



Ruta Gokhale

USER EXPERIENCE DESIGNER

CASE STUDY - COLLIBRA

CASE STUDY

The screenshot displays the Collibra Data Access interface. On the left, the 'Data Access' dashboard shows a 'Recent' section with four entries for 'Customer Churn Analysis Access' rules, each associated with 'Marketing, Product' group and 'PROC' asset. Below this is a 'Data Access Rules' table listing 18 rows of rules, mostly 'Active' with some 'Pending' or 'Failed' status. The right side of the screen is a modal window titled 'Create Data Access Rule'. It contains fields for 'Rule Name' (left empty), 'Description (optional)', and a complex 'Grant view access to' configuration. This configuration includes a 'Group' dropdown set to 'Asset Name', an 'except for' clause for 'Data Category', and conditions for 'Masking' and 'Hide' rows based on 'Data Classification' and 'Code Set'. A 'Summary' section provides a preview of the rule's effect on a 'Customer Churn Data Set' with columns like 'Customer ID', 'First Name', 'Last Name', etc., each with its access level (e.g., Masked, Full View, Filtered) and data category. At the bottom of the modal are 'Cancel' and 'Save' buttons.

<https://www.collibra.com/us/en/products/protect>

Helping data stewards and privacy teams in an organization manage access to data through pred-defined policies for protecting sensitive information

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 dataset.
- Granting access and approving these requests is a huge bottleneck for data stewards. It leads to increased turnaround times and higher waiting time for consumers of the data. Additionally, multiple copies of source data are created. Overall, it reduces efficiency of work.

PROPOSED SOLUTION - COLLIBRA PROTECT

- To address this issue, we proposed an access rule creation workflow which allows data stewards to grant access to groups of people and protect sensitive information.
- These permissions and data access levels are managed through the Collibra platform and pushed to the data source. The aim is to promote a safe data-open culture in organizations.

The screenshot shows the Collibra Protect interface, specifically the Data Access Rules section. The top navigation bar includes 'Browse', 'Search', and various system icons. The main header says 'Protect' and the sub-header is 'Data Access Rules'. Below this, there's a brief description of what data access rules do, followed by a 'Create Data Access Rule' button. A 'Recently Modified Rules' section lists four examples: 'Customer Churn Analysis Access', 'Employee informations Access', 'Product Analytics', and 'Product Inventory Protection', each with details like groups and protected assets. At the bottom is a detailed table of all data access rules, showing columns for Standard Name, Groups, Protected Assets, Owner, Status, and Synchronization. The table lists several rules, including 'Customer Churn Analysis Access', 'Employee Information Access', 'Product Analytics', and 'Product Inventory Protection', with their respective details and status indicators (e.g., Enforced, Queued for sync., Error).

Standard Name	Groups	Protected Assets	Owner	Status	Synchronization
Customer Churn Analysis Access	Marketing, Sales	PROC Customer Churn Analysis	Amy Jhones	Enforced	Synchronized
Employee informations Access	Human Resources	Employee Information, Employee details	Eliza Arquette	Queued for sync.	
Product Analytics	Analysts	PROC Product Usage Analysis	Dora Portman	Error	
Sales data Access	Product	DCAT EMEA Product Sales	Dora Portman	Enforced	Queued for sync.
Product Inventory Protection	Product	DCAT Product information	Frank Gradey	Queued for sync.	
Sales Data Access	Marketing, Product	Sales Data	Dora Portman	Enforced	Queued for sync.
Customer Churn Analysis	Marketing, Product	Unauthorized asset	Elisa Arquette	Enforced	Synchronized
Physical assets info rule	Building Facilities	PROC Buildings and External Offices, PROC Customer Churn Analysis ...	Dora Portman	Enforced	Synchronized

** the work and development for Collibra Protect was already underway when I started

PROJECT CONTEXT

Ideal flow for Policy Enforcement

At Collibra, there were some initiatives I worked on and some features I owned. For this case study, I want to focus on a specific project of Collibra Protect.

As a part of a beta program for this product, we conducted usability tests with 6 participants. The sessions were divided into two sections (40 mins of tasks and 20 mins of informal questions).

I've divided the case study into 2 parts. In the first part, I'll walk through the improvements made to the 'Create Data Access Rules' form, focussing on refinements to an already designed feature. In the second part, I'll show some initial brainstorm work for a new feature, focussing working through the "messiness". Both of these sections are based on some insights from the usability test.

