

CASE STUDY - COLLIBRA PROTECT

By - Ruta Gokhale

PROJECT DETAILS

- Impact - ***improved the usability, content and visual design*** of the form, to help users create complex queries successfully.
- Team - ***Sr. UX Designer (me)***, Lead UX Designer, Product Manager, Front-end developer, and Back-end developers
- Length - 6 weeks
- Target users - Privacy teams, Data Stewards, Governance Officer, Security Officer

Data Access Rule form

Define Rule

Rule Name
Description (optional)

Grant view access to

Group
for Asset Name
except for Data Category
with Masking for Data Category
and Hide rows where Data Classification has Code Set Option

Summary

Grant view access to [Group]
for [Assets]
except for [Data Category]
with [Masking] for [Data Category]
and [Show/Hide] rows where [Data Classification] has [Code Set] [Value]

Preview Generate Preview

Customer Churn Data Set

Column	Access	Data Category	Masking	Code Value
Customer ID	Masked	ID	1B504D3328E16FDF281D1FB9516DD90B	
First Name	None	Direct PII		
Last Name	None	Direct PII		
Region	Full View			
Country	Filtered			BE, NL
Lifetime value	Full View			
Last support date	Full View			
Start date	Full View			
Credit card number	Masked	Credit card number	*****9999	
Another column	Full View			
Also a column	Full View			
More data here	Full View			
There could	Full View			
Be lots of	Full View			
Columns	Full View			

Cancel Save

UNDERSTANDING THE PROBLEM

- Managing permissions for data in an organization can get cumbersome. The permissions vary across hierarchies and departments. Different groups of people may need varying levels of access to the same data.
- Granting access and approving these requests is a huge bottleneck for privacy teams or data stewards. It leads to longer waiting times or increased turnaround times for consumers of data (such as analysts, data scientists). Additionally, multiple copies of source data are created. Overall, it reduces efficiency of work.

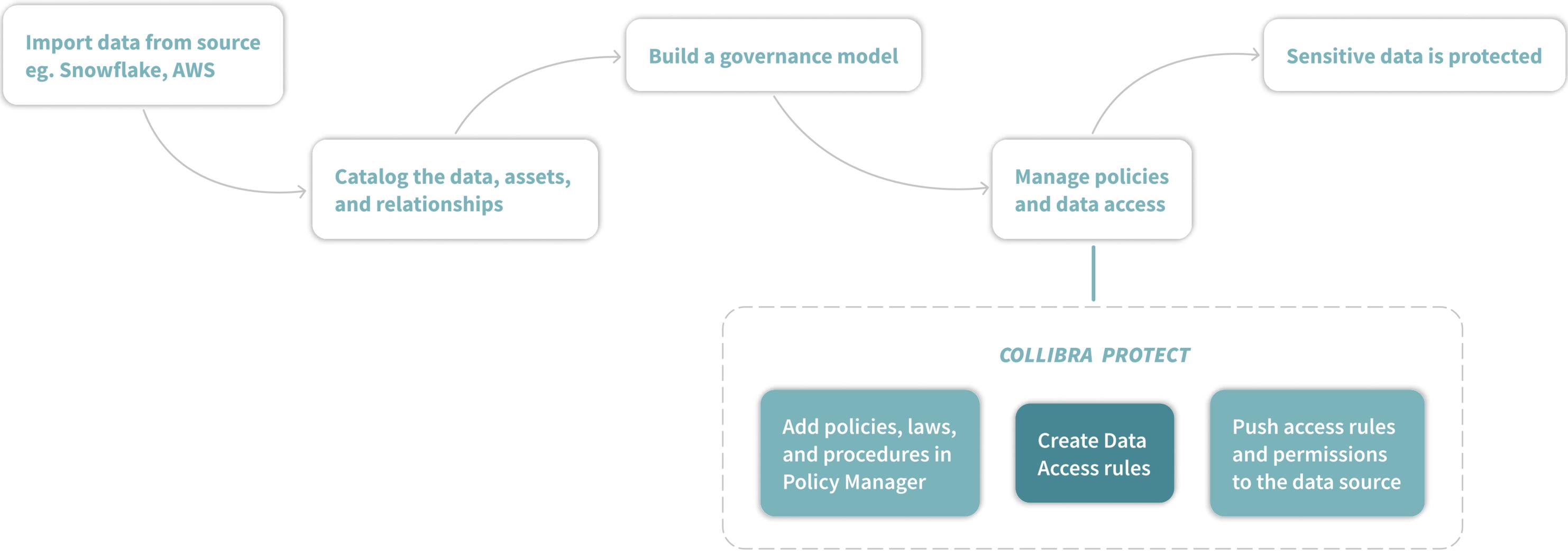
SOLUTION - COLLIBRA PROTECT

- Collibra Protect was developed to address this issue. Collibra Protect provides a *rule creation* capability. It allows privacy teams to streamline access to sensitive data.
- Collibra Protect becomes the central place to manage permissions and data access for different data sources.

