Applicable regulations

Collibra Data Privacy is designed for organizations that want to comply with one or more of the following regulations.

Regulation	Effective date
EU General Data Protection Regulation (GDPR)	25 May 2018
California Consumer Privacy Act (CCPA)	1 January 2020

Installing Collibra Data Privacy

This chapter applies to first-time installations of Collibra Data Privacy.

Before starting the installation process, we strongly recommend that you create a full backup of your Collibra Data Intelligence Cloud environment.

In this chapter

Minimum requirements

- Collibra Data Intelligence Cloud 2020.09

Prerequisites

- You downloaded the CMA files from the Collibra Community Downloads page.
- The following is true of your Collibra Data Intelligence Cloud environment, with regard to Collibra Data Privacy packaged asset types and relation types:
  - The packaged hierarchy of parent/children asset types must be maintained in your Collibra environment. The UUIDs of the packaged asset types must also be maintained in your environment.

- The packaged relation types (specifically, the combination of head asset types, roles, co-roles and tail asset types) must be maintained in your Collibra environment. The UUIDs of the packaged relation types must also be maintained in your environment.

> Warning We strongly advise that you not customize the Collibra Data Privacy operating model.

Installation files

There are separate CMA files for CCPA and GDPR. If you have purchased both modules, you need both CMA files. They are available on the Downloads page.

Files	Description
Product installation files: • ccpa-only-2022.01.0.cma • gdpr-only-2022.01.0.cma	Product installation files for CCPA and GDPR, respectively.
Sample content installation files: • ccpa-sample-content-2022.01.0.cma • gdpr-sample-content-2022.01.0.cma	Installation files for CCPA- and GDPR-specific sample content, respectively.

Install Collibra Data Privacy 2022.01

This procedure guides you through a first-time installation of Collibra Data Privacy.

> Warning If you have purchased both CCPA and GDPR modules, you need to complete this process for one of the modules, and then complete it again for the other.

Prerequisites

You have downloaded the relevant product installation files from the Downloads page.

Steps

1. Create a full backup of your Collibra Data Intelligence Cloudenvironment.
2. Sign in to Collibra using an account with Sysadmin privileges.
3. In the main menu, click , then **Settings**.
   » The Collibra settings page opens.
4. In the tab pane, click **Migration** → **Import**.
   » The **Migration Import** page appears.
5. From the Migration Import page, upload the CMA file.
   » Collibra validates the file and automatically downloads an import simulation report to your computer. It might take a few minutes to generate and download the report.
6. Select "Please confirm that a current backup containing data and history was made", and then click **Import**.
   » Collibra imports the CMA file and automatically downloads an import report.
7. Click **Done**.

What's next?

1. We strongly recommend that you install the packaged sample privacy and risk content.
2. If you have purchased both CCPA and GDPR modules:
   a. Complete this procedure again for the module you haven't yet installed.
   b. Install the packaged sample privacy and risk content for the module you haven't yet installed.

Installation of packaged resources

During installation, the installer searches for all resources (for example communities, domains, assets, relations, asset types, resource roles and workflows), by UUID, in the default location. If a particular resource is not found, it is created during the installation. If

the newly created resource has the same name as an existing resource, the name of the existing resource is amended with the suffix "_migration_timestamp".

> Tip After installation is complete, we recommend that you search in Collibra for the word "migration", to see which, if any, resources have been renamed and reconcile any conflicts that could arise due to the name change.

Import reporting

When you upload a CMA file for importing, Collibra Data Intelligence Cloud generates and automatically downloads an import simulation report in Microsoft Excel format.

The report contains sheets with the following pre-import information:

- Summary
- Processed resources
- Added resources
- Changed resources
- Added customization files
- Logs

When the CMA file is then imported, Collibra generates and automatically downloads an import report, to confirm the actual changes made to your Collibra environment.

Install sample privacy and risk content

This procedure installs the packaged Sample content community and various related domains and assets.

> Note This procedure is identical to the product installation procedure, with the exception that here you are uploading the sample content installation file. As is true for the product installation, there are separate sample content installation files for each regulation.

Prerquisites

- You have downloaded the relevant sample content installation files from the Downloads page.
- You have completed the product installation procedure.

Steps

1. Create a full backup of your Collibra Data Intelligence Cloudenvironment.
2. Sign in to Collibra using an account with Sysadmin privileges.
3. In the main menu, click , then **Settings**.
   » The Collibra settings page opens.
4. In the tab pane, click **Migration** → **Import**.
   » The **Migration Import** page appears.
5. From the Migration Import page, upload the CMA file.
   » Collibra validates the file and automatically downloads an import simulation report to your computer. It might take a few minutes to generate and download the report.
6. Select "Please confirm that a current backup containing data and history was made", and then click **Import**.
   » Collibra imports the CMA file and automatically downloads an import report.
7. Click **Done**.

Upgrading Collibra Data Privacy

This chapter is relevant to those who are upgrading to Collibra Data Privacy 2022.01.

> Note Only incremental upgrades are supported. This means, for example, that if you are using Collibra Data Privacy 2021.07 and you want to upgrade to 2022.01, you must first upgrade to 2021.10. Only from 2021.10 can you update to 2022.01.

Before starting the upgrade process, we strongly recommend that you create a full backup of your Collibra Data Intelligence Cloud environment.

> Warning
> - We strongly advise that you not customize any of the packaged workflows. If you want to use a packaged workflow as a basis for customization, be sure to make a copy of the workflow, rename the copy, edit it to suit your needs and deploy it. Making a copy of a workflow ensures that your customizations will not be overridden if we need to update the packaged workflows.
> - If you have customized any of the packaged workflows, you must edit the names and process IDs of the relevant workflows before upgrading, to avoid your customizations being overwritten during the upgrade. For complete information on how to edit a workflow name and process ID, see Change the diagram process properties and the accompanying the workflow documentation and tutorials, on the Collibra Developer Portal.

In this chapter

Minimum requirements

- Collibra Data Intelligence Cloud 2020.09

Prerequisites

- You previously installed Collibra Data Privacy 2021.10.

  > Note Only incremental upgrades are supported. This means, for example, that if you are using Collibra Data Privacy 2021.07 and you want to upgrade to 2022.01, you must first upgrade to 2021.10. Only from 2021.10 can you update to 2022.01.

- You downloaded the CMA files from the Collibra Community Downloads page.
- The following is true of your Collibra Data Intelligence Cloud environment, with regard to Collibra Data Privacy packaged asset types and relation types:
  - The packaged hierarchy of parent/children asset types must be maintained in your Collibra environment. The UUIDs of the packaged asset types must also be maintained in your environment.
  - The packaged relation types (specifically, the combination of head asset types, roles, co-roles and tail asset types) must be maintained in your Collibra environment. The UUIDs of the packaged relation types must also be maintained in your environment.

> Warning We strongly advise that you not customize the Collibra Data Privacy operating model.

Upgrade files

There are separate CMA files for CCPA and GDPR. If you have purchased both modules, you need both CMA files. They are available on the Downloads page.

Files	Description
• ccpa-only-2022.01.0.cma • gdpr-only-2022.01.0.cma	Product upgrade files for CCPA and GDPR, respectively.

Upgrade from Collibra Data Privacy 2021.10 to 2022.01

This procedure guides you through a Collibra Data Privacy upgrade, from 2021.10 to 2022.01.

> Warning If you have purchased both CCPA and GDPR modules, you need to complete this process for one of the modules, and then complete it again for the other.

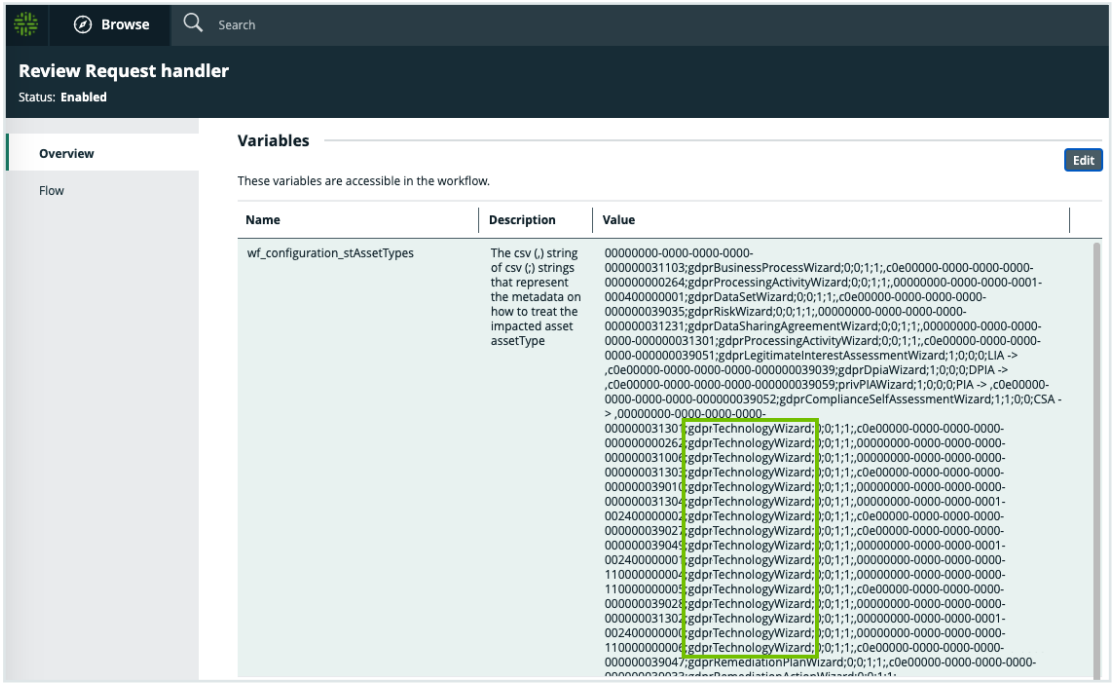
Steps

1. Create a full backup of your Collibra Data Intelligence Cloudenvironment.
2. Sign in to Collibra using an account with Sysadmin privileges.
3. In the main menu, click , then **Settings**.
   » The Collibra settings page opens.
4. In the tab pane, click **Migration** → **Import**.
   » The **Migration Import** page appears.
5. From the Migration Import page, upload the CMA file.
   » Collibra validates the file and automatically downloads an import simulation report to your computer. It might take a few minutes to generate and download the report.
6. Select "Please confirm that a current backup containing data and history was made", and then click **Import**.
   » Collibra imports the CMA file and automatically downloads an import report.
7. Click **Done**.
8. If necessary, edit the wf_configuration_stAssetTypes configuration variable in the Review Request handler workflow.

   > Note The configuration variable value must refer to "gdprTechnologyWizard".

   a. In the main menu, click , then **Settings**.
      » The Collibra settings page opens.
   b. In the tab pane, click **Workflows** → **Definitions**.

c. Click the Review Request handler workflow.
d. In the Variables section, find the **wf_configuration_stAssetTypes** configuration variable. It might refer, for example, to "gdprProposeTechnologyWizard". Ensure that it correctly refers to "gdprTechnologyWizard", as shown in the following image.



   - If it does, there is nothing more to do.
   - If it doesn't, you have to edit it.

e. Click ✎, to edit the value of the configuration variable.
f. Change every instance of the old workflow reference, to "gdprTechnologyWizard".

> Tip Copy/paste the entire configuration variable value into a text editor, replace every instance of the old string by "gdprTechnologyWizard", and then paste the new value into the value field.

g. Click **Save**.

What's next?

If you have purchased both CCPA and GDPR modules, complete this procedure again for the module you haven't yet installed.

Installation of packaged resources

During installation, the installer searches for all resources (for example communities, domains, assets, relations, asset types, resource roles and workflows), by UUID, in the default location. If a particular resource is not found, it is created during the installation. If the newly created resource has the same name as an existing resource, the name of the existing resource is amended with the suffix "_migration_timestamp".

> Tip After installation is complete, we recommend that you search in Collibra for the word "migration", to see which, if any, resources have been renamed and reconcile any conflicts that could arise due to the name change.

Import reporting

When you upload a CMA file for importing, Collibra Data Intelligence Cloud generates and automatically downloads an import simulation report in Microsoft Excel format.

The report contains sheets with the following pre-import information:

- Summary
- Processed resources
- Added resources
- Changed resources
- Added customization files
- Logs

When the CMA file is then imported, Collibra generates and automatically downloads an import report, to confirm the actual changes made to your Collibra environment.

Post-upgrade procedures

After you have successfully upgraded Data Privacy, we recommend that you carry out the following post-upgrade procedures:

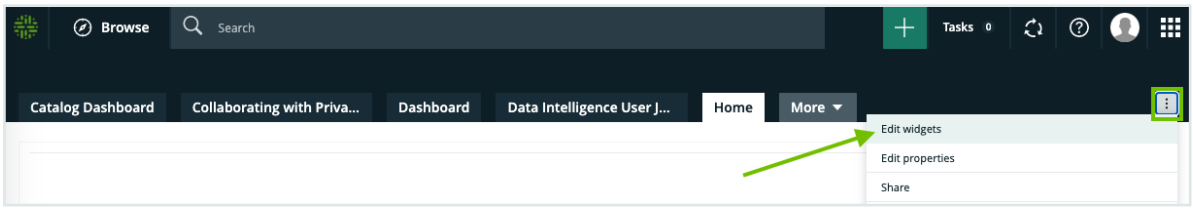
- Update Privacy Dashboard links
- Delete the Identifier attribute

Update Privacy Dashboard links

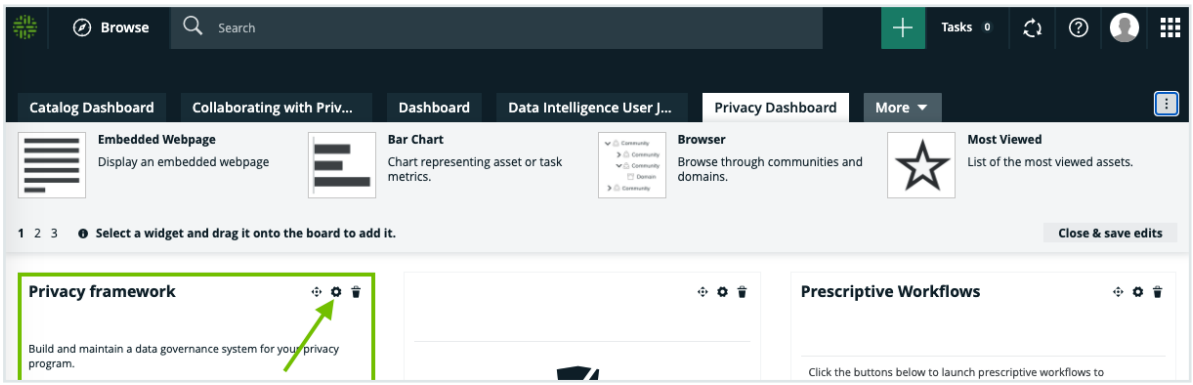
Follow this procedure to update links in the Privacy framework section of the Privacy Dashboard.

Steps

1. In the main menu, click .
   » The most recently opened dashboard is shown.
2. Next to the dashboard name, click , and then select the Privacy Dashboard.
3. In the dashboard toolbar, click ⋮ → **Edit widgets**.

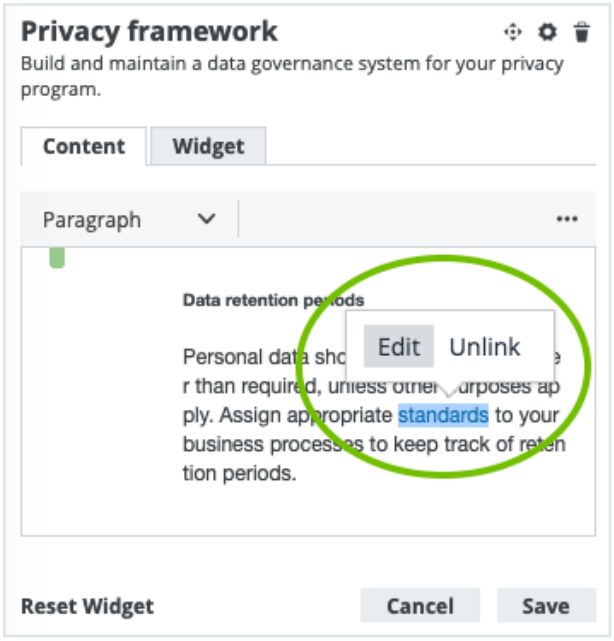


4. In the "Privacy framework" text widget, click .

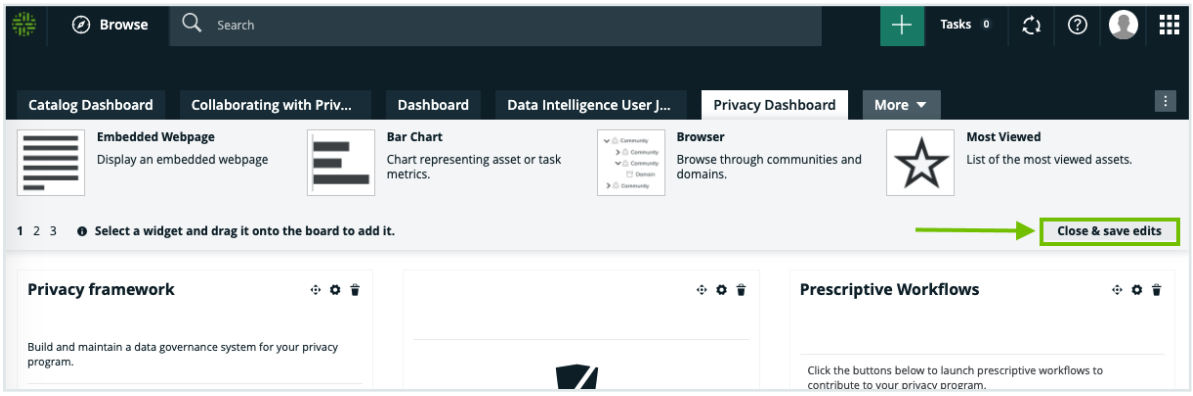


5. In the **Content** tab, scroll down to the "Data retention periods" section.

6. Click the “standards” link, and then select **Edit**.



   The **Insert/Edit Link** dialog box appears.
7. In the **URL** field, replace the current value with */search?q=*&asset_type=00000000-0000-0000-0000-000000031206*, and then click **Save**.
8. Scroll further down in the same widget and click the “roles and responsibilities” link.
9. Click **Unlink**, and then click **Save**.
10. Click **Close & save edits**.

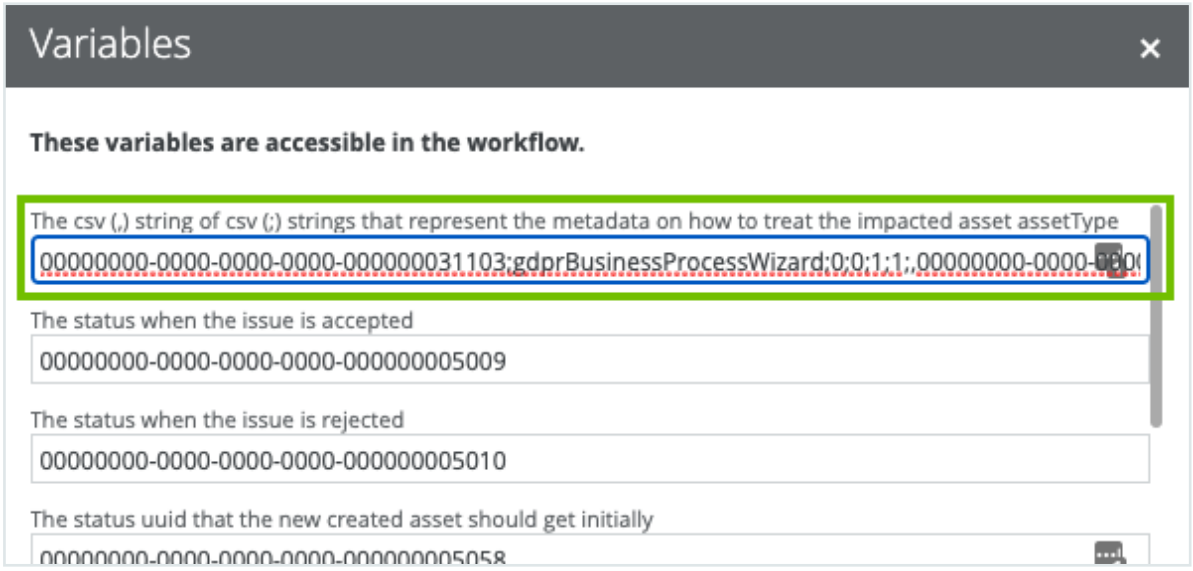


Delete the Identifier attribute

The Identifier attribute (UUID c0e00000-0000-0000-0001-000500000043) is no longer part of the Data Privacy operating model and can be deleted.

Steps

1. In the main menu, click ⠿, then ⚙ **Settings**.
   » The Collibra settings page opens.
2. Click **Workflows**.
   » The Workflows settings page appears on the **Definitions** tab page.
3. In the table, find the **Review Request handler** workflow and click it.
4. In the **Variables** section, click ✎.
   » The **Variables** dialog box appears.
5. In the variable field **The csv (,) string of csv (;) strings that represent the metadata on how to treat the impacted asset assetType**, delete the following strings:
   - 00000000-0000-0000-0000-000000031301;g-dprProcessingActivityWizard;0;0;1;1;
   - c0e00000-0000-0000-0000-000000000264;g-dprProcessingActivityWizard;0;0;1;1;



> Tip Copy the entirety of the value in the variable field and paste it into a text editor. You can then easily find and delete the two strings and copy/paste the remaining value into the variable field.

6. Scroll to the bottom of the **Variables** dialog box, and click **Submit**.

Preparation

This section:

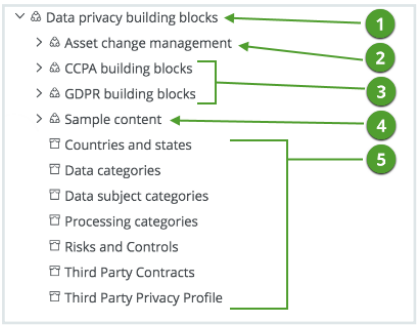
- Introduces key concepts, such as the community-domain structure, moving out-of-the-box domains, resource roles and responsibilities, key asset types and mappings, and third-party register.
- Helps to ensure that the right information is established for legal terms, policies, third-parties, systems and so forth. These are used as a way to constrain choices, so that information captured in the next phases is consistent and compliant.

Preparation methodology

Although there is no one method for setting up a data privacy program within Collibra Data Privacy, the following methodology addresses common, critical elements.

Packaged resources

To help you get up and running as quickly as possible with your compliance program, Collibra Data Privacy comes with the following packaged resources:

Organization Browser	Resource	Description
	1 Data privacy building blocks community	A top-level data privacy community that centralizes all your privacy-related data.
	2 Asset change management community	Community and domains that help you monitor your business and assessment assets and keep them up-to-date.
	3 Regulation-specific communities and domains	Communities and domains dedicated to the specific regulations with which you need to comply.
	4 Sample content	Community and domains with sample content that you can edit and use to suit your needs.
	5 Common data privacy domains	Domains with essential privacy-related assets.

The Data privacy building blocks community

Collibra Data Privacy comes with an example operational organization structure, composed of communities, subcommunities and domains. This structure is designed to meet your needs, whether you need to comply with one or several data privacy regulations.

The Data privacy building blocks community contains:

- Top-level domains that are applicable to all data privacy regulations.
- Subcommunities and domains applicable to specific data privacy regulations.

Top-level domains

The following table shows the domains in the Data privacy building blocks community.

Domain	Contents
Countries and states	Jurisdiction assets, for example United States and Belgium.
Data categories	Data Category assets, for example Payroll Information, Location Data and Contact Information.
Data subject categories	Data Subject Category assets, for example Applicants, Children and Visitors.
Processing categories	Processing Category assets, for example Archiving, Retrieval and Storage.

Asset change management community

This community contains the following domains, which are applicable to all regulations with which you need to comply:

Domain	Contents
Cron codes	Cron-related Code assets for use with Time-based Review Rule assets.
Event-based review rules	Assets used to trigger the review of related assets, based on changes to specified attributes or relations of related assets.

Domain	Contents
Frequencies	Business Term assets that describe various time frequencies, for example: Every year, on the 15th of April. These assets are related to Code Value assets that represent cron values matching Business Term descriptions, for example "0 0 0 15 APR".
Review Request classifications	Issue Category assets that describe the three types of review requests: time-based, event-based and manual review requests.
Time-based review rules	Assets used to trigger the review of other assets after an elapsed amount of time.

CCPA building blocks community

This community contains the following CCPA-specific domains:

Domain	Contents
CCPA articles	Assets that represent articles of CCPA.
CCPA glossary	CCPA-related Business Term assets.
CCPA purposes	Purpose assets, to which Business Process assets can refer.
CCPA-specific data categories	Data Domain assets, as specified by CCPA.
CCPA-specific data subject categories	Data Subject Category assets, as specified by CCPA.
Legal bases under CCPA	Legal Basis assets, as referred to for processing personal data.
PIA evaluation rules inventory	Threshold Assessment Rule assets, which represent the individual questions used in the PIA workflow.

Domain	Contents
Sample remediation actions and plans for CCPA	Sample Remediation Action and Remediation Plan assets.

GDPR building blocks community

This community contains the following GDPR-specific domains:

Domain	Contents
DPIA evaluation rules inventory	Threshold Assessment Rule assets, which represent the individual questions used in the DPIA workflow.
Data protection authorities	Party assets of Party Role Type Supervisory Authority.
GDPR Glossary	GDPR-related Business Term assets.
GDPR articles	Assets that represent articles of GDPR.
GDPR purposes	Purpose assets, to which Business Process assets can refer.
GDPR-specific data categories	Data Category assets, as specified by GDPR.
GDPR-specific data subject categories	Data Subject Category assets, as specified by GDPR.
Legal bases under GDPR	Legal Basis assets, as referred to for processing personal data.
Sample remediation actions and plans for GDPR	Sample Remediation Action and Remediation Plan assets.

Sample content community

This community contains the following domains, which are applicable to all regulations with which you need to comply.

> Note The sample content is not installed during the product installation procedure. There is a separate CMA file for the sample content, for each regulation.

> Warning The sample resources are strictly illustrative. They should not be edited. Editing the attributes of the sample resources might result in an error during any subsequent attempt to run the sample content installation file.

Domain	Contents
Sample HR processes	Sample Business Process assets for Human Resources-related processes.
Sample IT processes	Sample Business Process assets for IT-related processes.
Sample application inventory	Sample Application assets.
Sample assessment register	Sample assessment assets, for example PIA assets and Legitimate Interest Assessments assets.
Sample corporate data policies	Sample Policy assets.

Domain	Contents
Sample data dictionary - MDM application	• Physical Data Dictionaries for MDM system, Workday application and Workforce application. • Used to demonstrate GDPR Solution lineage capabilities on sample data assets. • Your specific dictionary could be split into multiple domains and could be governed by a different governance model.
Sample data dictionary - Workday application	
Sample data dictionary - Workforce application	
Sample data sets	Samples of Data Set assets that can be edited and related to your Business Process assets.
Sample Data Sharing Agreements	The formal contracts that document which data is shared between Controllers and Processors and how the data can be used.
Sample end-user computing inventory	
Sample internal parties (legal entities)	Internal Processors and Controllers of any personal data.
Sample lines of business	Sample Line of Business assets (also known as 'business areas') in a hierarchical way.
Sample marketing processes	Sample Business Process assets for marketing-related processes.

Domain	Contents
Sample personal data glossary	Sample Business Term assets, for example marital status and customer address.
Sample remediation actions and plans	Sample Remediation Action assets and Remediation Plan assets.
Sample risk and controls register	Sample Risk assets and Control assets.
Sample safeguard register	Sample Safeguard assets.
Sample third-party privacy profiles	Sample Party assets.

Privacy asset model

The following images provide an overview of the Collibra Data Privacy asset model, which provides an exhaustive description of:

- The responsible parties that must document and report data processing activities.
- Mandatory processing activity information that must be reported.

To provide visual clarity, the asset model is depicted in the following images with primary focus on three main asset types:

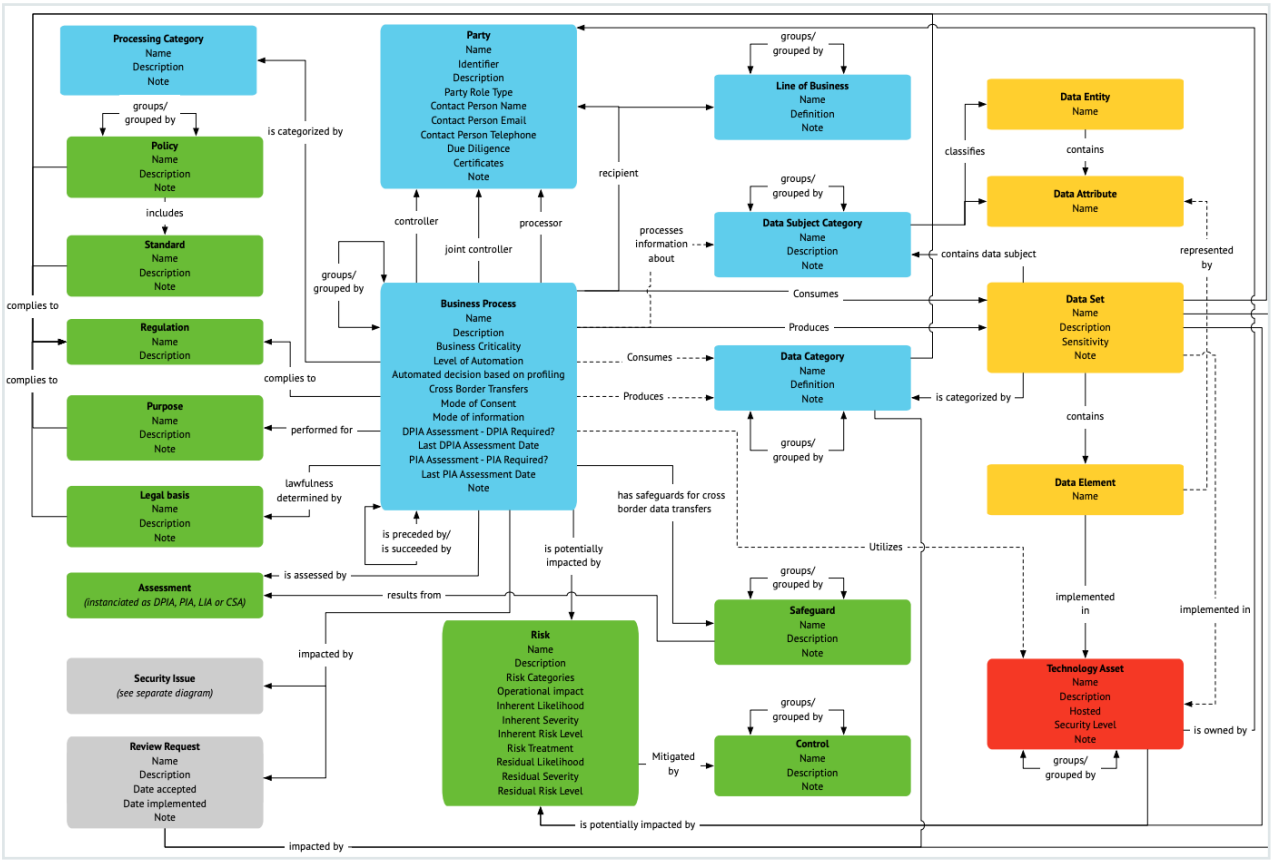
- Business Process
- Data Sharing Agreement
- Security Issue

Each color in the images represent a different asset type:

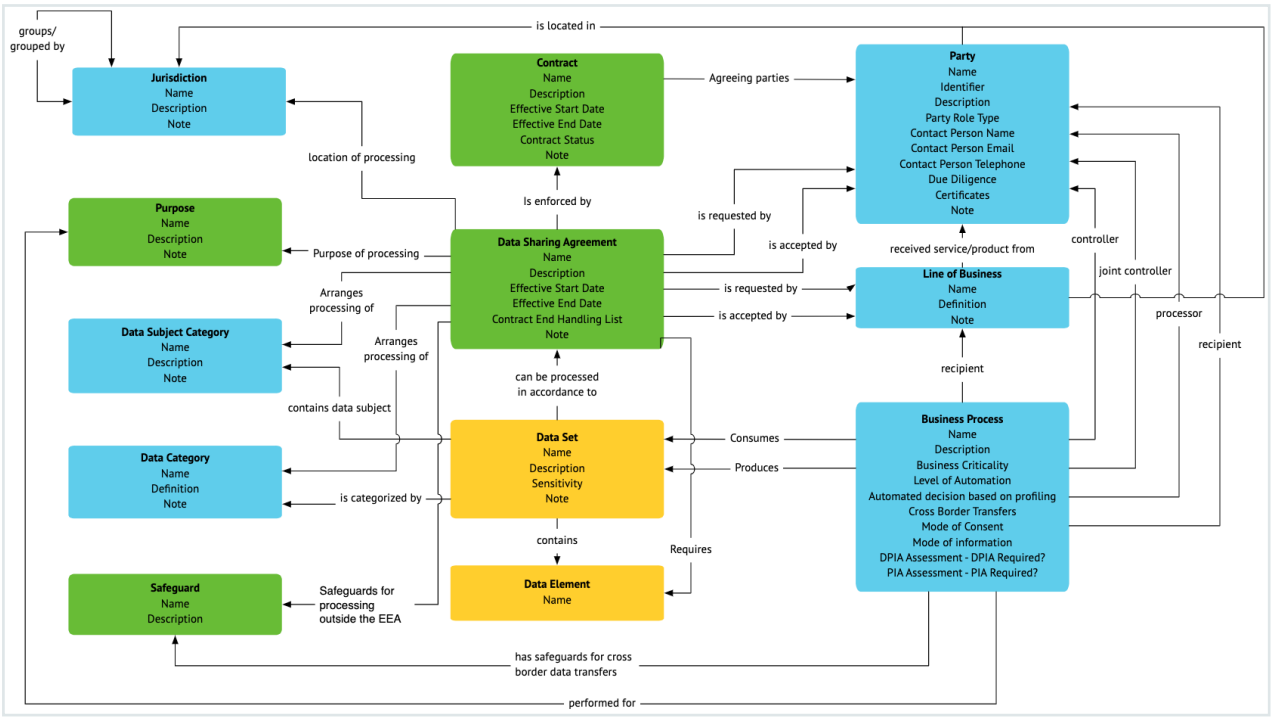
- Blue: Business Assets
- Yellow: Data Assets
- Green: Governance Assets

- Red: Technology Assets
- Grey: Issue Assets

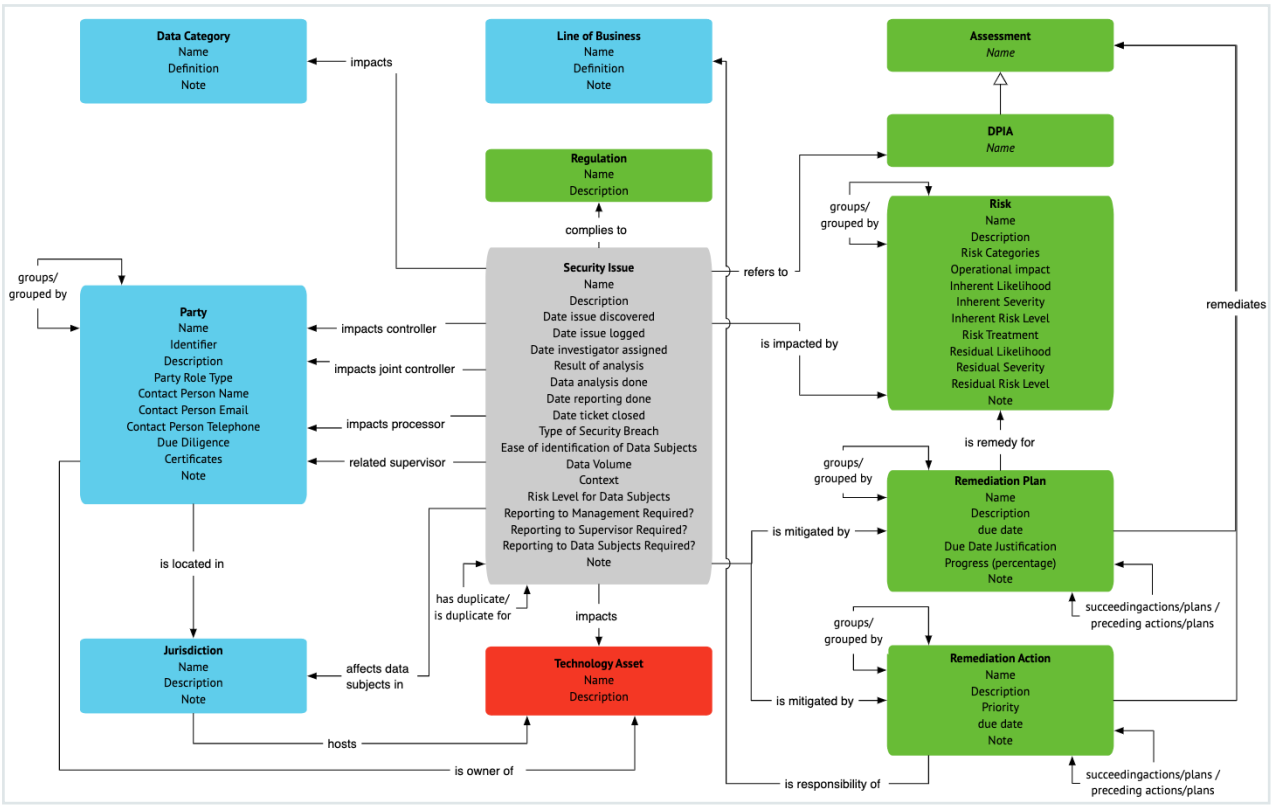
Focus on Business Process assets



Focus on Data Sharing Agreement assets



Focus on Security Issue assets



Setting up your community-domain structure

> Note This task applies only if your organization is new to Collibra and no community-domain structure is in place.