PART I - IMPROVING USABILITY OF THE 'CREATE DATA ACCESS RULE' FORM

DATA ACCESS RULE FORM

- The Data Access Rule form is really the crux of the Protect application.
- It allows data stewards (business users) of this application to create complex non-SQL (plain language) queries through a series of dropdowns to protect specific datasets, tables or columns from group(s) of users.

initial state of the form

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

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

OBJECTIVES OF THE USABILITY TEST

The primary objectives of the usability test were:

- Validate the hypothesis that - business users can understand and create plain language queries.
- Check whether users could understand the tasks and create progressively complex queries.
- Test the usability of the application.
- Understand how well this product fits in the workflow of privacy teams for an organization. Know more about the unknowns.

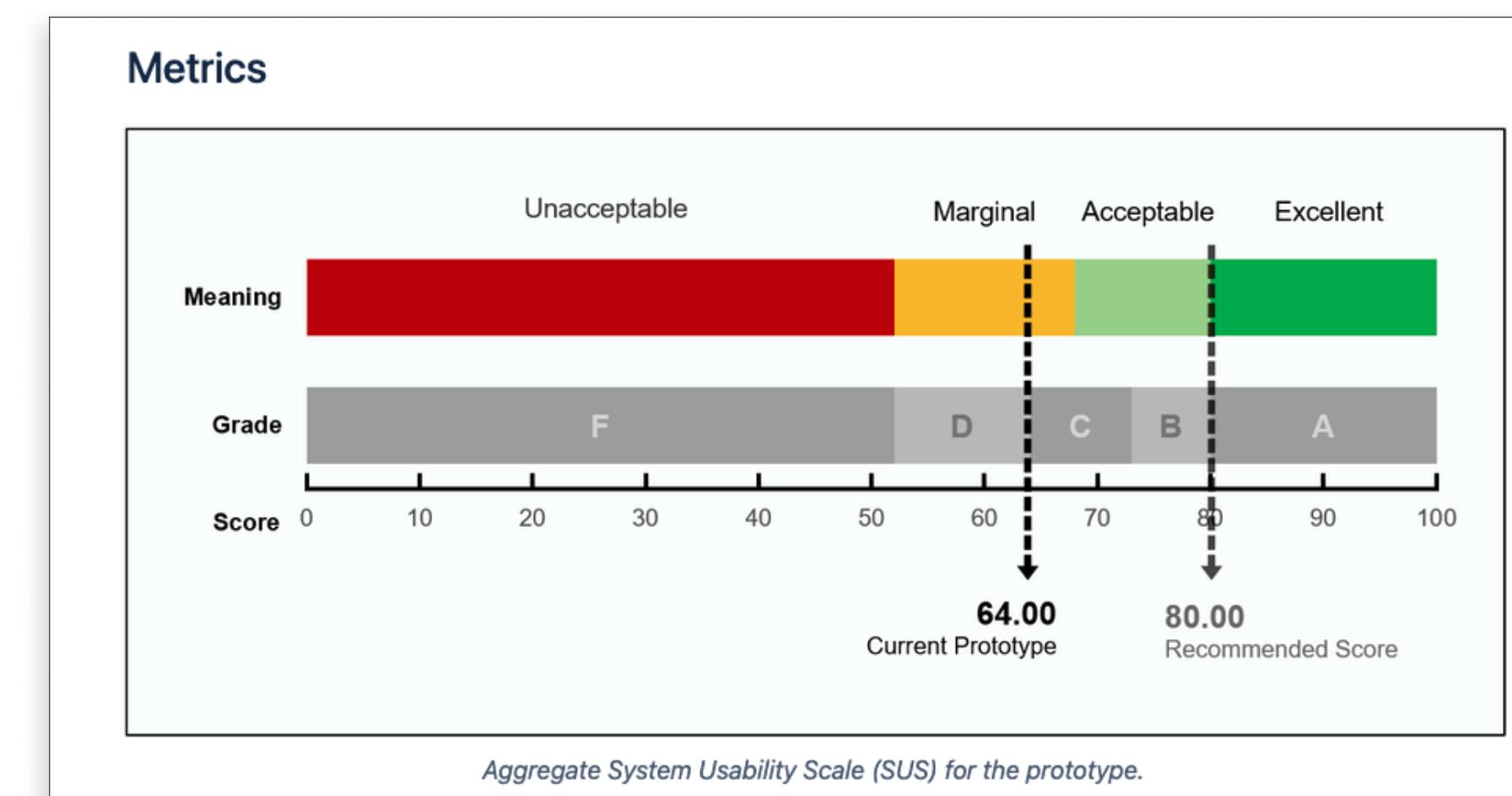
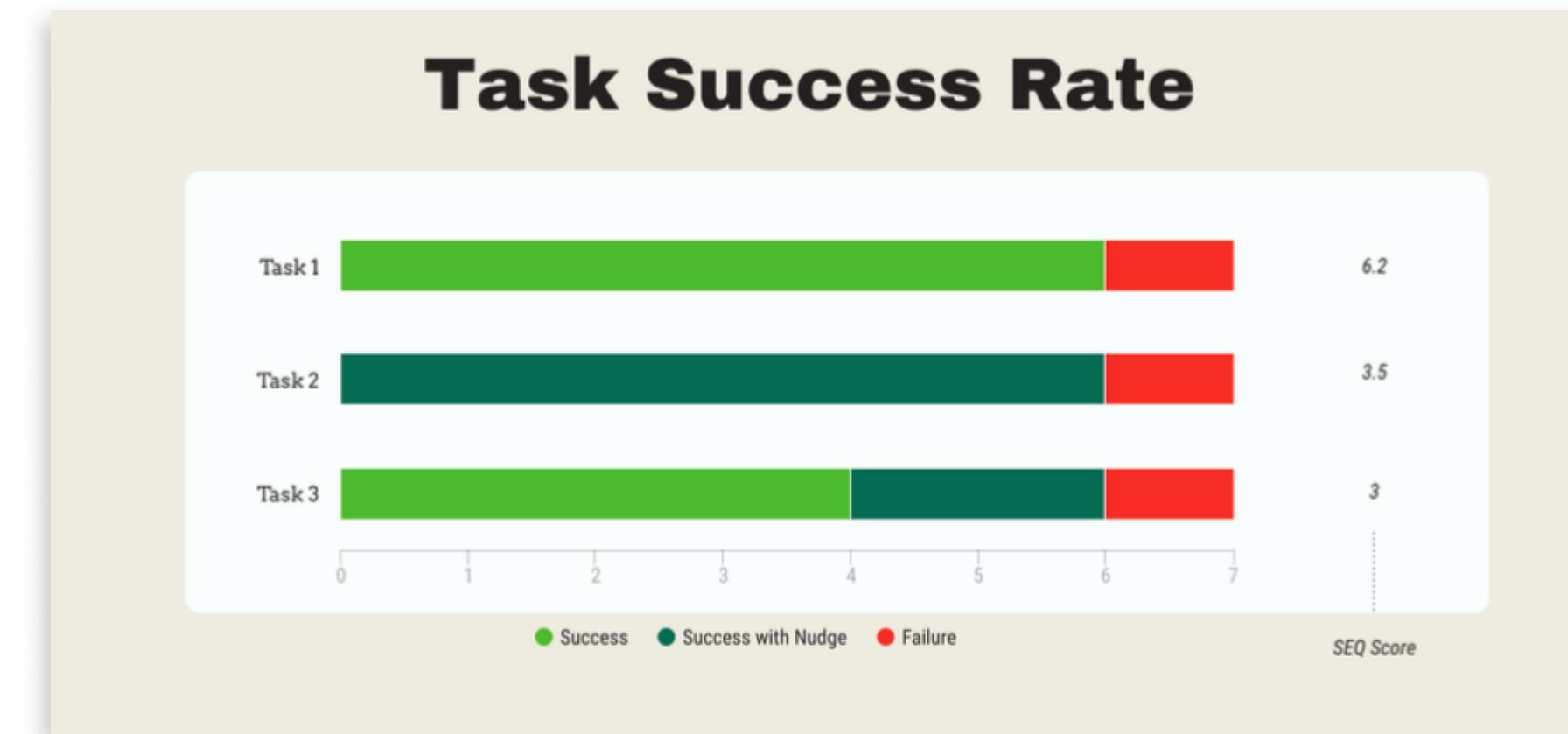
RESULTS FROM THE USABILITY TEST