The screenshot displays the 'Data Access' management interface. At the top, there are navigation options: 'Browse', 'Search', and 'Tasks 99'. Below this, the 'Data Access' header is visible, with tabs for 'Rules', 'Groups', and 'Audit'. The 'Recents' section shows four recent 'Data Access Rules' for 'Customer Churn Analysis Access', each associated with the 'Marketing, Product' group and the 'PROC' asset. Below this is the 'Data Access Rules' section, which contains a table of all rules. The table has columns for Rule Name, Status, Group, Asset, Last Modified, Created By, and Created Date. The rules are listed in descending order of last modified date, with the most recent rule at the top. The status of the rules varies, including Active, Pending, Failed, Delete Pending, and Not Deleted. The asset column shows 'PROC Customer Churn Analysis' for most rules, and 'Asset(s) deleted' for one rule. The created by column shows 'Dora Portman' for all rules, and 'User deleted' for one rule. The created date for all rules is 'Jan 1, 2022, 9:00 am'. There is an '+ Add Rule' button in the top right corner of the table area.

Rule Name	Status	Group	Asset	Last Modified	Created By	Created Date
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Pending	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Failed	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Delete Pending	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Not Deleted	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Failed	Marketing, Product	PROC Asset(s) deleted	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Failed	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	User deleted	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Jan 19th, 2022, 3:00 pm	Dora Portman	Jan 1, 2022, 9:00 am

COLLIBRA PROTECT WORKFLOW AT A GLANCE



USABILITY TEST INSIGHTS

- Descriptions of different terminologies wasn't very well understood.
- Users weren't confident of having completed a task successfully.
- Pushing protections from Collibra to the data source was seen as a highly useful feature.
- The maturity of an organization's data governance process is a big factor in deciding if this product will be immediately useful.

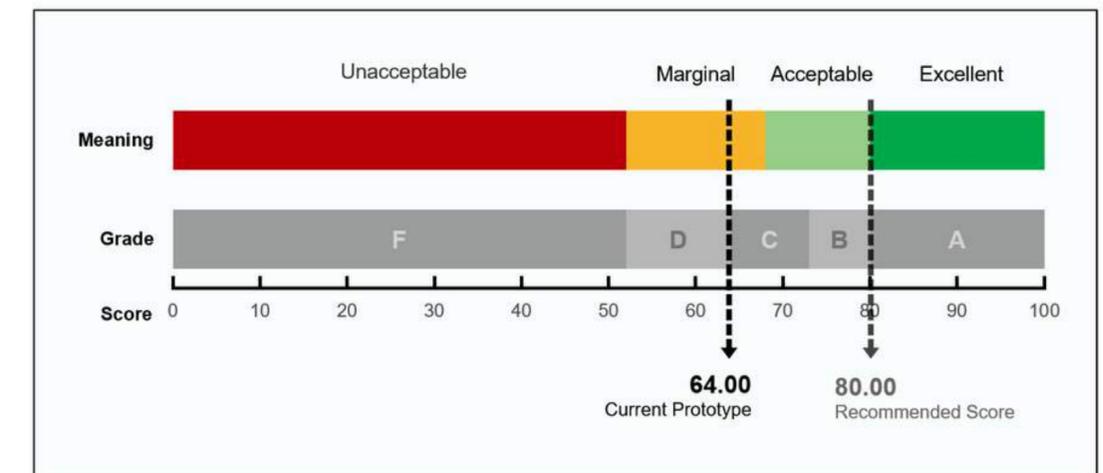
"It's funny that you said I protected [the data]. That wasn't really my feeling after completing [the task]."

– User describing the uncertainty he felt that the data was truly protected.

Each task asked users to create a "rule" that protected the database in a specific way. Each task got progressively difficult.



Metrics



Aggregate System Usability Scale (SUS) for the prototype.

FORM RE-DESIGN

Before

Create Data Access Rule

Define Rule

Rule Name

Description (optional)

Grant view access to

+

for +

except for +

with for +

and rows where has +

Preview

After

Create Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category. You can also conditionally filter rows based on code set values.

Rule Name *

Description

Set rule for

Select assets (data sets, data categories, or business processes) to create data access rules, for user groups imported from the data source. The rule will impact columns linked to the selected assets.

groups *

assets *

Grant access

Grant access to the data linked to these assets.

By selecting this option, additional access is given to the data tables or columns linked with the selected assets. If this box is unchecked, no access is given to the selected assets, but they can still be protected.