Things to consider

When working with Collibra, you can be as granular as you want when setting up your communities and subcommunities. There are no restrictions as to the rationale you use for creating your communities. However, as data privacy regulations focus mainly on business processes that produce and consume data, we find the following approach to be straightforward and effective:

1. One community per line of business.
   For example Sales, Marketing, Engineering, IT and Human Resources.

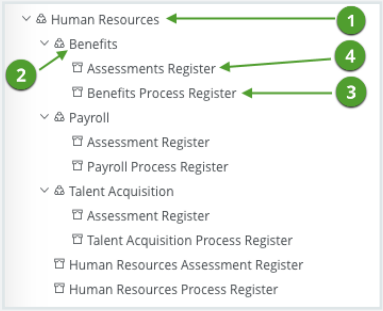
2. One or more subcommunities per community.
   For example Payroll, Benefits and Talent Acquisition could be considered three sub-communities that are grouped by the line of business Human Resources.
3. One Process Register domain per community and subcommunity, for storing your Business Process assets.
4. One Assessment Review Register domain per community and subcommunity, for storing your Assessment Review assets.
5. One Business Dimensions domain per community and subcommunity, for storing your Party assets.

> Note The packaged community-domain structure includes:
>
> - Domains with regulation-relevant assets, which serve as registers to which you can create additional in-kind assets.
> - Domains that serve as default domains when creating new assets. For example, the New Applications domain, which serves as the default domain for any new Technology Assets you create.

Tip If not already in place:

1. Create your communities and subcommunities, based on your organizational structure and business needs.
   For example:
   a. Create a Human Resources community.
   b. Create Benefits, Payroll and Talent Acquisition communities within the Human Resources community.
2. Create the following domains in each of the communities you created in step 1:
   a. A domain of the type Process Register, for storing your Business Process assets and Safeguard assets.
   b. A domain of the type Assessment Register, for storing you PIA and DPIA assets.
   c. A domain of the type Business Dimensions, for storing your Party assets.

   » The new community-domain structure appears in your Organization Browser.



Moving packaged resources

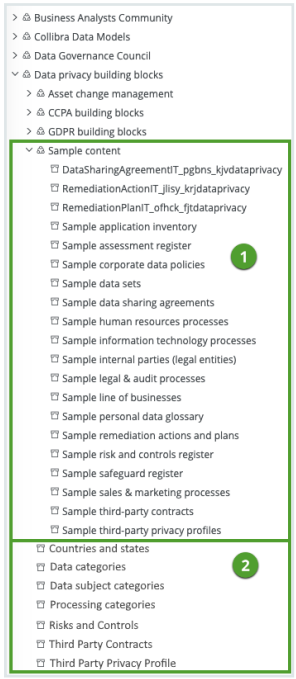
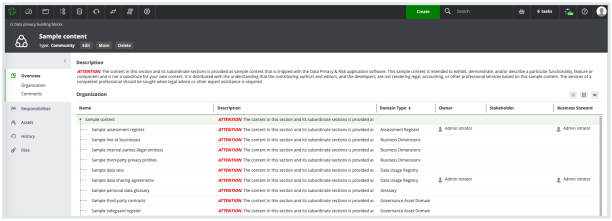
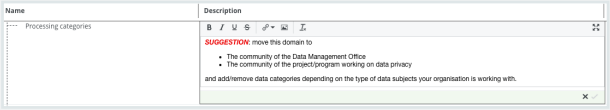
The following communities must not be deleted or edited, but they can be moved:

- Data Governance Council.
  This community is installed by the Collibra Data Intelligence Cloud installer, meaning it is not specific to Collibra Data Privacy. It includes domains that are the default domains for the onboarding of assets of certain asset types.
- Asset Change Management.
  This community is needed for certain asset change management process workflows.
- The building blocks communities of the relevant regulations, for example the CCPA Building Blocks community.

These communities include privacy regulation-specific resources, such as Purpose, Data Category, Data Subject Category assets.

The domains highlighted in the following table must not be deleted or edited. You should, however, move them to the relevant communities within your community-domain structure.

> Note The regulation-specific sample content referred to in the following table is available via CMA installation files that are separate from the Collibra Data Privacy CMA installation file.

Organization Browser	Description
	1 Domains of sample assets, such as Data Set assets and Line of Business assets. You can refer to these assets as templates for creating assets of the same asset type. Move these domains to the relevant communities within your community-domain structure. **Warning** The sample resources are strictly illustrative. They should not be edited. Editing the attributes of the sample resources might result in an error during any subsequent attempt to run the sample content installation file.  2 Domains of privacy-related assets that you will need as you carry out your data governance activities, for example Processing Category assets and Data Subject Category assets. **Tip** In the Description attribute of each domain are suggestions as to where you might want to move these domains. You can delete these suggestions from the Description attribute after moving the domains. 

Tip

1. Identify the relevant team in your organization for each of the domains in the Data privacy building blocks community.
   For example, you identify that the Finance department is best suited to take responsibility for the Sample finance and risk processes domain.
2. Move each domain to the relevant community in your community-domain structure.
   For example, you might move the Sample finance and risk processes domain to your Finance department's community.
3. Create any additional domains you might need, based on the advice in the Description attribute of the "sample" domains.

Privacy-related resource roles and permissions

A resource role is a role that consists of resource permissions and applies to a resource and its children. For example, if you assign a resource role to a domain, it also applies to all assets in the domain. If you assign a resource role to a community, it also applies to all its subcommunities, domains and assets in the community. The purpose of resource roles is to grant resource permissions to users through a responsibility. For example, they determine which users can edit assets via the asset page or in a workflow.

The following table shows the packaged privacy-related resource roles.

For the list of resource roles packaged in Collibra Data Intelligence Cloud, see Resource roles.

Resource role	Description
Business User	A user with responsibility over a domain, subject or process.
CISO	A senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

Resource role	Description
Data Protection Officer	A Data Protection Officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). The DPO is responsible for overseeing data protection strategy and implementation, to ensure compliance with the relevant regulations.
Data Steward	A Data Steward is a role within an organization responsible for using an organization's data governance processes to ensure fitness of data elements - both the content and metadata. Data Stewards have a specialist role that incorporates processes, policies, guidelines and responsibilities for administering organizations' entire data in compliance with policy and/or regulatory obligations. A data steward may share some responsibilities with a data custodian.
Privacy Steward	A role within an organization responsible for utilizing an organization's data governance processes to ensure compliance. Data Privacy Stewards have a specialist role that incorporates processes, policies, guidelines and responsibilities for determining which policy and/or regulatory privacy obligations organizations' data should comply with.

Data privacy resource permissions

A resource permission is a permission that applies to a resource and its children. It can be added to a resource role.

The following image highlights some of the packaged resource permissions for the resource roles Business Steward and Data Protection Officer. Notice that, by default, the Business Steward has all available asset-related permissions.

As Data Protection Officers have more of an advisory role, they likely have little interest in the day-to-day governance of individual assets. As such, the resource permissions configured for the Data Protection Officer are limited. By default, the Data Protection Officer can comment, add attachments and manage workflows and responsibilities.

Name	Required license	Business Steward	Data Protection Officer
Asset			
Add	Author	✓	×
Attribute			
Add	Author	✓	×
Remove	Author	✓	×
Update	Author	✓	×
Data			
Access Data	Consumer	✓	×
View Samples	Consumer	✓	×
Remove	Author	✓	×
Responsibilities			
Add	Author	×	×
Remove	Author	×	×
Update	Author	×	×
Tags			
Update	Consumer	✓	×
Update	Author	✓	×
Update Status	Author	✓	×
Update Type	Author	✓	×

Tip

> Note You can fully develop and maintain your data privacy and risk program with the packaged resource roles and configured permissions. You can skip this task if you have no specific use case for additional roles or permissions.

1. Determine whether or not your organization requires any additional resource roles to successfully govern your data privacy-related resources. If so, you can create new resource roles or edit the packaged resource roles.
2. Ensure that each resource role has the necessary resource permissions to enable the assigned users to fulfill their business responsibilities. Pay particular attention as to whether or not a specific resource role will participate in the management of workflows or carry out workflow tasks. If so, the role must have the Manage workflows permission.
   See Add or remove resource permissions for a resource role.

Important privacy-related personas

The following is an overview of the most important personas in Collibra Data Privacy. For each persona, we have added a radar chart that plots their expected skills and expertise.

Persona functions versus the packaged resource roles

The function mentioned in the bio of each persona relates to that persona's job within the organization. They can be viewed as job titles. Although these functions connote many of the packaged resource roles, they are not linked. For example, John Fisher's function, or job title, is Business Steward. That does not mean, however, that he is the only person in the organization that will be assigned the Business Steward resource role when working in Collibra Data Privacy.

Preston Sterling, whose job title is Privacy Officer, will certainly be assigned the Privacy Steward resource role for various resources in Collibra Data Privacy, but he will also be assigned the Business Steward resource role when onboarding risks during the risk assessment. This is so, because Risks require closer consideration from someone whose primary job focus is on risk-related matters. Furthermore, the risk assessment is configured to be completed, in large part, by a user assigned the Business Steward resource role.

In other words, one person with the right skills and expertise might be assigned to multiple resource roles.

It could also be advantageous to have one person assigned to multiple resource roles, for example Owner and Stakeholder, in the same domain. This is particularly interesting for smaller organizations that work in smaller teams.

William Parker

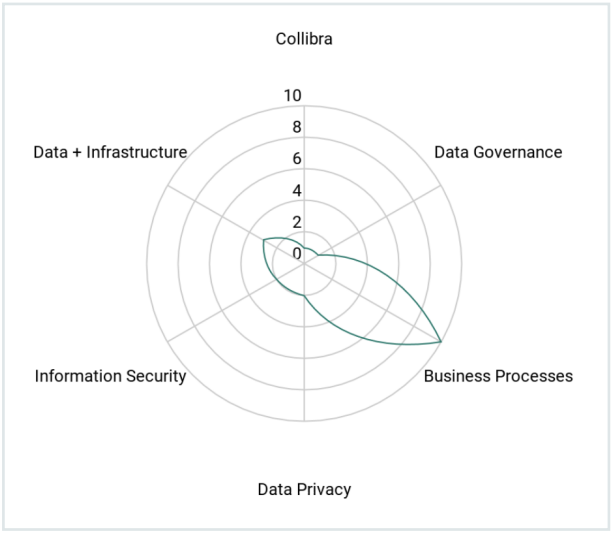
Function

Senior Marketing Analyst

Responsibilities

- Providing input on how the business processes personal data.
- Collaborating with John Fisher during the onboarding of business processes.

Skills and expertise



John Fisher

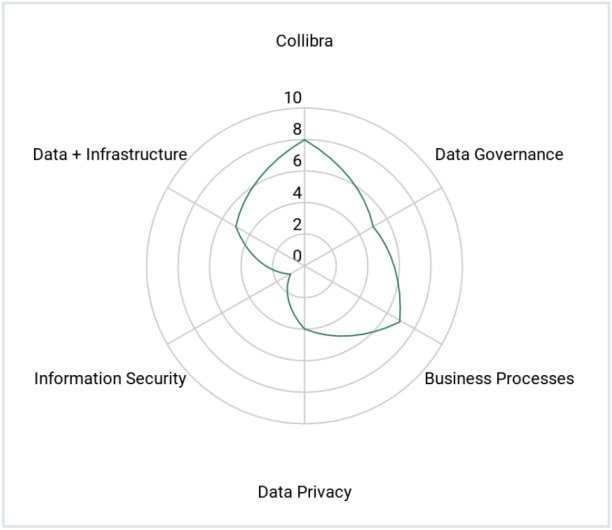
Function

Business Steward

Responsibilities

- Collaborating with the business, to onboard and describe business processes.
- Ensuring the stakeholders are involved during the onboarding of business processes and processing their feedback.
- Performing DPIA/PIA.
- Onboarding data sharing agreements, along with Preston Sterling.

Skills and expertise



Preston Sterling

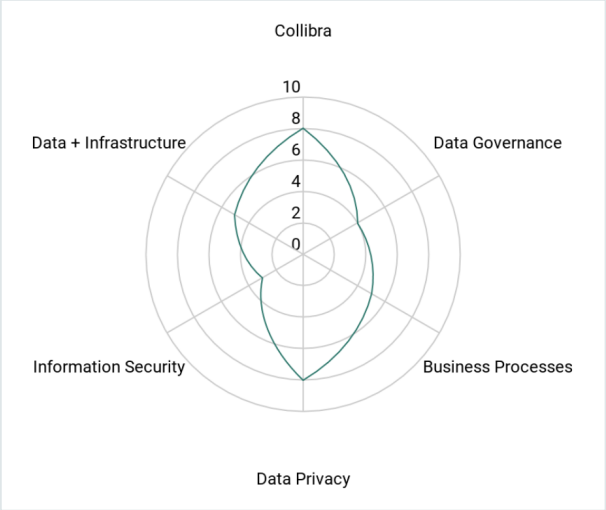
Function

Privacy Officer

Responsibilities

- Determining the legal bases and purposes for business processes.
- Indicating whether business processes constitute cross-border transfers and the controls needed when that's the case.
- Determining the Controller, Joint-Controllers, Processors and Third-Parties for business processes.
- Determining whether a DPIA/PIA is required.
- Helping John Fisher execute DPIA/PIA.
- Reviewing and assessing whether or not the DPIA/PIA has been correctly completed and whether its conclusions (whether or not to go ahead with the processing and which safeguards to apply) are in compliance with the GDPR/CCPA.
- Managing data sharing agreements and other privacy controls.
- Mapping data categories and data subject categories to the logical data model.
- Planning remediation actions to address outstanding risks detected during assessments or data breaches.
- Setting up the risk and control register, along with Dora Portman and Cis Souchek.
- Setting up third-party privacy profiles.

Skills and expertise



Luke O’Reilly

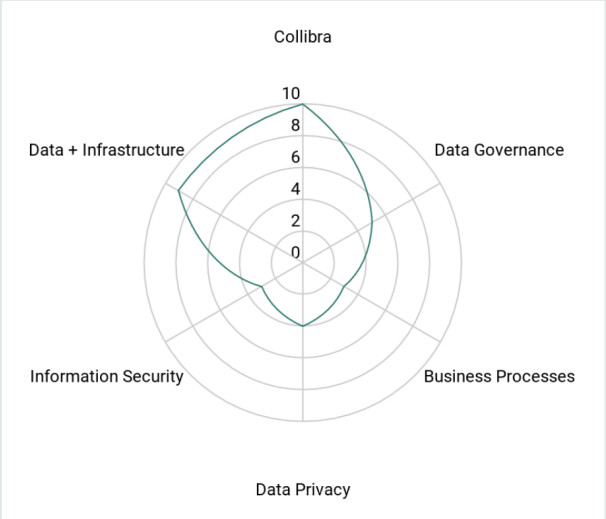
Function

Data Engineer

Responsibilities

- Mapping business processes to data sets (data mapping).
- Onboarding technology applications to the application inventory.
- Useing Catalog’s Automatic Data Classification and Guided Stewardship for personal information discovery.

Skills and expertise



Dora Portman

Function

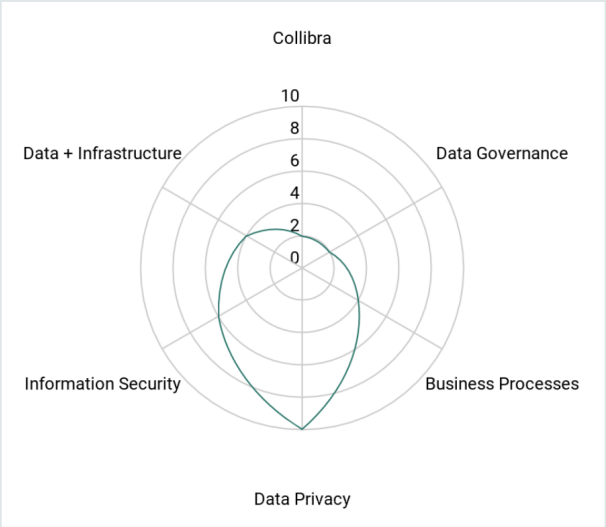
Data Privacy Officer

Responsibilities

- Determining privacy and data classification policies.
- Determining retention policies.
- Mapping data categories to data classification policies and privacy regulations.
- Determining DPIA/PIA threshold rules.
- Reviewing DPIA/PIA.
- Reporting, in case of a data breach.
- Determining the purpose register.

- Planning remediation actions to address outstanding risks detected during assessments or data breaches.
- Reporting progress of privacy program to senior management.
- Regulatory reporting.

Skills and expertise



Christina Souchek

Function / Resource role

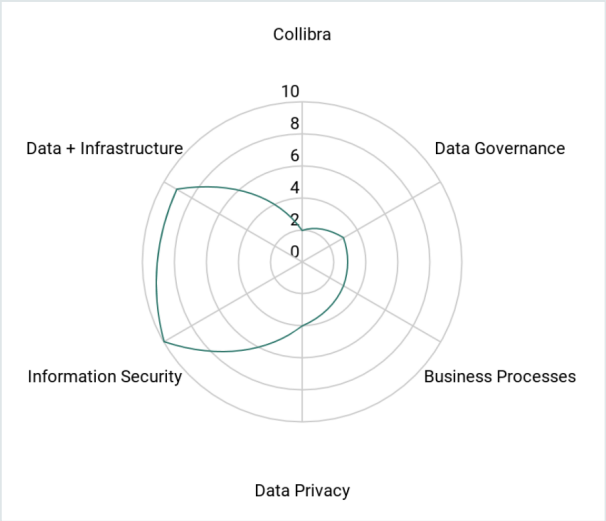
Chief Information Security Officer (CISO)

Responsibilities

- Managing the application inventory.
- Managing the risk and control register, along with Dora Portman and Preston Sterling.

- Determining what went wrong in a breach, dealing with those responsible if they're internal, and planning to avoid repeats of the same crisis (investigations and forensics).
- Ensuring all of the above initiatives run smoothly and get the funding they need, and ensuring corporate leadership understands their importance (governance).

Skills and expertise



Persona tasks

The following table provides an overview of the resource role and tasks required for each of the main privacy-related workflows. The resource roles are mapped to the required tasks for each workflow, in Collibra Data Intelligence Cloud.

> Tip Keep in mind that some personas, for example Preston Sterling, our Privacy Officer, is assigned the Business Steward role for certain resources and workflows, in addition to his more intuitive assignment to the Privacy Steward role, for other resources and workflows.

Business Process workflow

Persona	Resource role	Task
	Business User	Describes: • The business process at a high level. • The data that is used. • The applications that are involved. • With whom the data is shared.
	Business Steward	Aligns with the Business User to ensure the business process is accurately described and conforms to the data model.
	Data Steward	Finds a data set that corresponds to the description provided by the Business User and the Business Steward, and maps it to the business process. If the data set does not exist, he onboards a new data set.
	Privacy Steward	Validates or completes the legal meta-data, such as the purpose and legal basis for processing the data, and the cross-border indicator.
	Owner	Accepts ownership and approves the business process.
	Stakeholder	Optionally provides feedback during the onboarding of the business process.

Data Set workflow

Persona	Resource role	Task
	Business Steward	• Onboards the data set. • Adds the data categories, data subject categories and business terms. • Maps the data set to the business process and the technology assets.
	Owner	Accepts ownership and approves the data set.
	Stakeholder	Optionally provides feedback during the onboarding of the data set.

Technology Asset workflow

Persona	Resource role	Task
	Business Steward	• Onboards the technology asset. • Determines the vendor and the jurisdiction.
	Owner	Accepts ownership and approves the technology asset.

Persona	Resource role	Task
TBD	Stakeholder	Optionally provides feedback during the onboarding of the asset.

Data Sharing Agreement workflow

Persona	Resource role	Task
 or 	Business Steward	• Onboards the data sharing agreement. • Determines the legal aspects, such as the purpose and location of processing.
	Owner	Accepts ownership and approves the data sharing agreement.

Assessment (DPIA/PIA, LIA and CSA) workflows

Persona	Resource role	Task
	Business Steward	Completes the assessment.
	Privacy Steward	Provides feedback during the onboarding of the assessment.
	DPO	Optionally provides feedback during the onboarding of the assessment.
	Owner	Accepts ownership and approves the assessment.
	Stakeholder	Optionally provides feedback during the onboarding of the assessment.

Risk workflow

Persona	Resource role	Task
 or TBD	Privacy Steward (Preston Sterling or other, depending on the type of risk.)	• Onboard new privacy and security risks. • Determines their nature and the mitigating controls.
 or 	Owner (DPO or CISO, depending on the type of risk)	Accept ownership of and approve the risks.
	Stakeholder	Optionally provides feedback during the onboarding of the risks.

Remediation Plan and Remediation Action workflow

Persona	Resource role	Task
 or TBD	Business Steward (Preston Sterling or other, depending on the type of risk being addressed.)	Onboard remediation plans and actions to address outstanding privacy and security risks.
	DPO	Optionally provides feedback during the onboarding of the remediation plans and actions.
 or 	Owner (DPO or CISO, depending on the type of risk being addressed.)	Accepts ownership and approves the remediation plans and actions.
	Stakeholder	Optionally provides feedback during the onboarding of the remediation plans and actions.

Security Breach Managment Workflow

Persona	Resource role	Task
	Any user	Logs a potential data breach.
	Community Manager	Assigns investigation manager.
	Investigation Manager	Analyzes impact of the data breach.
	DPO	Reviews analysis of the data breach and reports, when necessary.

Creating responsibilities

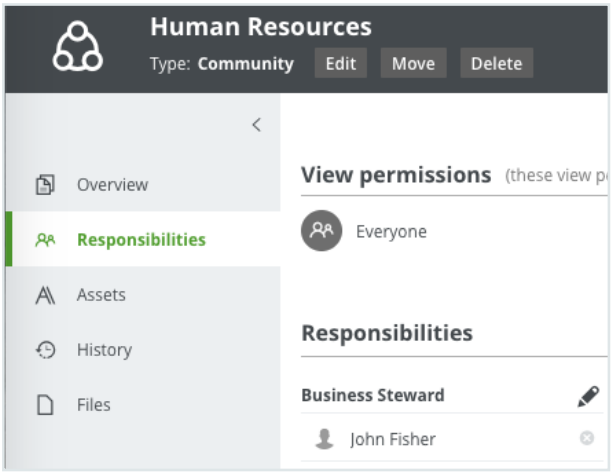
A responsibility is the assignment of one or more users and/or user groups to a resource role for a resource. An example responsibility would be user John Fisher assigned the Business Steward resource role for a Process Register domain.

After assigning users or user groups to a resource role for a resource, the users can act on the permissions conveyed to them via the resource role.

Before creating responsibilities, it is essential to:

- Decide which resource roles are needed to effectively govern your communities, domains and assets.
  For example, you decide to assign a Data Protection Officer for each community.
- Identify the people in your organization best suited to carry out the tasks expected of the various resource roles.

The following image shows the responsibility where the resource role Business Steward has been assigned to user John Fisher, for the resource Human Resources community.



Inherited responsibilities

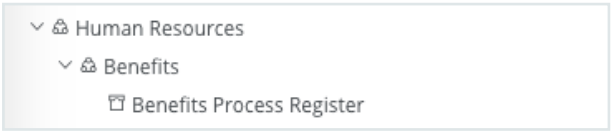
Child resources inherit responsibilities from their parent resources.

- If the resource is a community, the responsibilities are inherited by subcommunities, domains and assets in the community. If you are a Business Steward for a certain community, you are a Business Steward for all the domains and assets inside that community.
- If the resource is a domain, the responsibilities are inherited by the assets in the domain.
- If the resource is an asset, the responsibilities only apply to the asset itself, because assets never have children.

> Note Inherited responsibilities do not show up in a table or preview and they are not exported.

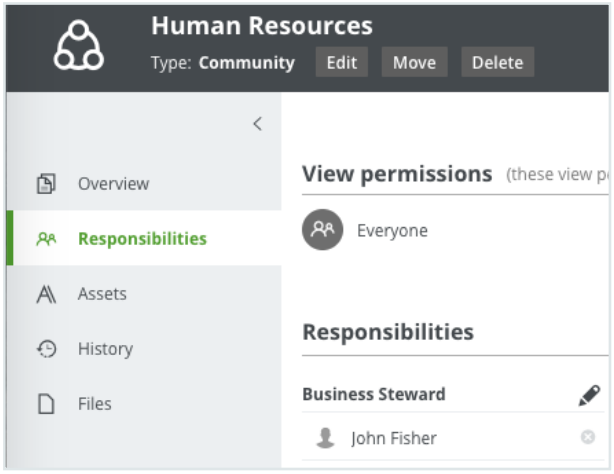
Example

Consider the following example community-domain structure:

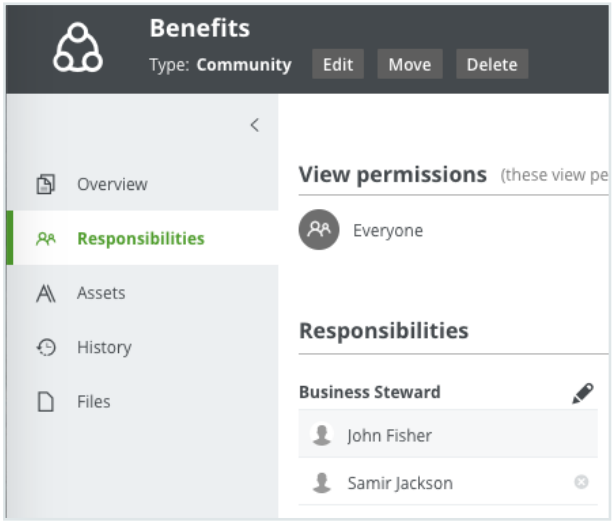


In this case, you could carry out the following steps:

1. Create responsibilities for the Human Resources community, knowing that the Benefits subcommunity, the Benefits Process Register domain and the assets within will inherit the responsibilities.



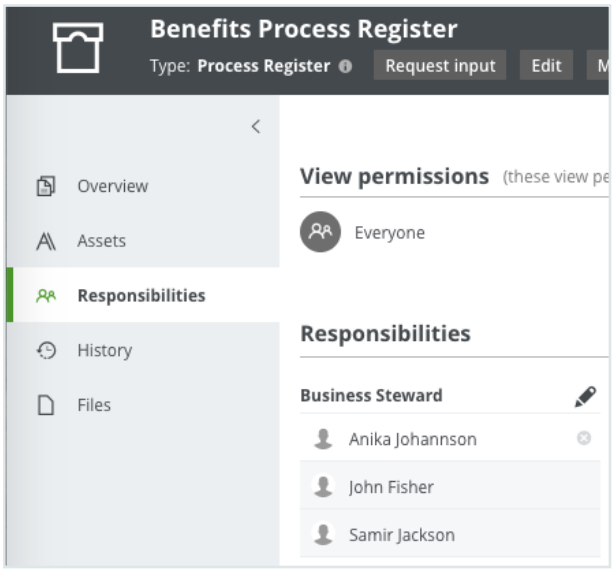
2. If necessary, create any additional responsibilities at the subcommunity and/or domain levels.
   As Samir Jackon is the subject matter expert for benefits-related data, he has been added as a Business Steward for the Benefits community.



> Note The gray background behind "John Fisher" indicates that the responsibility was inherited from the Human Resources community. The white background behind "Samir Jackson" indicates that the responsibility was directly created for the Benefits community.

As Anika Johannson is the person most closely tracking the Benefits department's

business processes, she has been added as a Business Steward for the Benefits Process Register domain.



3. If necessary, create any addition responsibilities at the asset level.

The following table shows the resource roles that have to be present as responsibilities, for specific domains, for the Collibra Data Privacy workflows to work, where:

- M: Mandatory
- O: Optional

Domain type / Resource role	Owner	Business Steward	Privacy Steward	Data Steward	Business User	Community Manager
Process Register	M	M	M	M	M	O
Assessment Register	M	M	O	O	O	O
Remediation Register	M	M	O	O	O	O
Risk and Controls Register	M	M	O	O	O	O

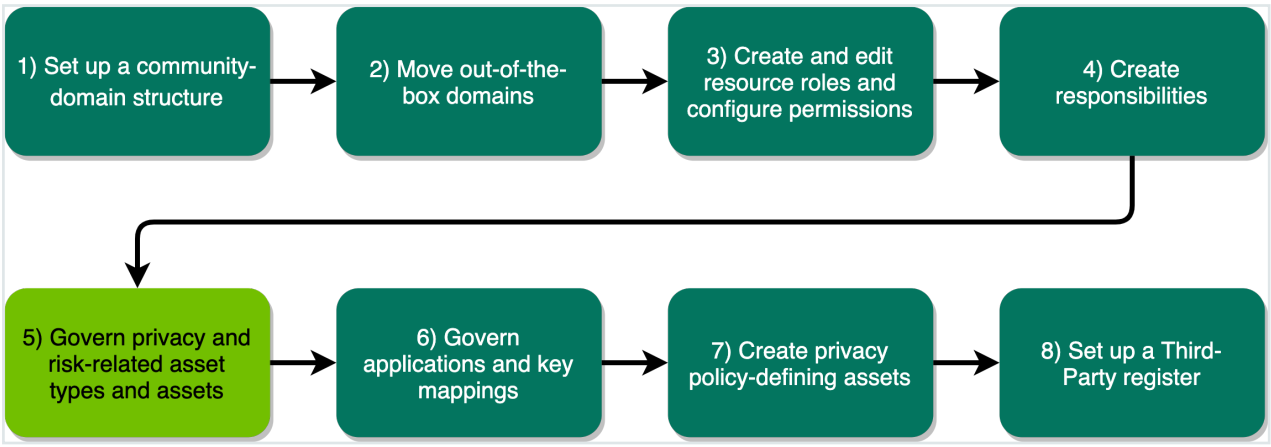
Domain type / Resource role	Owner	Business Steward	Privacy Steward	Data Ste-ward	Business User	Community Manager
Data Usage Registry	M	M	O	O	O	O
Application Inventory	M	M	O	O	O	O
Data Governance Council	O	O	O	O	O	X

Tip

1. Identify which resource roles you need to effectively govern your communities, domains and assets.
2. Identify the people in your organization who will take on these roles, for example Data Protection Officer, Business Steward, Privacy Steward, Issue Manager, Owner, and so on, for your various resources.
3. Create the following responsibilities for each of your domains:
   - Owner
   - Business Steward
   - Data Steward
   - Privacy Steward
   - Stakeholder
   - Business User
4. Create the Community Manager and Privacy Steward responsibilities for the New Data Issues domain. These responsibilities are required for the Log Potential Security Breach and Security Breach Management workflows.