Some observations and learnings from the usability test:

- The maturity of an organization's data governance process is a big factor in deciding if this product will be relevant.
- Descriptions of different terminologies as defined in the solution wasn't very well understood.
- Pushing Protections from Collibra to the data source was seen as a highly useful feature.

"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.



BRAINSTORM SHORT AND LONG TERM IDEAS

Combined Rules & Standards

Dedicated space for a Rule builder

Quick fixes for Rules for Rules form

Based on the usability test results, I sketched some ideas - some quick fixes and some possible long term strategies to better structure the information and features in the application.

IDENTIFY CONTENT SPECIFIC IMPROVEMENTS

Things to be done for landing page

- Define what should be in the description
 - Diff between Access vs. Policy
 - Diff. between Standards vs. Rule
- Reconsider Recents position, move up the description of Rules
- Tab names - rename
- Consistent labels
- What content should be displayed in the table?
 - Rules meta data or rule summary

Things to be done for forms

- Divide the Rule form drop downs to make it more readable and aid their understanding of protection/policies.
- Reconsider Define Rule/Standard title for the modal (we don't need it)
- Button labels
- Default name, description
- Description about Rules, Standards inside the modal to re-emphasize their purpose.

CONTENT IMPROVEMENTS

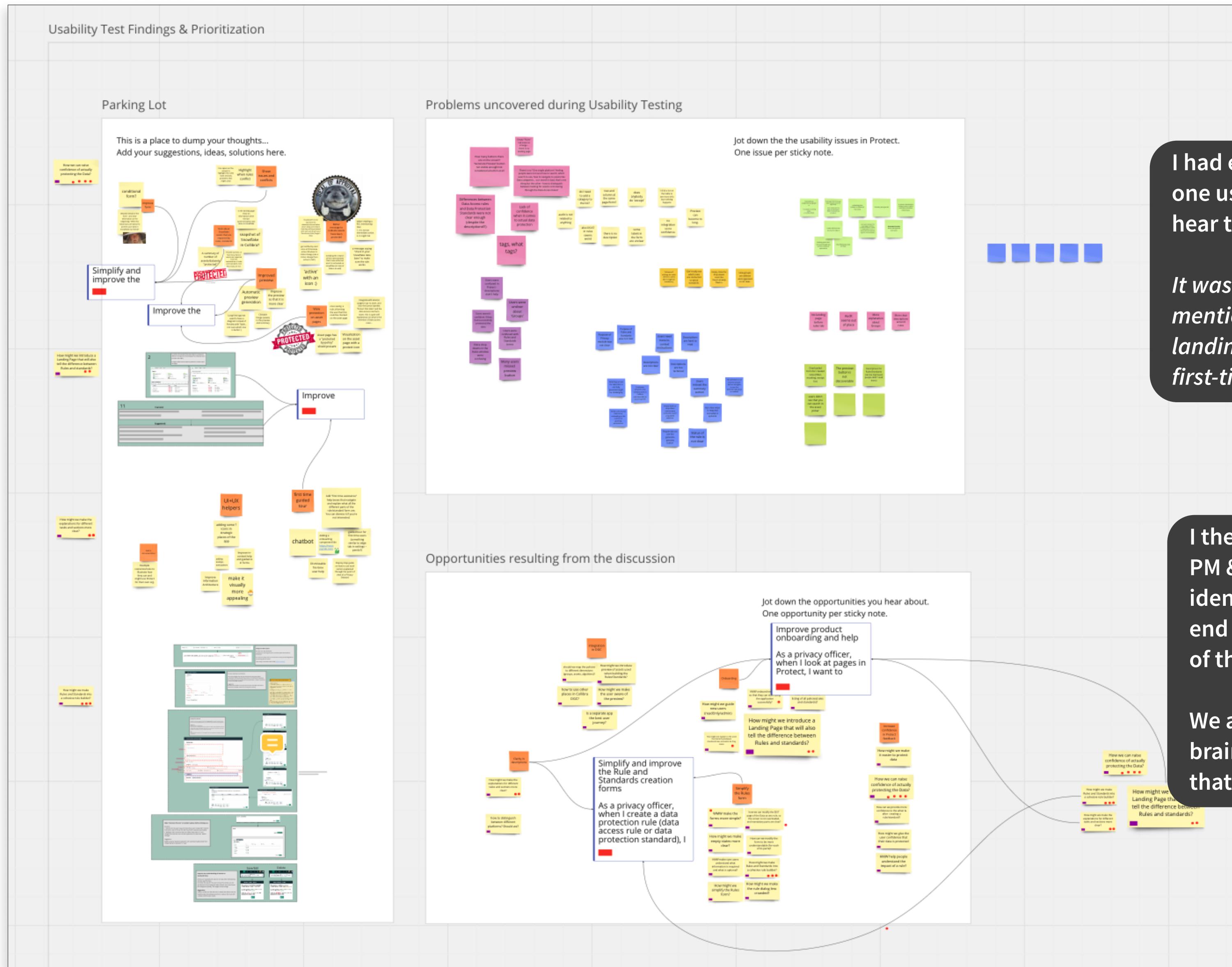
- Define, what to include in the description (on the landing page).
- Rename tabs with more descriptive labels.
- Consistent titles and labels throughout the application.
- Shift Recents down and change title of the page to match with the tab name.

Forms

- Modal titles, we don't need Define Rule/Standard at the top
- Button labels
- Add a default name description
- Add description about Rules, Standards to re-emphasize their purpose
- Divide Rule form drop downs into smaller chunks to make it more understandable

Content and its structure was identified as one of the major pain points in the application. Users were confused and unsure about certain descriptions, definitions or labels in the application. So I invited a technical writer to a small workshop. The aim was to identify areas for content improvement, need for restructuring things and consistency through the application.