Filter data

Use filter options to include or exclude data based on row values. Filtering is based on what value is stored in the cell of that particular column.

+ Filter

Mask data

Apply masking to protect parts of data so user groups do not see the content as it is, but instead see a masked version of it.

for

protect columns with ⓘ

+ Masking

DESIGN DETAILS - INFORMATION

Split the information (dropdowns) into separate sections, to make it more readable and easily digestible.

Create Data Access Rule

Define Rule

Rule Name

Description (optional)

Grant view access to

Group +

for Asset Name +

except for Data Category +

with Masking for Data Category +

and Hide rows where Data Classification has Code Set Option +

Preview

Create Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category. You can also conditionally filter rows based on code set values.

Rule Name *

Description

Set rule for

Select assets (data sets, data categories, or business processes) to create data access rules, for user groups imported from the data source. The rule will impact columns linked to the selected assets.

groups *

assets *

Grant access

Grant access to the data linked to these assets.

By selecting this option, additional access is given to the data tables or columns linked with the selected assets. If this box is unchecked, no access is given to the selected assets, but they can still be protected.

Filter data

Use filter options to include or exclude data based on row values. Filtering is based on what value is stored in the cell of that particular column.

+ Filter

Mask data

Apply masking to protect parts of data so user groups do not see the content as it is, but instead see a masked version of it.

for Data Category Data Classification

protect columns with Default masking ⓘ

+ Masking

DESIGN DETAILS - CONTENT

- Audited the language and content in the entire application, improved the UX copy.
- Made changes to labels and button text so that they're consistent throughout the application.
- Added headers and in-context help to help users understand what to expect in each section.

Create Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category. You can also conditionally filter rows based on code set values.

Rule Name *

Description

Set rule for

Select assets (data sets, data categories, or business processes) to create data access rules, for user groups imported from the data source. The rule will impact columns linked to the selected assets.

groups *

assets *

Grant access

Grant access to the data linked to these assets.

By selecting this option, additional access is given to the data tables or columns linked with the selected assets. If this box is unchecked, no access is given to the selected assets, but they can still be protected.

Filter data

Use filter options to include or exclude data based on row values. Filtering is based on what value is stored in the cell of that particular column.

+ Filter

Mask data

Apply masking to protect parts of data so user groups do not see the content as it is, but instead see a masked version of it.

for **Data Category** **Data Classification**

protect columns with ⓘ

+ Masking

⊞ Generate preview

Cancel **Save rule**

DESIGN DETAILS - VISUAL DESIGN

- Audited the UI elements of the form. Updated the design system components to the latest version.
- Modified the visual design of certain sections.

Create Data Access Rule

Define Rule

Rule Name

Description (optional)

Grant view access to

Group +

for Asset Name +

except for Data Category +

with Masking for Data Category +

and Hide rows where Data Classification has Code Set Option +

Preview

Create Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category. You can also conditionally filter rows based on code set values.

Rule Name *

Description

Set rule for

Select assets (data sets, data categories, or business processes) to create data access rules, for user groups imported from the data source. The rule will impact columns linked to the selected assets.

groups *

assets *

Grant access

Grant access to the data linked to these assets.

By selecting this option, additional access is given to the data tables or columns linked with the selected assets. If this box is unchecked, no access is given to the selected assets, but they can still be protected.

Filter data

Use filter options to include or exclude data based on row values. Filtering is based on what value is stored in the cell of that particular column.

+ Filter

Mask data

Apply masking to protect parts of data so user groups do not see the content as it is, but instead see a masked version of it.

for Data Category Data Classification

protect columns with Default masking ⓘ

+ Masking

FORM RE-DESIGN (POPULATED)

Before

Edit Data Access Rule

Define Rule

Rule Name: Customer Churn Access General

Description (optional): Access to customer churn numbers with sensitive things hidden and masked

Grant view access to:

- Marketing
- and Sales
- for Customer Churn Analysis
- and Customer Churn Analysis 2
- and Customer Churn Analysis 3
- except for Direct PII
- with SHA-2 Hashing for Customer ID
- with Show Last 4 for Credit card number
- with Replace with 9 for Age
- and Hide rows where Country has Country Code BE
- and Hide rows where Country has Country Code NL

Summary

Grant view access to Marketing and Sales for Customer Churn Analysis, Customer Churn Analysis 2, and Customer Churn Analysis 3 except for Direct PII with SHA-2 Hashing for Customer ID and with show last 4 for Credit card number and hide rows where Country has Country Code BE and hide rows where Country has Country Code NL.