   > Note The New Data Issues domain is in the Data Governance Council community. It is "hidden" in the community-domain browser, to avoid it being inadvertently deleted. You can find the domain by searching for it via the Search field

Privacy and risk-related asset types and assets

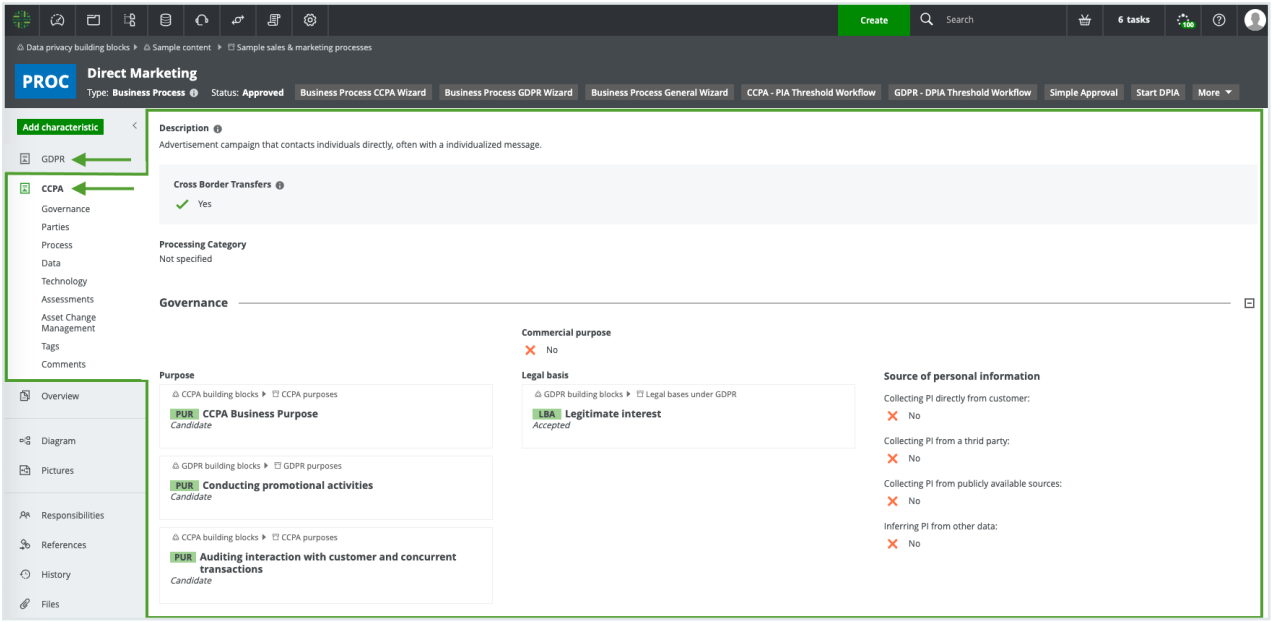


This section provides information on the assets and asset types that are required by Collibra Data Privacy, to effectively manage your privacy and risk program.

> Tip There are several ways to create assets, such as via the Collibra Data Privacy asset onboarding workflows. To create assets in bulk, you can perform what we refer to as the export/import roundtrip. For complete information, see Import assets in the Documentation Center.

Custom asset pages

Collibra Data Privacy provides a custom asset page for Business Process assets, which has custom information tabs for the relevant regulations.



> Important The following Collibra Data Privacy asset types and their related workflows and custom asset pages are deprecated:
>
> - CSA
> - DPIA
> - PIA
>
> These asset types, related workflows and custom asset pages are no longer included in the Collibra Data Privacy CMA installation files.

Required assets

The Business Process custom asset page requires instances of the following assets in your Collibra environment:

- An asset of the asset type Regulation, named "GDPR", if you purchased the GDPR module.
- An asset of the asset type Regulation, named "CCPA", if you purchased the CCPA module.

Required assets for packaged Collibra Data Privacy workflows

The following table show the types of assets that must be present in your Collibra Data Intelligence Cloud environment for the associated workflows to work.

Warning It is important to understand the significance of these asset types and the definition of the individual assets of these asset types. For example:

- The definition of a Data Category asset might make the difference between compliance and non-compliance with a specific regulation.
- The definition of a Purpose asset might forbid you from accommodating a data subject's right to be forgotten.

Asset type	Business Process onboarding workflows	Data Set onboarding workflows	Asset change management workflows	Technology Asset onboarding workflows
Policy	X			
Technology Asset	X	X		
Purpose	X			
Legal Basis	X			
Data Category	X	X		
Data Subject Category	X	X		
Party	X			X
Line of Business	X			

Asset type	Business Process onboarding workflows	Data Set onboarding workflows	Asset change management workflows	Technology Asset onboarding workflows
Data Set	X			X
Regulation	X			
Safeguard	X			
Business Process		X		
Data Element		X		
Data Sharing Agreement	X			
Remediation Action				
PIA Evaluation Rule				
Review Rule			X	
Code Value			X	
Retention Period (child of Standard)		X		
Regulation	X			
Jurisdiction				X
Processing Category	X			

Asset types by category

The following table shows the five categories of asset types.

Category	Description
Technology Assets	Physical assets used to process, transmit, analyze, and store information.
Data Assets	A type of asset that represents details of organizational data.
Business Assets	A type of asset that is exclusively used and governed by the business user community.
Governance Assets	A type of asset that is used to monitor and advocates to maximize performance or utilization of other Business and Data assets while minimizing the risk factors in alignment with Organizational/Business goals.
Issues	Various types of issues to be tracked: Data Issue, Security Issue, and Review Request

Technology assets

Technology assets represent the physical assets your organization uses to process, transmit, analyze and store information.

The global assignment for Technology Assets includes, among others, characteristics that allow you to identify:

- In which Technology Assets your personal data resides, and the security level of these assets.
- By which applications your personal data is being consumed and produced.
- In which jurisdiction your personal data is being hosted.
- Which risks and security issues could impact your applications.

The following table shows the relevant Technology asset types and example descriptions.

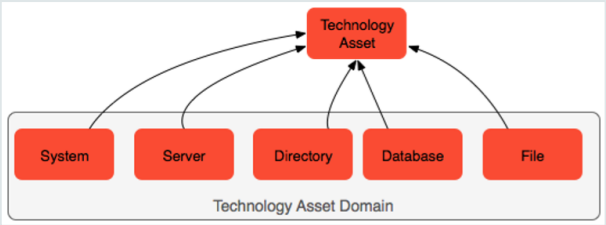
Asset type	Example description
Technology Asset	A piece of information technology (hardware, software, database, software platform) that helps an organization run a business application.
Application	A classification of computer program designed to perform specific tasks, such a word processing.
Database	A collection of data that is systematically organized or structured in order to make it easy to create, update and query the information.
Directory	An organizational structure that contains files and/or other directories.
End User Tool	A way in which a user can interact with data at rest, with manual intervention, to manipulate or consolidate data.
File	A collection of data that is treated by a computer as a unit, for the purposes of input and output.
File Group	A collection of physical files which, together, represent a single logical file.
Network	A computer network or data network is a digital telecommunications network that allows nodes to share resources. In computer networks, network-connected computing devices exchange data with each other using a data link.
Paper Document	A carrier of data in paper form.
S3 Bucket	An asset type that represents buckets in an Amazon S3 repository.
Server	A computer program or device that supports other computer programs and their users.
Software	Software is a collection of instructions that enables the user to interact with a computer or its hardware and perform tasks.

Asset type	Example description
System	Executable software that you can buy commercially off the shelf (COTS), or build internally, to automate one or more business functions that help run a business smoothly and efficiently.

Technology assets should be inventoried and related to all relevant policies, including:

- Policies pertaining to the type of information stored in the assets.
- Policies that address the handling and storage of backups.
- Asset end-of-life and disposal policies.
- Jurisdiction-focused policies.

Technology Assets by domain



> Tip Consider creating high-level Technology Assets first, such as Systems and Applications. Later, you can add more granular-level assets. In the global assignment of the relevant asset types, you can view the default attributes configured for each asset type. You can add any additional attributes to suit your needs.

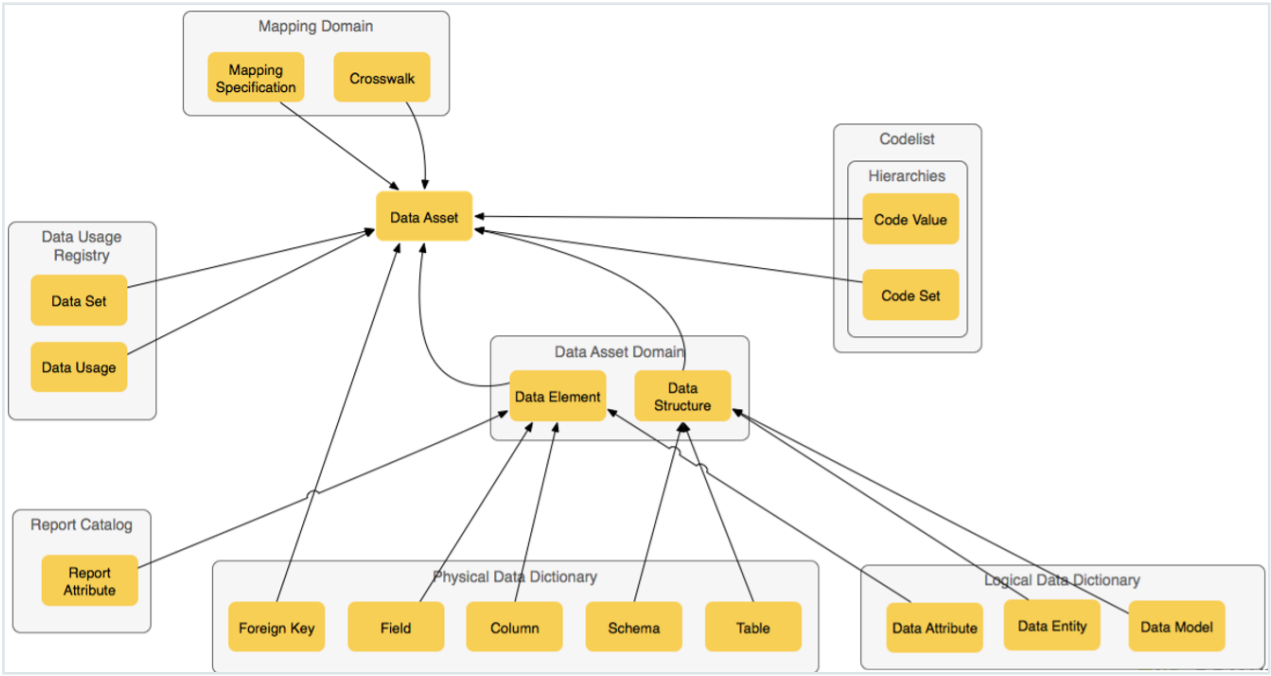
Data Assets

The following table shows the most relevant child asset types of Data Assets.

Asset type	Description
Data Entity	A unit of data that can be classified and can have a stated relationship to other units of data. Examples: Customer, Employee

Asset type	Description
Data Attribute	A specification that defines a property of a data entity. Examples: CustomerBirthDate, EmployeeFirstName
Data Set	A collection of related sets of Data Assets that are Data Elements or composed of Data Elements. Example: Customer contact information
Data Element	A unit of data that is defined for processing. It usually documents an aspect of something abstract. Examples: Person Birth Date, Person Address, Customer Account Number

Data Assets by domain

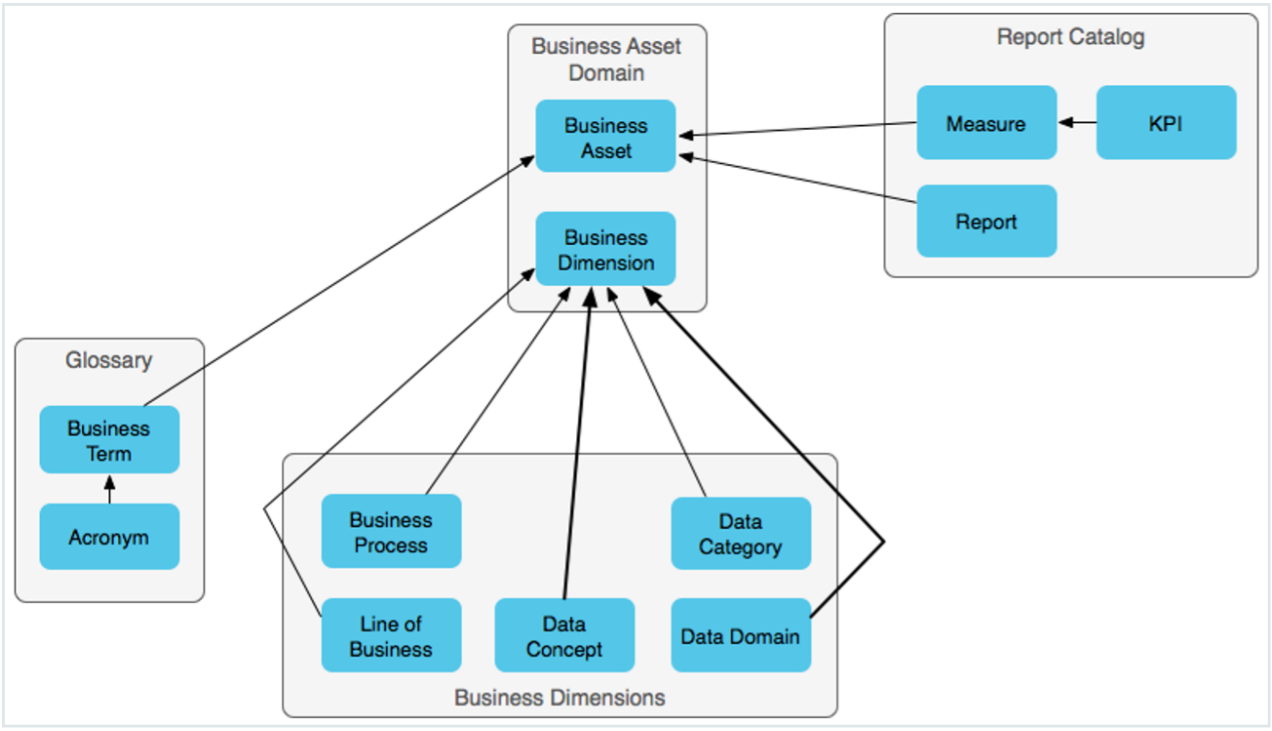


Business Assets

The following table shows the most relevant child asset types of Business Assets.

Asset type	Description
Party	An association, corporation, partnership, proprietorship, trust, or individual that has legal standing. A party has legal capacity to enter into agreements or contracts, assume obligations, incur and pay debts, sue and be sued, and to be held responsible for its actions.
Business Process	A set of activities and tasks that, once completed, produce a specific result and add value to the business. Examples: campaign management, talent recruitment and staffing.
Line of Business	Also known as a business unit or a business area, the line of business is a logical element or segment of an organization that serves a particular business need. Examples: asset management, retail, e-com, investment management.
Data Category	A data category is a grouping of information relating to an individual, be it their private, professional or public life. Data categories are not exclusive; information can transcend multiple categories.
Data Subject Category	A way in which a user can interact with data at rest, with manual intervention, to manipulate or consolidate data.
Jurisdiction	A hierarchical representation of how a business divides its market on the basis of geography, such as regions and countries. For example, North America is segmented into USA and Canada.

Business Assets by domain



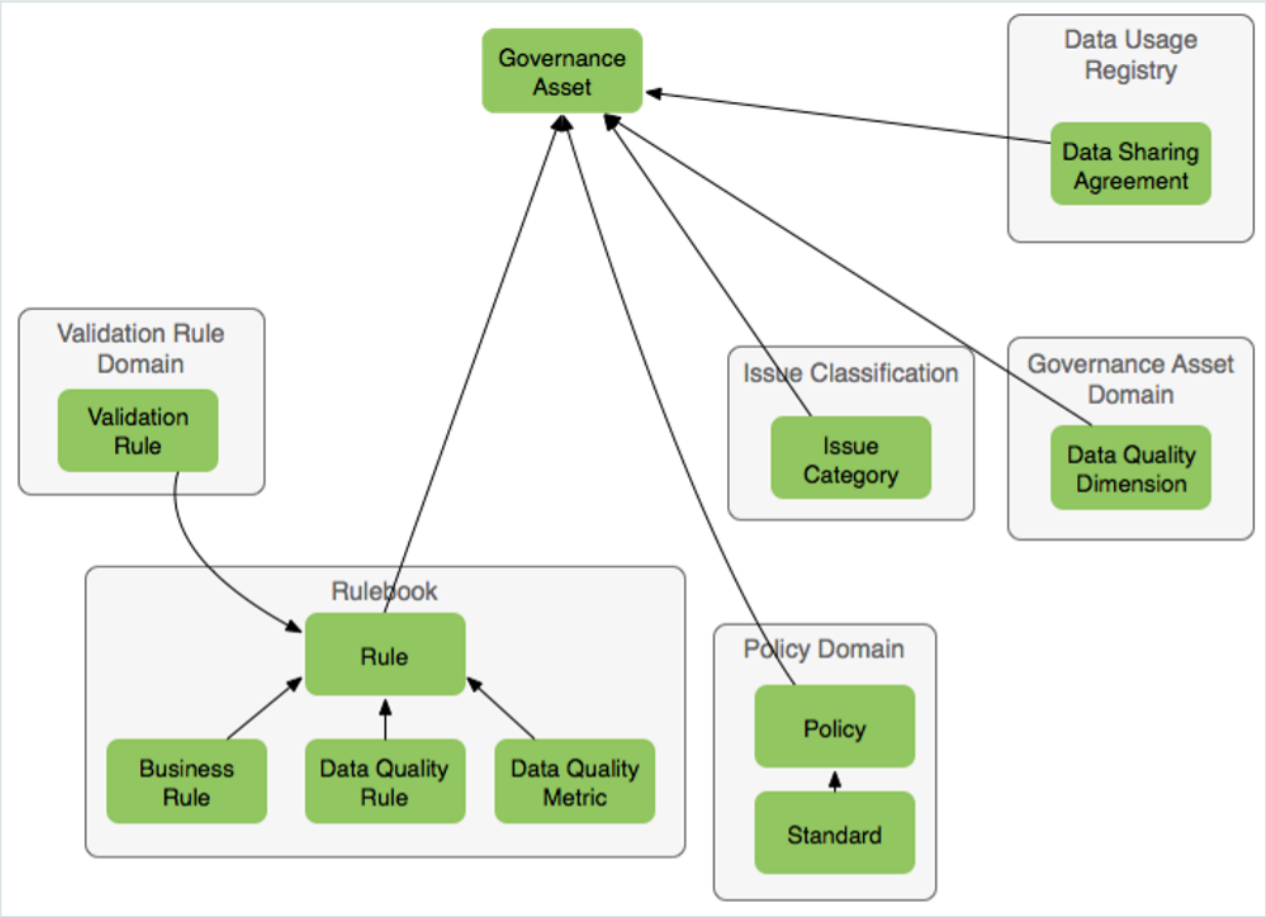
Governance Assets

The following table shows the most relevant child asset types of Governance Assets.

Asset type	Description
Policy	A statement of intent that is implemented by a set of rules. Policies are usually set by a data governance council.
Standard	A specific low-level mandatory action or rule that helps to enforce and support a policy. Example: All personal information must be encrypted with a specific encryption type.
Regulation	A directive made and maintained by an authority. For example, BCBS and Solvency.

Asset type	Description
Purpose	An asset that describes the reason for which another asset is created or for which another asset exists.
Legal Basis	The lawfulness of processing, as defined by Article 6 of GDPR. Personal data may be processed only if, and to the extent that, at least one legal basis applies. (Implicit for CCPA)
Assessment	A type of asset that is used to store the results of assessments as attributes and relations.
Safeguard	(GDPR) Safeguards for transfers of data and in particular Personal Information to third parties, other countries or international organizations.
Risk	An uncertain event that could create damage, injury, liability, loss or any other negative occurrence that is caused by external or internal vulnerabilities (Risk Sources), which can be avoided through controls.
Control	A measure taken to mitigate a risk. Any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Governance Assets by domain



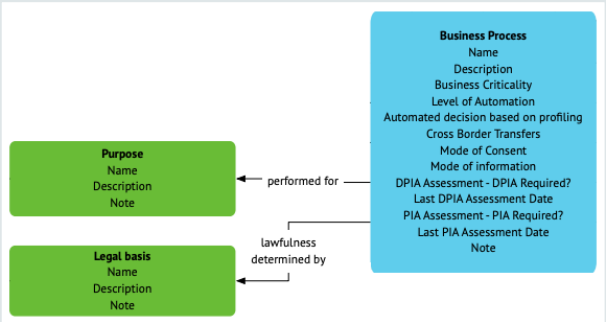
Issue Assets

The following table shows the most relevant child asset types of Issue Assets.

Asset type	Description
Security Issue	A security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Security issues can involve financial information, such as credit card or bank details; Personal Health Information (PHI); Personally Identifiable Information (PII); corporate trade secrets or intellectual property. Most security issues involve overexposed and vulnerable unstructured data, such as files, documents and sensitive information.
Review Request	Asset that groups all triggers that ask for a review or update to another asset

Purpose and Legal Basis assets

To give context to the concepts of purposes and legal bases, we can say that an organization performs business processes for specific purposes, with lawfulness determined by certain legal bases.



Purpose assets

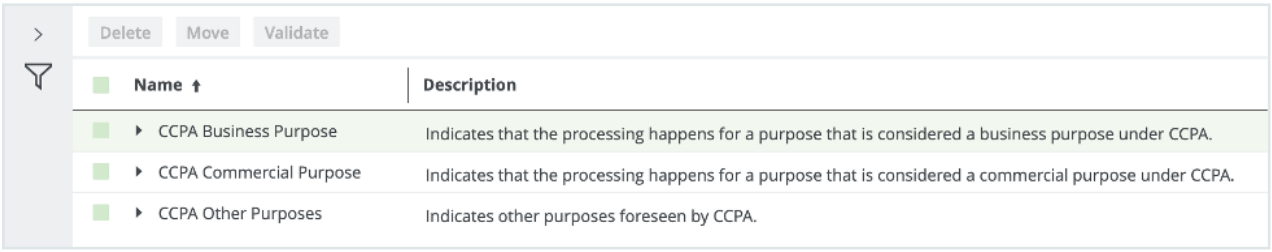
Purpose assets describe the reasons for which other assets are created or for which other assets exist, for example:

- Business purpose – The use of personal information for a business' or a service provider's operational purposes. Business purposes include:

    - Auditing.
    - Detecting security incidents.
    - Debugging.
    - Short-term transient use.
    - Performing services, for example customer service, order fulfillment or processing payments.
    - Internal research for technological development, maintaining quality or safety of a device or service.
- Commercial purpose – To advance a person's commercial or economic interests, enabling or effecting, either directly or indirectly, a commercial transaction.

There are important legal implications for Purpose assets. For example, the definition of a Purpose asset might forbid you from accommodating a data subject's right to be forgotten.

The following image shows an example list of Purpose assets.



> Note The Purpose assets you create will be available for selection when requesting access to data sets, during data shopping.

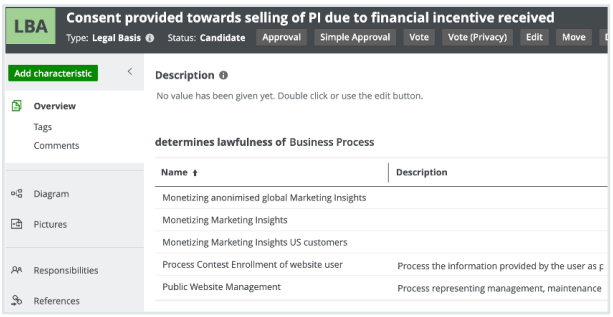
> Warning
> - Upon the request of a data subject, you must communicate the relevant purpose for using the data subject's personal information.
> - You cannot use a data subject's personal information for any purposes other than that for which the personal information is collected.

Legal Basis assets

Legal Basis assets describe the lawfulness of business processes that produce and consume personal information. Personal information can be processed only if, and to the extent that, at least one legal basis applies.

The Legal Basis asset type has the following attributes and relations in the global assignment:

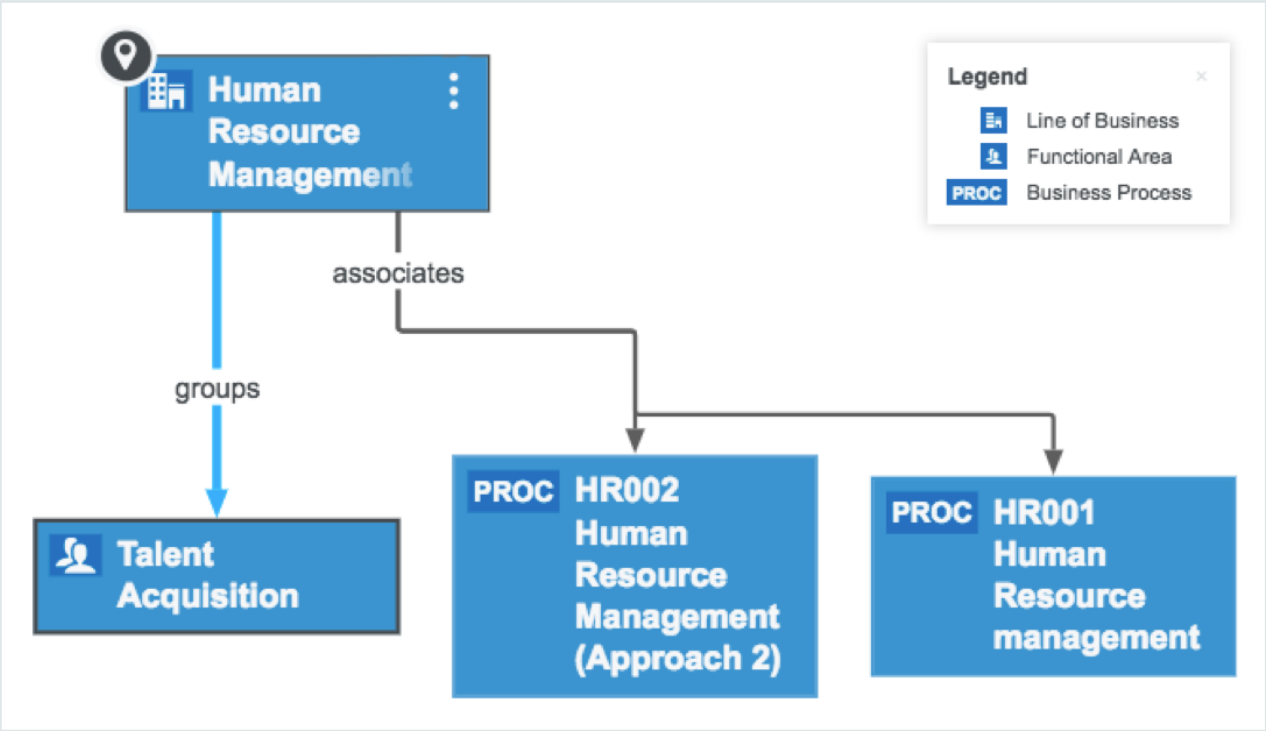
- Description.
- Note.
- Legal Basis determines lawfulness of Business Process.
- Legal Basis complies to / applies to Governance Asset.



Line of Business asset type

The Line of Business asset type helps you document your business units or business areas that serve a particular business need.

The following image shows an example of how the Line of Business asset Human Resource Management is related to Business Process assets for which it is responsible.



Tip We recommend that you first onboard the various lines of business, and then question the relevant stakeholders to map the lines of business to the business processes they follow. This helps to ensure completeness of the process register.

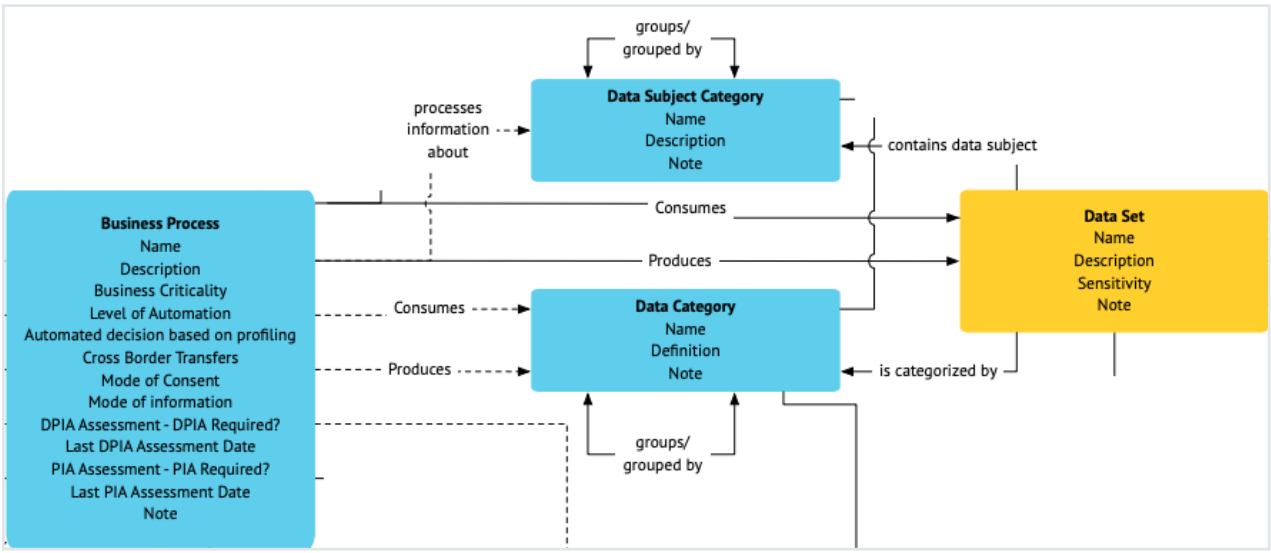
Data Categories

Data Categories allow Privacy Stewards to classify data, specifically as it concerns its level of sensitivity, value and criticality. They help determine privacy and security controls for the protection of the data.

Asset type	Description
Data Category	A classification of personal data elements that is managed by the Privacy team. Examples: • Biometric data • Financial data • Payment card information

Data categories are important, as they can determine the need for compliance with a specific regulation. For example, a data category that identifies personal health information would be exempt from CCPA because such information is covered under HIPAA.

> Note The Collibra Data Privacy custom asset pages require relations between the relevant Data Set and Data Category assets.



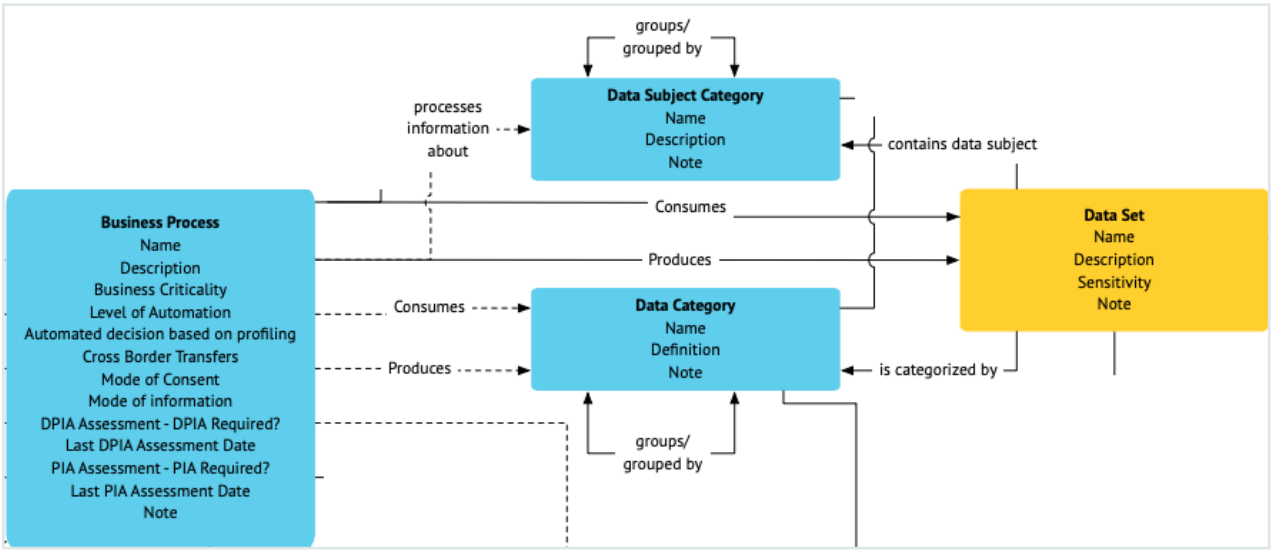
Data Subject Category

Asset type	Description
Data Subject Category	A classification of data subjects relevant to an organization. Can be used to categorize business-specific and regulation-specific categories. Examples: • Employees • Customers • Suppliers

Data subject categories are important, as they can determine the need for compliance with a specific regulation. For example:

- A data subject category that identifies employees would be exempt from CCPA until Jan 2021.

> Note The Collibra Data Privacy custom asset pages require relations between the relevant:
>
> - Data Set and Data Subject Category assets.



Regulation asset type and assets

Collibra Data Privacy comes with two Regulation assets:

- CCPA
- GDPR

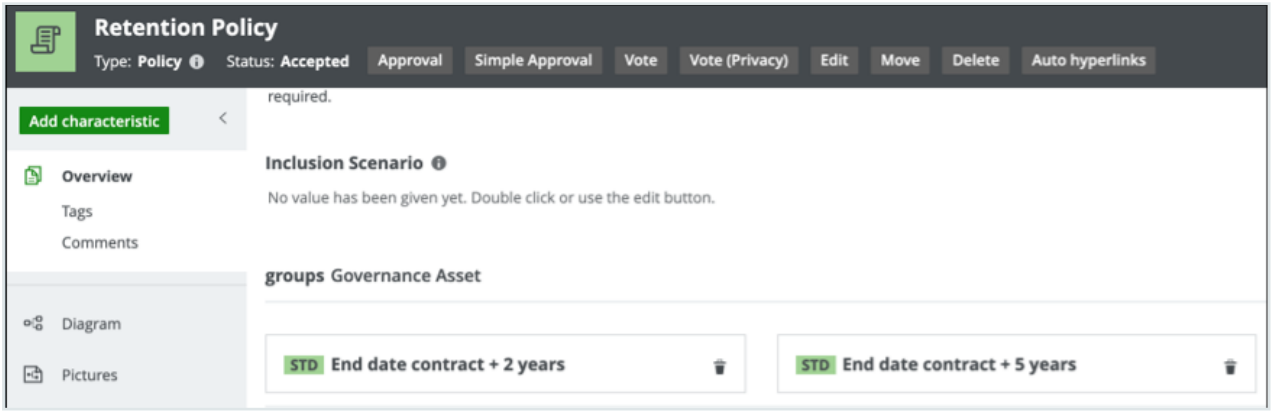
These assets are related to other assets, to fulfill the requirements of packaged custom asset pages. For example, every Business Process asset should be related to one or both of the assets, CCPA and GDPR, to allow the relevant custom Business Process asset page to be shown.

> Warning For these reasons, it is important that you not delete the Regulation assets CCPA and GDPR.

Retention policies

Retention policies are Standard assets that determine how long you can retain different types of data. When a specific retention period expires, the relevant information must be deleted.

> Note The packaged retention policies are merely examples. Determine the retention periods that apply to the data across your organization and create Standards



Safeguards

Safeguards are data protection guarantees for cross-border transfers of personal data. They are intended to guarantee the protection of personal data sent to recipients in countries for which data protection regulations are deemed inadequate.

You can use the Safeguard asset type to represent your safeguards.

When onboarding business processes, you can create relations between your safeguards and the relevant business processes that involve cross-border transfers of personal data.