BRAINSTORM IMPROVEMENTS WITH PM & DEVELOPERS



I had encouraged all the developers to attend at least one usability session, which they did! It was nice to hear they benefitted from that experience.

It was especially rewarding when one developer mentioned “I can now see why the description and the landing page might have felt confusing to the user. As a first-time user I realized it’s all very confusing for them.”

I then co-facilitated a brainstorming workshop with PM & Devs to identify areas of improvement. We identified problems and categorized them as front-end vs. back-end effort, size of effort, reprioritization of things on the roadmap.

We also talked about certain problems, and brainstorm possible very-high level solutions, what that effort would look like, and technical challenges.

IDENTIFIED AREAS OF IMPROVEMENT

We prioritized improvements and additions to improve the usability score of the product.

- Content - easy from a dev effort perspective.
Min effort, Max value.
 - Clearer and concise definitions.
 - Consistent labels.
- Improvements to landing page.
- Improvements to rule creation form
- Identifying and correcting components that are inconsistent with the design system.
- Next set of initiatives to focus for building more trust with the product and increasing value/desirability of the product.

IDENTIFIED AREAS OF IMPROVEMENT

We prioritized improvements and additions to improve the usability score of the product.

- Content - easy from a dev effort perspective.
Min effort, Max value.
 - Clearer and concise definitions.
 - Consistent labels.
- Improvements to landing page.
- Improvements to rule creation form
- Identifying and correcting components that are inconsistent with the design system.
- Next set of initiatives to focus for building more trust with the product and increasing value/desirability of the product.

surface-level fix

more thinking required, but relatively easy

deep-thinking and collaboration is necessary, dev effort very high

DESIGN EXPLORATIONS FOR RULE CREATION FORM

Improvements to Rule form

IN PROGRESS

Review Copy

Empty state

Design details

Notes/Questions for dev

Current Design with Guest access options

Dropovers

Changes for the Edit mode of this model

Error State

List of (intermediate) changes

Changes that can be tackled independently

Short term improvements

Pinned tabs

Pinned tab

Options for viewing multiple assets in Preview

Content reference when there is a conflict in the reading role

RULE CREATION FORM UPDATES

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 +

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 <input type="button"/>	Access <input type="button"/>	Data Category <input type="button"/>	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**

before

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 categories. You can mask or hide columns by their data category. You can also conditionally filter rows based on code logic.

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 * Start typing a group name and press enter

assets * Start typing an asset name and press enter

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 Start typing a data category name and press enter

protect columns with Default masking

+ Masking

Generate preview

Cancel **Save rule**

after

RULE CREATION FORM UPDATES

before

Removed complex rule creation conditions

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:

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**

Consistent labels.

Create Data Access Rule

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

assets * Start typing an asset name and press enter

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 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.

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

protect columns with Default masking

+ Masking

Generate preview

Cancel **Save rule**

after

Divided the content into sections for ease of understanding.

In-context help for what to expect from each section.

RULE CREATION FORM UPDATES

before

Removed complex rule creation conditions

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:

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			
Lifetime value	Full View			
Last support date	Full View			
Start date	Full View			
Credit card number	Masked	Credit card number	*****	
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**

Consistent labels.

Create Data Access Rule

Set rule for

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

Rule Name *

Description

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 particular column.

+ Filter

Mask data

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

Data Classification Start typing a data category name and press enter

Default masking

Cancel **Save rule**

Divided the content into sections for ease of understanding.

In-context help for what to expect from each section.

With these (majorly) front-end improvements, the main aim was to help users effectively use this form, a query builder to create complex protection policies. To do that, I made the labels consistent throughout the application, divided the information (dropdowns) into different sections and added in-context help for each section to help users understand the purpose of each section.

RULE CREATION FORM UPDATES

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 Asset deleted 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, Unknown asset, 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

Customer Churn Data Set

Column	Access	Data Category	Masking	Code Value
Customer ID	Masked	Customer 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			
Another column	Full View			
Age	Masked			
More data here	Full View			
There could	Full View			
Be lots of	Full View			
Columns	Full View			

Cancel Save

A version of the same form with populated fields to illustrate a more complex query to the developers and also strength-test the improved UI patterns.

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 also hide columns by their data category. You can also conditionally filter rows based on code set values.

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

+ 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

- PII 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

+ 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 i Delete

Summary

Grant access to Human Resources, Admins, Marketing, Managers, Executive Leadership 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, Personal Information and Geographic Information and show last 4 for Credit Card Information.