Preview Generate Preview

Column	Access	Data Category	Masking	Code Value
Customer ID	Masked	Customer ID	1B504D3328E16FDF281D1FB9516DD908	
First Name	None	Direct PII		
Last Name	None	Direct PII		
Region	Full View			
Country	Filtered			BE, NL
Lifetime value	Full View			
Last support date	Full View			
Start date	Full View			
Credit card number	Masked	Credit card number	*****9876	
Another column	Full View			
Age	Masked	Age	9	
More data here	Full View			
There could	Full View			
Be lots of	Full View			
Columns	Full View			

Cancel Save

After

Create Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category. You can also conditionally filter rows based on code set values.

Rule Name: Restrict access to personal data

Description: Protect all the PII and PI data of the org.

Set rule for

Select assets (data sets, data categories, or business processes) to create data access rules, for user groups imported from the data source. The rule will impact columns linked to the selected assets.

groups: Human Resources, Admins, Marketing, Managers, Executive Leadership, Tech Staff

assets: PII, Personal Information, Customer Data, Marketing Data

Grant access

Grant access to the data linked to these assets. By selecting this option, additional access is given to the data tables or columns linked with the selected assets. If this box is unchecked, no access is given to the selected assets, but they can still be protected.

Filter data

Use filter options to include or exclude data based on row values. Filtering is based on what value is stored in the cell of that particular column.

Include rows where Country has Country codes with Select code value: US, BE

Mask data

Apply masking to protect parts of data so user groups do not see the content as it is, but instead see a masked version of it.

for Data Category: Data Classification: Personal Information, Geographic Information

protect columns with: Default masking

for Data Category: Data Classification: Credit Card Number

protect columns with: Show last 4 characters

Summary

Grant access to Human Resources, Admins, Marketing, Managers, Executive Leadership and Tech Staff for PII, Personal Information, Customer Data, and Marketing Data. Include rows classified as a Country with a value equal to US and BE. With default masking for PII, Personal Information and Geographic Information and show last 4 for Credit Card Information.

Generate preview

Column name	Access	Masking	Masking Agent	Code Value
Customer ID	Masked	1B504D3328E16FDF281D1F1	DCAT	PII
First Name	Masked	68lsdhl%bcD5673Lob@d709	DCAT	Personal Information
Last Name	Masked	34I2dsn6o94dFG8%zVFR7	DCAT	Personal Information
Region	Full View			
Country	Filtered			BE, US
Lifetime value	Full View			
Last support date	Full View			
Start date	Full View			
Credit card number	Masked	*****9999		
Another column	Full View		DATI	Some data att
Also a column	Full View			
More data here	Full View			
There could	Full View			
Be lots of	Full View		DCAT	Personal Infor...
Columns	Full View			ID number

Cancel Save rule

DESIGN DETAILS

After

Set rule for

Select assets (data sets, data categories, or business processes) to create data access rules, for user groups imported from the data source. The rule will impact columns linked to the selected assets.

groups *

Human Resources X Admins X Marketing X Managers X
Executive Leadership X Tech Staff X

assets *

PII X PI X Personal Information X Customer Data X Marketing Data X

Before

Grant view access to

Marketing

and Sales

for Customer Churn Analysis

and Customer Churn Analysis 2

and Customer Churn Analysis 3

except for Direct PII

Create Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category. You can also conditionally filter rows based on code set values.

Rule Name *

Description

Set rule for

Select assets (data sets, data categories, or business processes) to create data access rules, for user groups imported from the data source. The rule will impact columns linked to the selected assets.

groups *

Human Resources X Admins X Marketing X Managers X
Executive Leadership X Tech Staff X

assets *

PII X PI X Personal Information X Customer Data X Marketing Data X

Grant access

Grant access to the data linked to these assets.
By selecting this option, additional access is given to the data tables or columns linked with the selected assets. If this box is unchecked, no access is given to the selected assets, but they can still be protected.

Filter data

Use filter options to include or exclude data based on row values. Filtering is based on what value is stored in the cell of that particular column.

Include rows where Country

has Country codes with Select code value

US X BE X

+ Filter

Mask data

Apply masking to protect parts of data so user groups do not see the content as it is, but instead see a masked version of it.

for Data Category Data Classification Start typing a data category name and press enter

PI X PI X Personal Information X
Geographic Information X

protect columns with Default masking

for Data Category Data Classification Start typing a data category name and press enter

Credit Card Number X

protect columns with Show last 4 characters

+ Masking

Summary

Grant access to Human Resources, Admins, Marketing, Managers, Executive Leadership and Tech Staff for PII, PI, Personal Information, Customer Data, and Marketing Data
Include rows classified as a Country with a value equal to US and BE
With default masking for PII, PI, Personal Information and Geographic Information
and show last 4 for Credit Card Information.