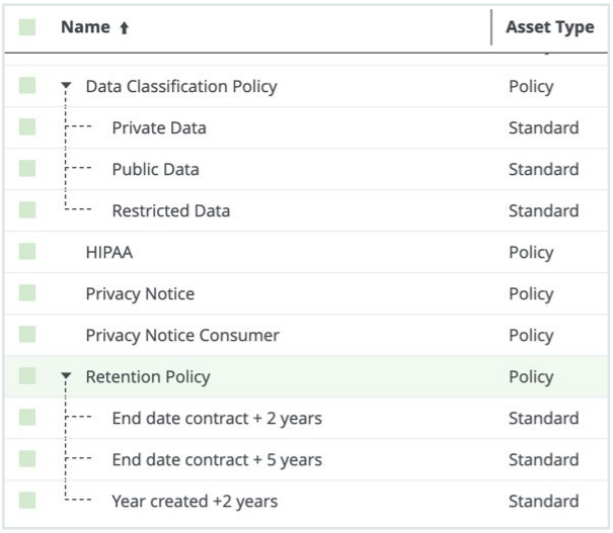
> Tip Review the packaged Sample safeguard register domain.
>
> 1. Review the packaged Sample safeguard register domain.
> 2. In the global assignment of the Safeguard asset type, ensure that the configured attributes meet your needs.
> 3. Create new Safeguard assets, as necessary.

Standards

Standards classify data based on their level of sensitivity and organizational impact, were the data disclosed, altered or destroyed without authorization. They are mandatory actions or rules that help to enforce and support policies.

Examples:

- Public
  You might use such a standard to classify your least sensitive data.
- Private
- Restricted
  You might use such a standard to classify your most sensitive data.



Key relationships

Head	Asset type assigned as head	Role	Co-role	Tail	Asset type assigned as tail
Governance Asset	Policy	groups	is included in	Governance Asset	Standard

Head	Asset type assigned as head	Role	Co-role	Tail	Asset type assigned as tail
Governance Asset	Standard	applies to	complies to	Governance Asset	Data Quality Dimension

Jurisidiction

Jurisdiction assets provide a hierarchical representation of how an organization divides its market on the basis of geography, such as regions and countries. For example, USA and Canada can be jurisdictions located in the jurisdiction North America.

Jurisdiction assets are important for identifying:

- The flow of personal data.
- Local privacy regulations.
- Where:
  - Technology assets are hosted.
  - Personal data is hosted.
  - Personal data is processed, as defined by a data sharing agreement.
  - Data subjects affected by security issues reside.

> Tip The packaged domain "Countries and states" includes Jurisdiction assets for the countries of the world, the 50 United States and more.

Processing Categories

Processing category assets categorize data processing activities according to the actions taken during the process.

Examples:

- Retrieval
- Storage

- Erasure or destruction
- Archiving

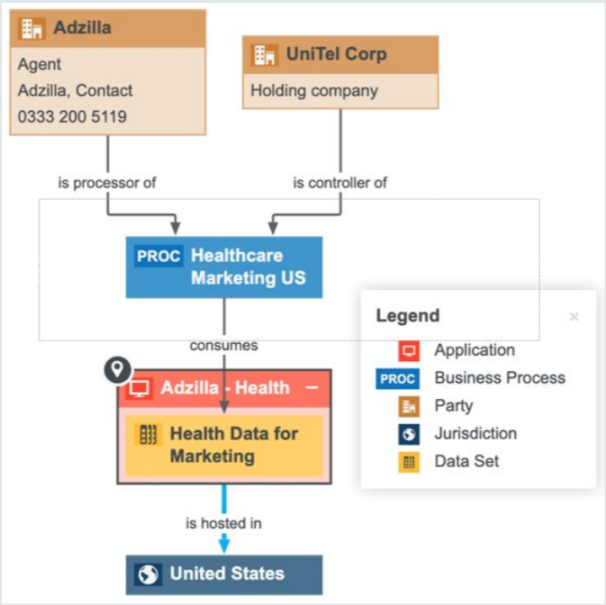
Keep in mind the following important points when considering Processing Category assets:

- For business processes that rely on data subject consent as the legal basis for processing personal data, consent must be obtained at the moment the data is collected or recorded.
- Processing categories must align with the specified purposes for processing personal data. For example, if your purpose for carrying out a business process is to sell personal information, the related processing category must be Disclosure or Dissemination.
- Processing categories represent the different processes deployed in the lifecycle of data. As such, they also play a role in pure data lifecycle management and risk management.
- Risk and privacy regulations do not apply to all processing categories in the same way. For example, GDPR applies differently to data archiving processes.

Applications and key mappings

It's important to maintain an inventory of the applications, across your organization, that consume and produce data. With a complete application inventory, you can map your applications to the personal data consumed and processed by each application, and set the security level for each application. With additional mapping, you can identify:

- In which Technology Assets your personal data resides, and the security level of these assets.
- By which applications your personal data is being consumed and produced.
- In which jurisdiction your personal data is being hosted.
- Which risks and security issues could impact your applications.



Tip

1. Identify the applications across your organization that consume or produce personal information.
2. Create new Application assets as necessary.
3. Analyze the packaged attributes configured in the global assignment for the Application asset type, and add any attributes you might want.

> Note Be sure to add the Security Level attribute to the Technology Asset global assignment. This attribute is essential for identifying the security level of the Technology Assets that host personal data and the Application assets that consume or produce personal information, those that could be potentially impacted by risks, and so on.

Privacy and data classification policies

To fill out your personal information assets with the necessary relations and attributes, your Privacy team has to first create a data classification policy and related standards, data categories and data attributes. Your Governance team can then map these privacy policy-defining assets to the physical data layer, meaning your System, Table and Column assets, to inherit the sensitivity characteristics, as defined by your Privacy team.

The following table describes the four privacy policy-defining asset types that are the focus of your Privacy team.

Asset type	
Policy	A statement of intent that is set by a council and is implemented by a set of standards. In this context, the policy determines how personal information across the organization is classified. Helps an organization determine the minimum privacy and risk controls, to mitigate privacy risk.
Standard	Standards classify data based on their level of sensitivity and organizational impact, were the data disclosed, altered or destroyed without authorization. They are mandatory actions or rules that help to enforce and support policies. Examples: • Public You might use such a standard to classify your least sensitive data. • Private • Restricted You might use such a standard to classify your most sensitive data.
Data Category	A classification of personal data elements that is managed by the Privacy team. Examples: • Biometric data • Financial data • Payment card information

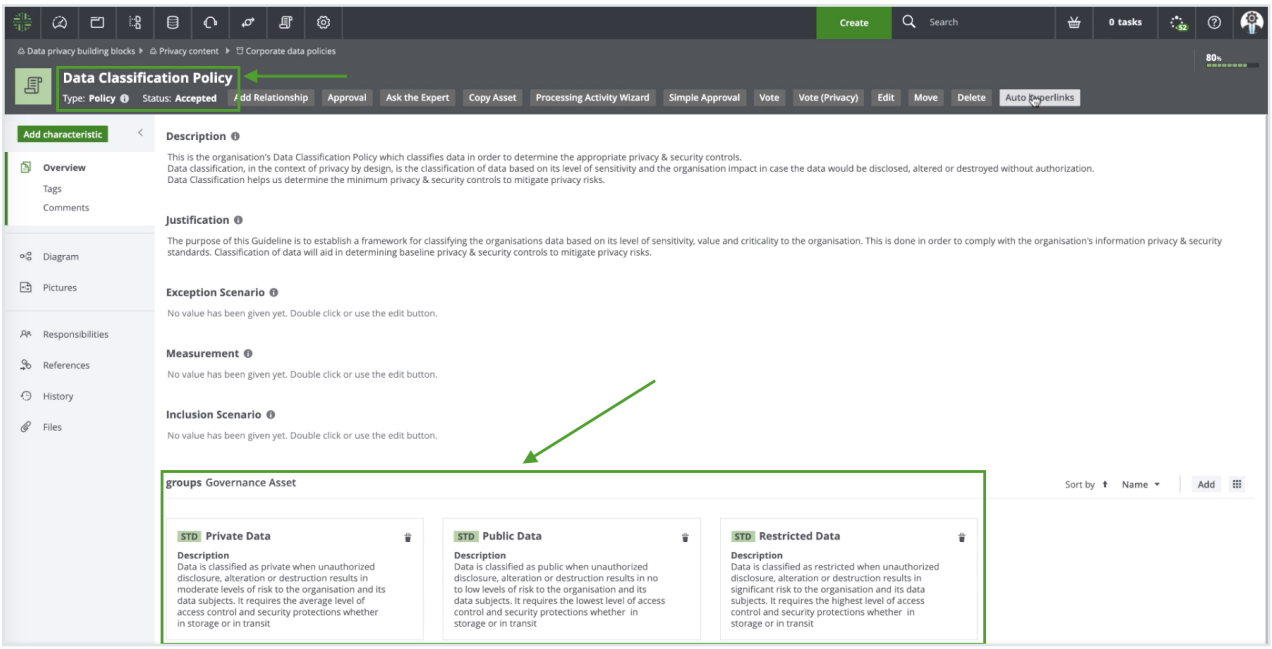
Asset type	
Data Attribute	A specification that defines a property of a data asset. For example, the data category Payment Card Information might contain, in part, the following data attributes: • Credit card number • Cardholder name • Security code.

Example lineage of a data classification policy and related standards, data categories and data attributes

Let's suppose your Privacy team has decided to distinguish all data across the organization with one of three "labels", or standards, based on different levels of sensitivity.

With such decisions made, a Privacy Steward creates:

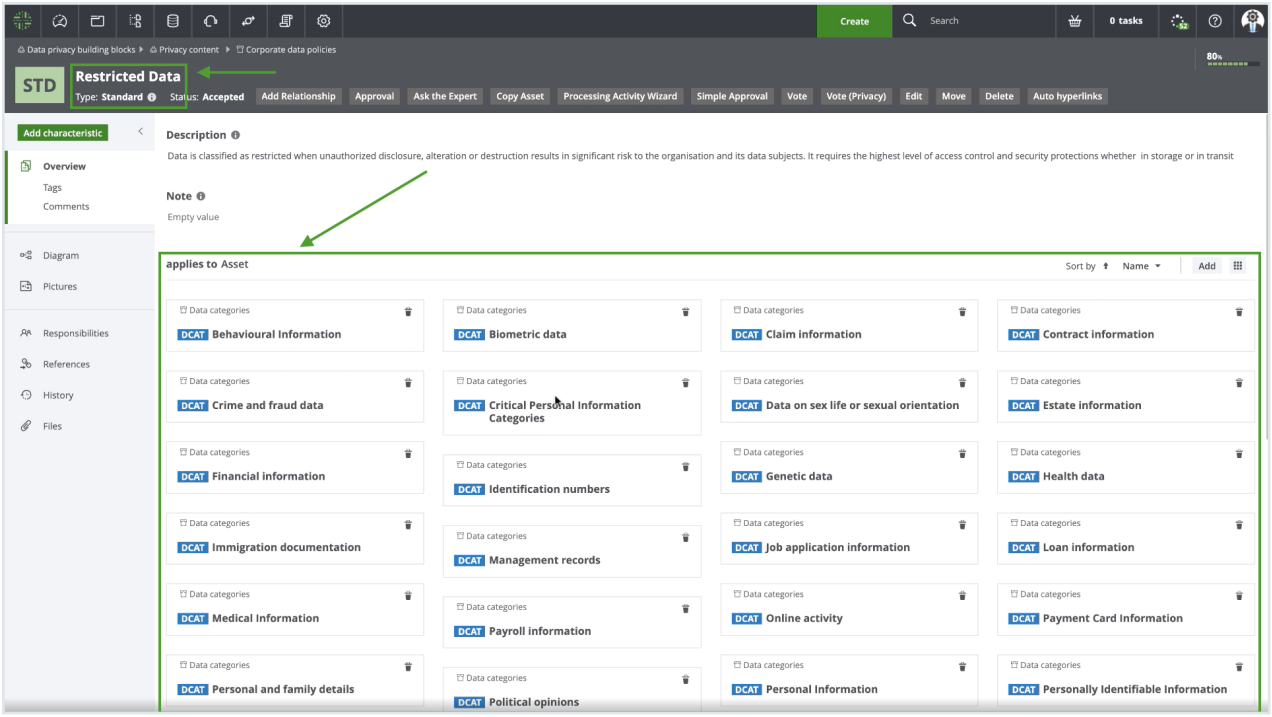
1. A Policy asset named Data Classification Policy, to fully describe all such decisions and details.
2. Three Standard assets; one named Public, to distinguish your least sensitive data; one named Private; and one named Restricted, to distinguish your most sensitive data.
3. A relation that groups the three Standard assets under the Data Classification Policy asset.



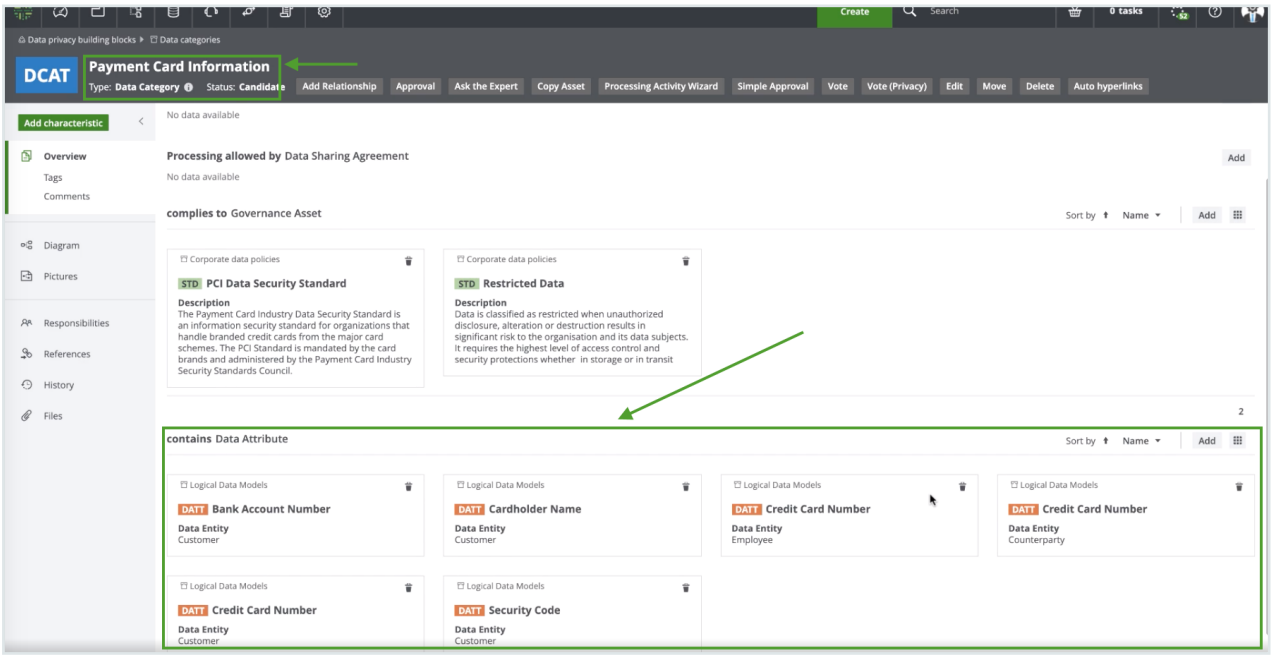
The Privacy steward then creates:

- Data Category assets, which help you to segregate all data across your organization according to subject matter.
- Relations, such that one of the Standards applies to each of the Data Category assets.

The following image shows which data categories have been deemed restricted.



Each Data Category asset, for example Payment Card Information, contains data attributes that are specific to payment card information, for example Cardholder Name and Credit Card Number. The following image shows the relations between the Data Category asset and the Data Attribute assets.



The Governance team can then map these privacy policy-defining assets to the physical data layer, meaning your systems, tables and columns.

Security attribute for System assets

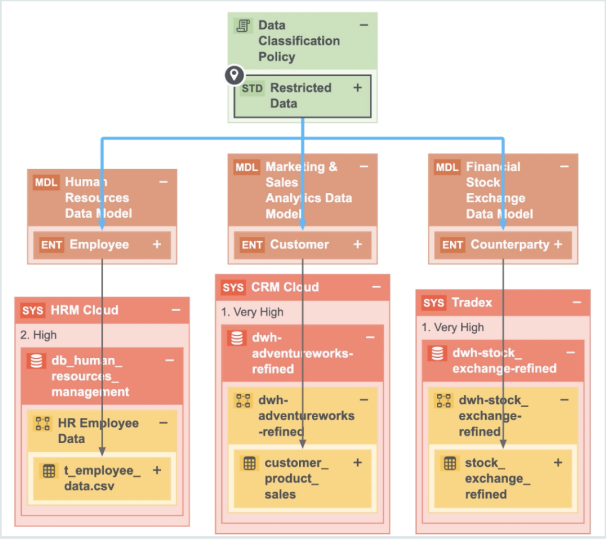
Your Governance team will map your Table assets and Column assets to the System assets that produce and consume data, so that you can quickly see in which systems PI is being used. Your InfoSec Stewards can add a security level attribute to the System assets, so that you can see whether or not your systems have the required level of security (this is an attribute of the system asset).

View a diagram of the mapping

The following image shows an example lineage diagram after mapping privacy policy-defining assets to the physical data layer.

Here we can identify:

- All the systems in which restricted data is stored, specifically HRM Cloud, CRM Cloud and Tradex.
- Whose restricted data is being stored, specifically Employee, Customer and Counterparty data.
- The security level of each system, for example "Very High" for the System assets CRM Cloud and Tradex.



Discovery

Discover and capture information related to personal information, business processes, third-parties, data sharing agreements and contracts.

Personal information discovery

To protect your personal information, you first need to identify it and appropriately classify it.

It is important to know:

- Where your data is stored.
  This is critical to helping you respond to individual rights requests, such as a request "to be forgotten". To respond appropriately, you need to be able to quickly know where personal information exists across your organization.
- Why you're storing the data, meaning the business and legal context.
  Generally speaking, you should not store data that is not critical to your business processes. However, some personal information needs to be kept to comply with legal obligations. Consider, for example, an individual's request to be forgotten. With this request, the individual's personal information will have to be deleted from most systems, but it can't be deleted if it is needed to comply with a legal obligation.

> Tip Follow our course Discover Your Sensitive Personal Information, on Collibra University.

How does Collibra Data Intelligence Cloud help you discover your personal information?

Your Privacy team first has to create a data class policy and standards, data categories and data attributes. Your Governance team then takes over, mapping these privacy policy-defining assets to your personal information assets, thereby endowing them with all the required attributes and relations. This mapping is aided greatly by Automatic Data Classification. Collibra Data Privacy is integrated with Catalog, allowing you to leverage Catalog's Automatic Data Classification capabilities to discover and classify your personal information.

Furthermore, after classifying a single column from a table, you can then simultaneous associate that column and all the other columns in the table with a particular data domain. This is made possible by Guided Stewardship.

> Tip For the discovery of business processes, see the The Business User Interface, a user-friendly webpage that allows users to start describing their business processes and related data.

Privacy and data classification policies

To fill out your personal information assets with the necessary relations and attributes, your Privacy team has to first create a data classification policy and related standards, data categories and data attributes. Your Governance team can then map these privacy policy-defining assets to the physical data layer, meaning your System, Table and Column assets, to inherit the sensitivity characteristics, as defined by your Privacy team.

The following table describes the four privacy policy-defining asset types that are the focus of your Privacy team.

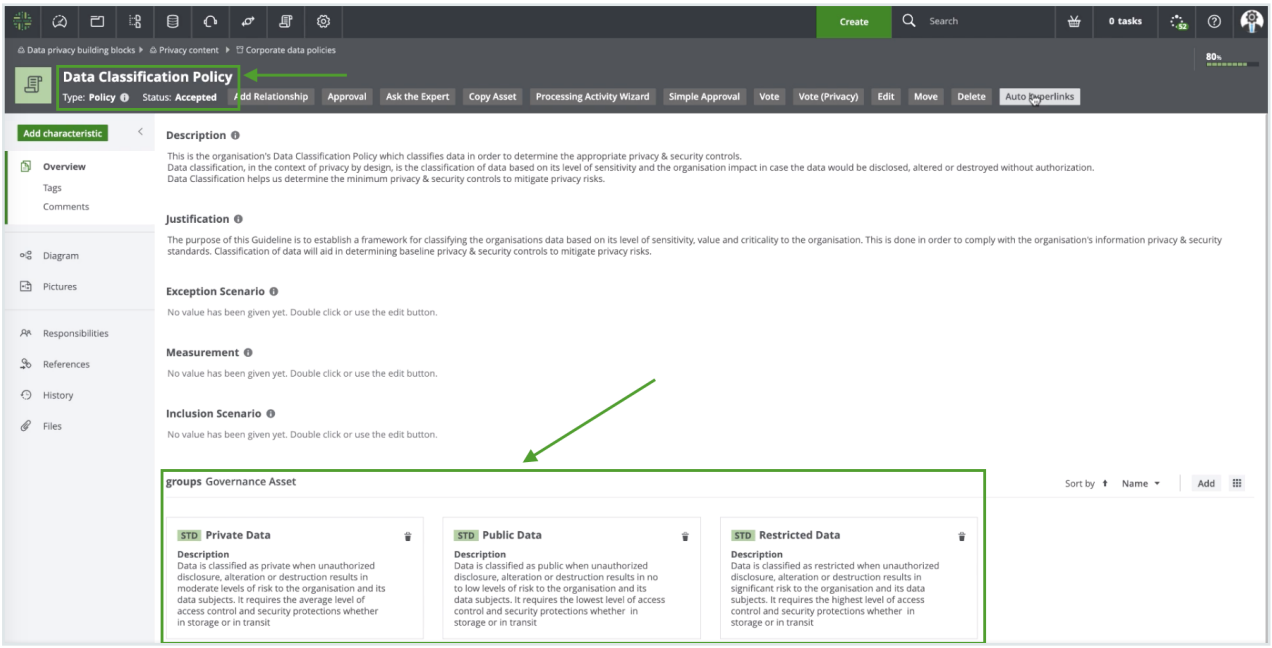
Asset type	
Policy	A statement of intent that is set by a council and is implemented by a set of standards. In this context, the policy determines how personal information across the organization is classified. Helps an organization determine the minimum privacy and risk controls, to mitigate privacy risk.
Standard	Standards classify data based on their level of sensitivity and organizational impact, were the data disclosed, altered or destroyed without authorization. They are mandatory actions or rules that help to enforce and support policies. Examples: • Public You might use such a standard to classify your least sensitive data. • Private • Restricted You might use such a standard to classify your most sensitive data.
Data Category	A classification of personal data elements that is managed by the Privacy team. Examples: • Biometric data • Financial data • Payment card information
Data Attribute	A specification that defines a property of a data asset. For example, the data category Payment Card Information might contain, in part, the following data attributes: • Credit card number • Cardholder name • Security code.

Example lineage of a data classification policy and related standards, data categories and data attributes

Let's suppose your Privacy team has decided to distinguish all data across the organization with one of three "labels", or standards, based on different levels of sensitivity.

With such decisions made, a Privacy Steward creates:

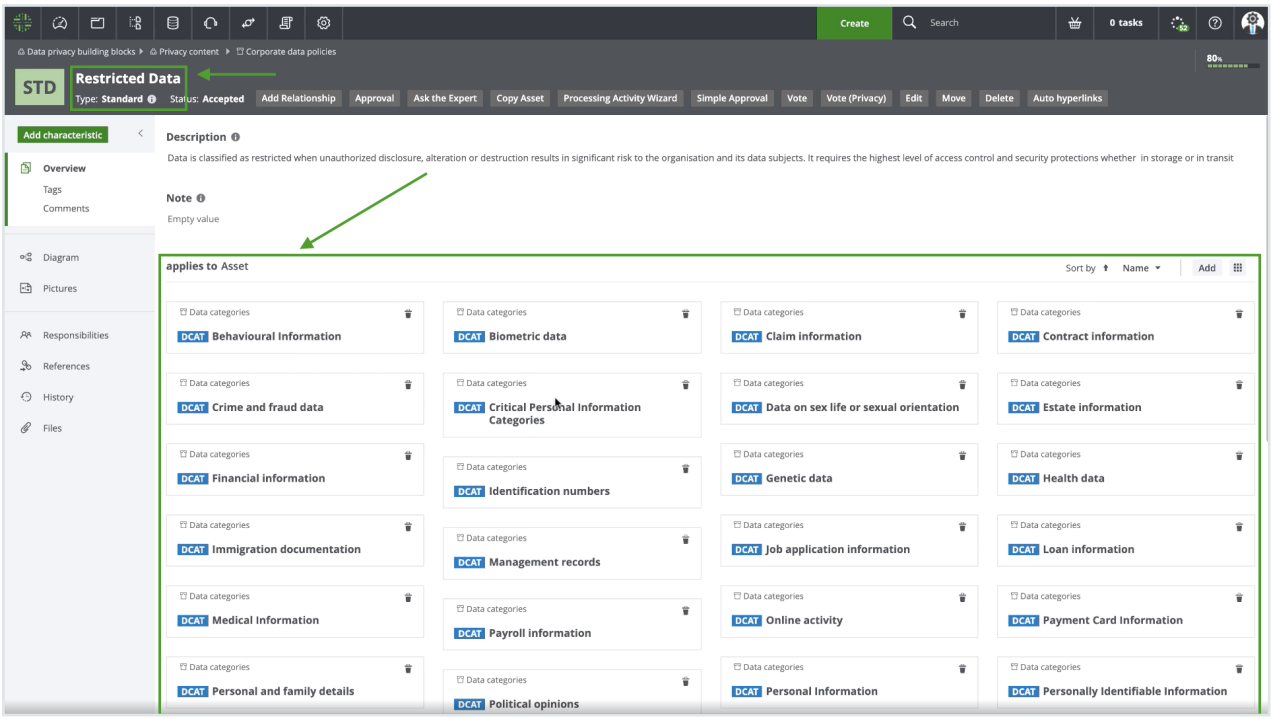
1. A Policy asset named Data Classification Policy, to fully describe all such decisions and details.
2. Three Standard assets; one named Public, to distinguish your least sensitive data; one named Private; and one named Restricted, to distinguish your most sensitive data.
3. A relation that groups the three Standard assets under the Data Classification Policy asset.



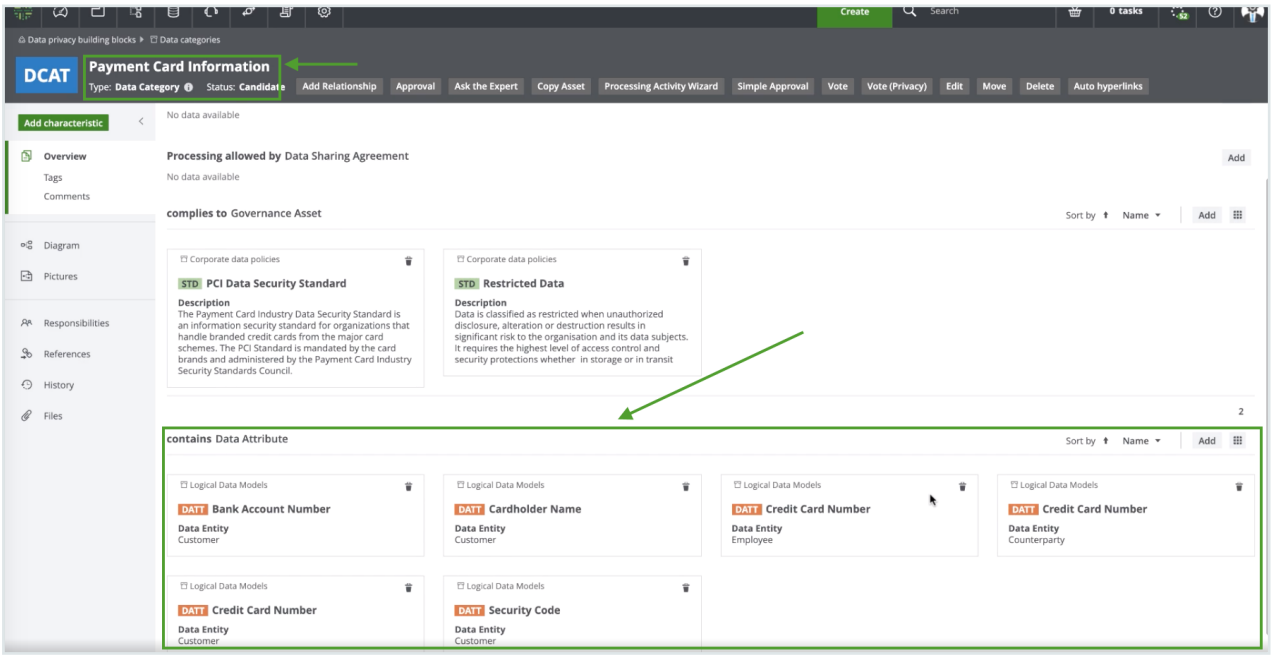
The Privacy steward then creates:

- Data Category assets, which help you to segregate all data across your organization according to subject matter.
- Relations, such that one of the Standards applies to each of the Data Category assets.

The following image shows which data categories have been deemed restricted.



Each Data Category asset, for example Payment Card Information, contains data attributes that are specific to payment card information, for example Cardholder Name and Credit Card Number. The following image shows the relations between the Data Category asset and the Data Attribute assets.



The Governance team can then map these privacy policy-defining assets to the physical data layer, meaning your systems, tables and columns.

Security attribute for System assets

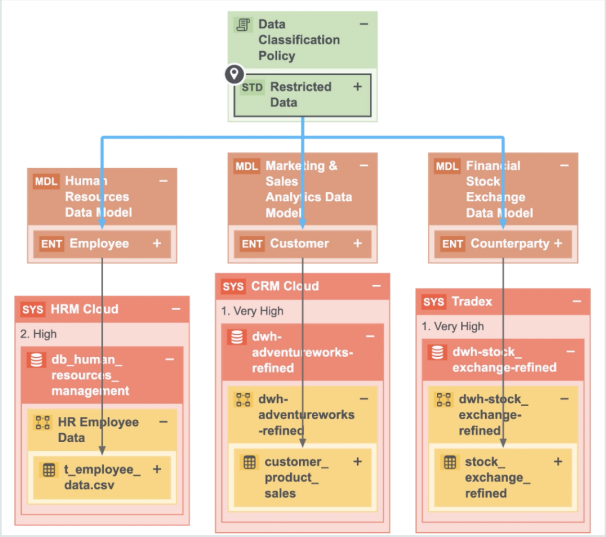
Your Governance team will map your Table assets and Column assets to the System assets that produce and consume data, so that you can quickly see in which systems PI is being used. Your InfoSec Stewards can add a security level attribute to the System assets, so that you can see whether or not your systems have the required level of security (this is an attribute of the system asset).

View a diagram of the mapping

The following image shows an example lineage diagram after mapping privacy policy-defining assets to the physical data layer.

Here we can identify:

- All the systems in which restricted data is stored, specifically HRM Cloud, CRM Cloud and Tradex.
- Whose restricted data is being stored, specifically Employee, Customer and Counterparty data.
- The security level of each system, for example "Very High" for the System assets CRM Cloud and Tradex.



Automatic Data Classification for discovery

When you register a data source in Collibra Data Intelligence Cloud, the process doesn't stop at ingestion. In order to unlock the full potential of Collibra, the data needs to be contextualized: it needs to be classified and connected to other nodes in the Data Intelligence knowledge graph. Automatic Data Classification adds context to your data.

For complete information, see About data classification.

Business process discovery

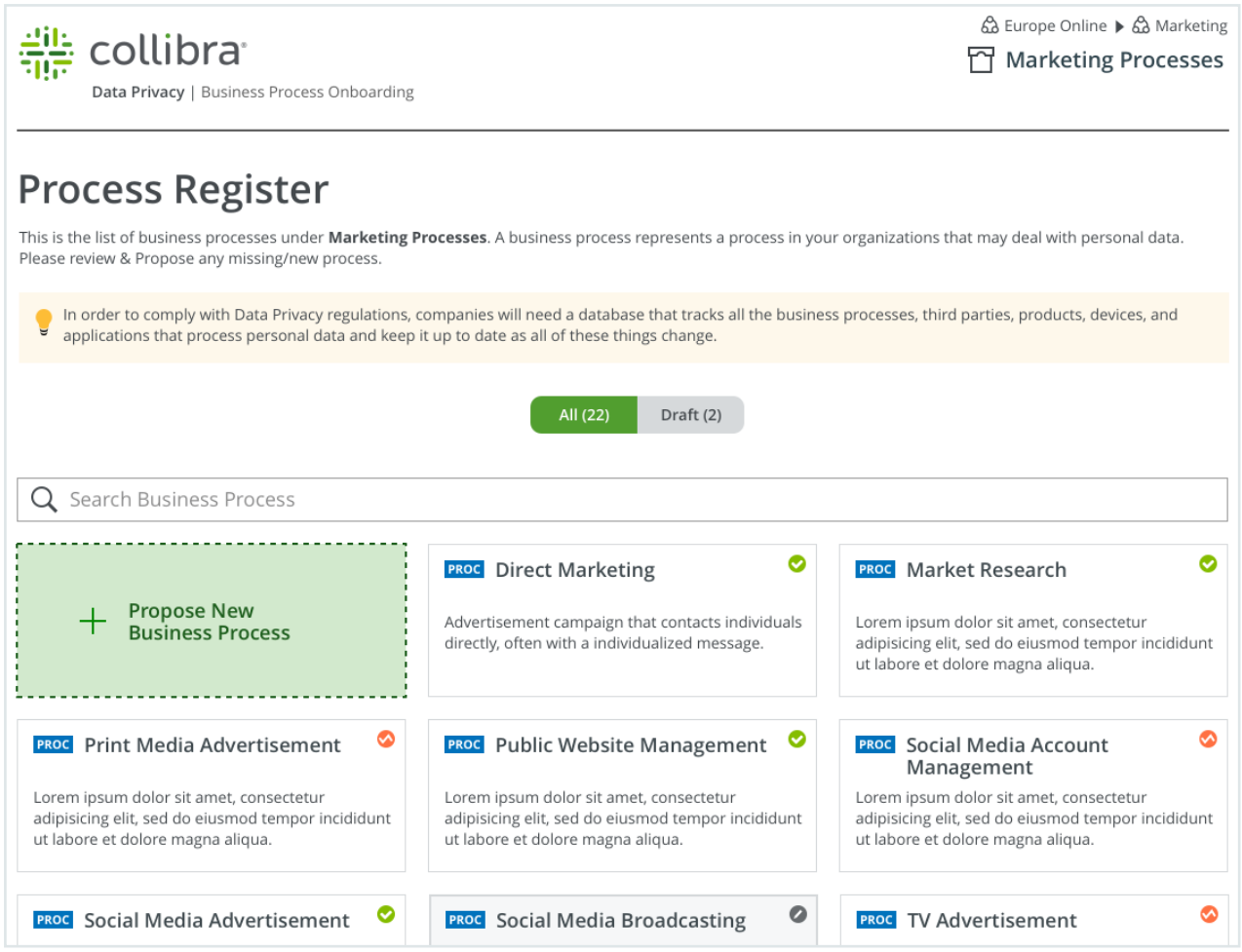
Business process discovery helps you to:

- Identify and capture your business processes that produce or consume personal information.
- Maintain complete Process Register domains.