Generate preview

PII PII Personal Information Geographic Information

+ Masking

Column name	Access	Masking	Masking Agent	Code Value
Customer ID	Masked	1B504D3328E16FDF281D1FI	DCAT PII	
First Name	Masked	68lsdh!%bcD5673Lob@d709	DCAT Personal Information	
Last Name	Masked	34!2ds\$n6o94dFG8%2sVFR7	DCAT Personal Information	
Region	Full View			BE, US
Country	Filtered			
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

DETAILS

Examples of detailed notes for certain specific sections of the form. The aim was be as unambiguous as possible and be precise with the acceptance criteria, and cover edge or error cases.

Tags

Asset deleted X
PII X Asset deleted X Personal Information X Customer Data X Marketing Data X

Summary

Grant access to Human Resources, Admins, Marketing, Managers, Executive Leadership and Tech Staff for PII, Asset deleted, 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.

Adding filters

Step I

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

Step II

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 Select a data classification
has Select a code set with Select a code value Delete

+ Filter

Step III

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

Step IV

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

Exclude rows where Country
has Country codes with Select code value PL X Delete

+ Filter

Improvements to the asset dropdowns

v1 - Intermediate solution

Custo
DCAT Customer Churn Analysis
DCAT Customer Churn Analysis II
PROC Customer Intake
Customer data

Proposed improvements to asset tags

PROC Customer Churn Analysis X

Possible improvement to icon shape once Protect moves to Arbor library

PROC Customer Onboarding Process X

v2 - Target solution

Custo
Data Privacy Building Blocks > Data Categories
DCAT Customer Churn Analysis
Data Privacy Building Blocks > Data Categories
DCAT Customer Churn Analysis II
Data Privacy Building Blocks > GDPR Laws > Customer Processes
PROC Customer Churn Analysis II
Business Analysts Community > Customer Data
Customer data

COMMUNICATING DESIGN DETAILS

Due to time constraints of the immediate release, all of these changes couldn't be accomplished at once, they had to be split into 2/3 stages.

I recommended an itemized list of changes that could be implemented immediately and the others could be postponed for later.

LIST OF (INTERMEDIATE) CHANGES

CHANGES THAT CAN BE TACKLED INDEPENDENTLY

1. Modal title
 - a. Change modal name (keeping it consistent with Create button on the landing page).
 - b. Remove Define Rule sub-heading.
2. Add rule description/explanation above the name.
3. Rule intro changes
 - a. Add a red asterisk to the Rule Name input to indicate its mandatory.
 - b. Increase width of Description field to the end of the window.
 - c. Remove (optional) from its label.
4. Add a divider component after the intro fields.
5. Groups dropdown
 - a. Add a 'groups' label with a red asterisk to indicate its mandatory.
 - b. Change placeholder text.
 - c. Change display to a tags-like UI.
6. Assets dropdown
 - a. Add an 'assets' label with a red asterisk to indicate its mandatory.
 - b. Change placeholder text.
 - c. Change display to a tags-like UI.
7. Masking
 - a. Introduce a header.
 - b. (Some more design work is needed).
8. Row filtering
 - a. Introduce a header.
 - b. (Some more design work is needed).
9. Remove Summary header (and section) in the empty state of the form.
10. Generate preview
 - a. Remove the section title Preview, only keep the button.
11. Preview section
 - a. Switch order of columns - Masking is 3rd, followed by Data Category(?).
 - b. Replace asset dropdown by a tab-view of assets for easy selection.
12. Change text of Save button to Save Rule.
13. Change styling of Error states
 - a. Mandatory input fields.
 - b. Deleted fields (design to be finalized).
 - c. Summary changes for deleted assets (design to be finalized).

SHORT TERM IMPROVEMENTS

Empty State

Filled out form

DOCUMENTING DESIGN SPECS

Rules Modal - FINAL DESIGNS

One final step was documenting all the details for the design. For this form, I jotted down important notes and design variations relevant to each section in the form for hand-off. This was the final deliverable.

This version will be available in the November release of the product.

Data Access Rules - Final designs and details

Empty State Filled-out Form

Details & Specifics

ACCESSIBILITY

PART II - DEVELOPING DESIGNS FOR INTEGRATION OF PROTECT WITH ANOTHER COLIBRA APPLICATION

ASSET PAGES IN COLLIBRA

- Data is ingested in Collibra and stored in the form of assets.
For eg. datasets, tables, columns exist as different types of assets in the Collibra platform.
- Each asset has a dedicated page which provides more meta data about it.
- Asset pages belong to a different part of the Collibra platform and are owned by a different team.