Generate preview

Column name	Access	Masking	Masking Agent	Code Value
Customer ID	Masked	1B504D3328E16FDF281D1F1	DCAT PII	
First Name	Masked	68Isch%6bcD5673Lob@d709	DCAT Personal Information	
Last Name	Masked	34I2ds\$n6o94dFG8%2zVFR7	DCAT Personal Information	
Region	Full View			
Country	Filtered			BE, US
Lifetime value	Full View			
Last support date	Full View			
Start date	Full View			
Credit card number	Masked	*****9999		
Another column	Full View		DATT Some data att	
Also a column	Full View			
More data here	Full View			
There could	Full View			
Be lots of	Full View		DCAT Personal Infor...	
Columns	Full View		ID number	

Cancel Save rule

DESIGN DETAILS

Before

with for

with for + -

with for + -

After

Mask data

Apply masking to protect parts of data so user groups do not see the content as it is, but instead see a masked version of it.

for

protect columns with

for

protect columns with characters

+ Masking

Create Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category. You can also conditionally filter rows based on code set values.

Rule Name *

Description

Set rule for

Select assets (data sets, data categories, or business processes) to create data access rules, for user groups imported from the data source. The rule will impact columns linked to the selected assets.

groups *

assets *

Grant access

Grant access to the data linked to these assets. By selecting this option, additional access is given to the data tables or columns linked with the selected assets. If this box is unchecked, no access is given to the selected assets, but they can still be protected.

Filter data

Use filter options to include or exclude data based on row values. Filtering is based on what value is stored in the cell of that particular column.

Include

has with

+ Filter

Mask data

Apply masking to protect parts of data so user groups do not see the content as it is, but instead see a masked version of it.

for

protect columns with

for

protect columns with characters

+ Masking

Summary

Grant access to **Human Resources, Admins, Marketing, Managers, Executive Leadership** and **Tech Staff** for **PI, PII, Personal Information, Customer Data, and Marketing Data**.
Include rows classified as a **Country** with a value equal to **US** and **BE**.
 With **default masking** for **PI, PII, Personal Information** and **Geographic Information** and **show last 4** for **Credit Card Information**.

Column name	Access	Masking	Masking Agent	Code Value
Customer ID	Masked	1B504D3328E16DFD281D1F1	DCAT	PII
First Name	Masked	68isdh%6cd5673lob@d709	DCAT	Personal Information
Last Name	Masked	342ds%6094dFG8%2vFR7	DCAT	Personal Information
Region	Full View			
Country	Filtered			BE, US
Lifetime value	Full View			
Last support date	Full View			
Start date	Full View			
Credit card number	Masked	*****9999		
Another column	Full View		DATT	Some data att
Also a column	Full View			
More data here	Full View			
There could	Full View			
Be lots of	Full View		DCAT	Personal Infor...
Columns	Full View			ID number

DESIGN DETAILS

Before

Summary

Grant view access to Marketing and Sales for Customer Churn Analysis, Customer Churn Analysis 2, and Customer Churn Analysis 3 except for Direct PII with SHA-2 Hashing for Customer ID and with show last 4 for Credit card number and hide rows where Country has Country Code BE and hide rows where Country has Country Code NL

After

Summary

Grant access to **Human Resources, Admins, Marketing, Managers, Executive Leadership and Tech Staff** for PII, PI, Personal Information, Customer Data, and Marketing Data **Include rows** classified as a Country with a value equal to US and BE With **default masking** for PI, PII, Personal Information and Geographic Information and **show last 4** for Credit Card Information.

Create Data Access Rule

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category. You can also conditionally filter rows based on code set values.

Rule Name *
Restrict access to personal data

Description
Protect all the PII and PI data of the org.

Set rule for
Select assets (data sets, data categories, or business processes) to create data access rules, for user groups imported from the data source. The rule will impact columns linked to the selected assets.

groups *
Start typing a group name and press enter
Human Resources X Admins X Marketing X Managers X
Executive Leadership X Tech Staff X

assets *
Start typing an asset name and press enter
PII X PI X Personal Information X Customer Data X Marketing Data X

Grant access
 Grant access to the data linked to these assets.
By selecting this option, additional access is given to the data tables or columns linked with the selected assets. If this box is unchecked, no access is given to the selected assets, but they can still be protected.

Filter data
Use filter options to include or exclude data based on row values. Filtering is based on what value is stored in the cell of that particular column.

Include rows where Country
has Country codes with Select code value
US X BE X Delete

+ Filter

Mask data
Apply masking to protect parts of data so user groups do not see the content as it is, but instead see a masked version of it.

for Data Category Data Classification Start typing a data category name and press enter
PI X PII X Personal Information X
Geographic Information X

protect columns with Default masking

for Data Category Data Classification Start typing a data category name and press enter
Credit Card Number X

protect columns with Show last 4 characters Delete

+ Masking

Summary
Grant access to **Human Resources, Admins, Marketing, Managers, Executive Leadership and Tech Staff** for PII, PI, Personal Information, Customer Data, and Marketing Data
Include rows classified as a Country with a value equal to US and BE
With **default masking** for PI, PII, Personal Information and Geographic Information
and **show last 4** for Credit Card Information.