Business process discovery is aided by the Business User Interface, a user-friendly webpage that allows users to start describing their business processes and related data.

The Business User Interface

The Business User Interface is a webpage that shows all of the Business Process assets in a domain. It's an easy way for users that might not be familiar with the technical details of your privacy and risk program or Collibra Data Intelligence Cloud, to start describing their business processes and related data.



> Note This webpage is not part of the Collibra interface, but it is associated with the Collibra environment from which the invitation email was sent. If the email recipient is not signed in to Collibra when clicking the link in the email, the user will be prompted to sign in, to access the webpage.

Accessing the Business User Interface

You can access the Business User Interface via:

- The **Go to the Business User Interface** button, which can be found on every Process Register domain page.
- The button in a Request input email invitation, if you were the recipient of such an email.

Proposing a New Business Process asset

Via the Business User Interface, users can open any of the Business Process assets in the domain and review the characteristics. The main objective, however, is to identify and propose any missing business processes relevant to that domain.

When a user clicks **Propose New Business Process**:

- A new webpage opens and the user can start specifying details relative to the process.
- A new Business Process asset is created in the domain.

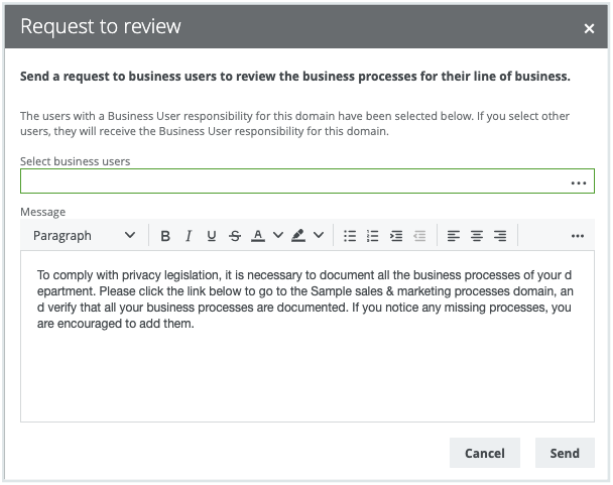
When the user has specified all the details and clicks **Submit**, a task is sent to the Owner for the domain, and the acceptance ownership step begins, followed by the remaining steps of the asset onboarding process.

> Tip This workflow is intended to encourage business users who might not be familiar with the technical requirements of a privacy and risk program or Collibra to propose new Business Process assets. Users who propose new assets are not required to complete all fields in the workflow. In fact, none of the fields are mandatory. The Business Steward, Data Steward and Privacy Steward will be called on to complete the required details, in the characteristics management phase.

Requesting input to a Process Register domain

As the Business Steward, Privacy Steward or Data Protection Officer for a Process Register domain, you can invite business users to participate in the development of the domain, by reviewing any existing Business Process assets in the domain and proposing any business processes that do not yet exist as assets.

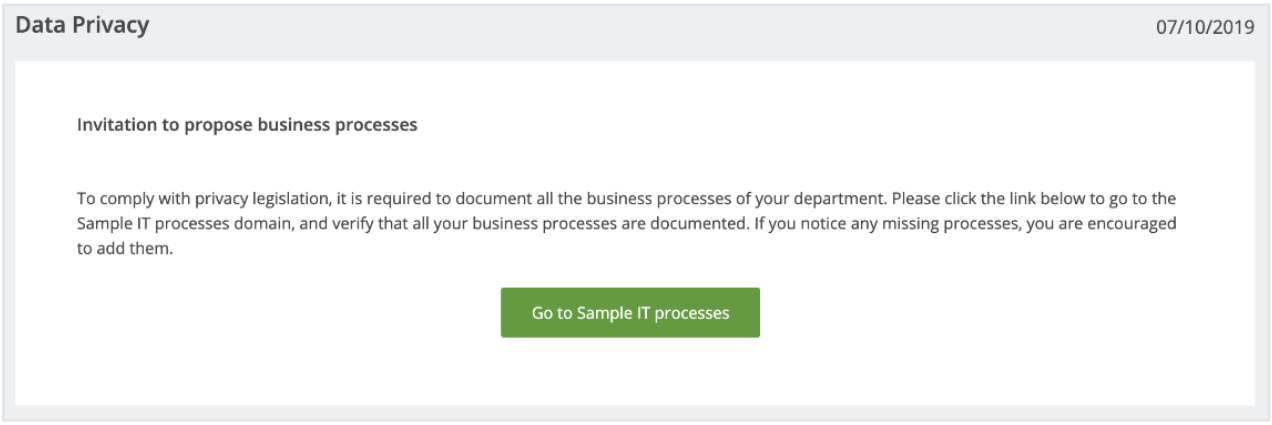
The **Request input** button, which is available in every Process Register domain, triggers the Invite to Business Process Register workflow. The workflow includes a form that can be used to write an invitation email and select recipients.



The form contains:

- A default set of email recipients, which is all the users that have the Subject Matter Expert responsibility for the domain.
- A default message, which you can edit and format as you like.

The following image shows an example of an invitation email:



The button in the invitation email leads to the Business User Interface, a webpage that shows all of the Business Process assets in the domain.

> Tip You can also access the Business User Interface directly via any Process Register domain, by clicking the **Business User Interface** button.

Request input

You can send an email to specified users, requesting their participation in the development of a Process Register domain.

Steps

1. Go to the relevant Process Register domain page.
2. Click **Request input**.
   » The Invite to Business Process Register workflow is started.
3. In the sidebar, enter the required information.

Field	Description
Select business users	The users to whom you want to send the email invitation.
Message	The body text of the email. You can leave the default text as it is or edit it to suit your needs.

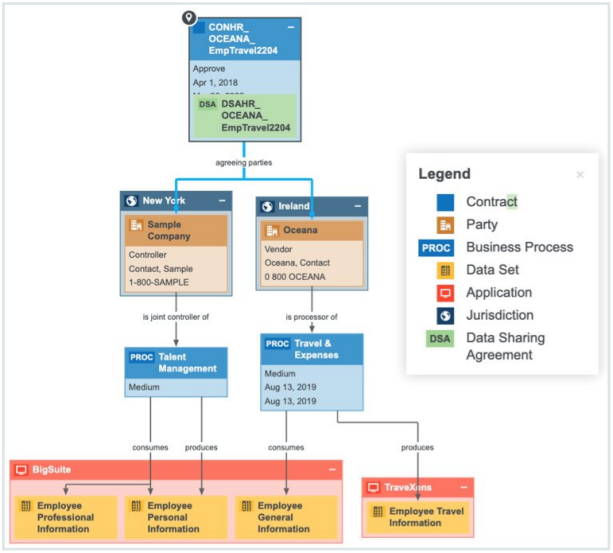
4. Click **Send**.
   » The email invitation is sent to all recipients.

Third-party register

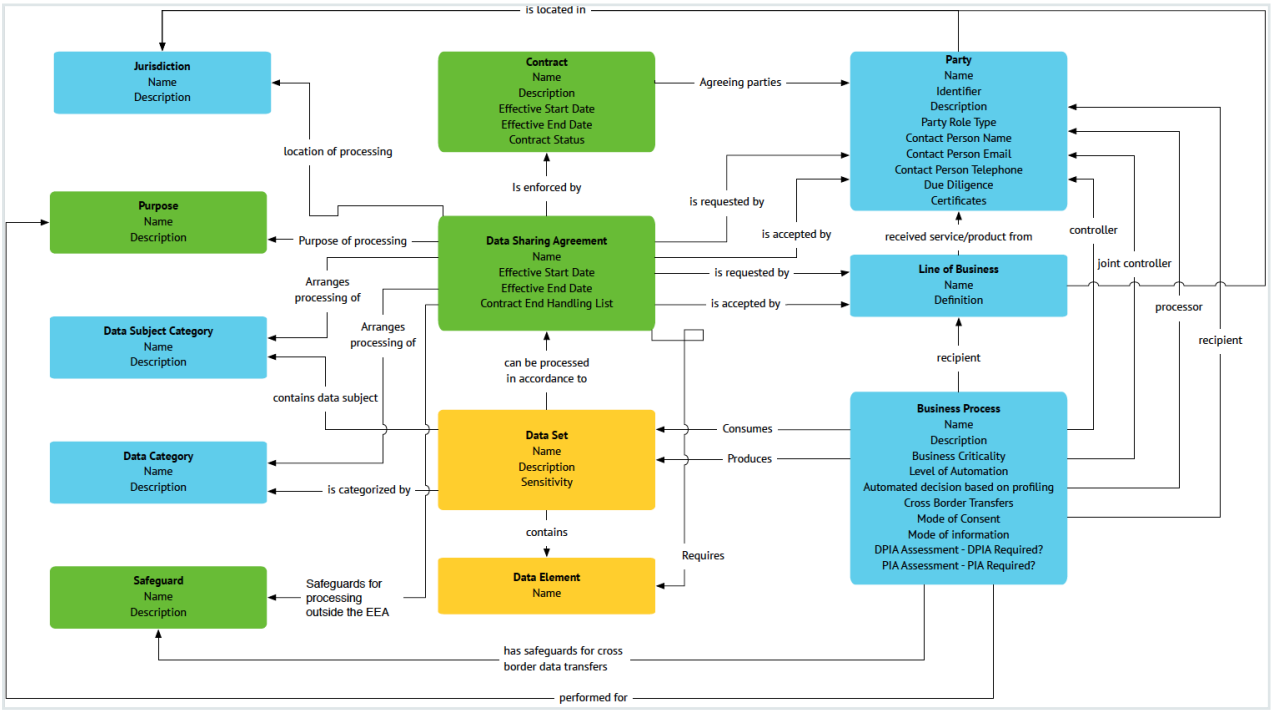
With an increasing number of personal data breaches traced back to third-parties, organizations are urged to implement or strengthen their privacy programs with regard to their vendor relationships. By mapping your business processes to your vendor management life cycle, you can begin to build a program that protects your data, customers, and reputation from risks introduced by third-parties.

We recommend that you create a third-party register domain, to store all the third-party privacy profiles specific to the community.

> Note In Collibra Data Privacy, all your third-parties are represented by Party assets. These Party assets are distinguished, in part, by the attribute Party Role Type. Example packaged Party Role Types include Business Partner, Controller, Distributor, Processor, Reseller and Subsidiary.



Asset model



Third-Party Privacy Profile

The Third-Party Privacy Profile enables you to:

- Create a profile record that includes relevant privacy information about your third-parties.
- Organize all the necessary information about the third-party, be it a vendor, supplier or other, in a single record, to provide the Data Protection Officer relevant third-party information, such as the contract in place, terms and conditions, data that is being shared, risk profile and more.

The information contained in the Third-Party Privacy Profile should help answer the following questions:

- What services does the third-party provide?
- How essential are these services to your organization?
- What will be the duration of the relationship with this third-party?
- What kind of data will the third-party have access to? Will the third-party store any of this data, and if so, how much?
- To which internal systems and applications will the third-party require access?
- What would the business impact be if there was a breach or the data was compromised through a third-party breach?
- Can you use the answers to these questions to assign a vendor a risk score of high, medium, or low?

Building blocks

Third-Party Privacy Profiles are composed of five major building blocks, each aimed at documenting specific information about third-parties.

Building block	Description
General	Provides basic information about the third-party, such as the type (for example, a vendor, contractor or government organization), where the third-party is located and who the contact person is.

Building block	Description
Privacy	A due diligence, focused on privacy matters, to consider the third-party's reputation, experience, history of incidents, and corporate policies and procedures, particularly as they relate to data security and privacy.
Contract	Information on the legal agreement between the third-party and the organization, to understand what is in scope, when the contract begins and ends, what the status of the relationship is, and to which internal business the product or service is being provided.
Service	It's important to consider how each third-party will interact with your data. Will they be collecting, assessing, processing, transmitting, or storing your data? This information is provided here, including where it is hosted, what data agreements are in place, what type of private data is involved, and so forth. Such information helps your organization evaluate the potential privacy and security risks that could arise if you engage with the third-party.
Risk	Creating a comprehensive risk profile for each vendor allows you to determine the level of risk to your organization, by measuring the probability or likelihood of risk against the severity of the consequence. The Third-Party Privacy Profile can help your organization determine whether your third parties are low risk or high risk, so you have a system that enables you to prioritize vendor risk appropriately and develop a targeted strategy to address these risks.

Creating third-party profiles

There are two methods for the initial creation of third-party privacy profiles:

- Via the Collibra APIs that allow Collibra Data Privacy to communicate with your organization's applications, to retrieve information about your third-parties, for example your vendor management system. For complete information, contact your Collibra Professional Services representative.
- Via import, using the Microsoft Excel template available on the Collibra Downloads page.

The resulting assets are Party assets. After the assets are created, the Privacy Steward can edit them to include all necessary privacy information that is missing.

> Note Each of these methods is designed to help you with the initial creation of your third-party profiles. After the initial creation via API or import:
>
> - Any edits to these Party assets should be made by the Privacy Steward, directly via the relevant asset page.
> - Additional Party assets should be created via the global Create biutton.

Basic and Full import template

The Microsoft Excel template comes with two spreadsheets:

- A Basic spreadsheet, which enables you to import all your third-party general information. The Privacy Steward can then add the rest of the building block information after the assets are created.
- A Full spreadsheet, which allows you to map all the information about your third-parties in a single import file. This is useful if the information is maintained in various systems throughout your organization.

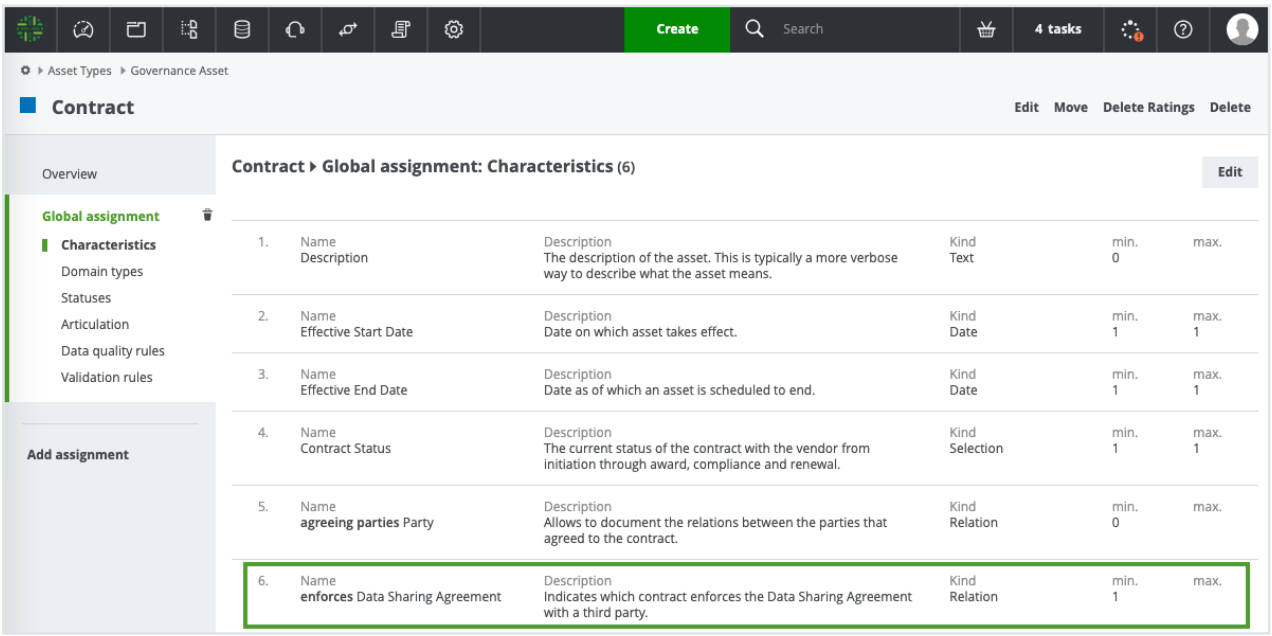
> Note The template is available on the Collibra Downloads page. You can use the same template for GDPR and CCPA.

Status evolution

Condition	The status of the asset...
When a third party profile is created by the API or import.	Is Candidate.
When the required information, as defined by the Privacy Office, is complete.	Becomes Approved.
When the business relation between your organization and the third-party has ended.	Becomes Obsolete.

Third-party contracts

Contract assets represent the contracts you have in place, and that govern the relationships you have, with your third-parties. The global assignment for the Contract asset type includes a relationship type that allows you to map your contracts to their relevant data sharing agreements.



Tip If you have contracts in place with your third-parties, but you haven't yet established data sharing agreements with them, you can:

1. Create Contract assets, to represent the contracts you have in place with your third-parties.
2. Create your new Data Sharing Agreement assets.
3. Map your Contract assets to the Data Sharing Assets that they enforce.

Third-Party Privacy Profile views

The packaged Third-Party Privacy Profile domain comes with two views:

- The Default view, which provides information about all the required attributes in the third-party privacy profile. This view is also used to import content for the first time.
- Third-Party Profile Privacy view, which shows key information about a third-party. There is a single record for each third-party, which includes all of the information about each building block.

Data sharing agreements and contracts

When a Controller engages the services of a Processor, the relationship and activities must be governed by a written contract. The contract is binding on the Processor, with regard to the Controller, and helps both parties understand their responsibilities and liabilities.

Warning Controllers are liable for their compliance with relevant laws and regulations. Furthermore, they must only appoint Processors that can provide sufficient guarantees that such legal requirements are met and the rights of data subjects protected. Processors are expressly obliged to comply with certain laws and can be fined or sanctioned for non-compliance.

Contractual obligations

The contract dictates, at a minimum, the following obligations toward the Processor:

- Act only on the written instructions of the Controller.
- Ensure that the people processing the data are subject to a duty of confidence.
- Take appropriate measures to ensure the security of processing.
- Engage sub-processors only with the prior consent of the Controller, and under a written contract.
- Assist the Controller in providing data subjects with access to their data and allowing data subjects to exercise their rights as defined by the relevant regulation.
- Assist the Controller in meeting its obligations in relation to:
    - The security of the business process.
    - The notification of personal data breaches.
    - Data protection impact assessments.
- Delete or return all personal data to the Controller, as requested, at the end of the contract.
- Submit to audits and inspections.
- Provide the Controller with any information it needs to ensure that both parties are meeting their respective obligations.
- Tell the Controller immediately if it is asked to do something that infringes upon the laws of the relevant jurisdiction.

Data Sharing Agreement workflow

The successful result of this workflow is an approved Data Sharing Agreement asset. Data Sharing Agreement assets are used to document the details of the contracts between Controllers and Processors.

The following attributes are essential to Data Sharing Agreement assets:

- The data processed.
- The data subject categories processed.
- The start date and end date of the contract.
- The location of processing.
- How data is handled at the end of the contract.
- The purpose of the processing.
- The safeguards in place for protecting the data in the case of cross-border transfers.

Relevant roles

Action	Role
Start the workflow.	Any user.
Review the asset.	Data Steward.
Approve or reject the asset.	The Owner for the domain in which the Data Sharing Agreement asset is created and stored.

Governance

Organize and govern your data with the help of:

- Workflows.
- Asset onboarding and change management processes.
- Reporting and process monitoring.

Process Register domains

The Process Register domain type enables you to create domains for:

- Storing your Business Process assets.
- Mapping your Business Process assets to the data consumed and produced by those processes.

Maintaining complete Process Register domains helps organizations to:

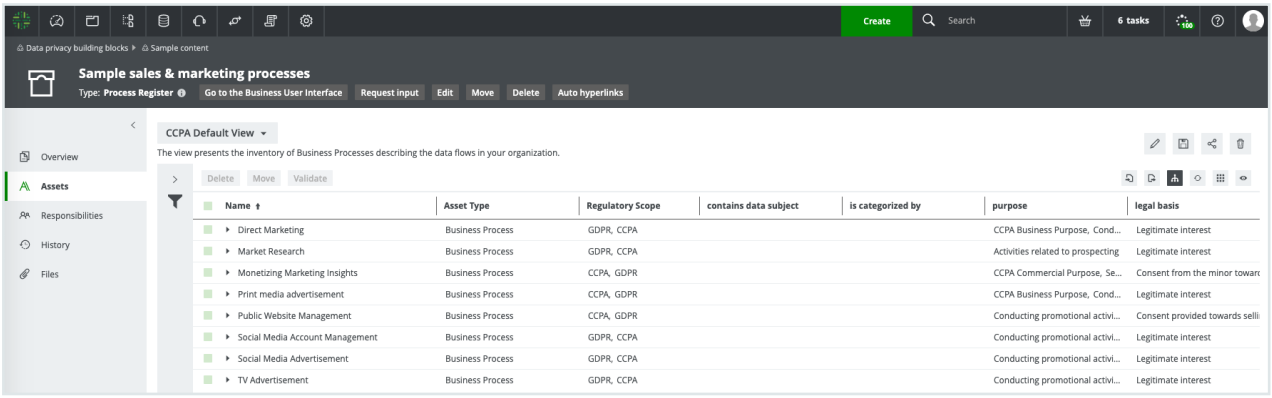
- Comply with data transparency requirements.
- Respond to consumer access requests and other consumer rights.
- Manage security and prevent data breaches.
- Manage Service Level Agreements with third parties.
- Leverage investments made to comply with a specific regulation, for other use cases, such as compliance with another data privacy regulation or data catalog use cases.

> Note As advised in the section Setting up your community-domain structure, we strongly recommend that you create a Process Register domain for each of your communities and subcommunities.

Default view

Process Register domains come with a default view that shows a hierarchy of:

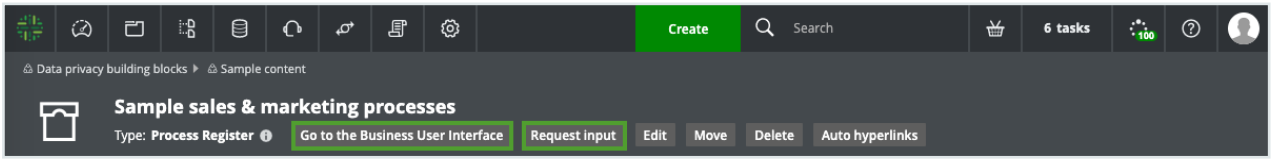
- Business Process assets.
- Data Set assets that are consumed or produced by these assets.



A collaborative hub for developing your assets

Process Register domains also serve as a hub from which to collaborate in the development of your Business Process assets. In every Process Register domain, there are two buttons that enable users to:

- Request input, to help develop the Process Register domain.
- Go to the Business User Interface, a user-friendly interface for working with a Process Register domain.



The Sample Process Register domains

Collibra Data Privacy comes with four packaged sample Process Register domains.

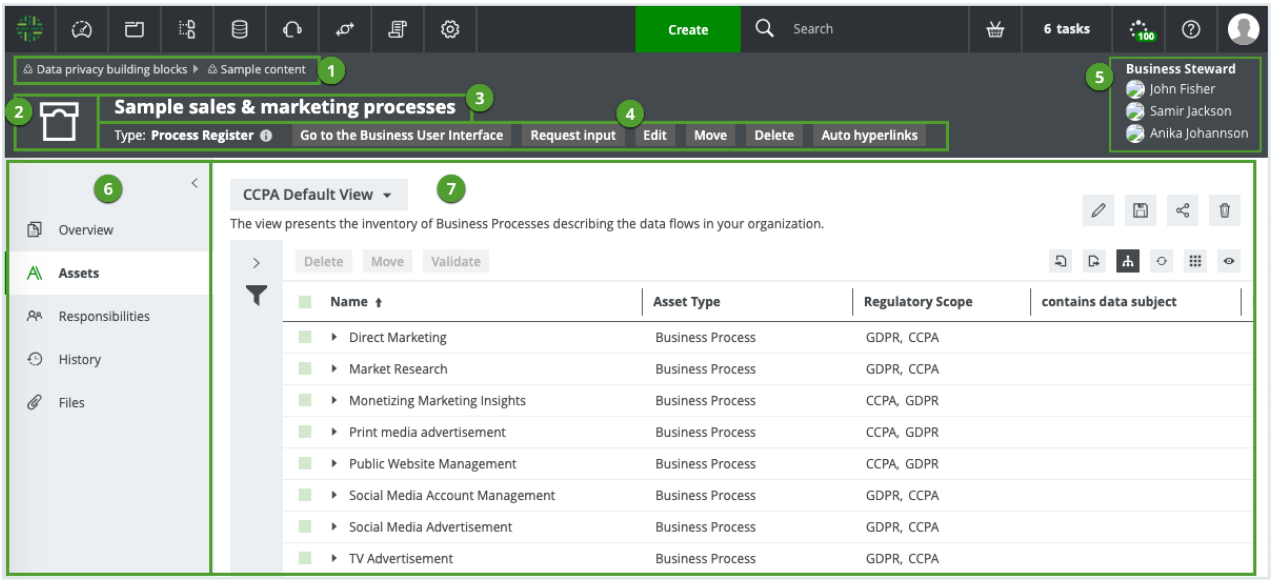
- Sample legal & audit processes
- Sample sales & marketing processes
- Sample information technology processes
- Sample human resources processes

These domains include sample Business Process assets, to give you a head-start in identifying your business processes, their characteristics and related elements. You can

edit these assets, move them to other Process Register domains and invite Business Stewards, Data Stewards and Privacy Stewards, to further develop them.

Process Register domain page overview

The domain page provides a complete overview of all information related to a domain.



Number	Section	Description
1	Breadcrumbs	The breadcrumbs of the current domain.
2	Domain type representation	The icon or abbreviation of the domain's type.
3	Domain name	The name of the domain.
4	Subheading	Various actions you can take, for example: • Go to the Business User Interface. • Request input.

Number	Section	Description
5	Stewards	The stewards of the domain. You can see up to three stewards on the domain page. If there are more, click **See all <number>** to see them on the **Responsibilities** page.
6	Tab pane	A collapsible pane that allows you to navigate to other pages of the domain and add characteristics. • **Overview**: Contains the description of and comments about a domain. • **Assets**: Displays the assets in the domain. • **Responsibilities**: Displays the view permissions and the responsibilities for a domain. • **History**: Displays which user has done what with this domain. • **Files**: Contains attachments.
7	Editor	The currently selected page, in this case the **Overview** page, which contains all the attributes that have been defined for the domain. Tip If you want to copy and paste text from other sources into a text field, we recommend that you click <>, and then paste the text into the **Show source code** field. This will remove any unwanted formatting or tagging of the text. For detailed information, see the knowledge base article on Collibra Support Portal.

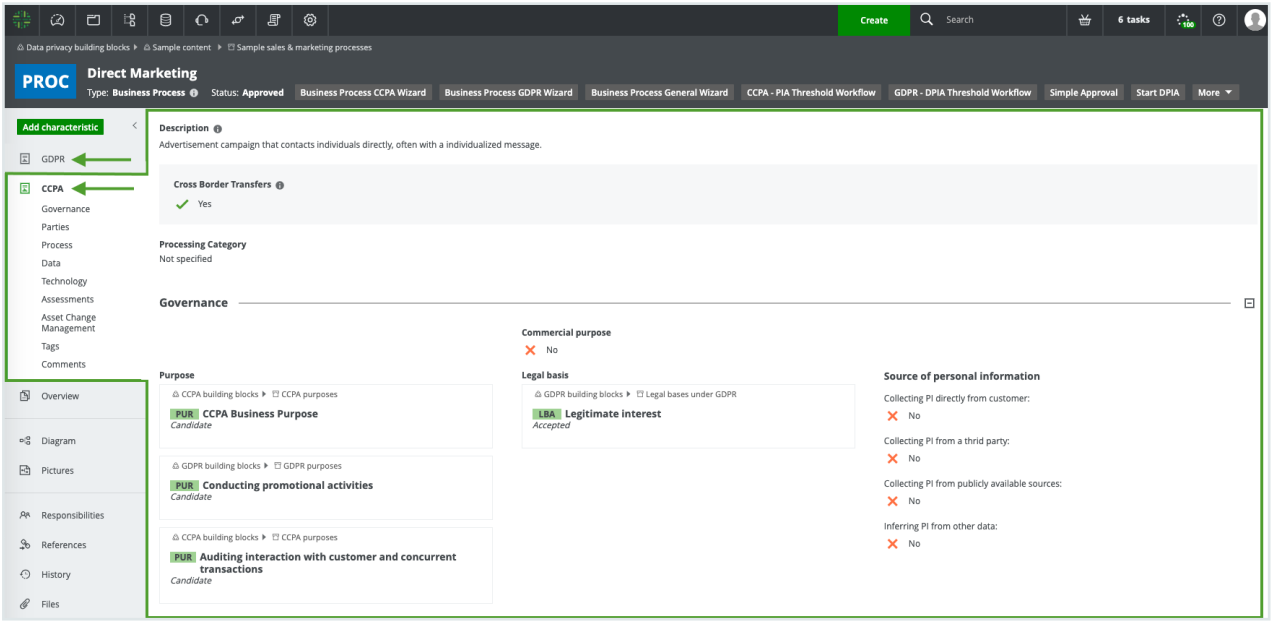
Business Process asset type

Business Processes are a set of activities and tasks that, once completed, produce a specific result and added value to the business. They are useful because they allow your

organization to abide by the requirements of the General Data Protection Regulation and to keep records of processing activities.

Business Process assets represent the business processes in your organization. For example, Human Resources is a business process that groups the business processes Payroll, Benefits and Talent Acquisition.

The following example image shows the asset page of a Business Process asset. In the tab pane, there is a separate tab for the information specific to each regulation by which the asset is governed. In this example, the asset is governed by both CCPA and GDPR.



> Note Future versions of Collibra Data Privacy will bring additional development and functionality to the Business Process asset page.

> Warning Collibra Data Intelligence Cloud is not compatible with third-party ad-blocker browser applications. Specifically, Business Process asset pages and Process Register domains will not load if you have an ad blocker installed.

Onboarding

The onboarding of Business Process assets follows the asset onboarding process.

Remediation plans and actions

If you become aware of certain risks, you can document your remediation plans and actions to reduce exposure, to a level that is aligned with your company's risk appetite.

Typically, a remediation action represents an actionable and measurable item to address a specific risk or combination of risks, whereas a remediation plan consists of a predefined sequence of remediation actions, used to address issues that require multiple actions to remedy.

During the onboarding of Remediation Plan assets, users are prompted to add related Remediation Action assets and can start the onboarding workflow for such assets.

You can map your Remediation Plan and Remediation Action assets to your Risk assets wen completing a DPIA/PIA or Legitimate Interest Assessment.

Workflows

Collibra Data Privacy comes with the following packaged workflows:

Workflow	Applicable regulations	Description
New Remediation Action	• CCPA • GDPR	Starts the creation, ownership acceptance and initial approval of a Remediation Action asset.
New Remediation Plan	• CCPA • GDPR	Starts the creation, ownership acceptance and initial approval of a Remediation Plan asset.

Treatment and review of proposed assets

The treatment and review workflow are started by the Business Steward, from the asset page of the relevant Remediation Plan or Remediation Action asset. It allows the Business Steward to:

- Document actions taken, and progress made, with regard to Remediation Plan and Remediation Action assets.

- Create relations with the assets that result from the Remediation Action, meaning a new Control asset.

> Note The completion of this workflow does not result in the creation of a new asset. Rather, new and/or modified attributes and relations are added to the relevant Remediation Plan or Remediation Action asset. The details of the work done are stored as comments.

If the implementation of the remediation plan or action spans a long time period, the Business Steward can use this workflow to log intermediate progress.

Workflows

Workflows are a key feature of Collibra Data Privacy. They automate processes and ensure collaboration among key stakeholders in your organization. The data privacy workflows allow you to fast-track your compliance efforts, by guiding users through the creation, approval and maintenance of assets.

Workflows are presented in wizard format, a sequence of dialog boxes, or forms, that prompt users to enter information.

Given certain limitations on the permissions of some data privacy-related roles, Collibra Data Privacy does not prevent users from editing an asset directly from the asset page. However, the asset onboarding and change management workflows include steps for the review, feedback and approval of assets. This holistic approach helps to ensure the quality and trustworthiness of your data. As such, we strongly recommend that users use the prescribed workflows for the creation and editing of assets.

> Warning
> - If you want to customize a packaged workflow, you should make a copy of the workflow, rename the copy, make your changes and then deploy it. This ensures that your customizations are not overridden if we need to update the packaged workflows.
> - Collibra Data Privacy comes with workflows for approving data privacy-specific assets. The Collibra Data Intelligence Cloud packaged approval workflows (Approval Process, Asset Approval Process and Simple Approval

Process) should not be used to approve data privacy-specific assets. As such, ensure that your Collibra approval workflows are not associated with data privacy-specific asset types, such as:
    - PIA
    - DPIA
    - Legitimate Interest Assessment
    - Compliance Self Assessment

  For information on how to associate a workflow with specific asset types, see View and edit workflow definition settings.
- Workflows are predefined to run a packaged data privacy configuration. Therefore, if you have customized the data privacy asset model, you have to reconcile your changes with the data privacy workflows.
- You can replace some of the packaged workflows with your customized workflows. You must ensure, however, that your workflows follow the same asset status evolution as that followed by the packaged workflows. For example, you can use a customized ownership acceptance workflow, as long as the asset status becomes Ownership accepted when the proposed target domain has been accepted.

Tip For complete information on workflows, see the Getting started with workflows, in the Collibra Developer Portal.

In this chapter

Packaged Collibra Data Privacy workflows

The following table shows the packaged workflows that are specific to Collibra Data Privacy.

Note The workflows noted as deprecated are no longer included in the Collibra Data Privacy CMA installation files. All instances of these workflows in your environment will continue to work. They will not be deleted when you install a new CMA file, but they are no longer updated and no longer supported.

Workflow	Applicable regulation	Description
Approval	CCPA, GDPR	Automates the approval of an asset. Includes a step that enables Stakeholders to provide feedback before the actual approval.
Assessments workflow	CCPA, GDPR	Enables users to submit completed assessments for review and approval or rejection.
Business Process Wizard	CCPA, GDPR	Enables users to create and edit the attributes of a Business Process asset, and launches other workflows that allow you to create and update attributes of a Business Process asset.
Business Process CCPA Wizard	CCPA	Enables users to provide the relevant attributes of a Business Process asset, specifically for compliance with CCPA. This workflow is started during the Business Process onboarding process, after the relation between the Business Process asset and the CCPA Regulation asset is established.
Business Process GDPR Wizard	GDPR	Enables users to provide the relevant attributes of a Business Process asset, specifically for compliance with GDPR. This workflow is started during the Business Process onboarding process, after the relation between the Business Process asset and the GDPR Regulation asset is established.
Business Process General Wizard	CCPA, GDPR	Enables users to create and update a subset of attributes of a Business Process asset. It is used in both the asset proposal and characteristics management phase of the asset onboarding process.