INTEGRATING PROTECT WITH ASSET PAGES

- In the usability test, we observed that people visited asset page of a particular assets(s) to validate whether the rule (protection) they created in Protect was implemented or not.
(It was clear, they wanted some feedback from Collibra' that helped them build confidence in the fact that their data will now indeed be protected because of the rule they just created.)
- Another use-case we had parallelly identified was - Data Consumers.
eg. an analyst or a data scientist who are interested in a particular data set, they visit the asset page and want to know if they have full, partial or no access to that data.

INTEGRATING PROTECT WITH ASSET PAGES

Questions and Ideas

What do we know?

- During a usability testing we discussed that people want to specific asset pages to validate if their policy was enforced or not.
- It is natural that people would integrate to a specific asset page and expect to view policies that affect to this asset. Also, create policies directly from this asset page.
- Developing this feature would reduce the time data application integration. It processes all data from Protect rather than multiple applications.

Asset pages (WIP)

- Asset pages are currently being developed by Sapient and team.
- From a dev perspective, there are no technical limitations.
- Link to Datasheet

Design questions to consider

- Where is the right place to integrate Protect functionality? Home & Create?
- Where you're on the asset page, how much asset parameters should you give?
- How many assets can you actually create in a single standard form?
- How to handle inheritance for data classification as they inherit assets?

Where to Integrate Protect in an Asset Page?

More things in the Overview page are quickly planned. Protect will need to have its own section.
There can be a small badge showing what security policy is in place or not.
More Policy details. Protect policy interface

Initial Sketches

Asset page

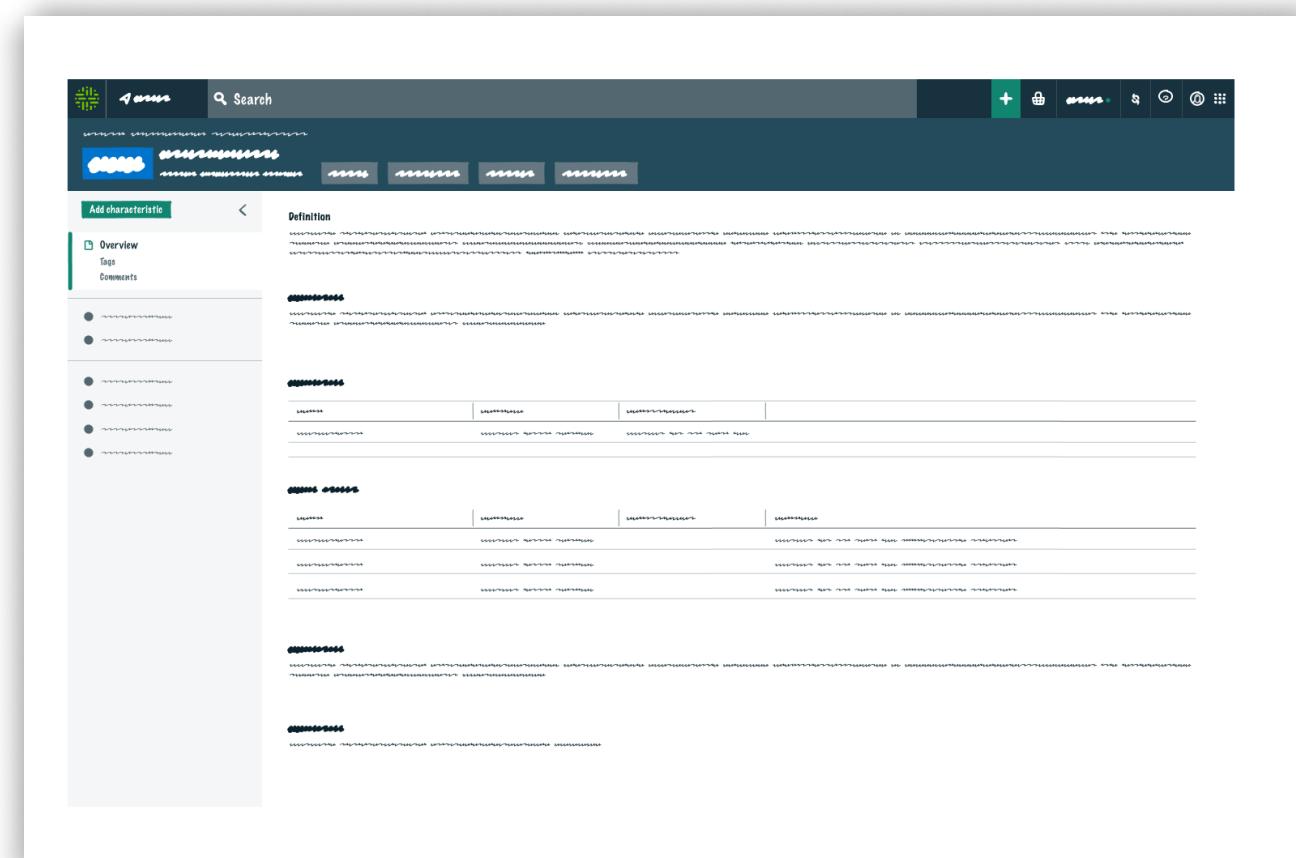
Here, the assets you can select for creating:
- Assets related to this asset.
- Summary of the policy is shown.
- Empowered View (Attachments?)