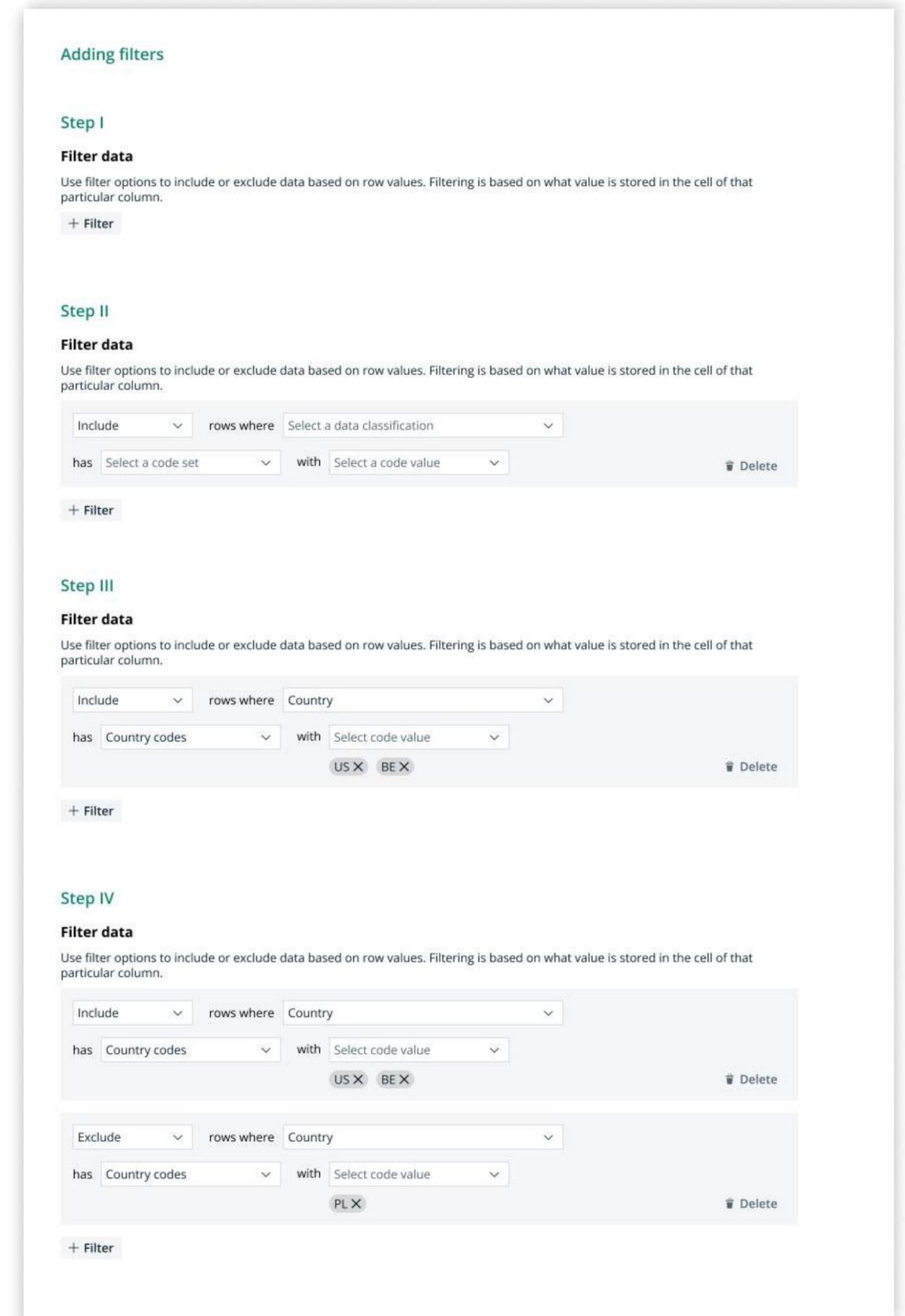
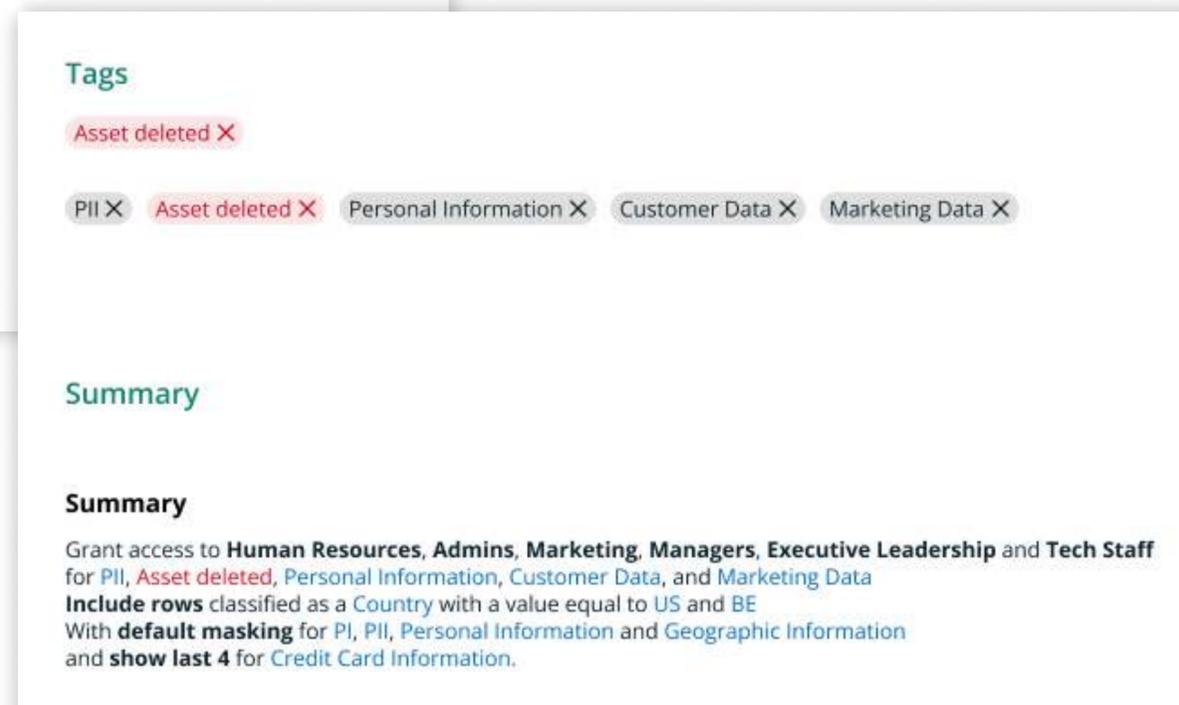