Workflow	Applicable regulation	Description
CCPA - PIA Threshold Workflow	CCPA	Determines whether or not a PIA is required. Note This workflow is deprecated.
Compliance Self Assess-ment Start	GDPR	Helps the Data Protection Officer assess and monitor an organization's compliance with GDPR. Note This workflow is deprecated.
Compliance Self Assess-ment Wizard	GDPR	Contains the set of wizard-style forms used in the Compliance Self Assessment workfow. Note This workflow is deprecated.
Data Set Wizard	CCPA, GDPR	Contains the set of wizard-style forms used in the New Data Set workflow.
Data Sharing Agreement Wiz-ard	CCPA, GDPR	Contains the set of wizard-style forms used in the New Data Sharing Agreement workflow.
DPIA Start	GDPR	Enables users to run a DPIA on a Business Process asset. Note This workflow is deprecated.
DPIA wizard	GDPR	Contains the set of wizard-style forms used in the DPIA workfow. Note This workflow is deprecated.

Workflow	Applicable regulation	Description
GDPR - DPIA Threshold Workflow	GDPR	Determines whether or not a DPIA is required. Note This workflow is deprecated.
Go to the Business User Interface	CCPA, GDPR	Opens the Business User Interface, a user-friendly interface for Process Register domains.
Govern Asset	CCPA, GDPR	Acts as the main dispatcher workflow to guide users through the completion, ownership acceptance and approval of an asset.
Govern Asset Launcher	CCPA, GDPR	Starts the Govern Asset workflow.
Informed Domain Selection (Sub Process)	CCPA, GDPR	Enables users to select a domain, and is used as a building block in other workflows.
Invite to Business Process Register	CCPA, GDPR	Invites business users to contribute to the development of Process Register domains.
Launch governance workflow on business process	CCPA, GDPR	Starts the governance workflow on a Business Process asset. It can be used by external applications to trigger the asset governance workflow, while managing the configuration in Collibra.

Workflow	Applicable regulation	Description
Legitimate Interest Assessment Start	CCPA, GDPR	Guides users through the creation, completion, ownership acceptance and initial approval of a Legitimate Interest Assessment asset. Note This workflow is deprecated.
Legitimate Interest Assessment Wizard	CCPA, GDPR	Contains the set of wizard-style forms used in the Legitimate Interest Assessment workflow. Note This workflow is deprecated.
Log Potential Security Breach	CCPA, GDPR	Enables users to log a potential security breach.
Manual Review Request	CCPA, GDPR	Enables users to request a review of an asset. The workflow creates a Review Request asset, which prompts the Business Steward for the target asset to review the content of the target asset.
Manual Review Request CCPA	CCPA	Enables users to request a review of a CCPA-specific asset. The workflow creates a Review Request asset, which prompts the Business Steward for the target asset to review the content of the target asset.
Manual Review Request GDPR	GDPR	Enables users to request a review of a GDPR-specific asset. The workflow creates a Review Request asset, which prompts the Business Steward for the target asset to review the content of the target asset.
New Business Process	CCPA, GDPR	Starts the creation, ownership acceptance and initial approval of a Business Process asset.

Workflow	Applicable regulation	Description
New Data Set	CCPA, GDPR	Starts the creation, ownership acceptance and initial approval of a Data Set asset.
New Data Sharing Agreement	CCPA, GDPR	Starts the creation, ownership acceptance and initial approval of a Data Sharing Agreement asset.
New Remediation Action	CCPA, GDPR	Starts the creation, ownership acceptance and initial approval of a Remediation Action asset.
New Remediation Plan	CCPA, GDPR	Starts the creation, ownership acceptance and initial approval of a Remediation Plan asset.
New Risk	CCPA, GDPR	Starts the creation, ownership acceptance and initial approval of a Risk asset.
New Technology	CCPA, GDPR	Starts the creation, ownership acceptance and initial approval of a Technology asset.
Ownership Acceptance (Sub Process)	CCPA, GDPR	Enables the acceptance of ownership of an asset. It includes a step in which stakeholders can provide feedback before the actual approval.
PIA Start	CCPA	Enables the user to run a PIA on a Business Process asset. Note This workflow is deprecated.
PIA wizard	CCPA	Contains the set of wizard-style forms used in the PIA workfow. Note This workflow is deprecated.

Workflow	Applicable regulation	Description
Propose Ownership	CCPA, GDPR	Enables users to propose ownership of a newly created asset.
Remediation Action Wizard	CCPA, GDPR	Enables users to create and update the characteristics of a Remediation Action asset.
Remediation Plan Wizard	CCPA, GDPR	Enables users to create and update the characteristics of a Remediation Plan asset.
Request Assets Access	CCPA, GDPR	Enables user to request access to assets that were added to the Data Basket. The Owners for the relevant assets receive a task to approve the access request.
Review Request Handler	CCPA, GDPR	Prompts Business Stewards to review the details of a Review Request asset and accept or reject the asset.
Review request handler (sub process)	CCPA, GDPR	Informs the Review Request Handler workflow that the changes have been made to an asset.
Risk Wizard	CCPA, GDPR	Enables users to create and update the characteristics of a Risk asset.
Security Breach Management	CCPA, GDPR	Enables the management of a security breach. It assigns an Issue Manager, who collects the information necessary to respond.
Technology Wizard	CCPA, GDPR	Enables users to create and update the characteristics of a Technology asset.
Time based asset review	CCPA, GDPR	Monitors Time-Based Review Rule assets and creates Review Request assets, when triggered.

Workflow	Applicable regulation	Description
Update asset directly	CCPA, GDPR	Enables Business Stewards to start the asset change management process, without creating Review Request assets, assigning tasks to themselves to approve, or triggering the Review Request Handler workflow.
Voting Sub Process (Privacy)	CCPA, GDPR	A sub-process that determines how voting is handled in other processes. It is configurable and is not intended to be used as a standalone workflow.

Default domains

Some of the data privacy workflows result in the creation of new assets. The following table shows the default domains in which the new assets are created.

Asset type	Default domain	Community
Business Process	New Processes	Data Governance Council
Data Set	New Data Sets	Data Governance Council
Data Sharing Agreement	New Governance Assets	Data Governance Council
Remediation Action	New Governance Assets	Data Governance Council
Remediation Plan	New Governance Assets	Data Governance Council
Risk	New Governance Assets	Data Governance Council
Security Issue	New Data Issues	Data Governance Council
Technology	New Applications	Data Governance Council

You can specify a different domain for the creation of such assets.

> Note The concept of a default domain does not apply to:
>
> - Assessment assets, Time-based Review Rule assets and Event-based Review Rule assets, all of which are created in the domain of the user's choosing during the relevant workflow.
> - Review Request assets, which are created in a domain of type Issue Vocabulary, in the community of the related asset. The Issue Vocabulary domain is a "hidden" domain that exists in every community. It cannot be reconfigured.

Specify a domain for the creation of new assets

Assets created via the Collibra Data Privacy workflows are created in default domains. You can specify a different domain for the creation of such assets.

> Warning It is critical that you not delete any of the default domains without specifying new domains. Without specified domains, the data privacy workflows will not run.

Steps

1. In the main menu, click , then **Settings**.
   » The Collibra settings page opens.
2. Click **Workflows**.
   » The Workflows settings page appears on the **Definitions** tab page.
3. Click the relevant workflow.
   For example, the Business Process Wizard workflow, which creates Business Process assets.
4. In the **Variables** section, click .
   » The Variables dialog box appears.
5. Scroll down to the variable "Please provide the ID of the default domain for a new Business Process".
6. Enter the UUID of the new default domain.
7. Click **Submit**.

Easy Business Process Proposal option

A well-develop Business Process asset has all the necessary characteristics, from the business, data-mapping and legal perspectives. Developing such an asset requires the specialized knowledge of Business Stewards, Data Stewards and Privacy Stewards.

The Easy Business Process Proposal option is designed to:

- Help Collibra Data Privacy users who identify the need for new assets, but might be deterred from proposing them due to all the business, data-mapping and legal considerations brought forth during the asset proposal phase, which are likely beyond the users' areas of expertise.
- Encourage the proposal of new assets, by:
  - Simplifying the Business Process asset proposal workflow for the user.
  - Automatically deferring specialized considerations to the relevant subject matter experts, to be addressed during the characteristics management phase.

Details

Enabled/Disabled	Description
Enabled	All workflow forms that address data mapping and legal considerations are skipped in the asset proposal phase. These forms are presented to the Business Steward, Data Steward and Privacy Steward during the characteristics management phase of the onboarding process.
Disabled	All workflow forms, including those that address data mapping and legal considerations, are included in the asset proposal phase. > Note Even though these workflow forms will be included, there are no mandatory forms or fields in the asset proposal phase.

> Note This option is enabled, by default. No action is required of you, to benefit from this option.

Enable or disable the Easy Business Process Proposal option

You can enable or disable the Easy Business Process Proposal option.

Steps

1. In the main menu, click , then **Settings**.
   » The Collibra settings page opens.
2. Click **Workflows**.
   » The Workflows settings page appears on the **Definitions** tab page.
3. Click the Business Process Wizard.
4. In the **Variables** section, click .
   » The **Variables** dialog box appears.
5. Scroll down to the variable "Enable the Easy Business Process Proposal option".
6. In the drop-down list, select:
   - **True**, to enable the option
   - **False**, to disable the option.
7. Scroll to the bottom of the **Variables** dialog box, and then click **Submit**.

Regulation-specific workflow forms

The data privacy workflows are designed to automate your governance processes, regardless of the regulation with which you need to comply. However, if there are regulation- or policy-specific considerations that you would like to introduce during the asset onboarding process, this feature accommodates that need.

You can design your own regulation- and policy-specific workflow forms for the onboarding of Business Process assets. Your custom forms will be completed by the Privacy Steward, in the appropriate phase of the onboarding process.

> Note This feature is available for the onboarding process of Business Process assets only.

Add regulation-specific workflow forms

You can add customized, regulation-specific workflow forms for the onboarding of Business Process assets.

Steps

1. Create a workflow that includes your customized regulation-specific workflow forms. We recommend that you copy the Business Process GDPR Wizard workflow, which is packaged specifically for this purpose, and customize it outside of Collibra Data Intelligence Cloud. You can then deploy your customized workflow.

   > Warning Ensure that your customized workflow has a unique name and "processRef" before uploading it back into Collibra. That way it will not be overwritten when upgrading your Collibra environment.

2. Configure the Business Process Wizard workflow.
   a. In the main menu, click , then **Settings**.
      » The Collibra settings page opens.
   b. In the tab pane, click **Workflows** → **Definitions**.
   c. Click the **Business Process Wizard**.
   d. In the **Variables** section, click .
      » The Variables dialog box appears.
   e. Scroll down to the variable "Please provide the General Information workflow reference ID that is used in the Business Process asset proposal phase and the characteristics management phase".
   f. In the variable field, enter the UUID of the relevant Regulation asset, followed by a comma "," followed by the "processRef" of your customized workflow. For example: `c0e00000-0000-0000-4400-000000000000,privYourCustomizedBusinessProcessGDPRWizard`, where:

- "c0e00000-0000-0000-4400-000000000000" is the UUID of the GDPR Regulation asset.
- "privYourCustomizedBusinessProcessGDPRWizard" is the "processRef" of your customized workflow.

g. Scroll to the bottom of the **Variables** dialog box, and then click **Submit**.

Business Process General Wizard workflow

The Business Process General Wizard workflow is a collection of workflow forms presented to:

- The Business User in the asset proposal phase of the asset onboarding process.
- The Business Steward in the characteristics management phase.

You can customize this workflow. As the name indicates, the purpose is to capture the most general information about the proposed asset, such as:

- A description of the proposed asset.
- Related Processing Categories assets.
- Related Technology assets.
- An estimation of the degree to which the process is automated.
- Whether or not the process is considered business-critical.

> Note This workflow can only be customized for the onboarding of Business Process assets.

Customize the Business Process General Wizard workflow

You can customize the Business Process General Wizard workflow to meet your needs.

Steps

1. Create a customized workflow that includes your customized general information forms.

> Tip We recommend that you copy the Business Process General Wizard workflow, customize it outside of Collibra Data Intelligence Cloud, and then upload the customized workflow back into Collibra.

> Warning Ensure that your customized workflow has a unique name and "processRef" before uploading it back into Collibra. That way it will not be overwritten when upgrading your Collibra environment.

2. Configure the Business Process Wizard workflow.
   a. In the main menu, click , then **Settings**.
      » The Collibra settings page opens.
   b. In the tab pane, click **Workflows** → **Definitions**.
   c. Click the **Business Process Wizard**.
   d. In the **Variables** section, click .
      » The **Variables** dialog box appears.
   e. Scroll down to the variable "Please provide the General Information workflow reference ID that is used in the Business Process asset proposal phase and the characteristics management phase".
   f. In the variable field, enter the "processRef" of your customized workflow. For example: `privYourCustomizedBusinessProcessGeneralWizard`.
   g. Scroll to the bottom of the **Variables** dialog box, and then click **Submit**.

Asset onboarding and change management

Collibra Data Privacy offers standardized procedural flows for the creation and maintenance of data privacy-related assets. There are two main processes:

- **Asset onboarding**: The process of creating a new asset and agreeing to its characteristics.
- **Asset change management**: The process of making changes to an approved asset.

The distinction between the types of data privacy assets

In the context of asset onboarding and asset change management, it is important to draw a distinction between three general categories of data privacy-related assets:

Category	Description
Business Process assets	• Stored in Process Register domains. • The ownership and characteristics of these assets can be updated at any time over the life of the asset. • For these assets, the Business Steward, Data Steward and Privacy Steward are all required to contribute in the characteristics management phase.
Other business assets (meaning other than Business Process assets), including asset types: • Data Set • Technology • Data Sharing Agreement • Risk • Remediation Plan • Remediation Action	• The ownership and characteristics of these assets can be updated at any time over the life of the asset. • For these assets, only the Business Steward is required to contribute in the characteristics management workflow.

Category	Description
Assessment assets: • Privacy Impact Assessment (PIA) • Data Protection Impact Assessment (DPIA) • Legitimate Interest Assessment (LIA) • Compliance Self Assessment (CSA)	• These assets assess a situation at a specific moment in time. As such, their characteristics cannot be updated. If an assessment asset is deemed to be outdated, a new assessment asset is required. > Note The new assessment asset is a copy of the previous assessment asset, meaning it has all of the same characteristics as the previous assessment asset. The new asset is updated and eventually approved. The status of the previous assessment asset simultaneously becomes Obsolete.

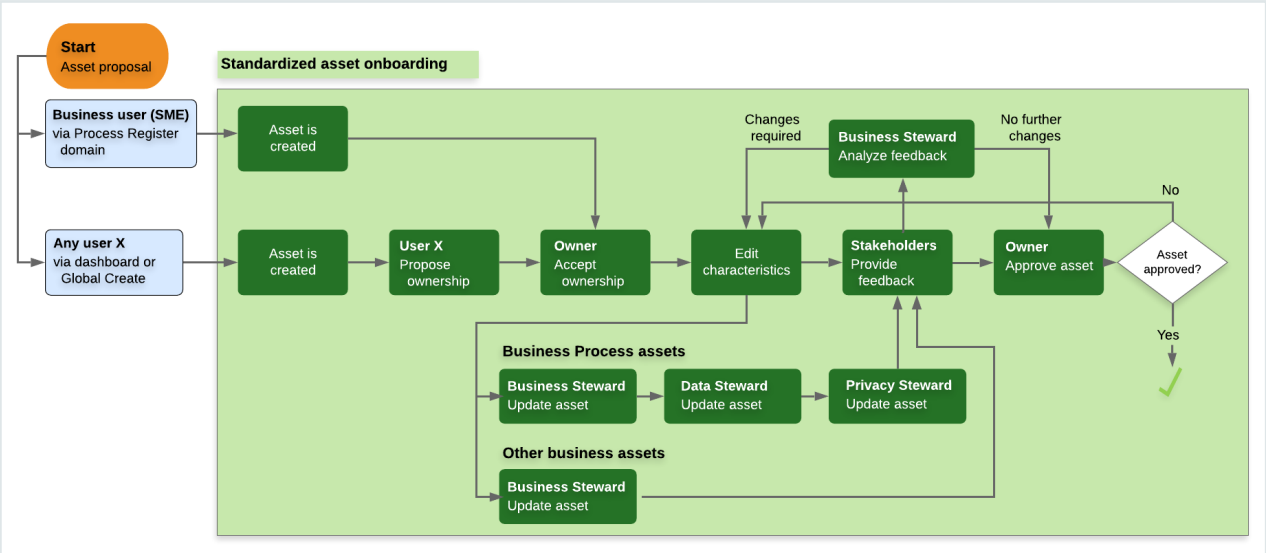
Asset onboarding

The objective of the asset onboarding process is to provide a standardized procedural flow for the creation of data privacy and risk assets.

> Important This process does not apply to assessment assets. For complete information on conducting and managing assessments, see Collibra Assessments.

Visual overview of the asset onboarding process

The following image illustrates the flow of the asset onboarding process for Business Process assets and other business assets, such as Risk assets and Data Set assets.



To progress through this process and advance a proposed asset towards approval, users complete a succession of workflows.

Onboarding Business Process assets and other business assets

The following table shows the phases involved in the onboarding of Business Process assets and other business assets.

Asset types	Phases
• Business Process • Data Set • Technology Asset • Data Sharing Agreement • Risk • Remediation Plan • Remediation Action	1. Asset proposal. 2. Ownership proposal. 3. Ownership acceptance. 4. Characteristics management. 5. Approval.

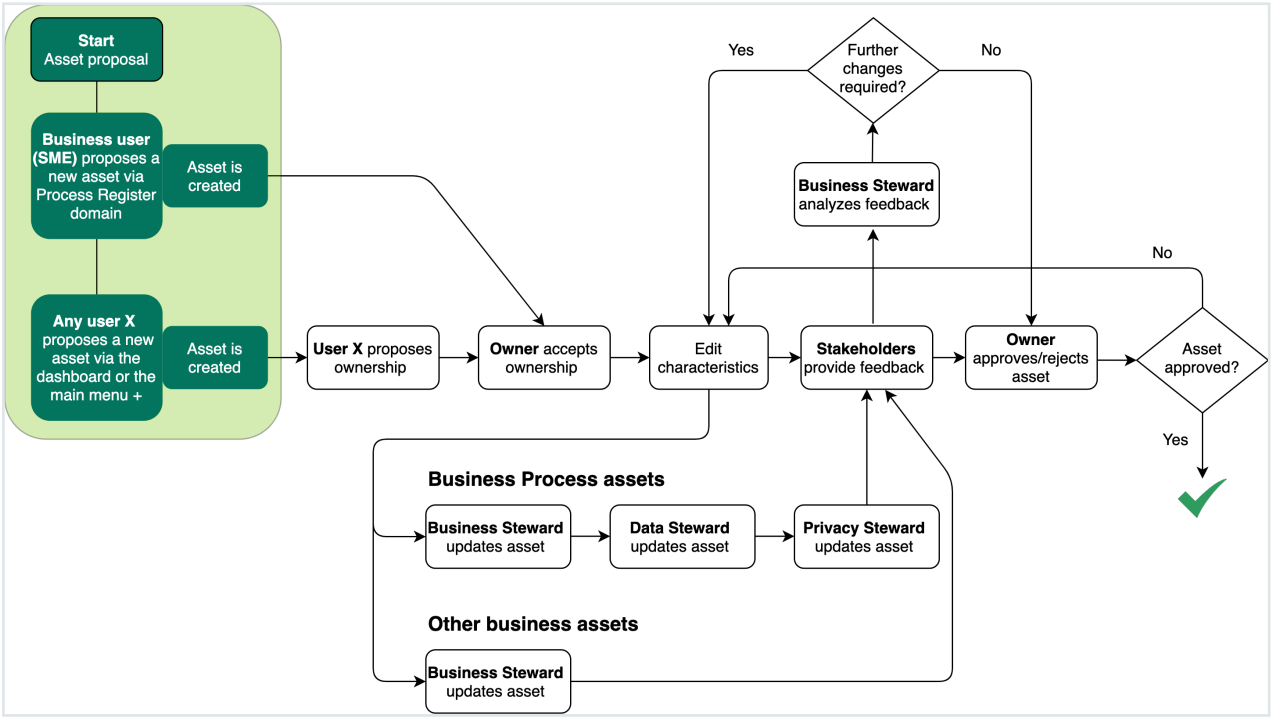
Onboarding assessment assets

The onboarding process for assessment assets varies slightly.

Asset types	Phases
• Privacy Impact Assessment (PIA) • Data Protection Impact Assessment (DPIA) • Legitimate Interest Assessment (LIA) • Compliance Self Assessment (CSA)	1. Ownership proposal. 2. Characteristics management. 3. Ownership acceptance. 4. Approval.

Asset proposal

In this phase of the asset onboarding process, users progress through a series of workflow forms, to create a new asset and add characteristics to the asset.



The following are a few examples of asset proposal workflows:

- New Business Process
- Risk Wizard

- Start PIA
- Remediation Action Wizard

Who can start these workflows?

By default, any user can start a workflow; however, you can edit the workflow configuration options to restrict the right to certain resource roles on the parent asset. For example, you can restrict the right to start a workflow to the Owner or Business Steward resource roles.

Some workflows for the creation of assessment assets, for example the Legitimate Interest Assessment workflow, can only be started by the Owner or the Business Steward for the related Business Process asset.

When a user starts an asset proposal workflow, that user is assigned the responsibility of Stakeholder for the newly created asset.

The default domains

When you start an asset proposal workflow, an asset is created in the default domain. You can specify a new default domain for such assets.

In the ownership proposal workflow, the user proposes a long-term domain for the asset. If ownership is accepted in the ownership acceptance workflow, the asset is moved to the proposed domain.

> Note Collibra Data Intelligence Cloud can be configured to allow for multiple assets with identical names in a single domain. However, this is not allowed in the data privacy-specific default domains, where all asset names must be unique.

Canceling the asset proposal

Asset proposal can be canceled anytime before the asset has been approved; however, there is currently no automated cancellation procedure. The user can simply exit the relevant workflow. The Business Steward for the domain in which the newly created asset resides can then delete the asset.

> Tip In the workflow wizard, clicking **x** to close the dialog box pauses the workflow. It does not cancel the workflow. The created asset remains in the default domain. The user can resume the workflow from the My Tasks page, at another time.
>
> 
>

Output and status evolution

The following table shows the status evolution, based on the possible conditions.

Condition	The status of the asset...
A user starts an asset proposal workflow.	Is New.
The asset proposal workflow is complete.	Becomes Candidate.

Tip

1. Start a workflow to propose a new asset:

For asset types...	Start the workflow via...
◦ Business Process	◦ The Privacy Dashboard. ◦ The Invite to Business Process Register workflow.
◦ Data Set ◦ Technology Asset ◦ Data Sharing Agreement ◦ Risk ◦ Remediation Action ◦ Remediation Plan ◦ Compliance Self Assessment (CSA)	◦ The Data Protection Dashboard.
◦ Privacy Impact Assessment (PIA) ◦ Data Protection Impact Assessment (DPIA) ◦ Legitimate Interest Assessment (LIA)	◦ The related Business Process asset page.

2. Complete the workflow forms. There are no mandatory fields in the workflow forms. The objective here is to create the asset. In the characteristics management phase of the onboarding process, the various stewards are called on to develop the asset in accordance with their areas of expertise.

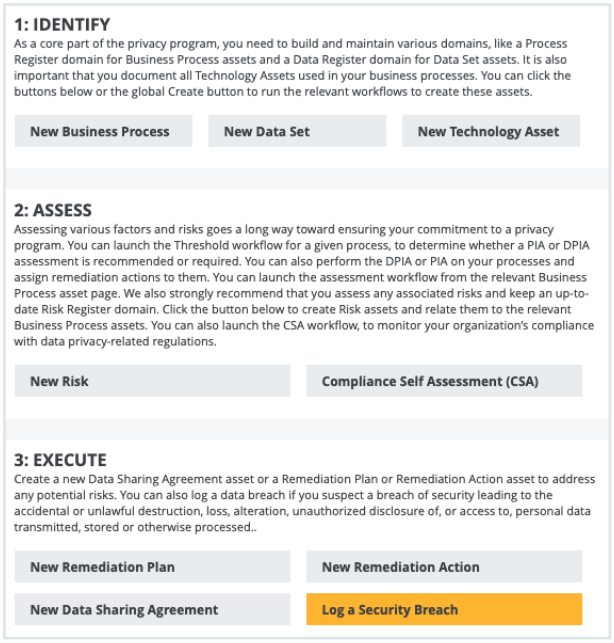
> Note The ownership proposal workflow forms follow immediately after the series of asset proposal workflow forms.

Propose an asset via the Privacy Dashboard

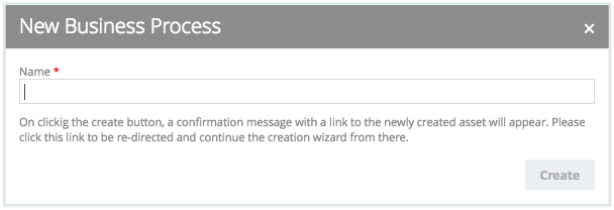
You can propose a new asset via the Privacy Dashboard.

Steps

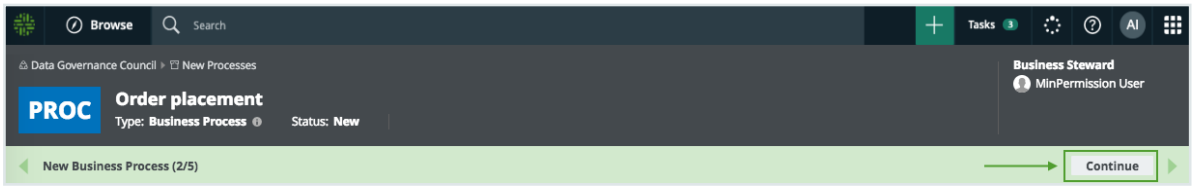
1. On the Privacy Dashboard, click the relevant workflow button, for example **New Business Process**.



   » In this example, the **New Business Process** workflow wizard appears.



2. Enter a name for the new asset.
   » An asset with the status New is created in the default domain.
3. Go to the asset page of the newly created asset.
4. Click **Continue**, to continue to launch the next form in the workflow wizard.

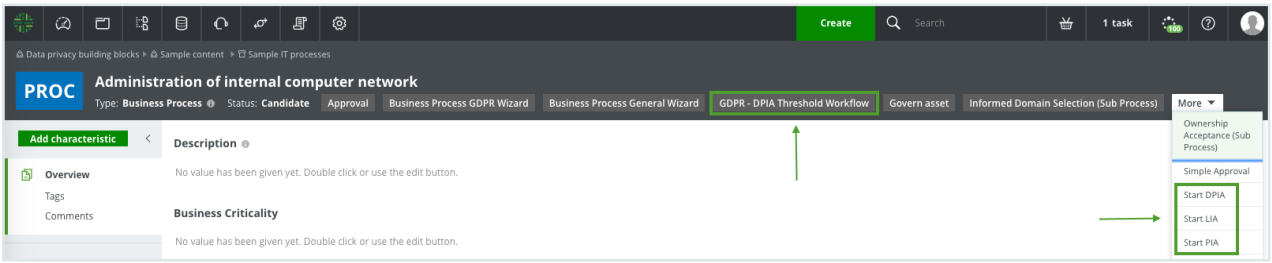


Start an assessment workflow via the related Business Process asset page

PIAs, DPIAs and Legitimate Interest Assessments assess certain aspects of approved Business Process assets. As such, they can only be proposed via the related Business Process asset page.

> Tip When a proposed Business Process asset has been approved:
>
> - The Threshold workflow has to be run.
> The Threshold workflow determines whether or not a PIA workflow or DPIA workflow has to be run for the Business Process asset.
> - If Legitimate Interest was selected as the legal basis during the proposal phase for the Business Process asset, the Legitimate Interest Assessment workflow has to be run.

To start an assessment workflow, go the asset page of the relevant Business Process asset, and then click the appropriate workflow link.



Email notifications and tasks

When a workflow is completed during the asset onboarding and asset change management processes, the relevant users or user groups involved in the next phase:

- Receive a task on their My Tasks pages.
- Are notified of the task, via email.

Suppose, for example, that a user group with five users is assigned the Business Steward role for a given domain. If a task is assigned to that group of Business Stewards, all five users will receive a task. However, only one user can start the task.

When one user has started the relevant workflow, the task is disabled and removed from the My Tasks pages of all other users that received the task.

The user that started the workflow for the task has to finish the workflow, or cancel it, depending on the workflow. For that user, the task remains on the My Tasks page until the workflow is complete. The user can pause the workflow at any time, and any information that was entered is saved. The workflow can then be continued from the My Tasks page.

Pausing and restarting a workflow

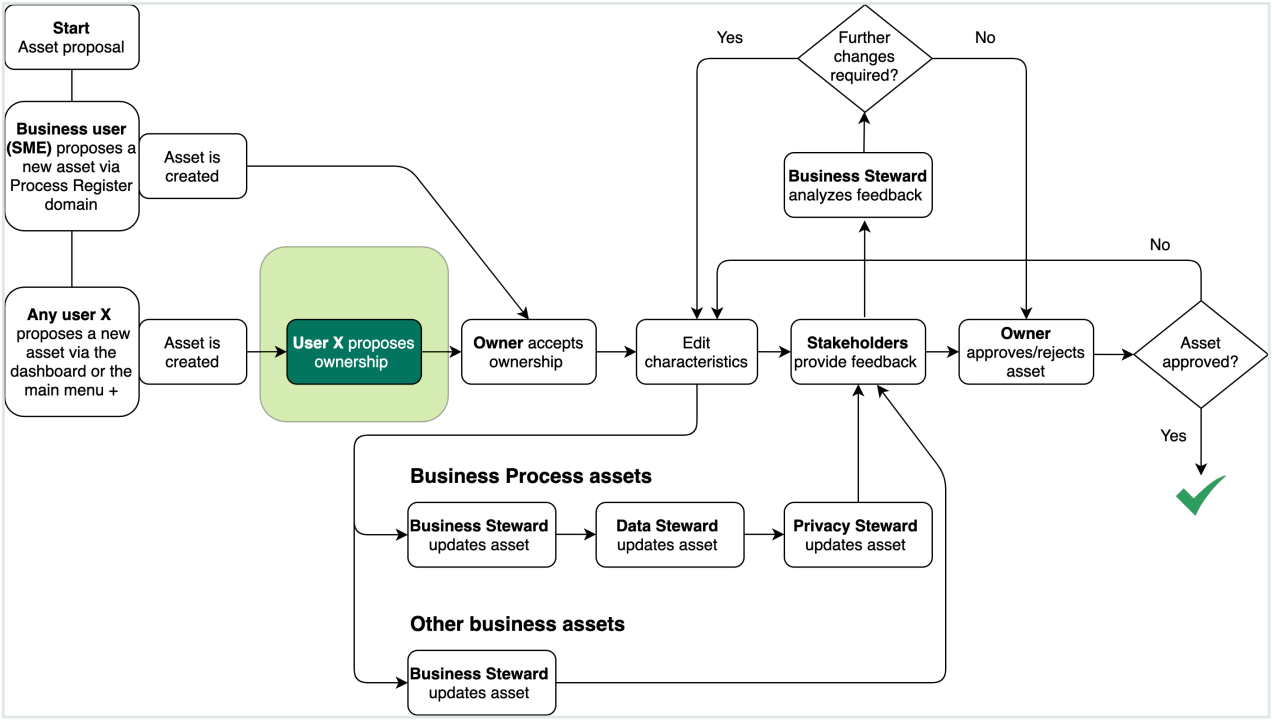
If you have started a workflow and need to step away or shut down before completing it, you can pause the workflow and restart it at another time, without losing any of the information you've entered or the selections you've made.

Wherever you are in the workflow, click **Save all changes** or simply click **x** to close the workflow wizard. The asset is saved in the default domain.

When you're ready to continue with the workflow, go to the My Tasks page and select the workflow.

Ownership proposal

In this phase of the asset onboarding process, the user who started the asset proposal workflow proposes ownership of the asset.



Ownership at the domain level

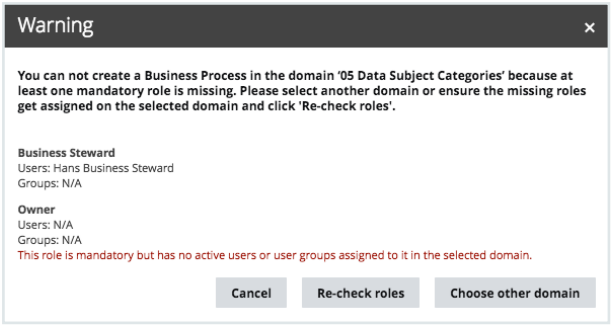
In the asset proposal workflow, the new asset is created. In this step, the user who proposed the asset proposes the domain in which the asset will be stored long-term. If accepted via the ownership acceptance workflow, the Owner for the proposed domain becomes the Owner for the asset, as the responsibility is inherited from the domain.

Mandatory responsibilities in the target domain

When the user selects a target domain for proposal, Collibra Data Privacy verifies that the domain has the responsibilities necessary to complete the onboarding process.

If the proposed domain is lacking the necessary responsibilities, a dialog box shows which responsibilities are missing. The user can then:

- Cancel the ownership proposal.
- Create the necessary responsibilities in the target domain and then click **Re-check roles**, to continue with the ownership proposal.
- Choose a different target domain.



Tip To successfully use the packaged data privacy workflows, you need to create the following responsibilities for each of your data privacy-related domains:

- Data Protection Officer
- Owner
- Business Steward
- Data Steward
- Privacy Steward
- Community manager
- Issue Manager
- Subject Matter Expert
- Stakeholder
- Requester

Canceling the workflow

To cancel the ownership proposal workflow, the user can click **Cancel** in the workflow wizard. In this case:

- The task is removed from the user's My Tasks page.
- The asset remains in the default domain, with the status Candidate.
- The ownership proposal workflow can be restarted at any time, from the relevant asset page.

Tip In the workflow wizard, clicking **x** to close the dialog box pauses the workflow. It does not cancel the workflow. The user can resume the workflow from the My Tasks page, as long as the asset status is Candidate.