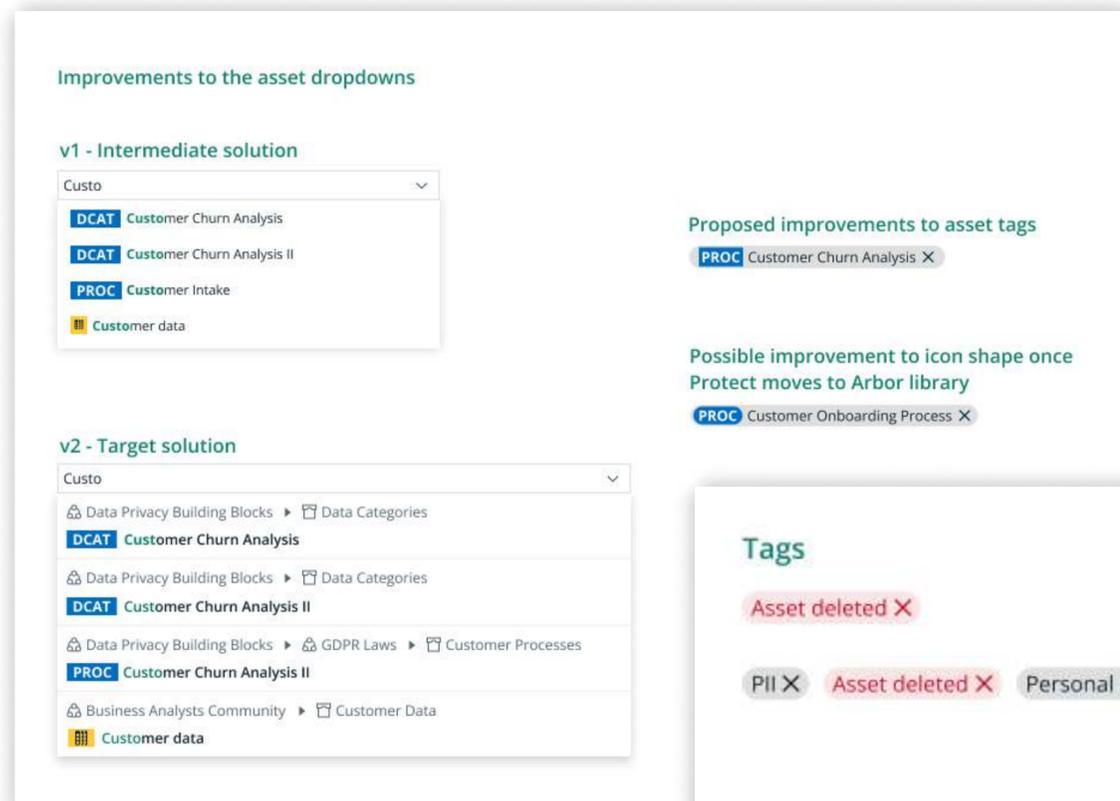
Generate preview