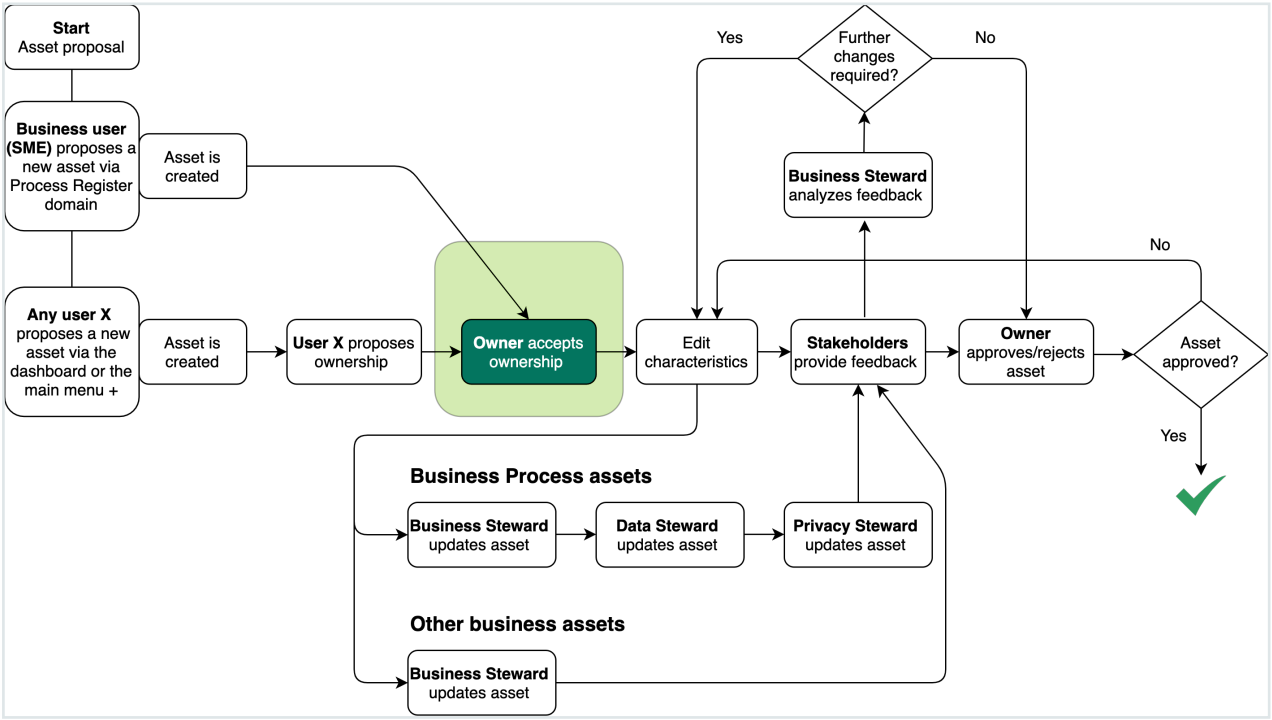
Output and status evolution

The following table shows the status evolution, based on the possible conditions.

Condition	The status of the asset...
Before any action is taken.	Is Candidate.
When a user selects a target domain for proposal and confirms the selection.	Becomes Ownership proposed.

Ownership acceptance

In the ownership proposal phase, a user proposes a domain for the newly created asset. In this phase, the Owner or the Business Steward for the proposed domain accepts or rejects the proposal.



Starting the workflow

The relevant ownership acceptance workflow is automatically triggered at the completion of the ownership proposal phase.

The Owner and the Business Steward for the proposed domain receive a task that triggers a workflow to accept or reject the proposal.

The default configuration is such that only one Owner or Business Steward can accept or reject the ownership proposal, even if there are multiple Owners or Business Stewards for the proposed domain. However, you can configure Collibra Data Privacy so that multiple Owners or Business Stewards can vote to accept or reject the ownership proposal.

This task persists until an Owner or Business Steward accepts or rejects the proposal. If no action is taken, the packaged escalation process is run, in accordance with its configuration.

Due dates and the escalation process

Each task in a workflow has to be completed within a certain, configurable amount of time. The due date for each task is shown on the My Tasks page of the relevant users.

When the due date for an uncompleted task is approaching, the users assigned to the task are notified via email that the task is about to expire. Optionally, you can configure Collibra Data Privacy so that the user(s) receive a second task, to reassign the first task to another user or user group. This reassignment task is automatically removed if the original task is completed or the due date is reached without action.

If the task has not been completed by the due date, the relevant users (as defined by the responsibilities for the domain) are notified that the task was not completed. The task is abandoned and the onboarding process can continue without further delay.

Acceptance or rejection of the ownership proposal

When accepting or rejecting ownership, the Owner or Business Steward can provide a free-text explanation for the decision to accept or reject ownership. The text is recorded as a comment on the asset page.

Acceptance

If ownership is accepted, the asset is moved to the target domain.

By moving the asset to the target domain, any responsibilities not added directly at the asset level are inherited from the domain. Responsibilities that were added at the asset level remain unchanged.

> Note Moving an asset from a default domain to a target domain might result in changes to the scoped assignment. This means the characteristics shown on the asset page might vary. However, none of the characteristics are removed, they just might not be shown. The user assigned to the Sysadmin global role has to configure the scopes and assignments so that the user can see the correct characteristics for the relevant domain.

Rejection

If ownership is rejected, the asset remains in the default domain. The Owner or Business Steward for the proposed domain can counter-propose an alternative domain, and the Owner or Business Steward for the counter-proposed domain receives a task, to accept or reject the counter-proposal.

If ownership is rejected, the user who proposed ownership is notified and either:

- The ownership proposal workflow has to be run again.
- The newly created asset can be manually deleted from the Collibra Data Governance Center environment.

> Tip In the case of a rejection of ownership, we recommend that the appropriate stakeholders communicate as to why the proposal was rejected and, if possible, agree on a target domain for the asset. The ownership proposal workflow can then be run again.

If the Owner of the target domain does not propose an alternative domain, the user that proposed the domain in the first place is notified via a task. The task triggers the ownership proposal workflow, via which the user can propose an alternative domain.

If an alternative domain is selected, the Owner or Business Steward of the alternative domain will get a task to accept or reject the ownership of the proposed asset. The steps that follow are identical to the initial domain proposal.

Output and status evolution

In this phase of the onboarding process, the asset can undergo the following changes:

- If the ownership proposal is accepted, the asset moves from the default domain to the proposed domain.
- The status of the asset changes.
- One or more additional comments can be added to the asset.

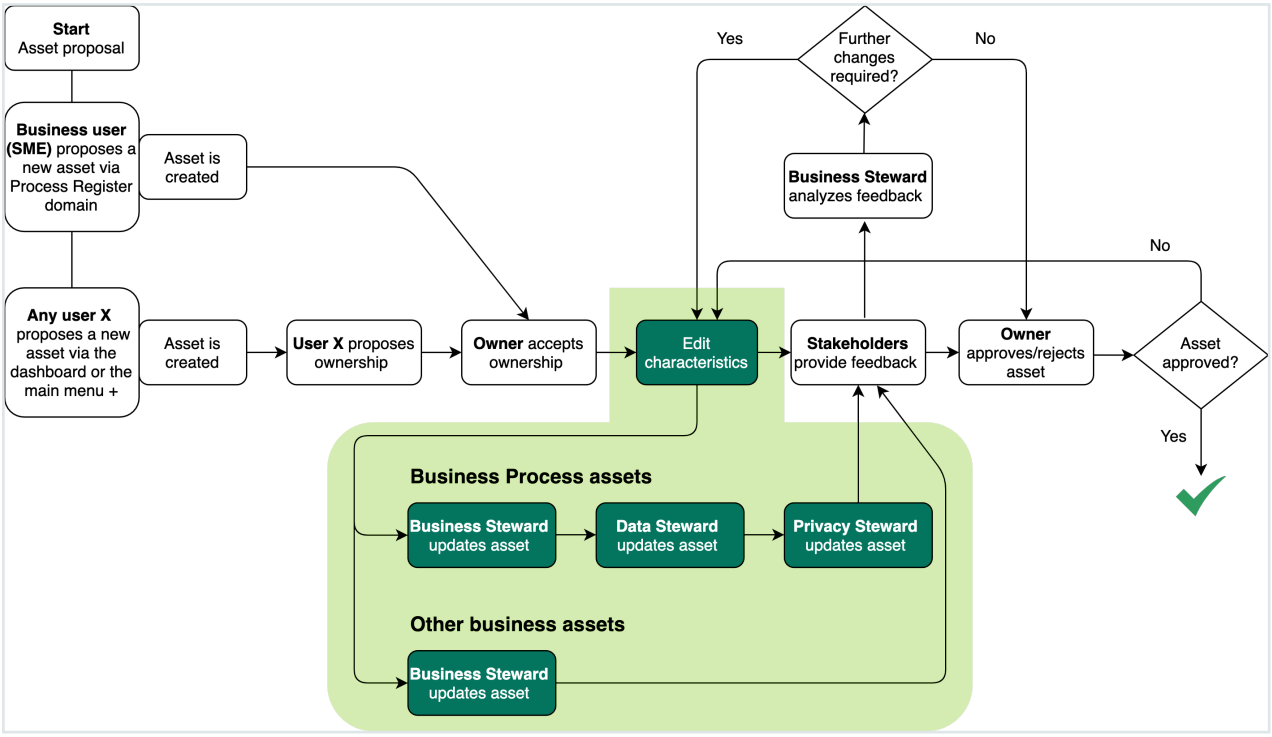
The following table shows the status evolution, based on the possible conditions.

Condition	The status of the asset...
Before any action is taken.	Is Ownership proposed.
If the Owner for the proposed domain accepts the ownership proposal.	Becomes Ownership accepted.
If the Owner for the proposed domain rejects the ownership proposal and does not propose an alternative target domain (in which case, the user that initially proposed ownership has to rerun the ownership proposal workflow).	Becomes Ownership rejected.
If the Owner for the proposed domain rejects ownership, but proposes an alternative target domain.	Becomes Ownership proposed.

Characteristics management

The characteristcs management phase figures in both the asset onboarding process and the asset change management process.

In this workflow, the Owner, Business Steward, Data Steward and Privacy Steward can, in turn, edit the characteristics of the asset.



If the Business Steward or Owner for the proposed domain accepts ownership via the ownership acceptance workflow, they receive a task prompting them to either:

- Edit the characteristics of the proposed asset.
- Go directly to the asset approval workflow.

The Business Steward decides to edit the characteristics

> Note This is the entry point for editing an approved asset, when a Business Steward clicks the **Start update workflow** button on the asset page of the relevant asset.

The Business Steward clicks the task in My Tasks and starts the relevant workflow.

- For Business Process assets, the Business Steward, Data Steward and Privacy Steward are prompted, in succession, to edit the asset in accordance with each users area of expertise.

- For other business assets, such as Risk and Technology assets, only the Business Steward is prompted to edit the asset.

When the relevant stewards have completed the workflow, the Owner for the asset receives a task to accept or reject the changes.

- If the Owner accepts the changes, the asset approval workflow is automatically triggered.
- If the Owner rejects the changes, the Business Steward can either:
  - Re-run the workflow and further edit the characteristics.
  - Start the asset approval workflow.

> Note Although we recommend that you use workflows to manage the editing of assets, the Business Steward and Owner can always edit assets directly via the relevant asset pages. Doing so does not trigger further review of the asset or the approval workflow.

The Business Steward decides to not edit the characteristics

In this case, the Business Steward starts the asset approval workflow, and the Owner or Data Protection Officer receives a task to approve the asset.

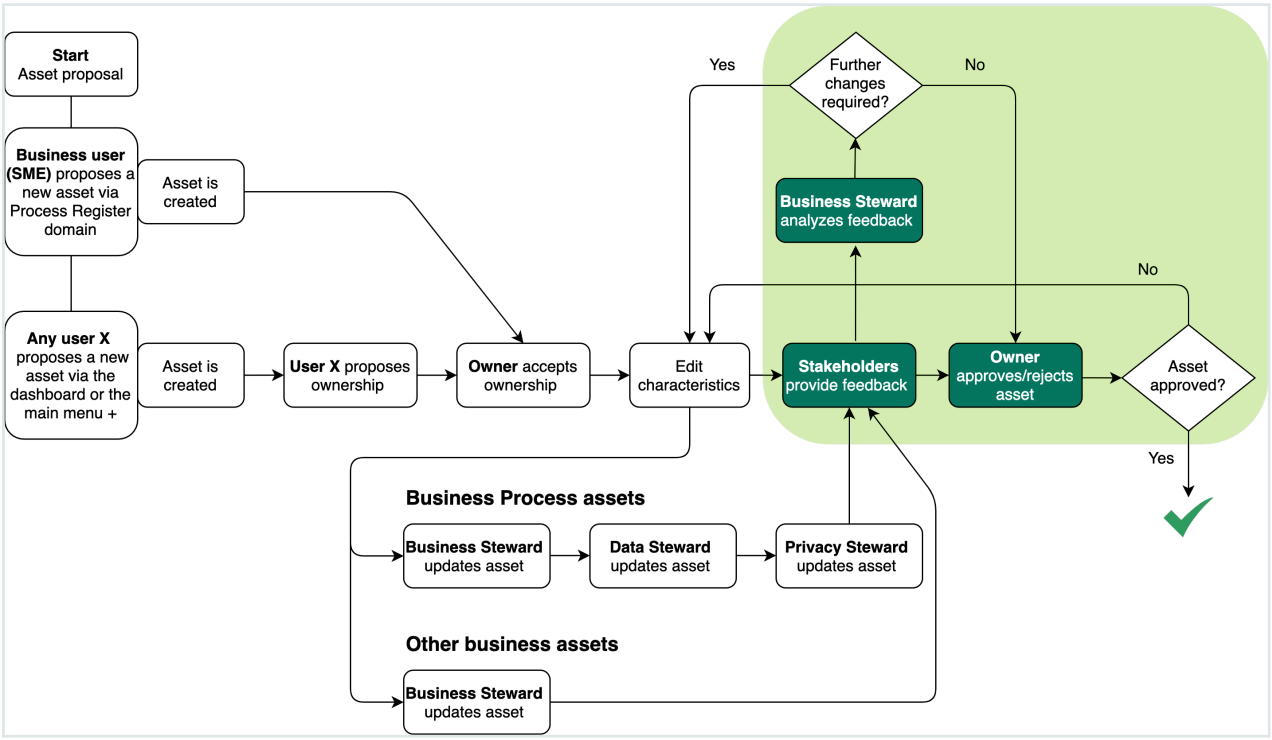
Output and status evolution

The following table shows the status evolution, based on the possible conditions.

Condition	The status of the asset...
Before any action is taken.	Is Ownership accepted.
The Business Steward starts the workflow to edit the characteristics of the asset.	Remains Ownership accepted.
The stewards complete the workflows to edit the characteristics of the asset.	Becomes Approval pending.

Condition	The status of the asset...
The Business Steward skips the characteristics management workflow and starts the asset approval workflow.	Becomes Waiting for feedback.

Approval



In the Approval workflow:

1. Stakeholders provide feedback on the content and/or ownership of the asset.
2. The Business Steward or Owner considers the feedback and approves or rejects the asset.

Starting the workflow

The Approval workflow is triggered in one of two ways:

- Automatically, when the Owner for the asset accepts the changes that were made during the characteristic management phase.

- Manually, by the Business Steward or Owner clicking **Approval** on the asset page of the asset.

> Note It is not possible to start the approval workflow if any other workflow is running for the asset.

Providing feedback

Before the actual approval, a configurable set of users (by resource role), per asset type, can provide feedback on the ownership and contents of the asset. These stakeholders:

- Indicate agreement with, or objection to:
  - the ownership of the asset, as determined by the domain in which the asset is stored.
  - the content of the asset, meaning the characteristics.
- Provide a free-text comment, if objecting to the ownership, content or both.
  The feedback is added as a comment on the asset page of the asset.

> Note The feedback provided by stakeholders is not an approval or rejection. It is simply a means for the stakeholders to express their agreement or objection. The Business Steward or Owner will take the feedback into consideration and ultimately:
>
> - Approve or reject the asset, if in the asset onboarding process.
> - Approve or reject the changes to the asset, if in the asset change management process.

Mandatory and optional stakeholders

You can configure two sets of stakeholders from which to solicit feedback:

- A set for which feedback is mandatory.
  For mandatory stakeholders, there is no timeout period for the submission of their reviews. The workflow is blocked until all mandatory stakeholders have submitted their reviews.
- A set for which feedback is optional.
  Optional stakeholders are subject to a configurable timeout period. When the timeout period expires, they can no longer provide feedback.

> Tip We recommend that you include:
>
> - The Stakeholder resource role, among those designated as optional stakeholders.
> - The Data Protection Office resource role, among the mandatory stakeholders.

Processing the feedback

After all mandatory stakeholders have provided feedback and either all optional stakeholders have submitted their feedback or the timeout period has expired, two scenarios are possible:

Scenario	What happens next?
None of the stakeholders have objected to the ownership or the content.	The approval workflow automatically continues. The relevant approver (by default, the Owner) receives an approval task.
One or more stakeholders have objected to either the ownership, the content or both.	The Business Steward receives a task to review the feedback. Depending on the reason for the objections, the Business Steward can either: ◦ Continue with the approval, without making further changes to the proposed asset. ◦ Reject the asset and, as appropriate, manually restart the ownership proposal workflow or the workflow to edit the characteristics of the asset.

Status evolution

The following table shows the status evolution, based on the possible conditions.

Condition	The status of the asset...
Before any action is taken.	Is Waiting for feedback.
For the duration of the feedback window, which closes when the configured timeout period has expired or when all mandatory stakeholders have submitted feedback.	Is Waiting for feedback.
The feedback window has closed, but the Business Steward has not yet completed the feedback review. This status is only applicable if one or more stakeholders objects to the ownership and/or content of the asset.	Becomes Feedback review.
No objections to the ownership or content of the asset were submitted and the Business Steward has completed the feedback review, but the Owner has not yet: • Approved or rejected the proposed asset, if in the asset onboarding process. • Approved or rejected the changes to the asset, if in the asset change management process.	Becomes Approval pending.
The Owner: • Approves the asset, if in the asset onboarding process. • Approves the changes to the asset, if in the asset change management process.	Becomes Approved.
The Owner: • Rejects the asset, if in the asset onboarding process. • Rejects the changes to the asset, if in the asset change management process.	Becomes Rejected.

Notifications

When the Owner has accepted or rejected the proposed asset, notification of the approval or rejection is sent via email to:

- The Business Steward.
- The user who proposed an asset or initiated an edit to an approved asset.
- All stakeholders, mandatory and optional, who were asked to submit feedback.

Asset change management

Whereas the result of the asset onboarding process is a new asset with the status Approved, asset change management is the standardized procedure for making changes to such approved assets.

Collibra Data Privacy offers three means by which to trigger a review request.

Triggering an asset review request

You may want, or need, to periodically review your approved data privacy-related assets. As shown in the following table, there are three means by which to trigger a review.

> Note When a review request is triggered, a Review Request asset is created; however, there is no obligation on the part of the Business Steward or Owner to carry out a change to the asset. It is simply a request to review the asset.

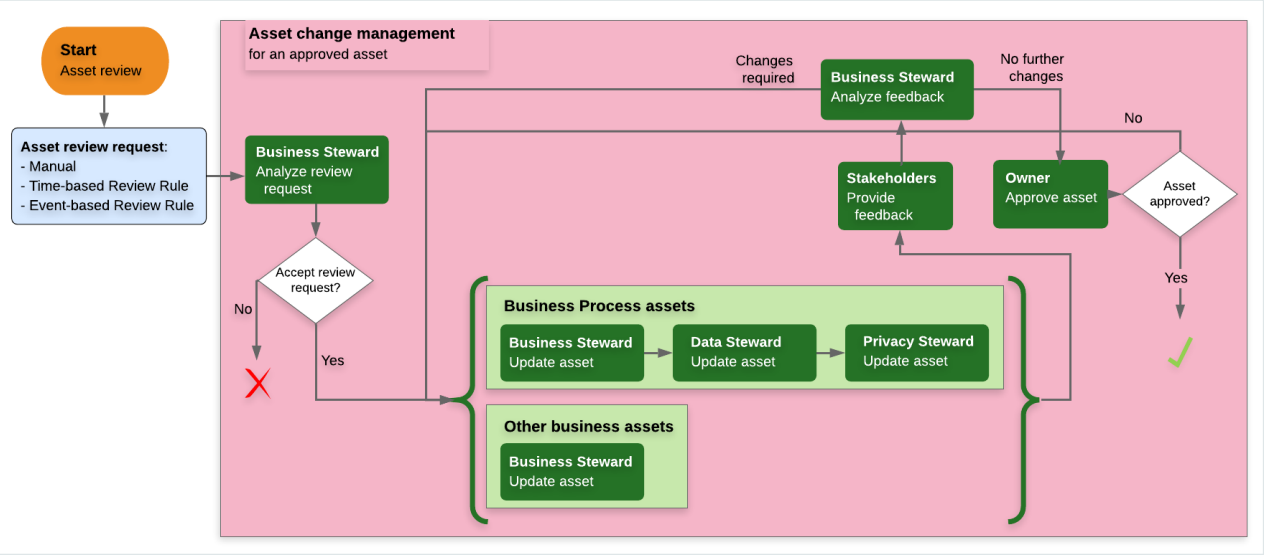
Trigger types	Description	Trigger mechanism
Manual	A trigger that is manually actioned by a user if, for example, the user wants to request a review of a Business Process asset considered to be incomplete or inaccurate. Any user can manually request a review of an approved asset.	Any user clicks **Submit review request**: • On an asset page of an approved asset. • In an asset view. From an asset view, you can trigger a review request for multiple assets, of different asset types, at the same time. • In a traceability view.
Time-based	A trigger that is automatically actioned at a specified frequency. This is useful for assessment assets for which you might be required to review periodically to comply with a regulation.	A Time-based Review Rule asset that dictates, for example, that all PIA assets should be reviewed every 12 months.
Event-based	A trigger that is automatically actioned by the fact of changes made to specified characteristics of a related asset.	An Event-based Review Rule asset that dictates, for example, that Business Process assets should be reviewed if changes have been made to related Technology assets.

Update an asset directly

In addition to the three scenarios described in the preceding section, the Update asset directly workflow enables Business Stewards to start the asset change management process, without creating Review Request assets, assigning tasks to themselves to approve, or triggering the Review Request Handler workflow.

Asset change management process summary

This section provides an example overview of the asset change management process.



> Note Assessment assets assess a situation at a specific moment in time. As such, their characteristics cannot be updated. If an assessment asset is deemed to be outdated, a new assessment asset is required. The new assessment asset is either an entirely new asset or a copy of a previous assessment asset. In the latter case, the asset inherits all of the characteristics from the previous assessment asset, which are then updated and eventually approved. At that point, the status of the previous assessment asset becomes Obsolete.

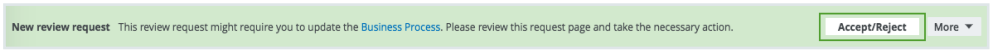
A review request is triggered

Let's suppose a review request is triggered for one of your Business Process assets. In this case:

- A Review Request asset is created.
  The Review Request asset is related to the Business Process asset by the relation type *[Asset] impacts / is impacted by [Issue]*
- The Review Request Handler workflow is triggered and the Business Steward and Owner for the Business Process:
  - Are notified via email.
  - Receive tasks in their respective My Tasks pages.

The Review Request asset is reviewed

The Business Steward or Owner reviews the details of the Review Request asset and decides whether or not changes to the Business Process asset are warranted.

Condition	What's next?
Changes are warranted.	1. On the Review Request asset page, the Business Steward or Owner clicks **Accept/Reject**.  » The **New review request** dialog box appears. 2. The Business Steward or Owner optionally enters a reason for accepting the review request, and then clicks **Accept**. » The Characteristics Management workflow is started. » The status of the Business Process asset becomes Under Review. » The status of the Review Request asset becomes Accepted. » If the review request was triggered manually by a user, that user is notified via email that the Business Process asset is under review.
Changes are not warranted.	1. On the Review Request asset page, the Business Steward or Owner clicks **Accept/Reject**. » The **New review request** dialog box appears. 2. The Business Steward or Owner optionally enters a reason for rejecting the review request, and then clicks **Reject**. » The status of the Business Process asset remains Approved. » The status of the Review Request asset becomes Rejected. » The relation between the Business Process asset and the Review Request asset is maintained, for auditing purposes. » If the review request was triggered manually by a user, that user is notified via email that the Business Process asset will not be updated.

Review Rule assets

Business Stewards and Owners can configure review rules to trigger the review of assets of specified asset types. There are two types of review rules:

- Time-based Review Rule.
- Event-based Review Rule.

> Note These two asset types are child asset types to the parent asset type Review Rule, which is a child of parent asset type Governance Asset.

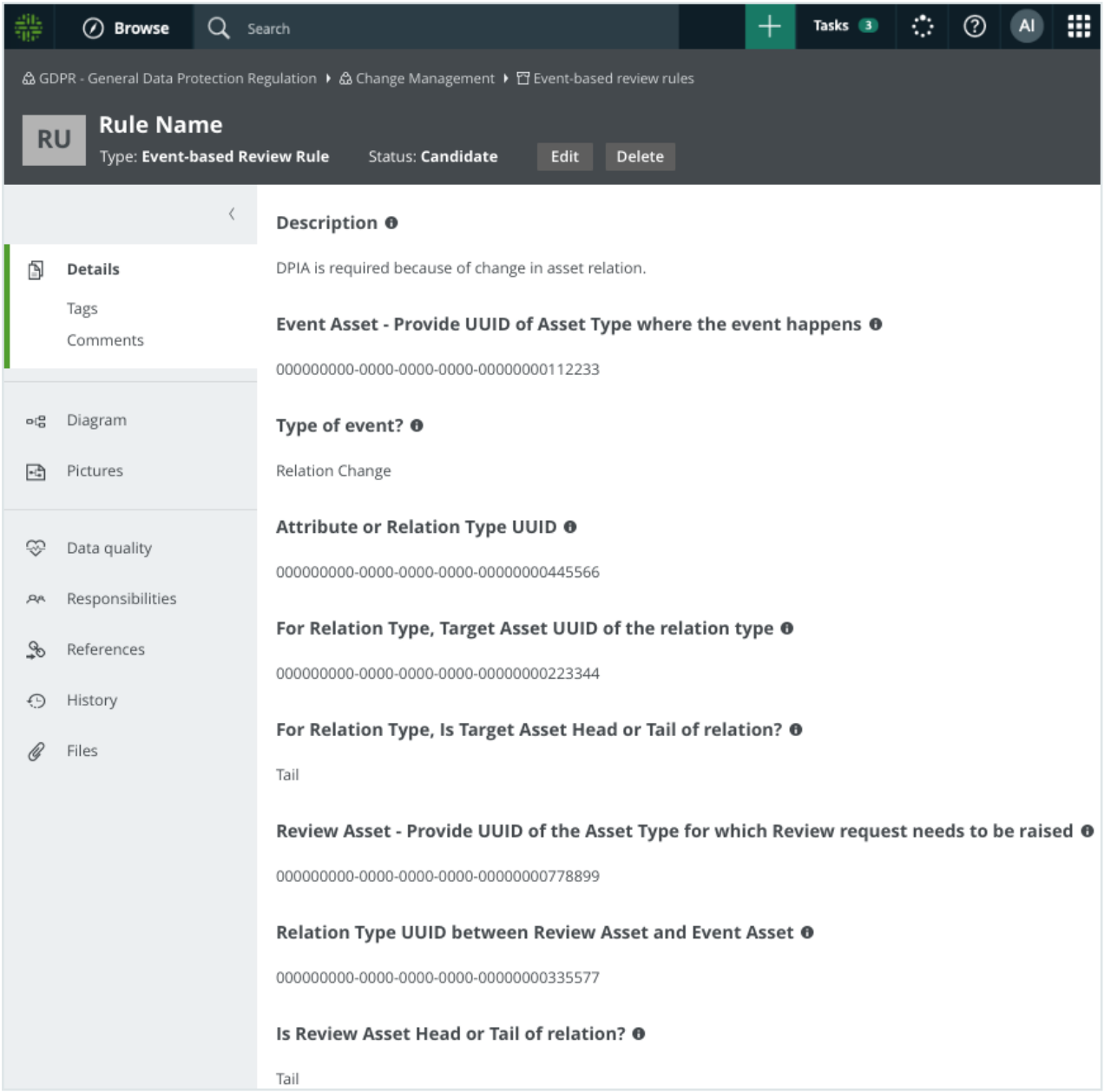
When the configured conditions are met:

- A Review Request asset is automatically created.
- A task is assigned to the Business Steward, to prompt a review of the related asset.

Review Rule assets can be:

- Created by clicking + in the main menu.
- Configured by editing a packaged Review Rule asset.
- Selected during the asset onboarding process, in which case a relation is created between the newly proposed asset and the Review Rule asset.

As shown in the following image, the conditions upon which a review is triggered are stored as attributes in the respective asset.



Packaged review rule assets

Collibra Data Privacy comes with packaged Time-based and Event-based Review Rule assets, which you can configure to suit your needs. They are stored in their respective domains, in the Asset Change Management subcommunity of the Data privacy building blocks community.

Time-based review rule

As a Business Steward or Owner for a domain, you can create Time-based Review Rule assets to trigger the review of assets in your domain, after an elapsed amount of time. This is particularly useful for scheduling reviews of your assessment assets, for some of which data privacy regulations encourage periodic reviews.

Time-based review rules are founded on the cron value specified in the Frequency attribute. At the specified frequency, a Review Request asset is created, prompting a review of the related asset. For more information on cron, see Cron syntax.

To eliminate the chance of overly frequent review requests, the cron value of the Frequency attribute is linked to the value of the Last Modified attribute of the related asset.

Example
You configure a Time-based Review Rule asset to trigger the review of related Technology Assets every 12 months. Suppose, then, that a related Technology Asset is updated for a reason unrelated to your Time-based Review Rule asset. When the changes have been approved, its Last Modified date is updated. In accordance with the cron value specified in your Time-based Review Rule asset, the related Technology Asset will be reviewed 12 months after it was last modified.

Time-based reviews can only be triggered for assets that have the status Accepted or Approved.

Example
You configure a Time-based Review Rule asset to trigger the review of all PIA assets 12 months after their status becomes Accepted. When the 12 months have elapsed:

- A Review Request asset is created with the status New.
- The status of the Time-based Review Rule asset does not evolve; it remains Accepted.
- The following relations are established:
  - The Time-based Review Rule asset is related to the PIA by the relation type: *Assessment assesses / is assessed by Asset*
  - The Review Request asset is related to the PIA by the relation type: *[Asset] impacts / is impacted by [Issue]*.

PIA assets cannot be updated (see Asset onboarding and change management), so you start the PIA workflow for the relevant asset.

- The status of the new PIA is New.
- The status of the original PIA remains Approved, until the new PIA asset is approved. At that time, the status of the original PIA asset becomes Obsolete.
- For audit purposes, the relations between the related asset and both PIA assets remain intact.

Create a Time-based Review Rule asset

There are two ways by which you can create Time-based Review Rules assets:

- Via the global **Create** button.
- By editing a packaged Time-based Review Rule asset.

Via the global Create button

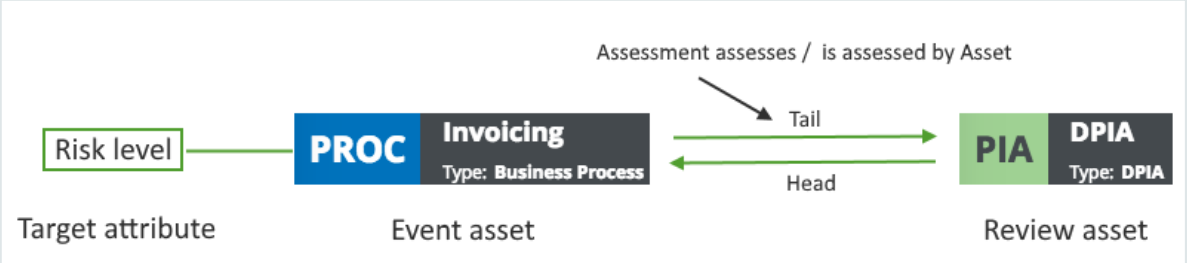
1. In the main menu, click the **Create** (+) button.
   » The **Create** dialog box appears.
2. Select **Time-based Review Rule**.
3. Enter the required information.

Field	Description
Type	The asset type. This is pre-populated.
Domain	The domain in which the asset will be created.
Name	The name of the asset.

4. Go to the asset page of the newly created asset.

5. Enter the required information.

Example The following image illustrates the example scenario that is referred to in this step of the procedure.



Field	Description
Description	A description of the review rule. The text you enter in this field will be added as a comment in the Review Request asset that is created when the rule triggers the review of the related asset. Example "Review Data Protection Impact Assessment with a "High" final risk score, every 12 months. Please consider reviewing the PIA asset for related Business Process assets, if the overall risks to the related data subjects, and attributes like Controller, Processor, Purpose or Sensitivity associated with this Business Process asset have changed significantly."

Field	Description
Revision frequency	The frequency with which related assets are to be reviewed. For this attribute, you have to select a cron value. Cron values are represented by Code Value assets, in the CRON codes domain. > Example The cron code "0 0 0 15 APR ? *" equates to every year, on 15 April.
Review Asset - Provide UUID of the Asset Type for which Review request needs to be raised	The UUID of the asset type to which this rule will apply. > Example The UUID of the asset type PIA.
Filter assets of Review Asset Type based on an attribute value	Specify whether or not this rule will also depend on the value of a certain attribute, in addition to the cron value in the Revision frequency attribute. For example, you want to review all Business Process assets every 12 months, but only if the value of the Risk attribute is "High". The possible values are: ◦ Yes - filter based on attribute value. ◦ No - apply rule to all assets.
If yes, provide attribute type UUID	This only applies if you choose **Yes - filter based on attribute value** for the previous attribute. > Example The UUID of the Risk attribute.

Field	Description
Attribute value to filter on	The value that would trigger a review. Example Risk attribute, value equals "High".

6. In the subheading, click **Edit**.

» The Edit <asset name> dialog box appears.

7. In the **Status** field, select **Enabled**.

Edit a packaged Time-based Review Rule asset

1. Go to the asset page of a packaged Time-based Review Rule asset.

> Tip You can find these assets in the Asset Change Management subcommunity, in the Data privacy building blocks community.

2. Edit the asset's attributes and relations to meet your needs.

Event-based review rule

As a Business Steward or Owner for a domain, you can create Event-based Review Rule assets to trigger the review of other assets, based on changes to specified attributes or relations of those assets.

The value of the "Type of event" attribute in the Event-based Review Rule asset determines the basis upon which a review request is triggered.