Column name	Access	Masking	Masking Agent	Code Value
Customer ID	Masked	1B50403328E16FDF281D1F1	DCAT PII	
First Name	Masked	68isdh%6bcD5673lob@d709	DCAT Personal Information	
Last Name	Masked	34I2ds%6o94dFG8%2%VFR7	DCAT Personal Information	
Region	Full View			
Country	Filtered			BE, US
Lifetime value	Full View			
Last support date	Full View			
Start date	Full View			
Credit card number	Masked	*****9999		
Another column	Full View		DATT Some data att	
Also a column	Full View			
More data here	Full View			
There could	Full View			
Be lots of	Full View		DCAT Personal Infor...	
Columns	Full View		ID number	

Cancel Save rule

DESIGN DETAILS

Added detailed documentation, covering error states and other specs for developers.



Rules Modal - FINAL DESIGNS

Data Access Rules - Final designs and details

Empty State



Filled-out Form



Details & Specifics



Groups (x) open



Asset selection



Filtering



ACCESSIBILITY



Moving



Summary



Preview section



Deleted assets



Error state



When Grant access or Making useful are selected



Spacing



CONCLUSION

As I reflect on the project outcomes, here are a few things I am proud of accomplishing:

- Improved the usability of the application in an efficient way.
- Built trust with the product manager and good rapport with the developers.
- Discovered better touchpoints and an improved design process.

Protect

Data Protection Standards | **Data Access Rules** | Data Source Policies | Groups | Audit

Data Access Rules

Data access rules can be used to **grant groups access** to a less restrictive view of the data that overrides default data from a Data Protection Standard.

Want to define a default data protection? Create a [Data Protection Standard](#).

[Create Data Access Rule](#)

Recently Modified Rules

Customer Churn Analysis Access
Data Access Rule

Group
Marketing, Product

Asset
PROC Business Process: Customer Churn A...

Customer Churn Analysis Access
Data Access Rule

Group
Marketing, Product

Asset
PROC Business Process: Customer Churn...

Customer Churn Analysis Access
Data Access Rule

Group
Marketing, Product

Asset
PROC Business Process: Customer Churn A...

Customer Churn Analysis Access
Data Access Rule

Group
Marketing, Product

Asset
PROC Business Process: Customer Churn A...

Rule Name	Synchronization Status	Groups	Affected Asset	Rule Type	Created by	Created Date	Last Modified
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Grant access	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Pending	Marketing, Product	PROC Customer Churn Analysis	Grant access and protect de	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Failed	Marketing, Product	PROC Customer Churn Analysis	Grant access	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Delete Pending	Marketing, Product	PROC Customer Churn Analysis	Grant access	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Not Deleted	Marketing, Product	PROC Customer Churn Analysis	Protect data	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Protect data	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Grant access and protect de	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Grant access and protect de	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Grant access and protect de	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Grant access and protect de	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Grant access and protect de	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Failed	Marketing, Product	PROC Asset(s) deleted	Protect data	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Failed	Marketing, Product	PROC Customer Churn Analysis	Grant access	User deleted	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm
Customer Churn Analysis Access	Active	Marketing, Product	PROC Customer Churn Analysis	Grant access	Dora Portman	Jan 1, 2022, 9:00 am	Jan 19th, 2022, 3:00 pm

Create Data Access Rule ✕

Use data access rules to grant groups different access to the same data in data sets, business processes, or identified by data categories. You can mask or hide columns by their data category. You can also conditionally filter rows based on code set values.

Rule Name *

Description

Set rule for

Select assets (data sets, data categories, or business processes) to create data access rules, for user groups imported from the data source. The rule will impact columns linked to the selected assets.

groups *

assets *

Grant access

Grant access to the data linked to these assets.

By selecting this option, additional access is given to the data tables or columns linked with the selected assets. If this box is unchecked, no access is given to the selected assets, but they can still be protected.

Filter data

Use filter options to include or exclude data based on row values. Filtering is based on what value is stored in the cell of that particular column.

+ Filter

Mask data

Apply masking to protect parts of data so user groups do not see the content as it is, but instead see a masked version of it.

for **Data Category** **Data Classification**

protect columns with ?

+ Masking

[Generate preview](#)

[Cancel](#) [Save rule](#)

THANK YOU