Value of "Type of event" attribute	Description
On attribute change	Event-based Review Rule founded on changes to one or more specified attributes of a related asset of a specified asset type. Example You create an Event-based Review Rule asset that triggers the review of a related PIA asset if the value of the Sensitivity attribute of a Data Set asset changes. If the value of the attribute changes, and therefore the related Data Set asset is affected, a review of the PIA related to that Data Set is needed.
On relation change	Event-based Review Rule founded on changes to one or more specified relations of a related asset of a specified asset type. Example You create a Event-based Review Rule asset that triggers the review of a related PIA asset if the relation between a related Controller asset and a Business Process asset changes.

Note Event-based review rules are triggered by changes to assets resulting specifically from asset change management workflows. This means that changes to assets made directly via an asset page will not trigger a review of the asset.

Create an Event-based Review Rule asset

There are two ways by which you can create Event-based Review Rules assets:

- Via the global **Create** button.
- By editing a packaged Event-based Review Rule asset.

Via the global Create button

1. In the main menu, click the **Create** (+) button.
   » The **Create** dialog box appears.
2. Select **Event-based Review Rule**.
3. Enter the required information.

Field	Description
Type	The asset type. This is pre-populated.
Domain	The domain in which the asset will be created.
Name	The name of the asset.

4. Go to the asset page of the newly created asset.
5. Enter the required information.

Example The following image illustrates the example scenario that is referred to in this step of the procedure.

Field	Description
Description	A description of the review rule. The text you enter in this field will be added as a comment in the Review Request asset that is created when the rule triggers the review of the related asset. > Example "A Review Request has been triggered due to an update to the Legal Basis of a business process. Please consider reviewing the PIA asset related to this Business Process asset, as this change might impact your assessment of legal bases in the PIA asset. As a result, you might be required to change the Final Risk score of the assessment, or request authority from your data subjects to continue deploying the business process."
Event Asset - Provide UUID of Asset Type where the event happens	The UUID of the asset type that this review rule will monitor. Assets of the specified asset type will be subject to review if triggered by this rule. > Example The UUID of the Business Process asset.
Type of event	Determines the type of change that will trigger a review of a related asset. The possible values are: ◦ On attribute change. ◦ On relation change. > Example In this example, we have chosen **On relation change**.

Field	Description
Attribute or Relation Type UUID	The UUID of the attribute or relation type (depending on your choice in the **Type of event** field) that this review rule will monitor. Example The UUID of the relation type *Legal Basis determines lawfulness of / lawfulness determined by Business Process*.
For Relation Type, Target Asset UUID of the relation type	The UUID of the asset type of the target asset. Example The UUID of the asset type Legal Basis. Note This field only applies if you selected **On relation change** in the **Type of event** field.
For Relation Type, Is Target Asset Head or Tail of the relation?	Specify whether the target asset represents the head or tail in the relation with the event asset. Example The asset type Legal Basis is the head of the relation type *Legal Basis determines lawfulness of / lawfulness determined by Business Process*. Note This field only applies if you selected **On relation change** in the **Type of event** field.

Field	Description
Path to Review Asset Type	A set of complex relations that specifies the path from the asset in which the change occurred (the event asset), to the asset that should be reviewed. Use a progressive sequence to specify the order of the path: ◦ Sequence 1 is the path from the event asset, to the first-level asset, as determined by the specified relation type. ◦ Sequence 2 is the path from the first-level asset to second-level asset, again as determined by the specified relation type. ◦ You can specify as many sequences as is necessary. ◦ The last review asset type, as per the sequences in the table, is the asset type for which a review request is created.
Relation Type UUID	The UUID of the relation type between: ◦ For Sequence 1: the event asset and the first-level review asset type. ◦ For subsequent sequences: the first-level review asset type and the subsequent level review asset types. ◦ For the last sequence: the previous level review asset type and the asset type for which a review request will be created. Example The UUID of the relation type *Assessment assesses / is assessed by Asset*.

Field	Description
Review Asset Type UUID	The UUID of the asset type of: ◦ For Sequence 1: the first-level review asset type. ◦ For subsequent sequences: the subsequent level review asset types. ◦ For the last sequence: the asset type for which a review request will be created. Example The UUID of the asset type PIA.
Head/Tail	Specify whether: ◦ For Sequence 1: the event asset represents the head or tail in the relation with the first-level review asset type. ◦ For subsequent sequences: the preceding level review asset types represent the head or tail in the relation with their successive level asset types. ◦ For the last sequence: the penultimate level asset type represents the head or tail in the relation with the asset type for which a review request will be created. Example The asset type PIA is the head in the relation type *Assessment assesses / is assessed by Asset*.

6. In the subheading, click **Edit**.

» The Edit <asset name> dialog box appears.

7. In the **Status** field, select **Enabled**.
The Event-based Review Rule asset is enabled and will be detected by the Govern Asset workflow.

Edit a packaged Event-based Review Rule asset

1. Go to the asset page of a packaged Event-based Review Rule asset.

   > Tip You can find these assets in the Asset Change Management subcommunity, in the Data privacy building blocks community.

2. Edit the asset's attributes and relations to meet your needs.

Govern Asset workflow

This workflow monitors all enabled Event-based Review Rule assets.

When the conditions configured in an enabled Event-based Review Rule asset are met, this workflow either:

- Creates a new Review Request asset, to prompt the Business Steward or Owner to review the related asset.
- If the related asset is already under review, meaning an in-process Review Request asset exists, it updates that Review Request asset. Specifically, the description of the review request is added as a comment in the existing Review Request asset.

The Review Request Handler workflow is also triggered to manage the acceptance or rejection of the review request.

Review Request asset

When an asset review is triggered, either manually or via a Time-based or Event-based Review Rule, a Review Request asset is created and the Review Request Handler workflow is started.

The following is true of the Review Request asset:

- It is created in a domain of type Issue Vocabulary, in the community of the related asset.

> Warning The Issue Vocabulary domain is a "hidden" domain that exists in every community. This means it doesn't appear in the Collibra Browser, which helps to avoid it being inadvertently deleted. For some workflows to work correctly, it is imperative that you not delete such hidden domains. You can view all the assets in hidden domains via the Data Helpdesk.

- The name of the asset is formatted as: [RR] <related asset name> - creation date of Review Request asset
  For example: **[RR] Invoicing - 2019/04/15**
- It has the status New.
- It is linked to the related asset by the relation type *[Asset] impacts / is impacted by [Issue]*.

Multiple review requests for a single asset

Over the lifetime of any privacy-related asset, the asset may need to be reviewed and updated. It is possible to have multiple, simultaneous review requests for a single asset. Keep in mind, however, that if there are multiple Review Request assets for a single asset, only one will have the status New, Accepted, or Rejected. All others will have the status Obsolete.

Example
Let's say that a user finds the description of an approved Business Process asset to be misleading. The user manually triggers a review request and a Review Request asset is created. At this point:

- The Review Request Handler workflow is triggered.
- The status of the Business Process asset is Approved.
- The status of the Review Request asset is New.
- The relation *[Issue] impacts / is impacted by [Asset]* is automatically added between the two assets.

The Business Steward reviews the request, agrees that a change is warranted, and the Business Process asset follows the asset change management process.

- The status of the Business Process asset becomes In review.
- The status of the Review Request asset is In review.

However, before the changes to the Business Process asset are approved, two more review requests are triggered for the same Business Process asset. Because the recent changes have not yet been approved, no new Review Request assets are created for the two new review requests. Rather, the details of the new requests are added as comments in the existing Review Request asset, and the Business Steward is notified of the new requests.

Eventually all of the changes to the Business Process asset are made and formally approved via the approval workflow. At this point:

- The status of the Business Process asset becomes Approved.
- The status of the Review Request asset becomes Implemented.
- For audit purposes, the relation between the two assets is maintained.

Now let's say that a new review request is triggered for the same Business Process. In this case:

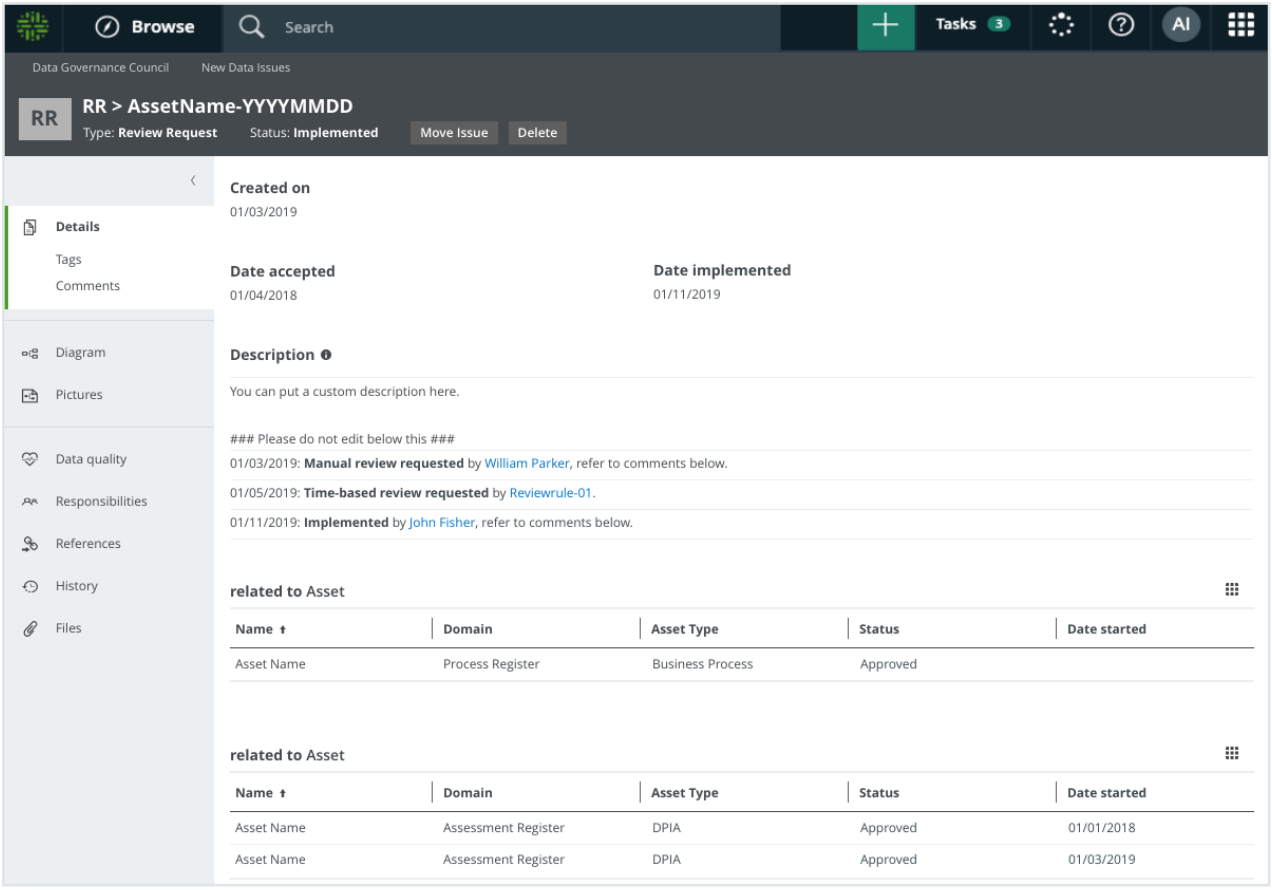
- A new Review Request asset is created.
- The Business Process asset is now:
  - related to the new Review Request asset, which has the status New.
  - related to the original Review Request asset, the status of which goes from Implemented to Obsolete.

The relations between the Business Process asset and its related Review Request assets will be maintained for the life of the Business Process asset. If there are multiple Review Request assets related to the Business Process asset, exactly one will have the status New, In review, or Rejected. All others will have the status Obsolete.

Review Request asset page

The Review Request asset page contains all of the details about the review request.

If additional review requests are triggered for an asset that is already under review, the details of each additional request are added as comments on the Review Request asset page.



Review Request Handler workflow

When an asset review is triggered:

- A new Review Request asset is created, with the status New.
- The Review Request Handler workflow is triggered.

This workflow prompts the Business Steward to review the details of the Review Request asset and accept or reject the asset.

If the Review Request asset is...	Then...
Accepted	The status of the Review Request asset becomes Accepted. Note If the asset to be reviewed is an assessment asset, the Business Steward can choose to either: • Create a new assessment asset. • Copy the attributes, relations and non-inherited roles from the existing approved assessment. The new assessment asset is created with the status Candidate. The status of the previously existing assessment asset becomes Obsolete. The Review Request Handler (Sub Process) workflow is triggered on the business asset to be reviewed or the new assessment asset, and the asset follows the asset change management process. When the proposed changes have been approved: • The status of the Review Request asset becomes Implemented. • The status of the updated asset becomes Approved.
Rejected	• The status of the Review Request asset becomes Rejected. • The status of the asset to be reviewed remains Approved.

Requester and Stakeholder responsibilities

If an asset review is triggered manually, the user that triggered the review request:

- Is assigned the Requester responsibility for the Review Request asset.

- Can select **Notify me on the progress of the asset(s)**, when triggering the request, to also be assigned the Stakeholder responsibility for the Review Request asset.

- Receives notifications about any changes to the Review Request asset.

Status evolution

Review Request assets can have the following statuses:

Condition	Status
The Review Request asset is created.	New
The Business Steward reviews the Review Request asset and decides that change to the related asset is warranted.	Accepted
The Business Steward reviews the Review Request asset and decides that no change to the related asset is warranted.	Rejected
The related asset has been updated and all changes have been approved.	Implemented
For a given asset, a related Review Request asset exists with the status Implemented. For the same asset, a new Review Request asset is created.	• The status of the new Review Request asset is New. • The status of the implemented Review Request becomes Obsolete.

Edit an approved asset as a Business Steward

There are three means by which to trigger the review of an approved asset. In each case:

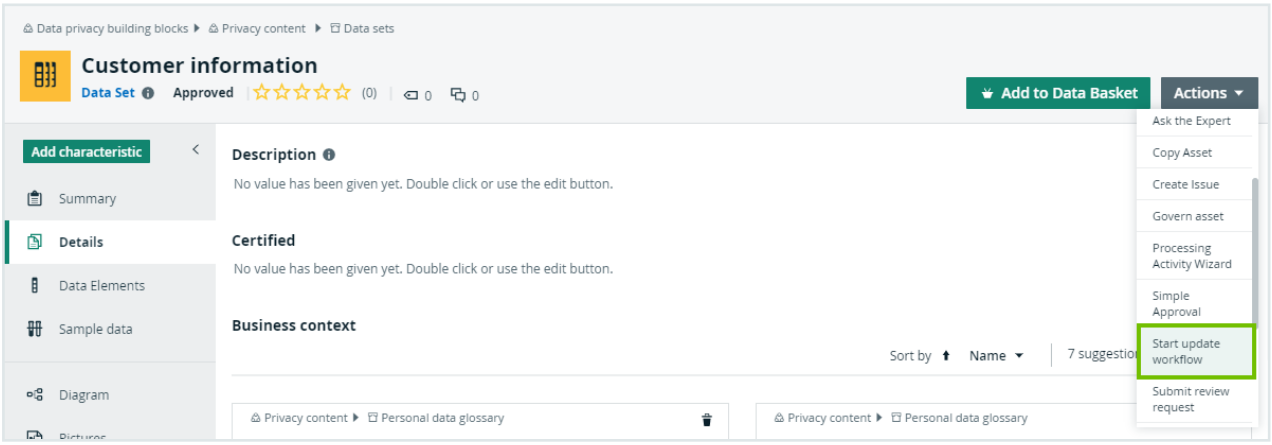
- A Review Request asset is created.
- A task is assigned to the Business Steward of the relevant asset.
- The Review Request Handler workflow is started.

The Business Steward reviews the details of the request and accepts or rejects the Review Request asset.

But what if a Business Steward wants to edit an approved asset? The Update asset directly workflow enables Business Stewards to start the asset change management process, without creating Review Request assets, assigning tasks to themselves to approve, or triggering the Review Request Handler workflow.

Starting the Update asset directly workflow

Any Business Steward can start this workflow by clicking **Start update workflow** on the asset page of the relevant approved asset.



This triggers the Characteristics management phase of the asset change management process.

- For Business Process assets, the Business Steward, Data Steward and Privacy Steward are prompted, in succession, to edit the asset in accordance with each users area of expertise.

- For other business assets, such as Risk and Technology assets, only the Business Steward is prompted to edit the asset.

Applicable asset types

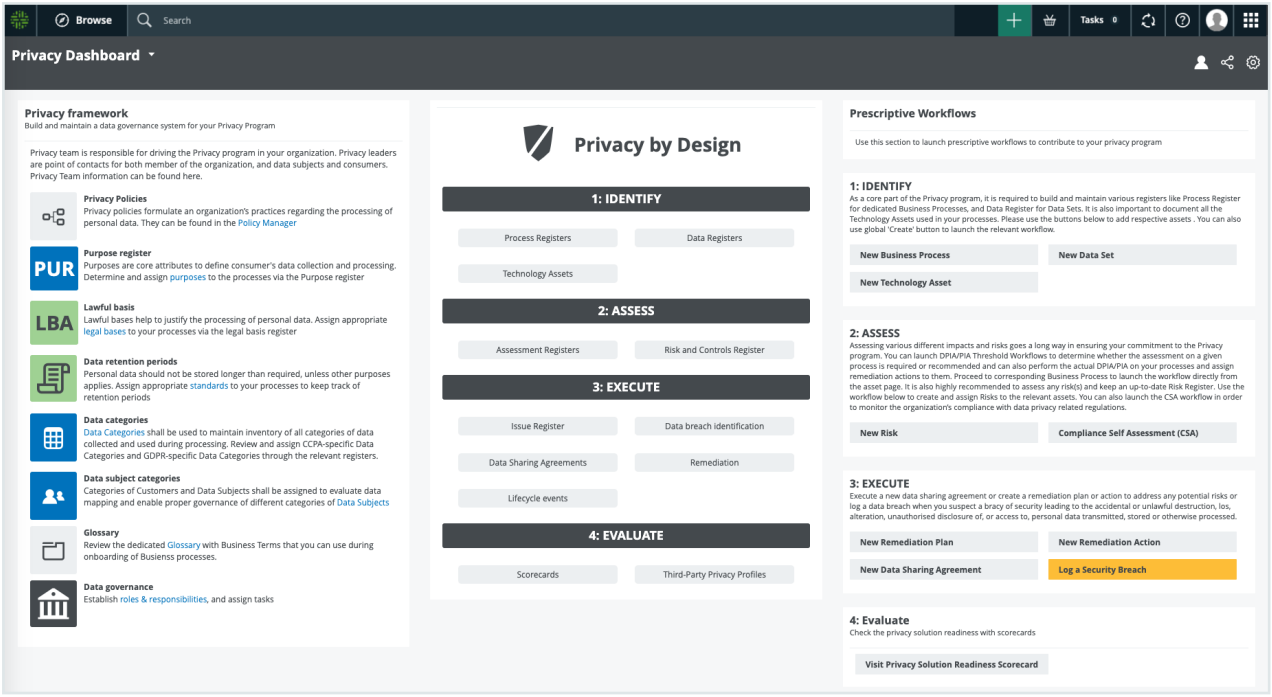
Applicable asset types are the following:

- Business Process
- Data Set
- Technology Asset
- Data Sharing Agreement
- Risk
- Remediation Plan
- Remediation Action
- Privacy Impact Assessment (PIA)
- Data Protection Impact Assessment (DPIA)
- Legitimate Interest Assessment (LIA)
- Compliance Self Assessment (CSA)

> Note Remember that assessment assets cannot be edited. If an assessment asset is deemed to be outdated or inaccurate, a new assessment asset is required. If a Business Steward clicks **Start update workflow** on the asset page of an assessment asset, the respective workflow to create a new assessment asset will start.

Privacy Dashboard

The Privacy Dashboard is the packaged dashboard for your privacy and risk program. It serves as a landing page for stakeholders and those interested in your program. The dashboard contains several sections that inform users on the various aspects of your program and enable them to start workflows.



Start workflows

Users can start the following workflows from this dashboard:

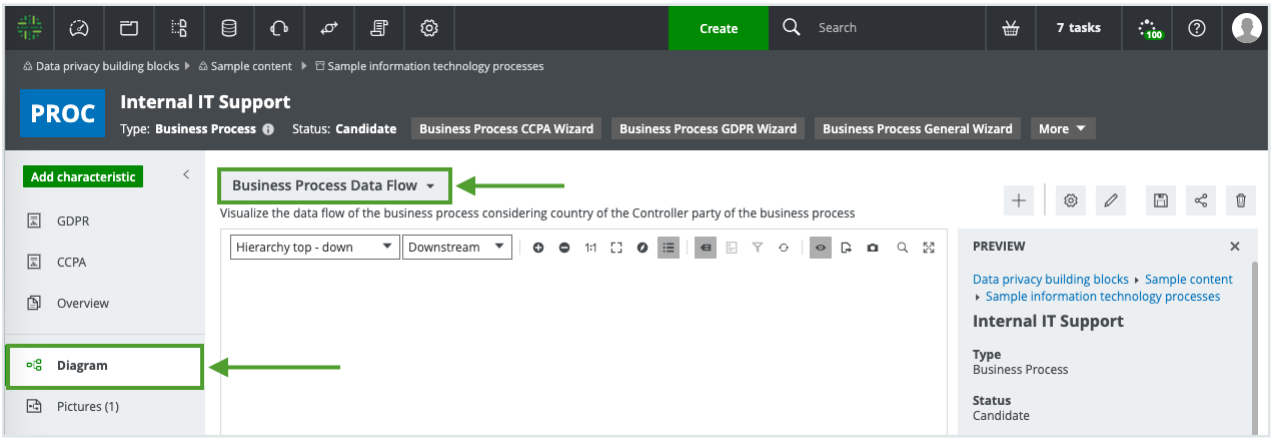
- New Business Process: to create Business Process assets that are used to document high-level business processes.
- New Data Set: to create Data Set assets that contain personal data.
- New Technology Asset: to create a Technology Asset.
- New Risk(s): to create Risk assets; determine their events, risks sources and consequences; the controls that are used to mitigate the risks; the inherent and residual likelihood; the severity and risk level; and the assets to which the risks are related.
- Compliance Self Assessment: to help monitor your organization’s compliance with GDPR.
- New Remediation Plan: to create Remediation Plan assets that group multiple Remediation Action assets.
- New Remediation Action: to create Remediation Action assets that address one or more Risk assets.
- New Data Sharing Agreement: to create Data Sharing Agreement assets that govern the relationship and activities between a Controller and a Processor, and help both parties understand their responsibilities and liabilities.

- Log a Security Breach: to log a potential breach of security that could lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Privacy-related diagram views

Data privacy regulation compliance is a perfect use case for highlighting the powers of Collibra Data Intelligence Cloud's diagram capabilities. To view a diagram of an asset, go to the relevant asset page and click **Diagram** in the Tab pane.

To see all available views, click ▼ next to the default view.



The following table highlights some particularly useful views.

View	Description
Business Process Data Flow View	The default view for Business Process assets is the Business Process Data Flow View. This view shows where data comes from and where it goes, the related Party assets, the related Application, Directories and File assets, and in which Jurisdictions the activities take place. In a glance, you can view how data flows across borders, which can help you with the analysis required for cross-border transfers. You can use this high-level view as a starting point for discovery.

View	Description
Business Process Activity with Recipient View	The Business Process Activity with Recipient View provides a granular view of Business Process assets. It shows: • All supporting Technology Assets, for example Application, Directory and File assets. • All Party assets. • All Jurisdiction assets. This view is best suited for a detailed analysis of a Business Process asset.
Parties and Technology used in Process View	It's important to know which technology assets you use and which parties are involved in your processes. This view shows exactly that.
Vendor Impact View	The Vendor Impact View only shows Party assets of the Party Role Type "Third Party". It shows the same information as the Parties and Technology Used in Process View, but filters out all Party assets that are not of the Party Role Type "Third Party".

For complete information on working with diagrams, see Diagrams.

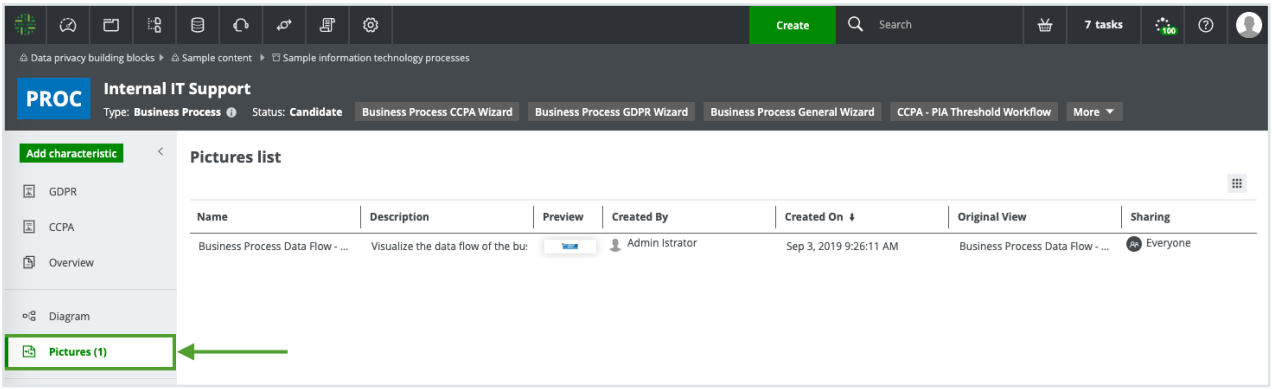
Working with pictures

A picture is a copy of a diagram that is stored separately from the original. You can edit the pictures in the same way you edit diagrams, but there are fewer options available.

Pictures are an easy way to save a diagram after you configured it. You can then reuse it later.

Business processes can change on a regular basis. If a change to a business process introduces greater risk to the rights and freedoms of data subjects, you will have to re-run a PIA. As such, a saved collection of pictures can help during audits.

You can work with pictures similarly to how you work with traceability views. You can move nodes, collapse and expand boxes, export, and so forth.



For complete information on working with pictures, see Pictures.

Reporting Data Layer

The objective of the Reporting Data Layer is to make reporting easier for Collibra Data Intelligence Cloud customers. It captures all your reporting data from Collibra and enables you to build reports, to visualize the data.

The Reporting Data Layer can retrieve vast amounts of data, while retaining history, and without jeopardizing Collibra front-end performance. You can then use the Insights widget to show Tableau reports, or any report that can be shown as an iframe, on your Collibra dashboard. If you're not using Tableau, you can still leverage the definition of the SQL view.

For some example reports, showing how you can leverage the power of the Reporting Data Layer, see Dashboard reports.

For complete information, see Introduction to the Reporting Data Layer in the Documentation Center.

Managing security breaches

Collibra Data Privacy offers a framework for managing potential and actual security breach issues. It consists of the following elements:

- The Log Potential Security Breach workflow.
- The Security Breach Management workflow.
- Personal Data Impact Analysis View.
- The Data Helpdesk, where all Security Issue assets can be viewed.

Workflows

The workflows help you to:

1. Log a potential security breach.
   If someone suspects a potential breach, it has to be logged and investigated.
2. Investigate any potential security breaches that have been logged.
   Not every potential breach is an actual breach. Some potential breaches are the result of other breaches.
3. Report actual security breaches to the appropriate stakeholders.
   During the workflow, users are prompted to add evidence of notification to the Supervisory Authority. Such evidence is added as attachments in the Files tab, where you can add more files at any time.

Log Potential Security Breach workflow

The result of the Log Potential Security Breach workflow is a Security Issue asset. It entails some preliminary information, such as the Technology assets that might have been affected by the potential breach. This information is recorded as attributes in the Security Issue asset.

Keep in mind that the Security Issue asset does not represent an actual data breach, but rather a potential data breach, which requires further investigation. Upon investigation, the possible conclusions are the following:

- There was no breach.
- There was a singular, stand-alone breach.
- There was a breach that is part of a bigger breach.

> Note Before starting this workflow, ensure that the Community Manager and Privacy Steward responsibilities have been created for the New Data Issues domain, to match the resource roles that appear in the Roles section of the workflow settings.
>
> The New Data Issues domain:
>
> - Is the domain in which the Security Issue is created and stored.
> - Is located in the Data Governance Council community.
> - Is "hidden" in the community-domain browser, to avoid it being inadvertently deleted.
>
> You can view all the assets in this domain via the Data Helpdesk. You can also find the domain by searching for it via the Search field.

Start the workflow

You can log a potential data breach via the Privacy dashboard or by clicking + in the main menu.

Security Breach Management workflow

Th Security Breach Management workflow helps you to manage security breach issues.

When a Security Issue is created via the Log a potential security breach workflow, this workflow starts automatically. It is an extended version of the Collibra Data Intelligence Cloud packaged Issue Management workflow, tailored for your privacy and risk program.

> Warning To use this workflow, the Community Manager responsibility must be created for the New Data Issues domain.

Relevant resource roles

The workflows involve the following roles:

Resource role	Tasks
The Community Manager for the New Data Issues domain in which the Security Issue is created.	Assigns an Issue Manager for the Security Issue asset. Note • If the Community Manager responsibility has not been created for the New Data Issues domain, a task is sent to the Sysadmin global role, by default, to create the responsibility. • To configure a role other than the Sysadmin global role for this task, use the variable "User expression is for the 'Admin' role in process" in the general workflow settings. • The workflow cannot continue until the Community Manager responsibility has been created.

Resource role	Tasks
Issue Manager	Collects and provides all necessary information by completing the workflow. As for any resource role, the Issue Manager resource role can be assigned to a single user, a user group or both. If the Issue Manager role is assigned to a user group, the task appears in the list of tasks for every user in the group, and any user can launch the task. When any single user accepts the role and completes the task, the task is removed from the task list for all other users. Warning If you assign the role of Issue Manager to a user group, and a single user rejects the task, the task is rejected for all users in the group and any individual user to whom you may have assigned the resource role.
Privacy Steward	Reviews the analysis and accepts or rejects the Security Issue asset. If the asset is accepted, the Privacy Steward then reports to the relevant stakeholders.

Privacy Steward tasks

If the Issue Manager determines that there has been a data breach, the Privacy Steward reviews the analysis and accepts or rejects the Security Issue asset.

Reject or accept?	What's next?
Reject	The Security Issue asset is assigned back to the Issue Manager, who has to revise the details.

Reject or accept?	What's next?
Accept	The Privacy Steward receives two tasks for each stakeholder to which reporting is due: • A task to notify the Stakeholder. • A task to add evidence of notification in the Security Issue asset. When the Privacy Steward has notified all relevant stakeholders, the status of the Security Issue asset becomes Resolved, and it can be archived.

Reporting to stakeholders

The perceived level of risk to data subjects determines to whom the Privacy Steward has to report.

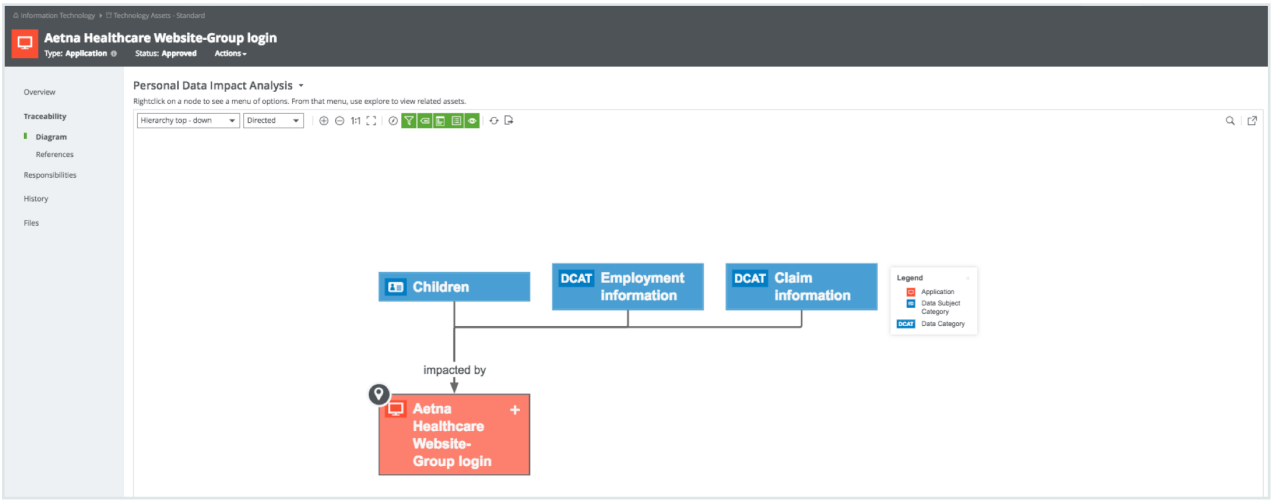
Perceived level of risk	You must report to...
No risk	• No one, although you might want to report to internal stakeholders, such as management.
Low to moderate	• Internal stakeholders. • Supervisor authority.
High	• Internal stakeholders. • Supervisory authority. • Data subjects.

Personal Data Impact Analysis View

The Personal Data Impact Analysis View helps you analyze the impact of a security breach of your personal data, by showing you the Data Category and Data Subject

Category assets that have been impacted by the breach.

The following image shows an example of the Personal Data Impact Analysis view. It shows that when Aetna Healthcare Website Login is breached, data on Children, Employment Information and Claim Information will be compromised. To manage the data breach, you have to store this view during the workflow.



Remediation plans and actions

If you become aware of certain risks, you can document your remediation plans and actions to reduce exposure, to a level that is aligned with your company's risk appetite.

Typically, a remediation action represents an actionable and measurable item to address a specific risk or combination of risks, whereas a remediation plan consists of a predefined sequence of remediation actions, used to address issues that require multiple actions to remedy.

During the onboarding of Remediation Plan assets, users are prompted to add related Remediation Action assets and can start the onboarding workflow for such assets.

You can map your Remediation Plan and Remediation Action assets to your Risk assets wen completing a DPIA/PIA or Legitimate Interest Assessment.

Workflows

Collibra Data Privacy comes with the following packaged workflows:

Workflow	Applicable regulations	Description
New Remediation Action	• CCPA • GDPR	Starts the creation, ownership acceptance and initial approval of a Remediation Action asset.
New Remediation Plan	• CCPA • GDPR	Starts the creation, ownership acceptance and initial approval of a Remediation Plan asset.

Treatment and review of proposed assets

The treatment and review workflow are started by the Business Steward, from the asset page of the relevant Remediation Plan or Remediation Action asset. It allows the Business Steward to:

- Document actions taken, and progress made, with regard to Remediation Plan and Remediation Action assets.
- Create relations with the assets that result from the Remediation Action, meaning a new Control asset.

> Note The completion of this workflow does not result in the creation of a new asset. Rather, new and/or modified attributes and relations are added to the relevant Remediation Plan or Remediation Action asset. The details of the work done are stored as comments.

If the implementation of the remediation plan or action spans a long time period, the Business Steward can use this workflow to log intermediate progress.