The same modal can be expanded to planning and funding. You can view Child Categories and Child Objectives that are related to this asset. (Currently Protect already does this)
The overall idea is, if you need access to all assets, navigate to Protect application.

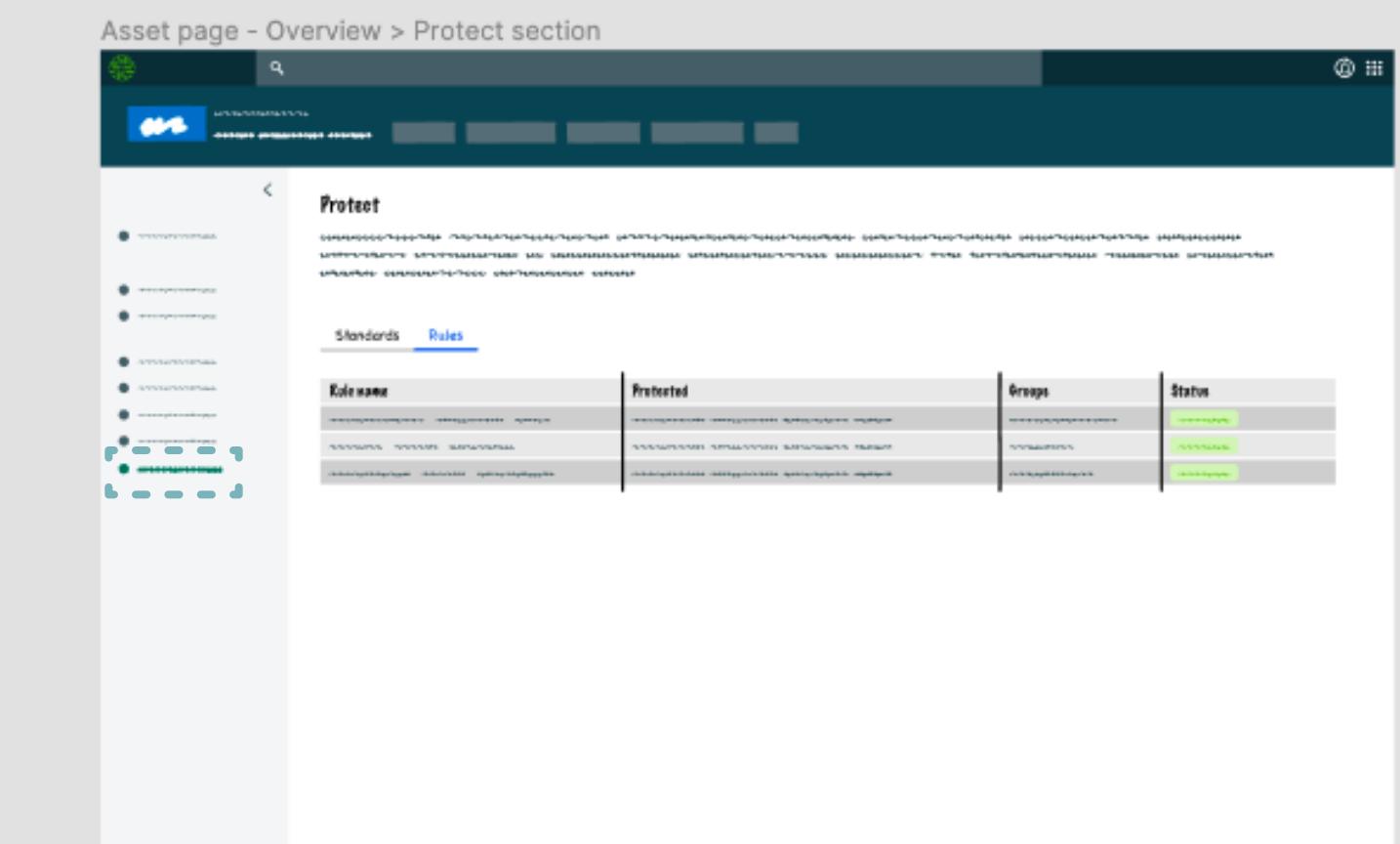
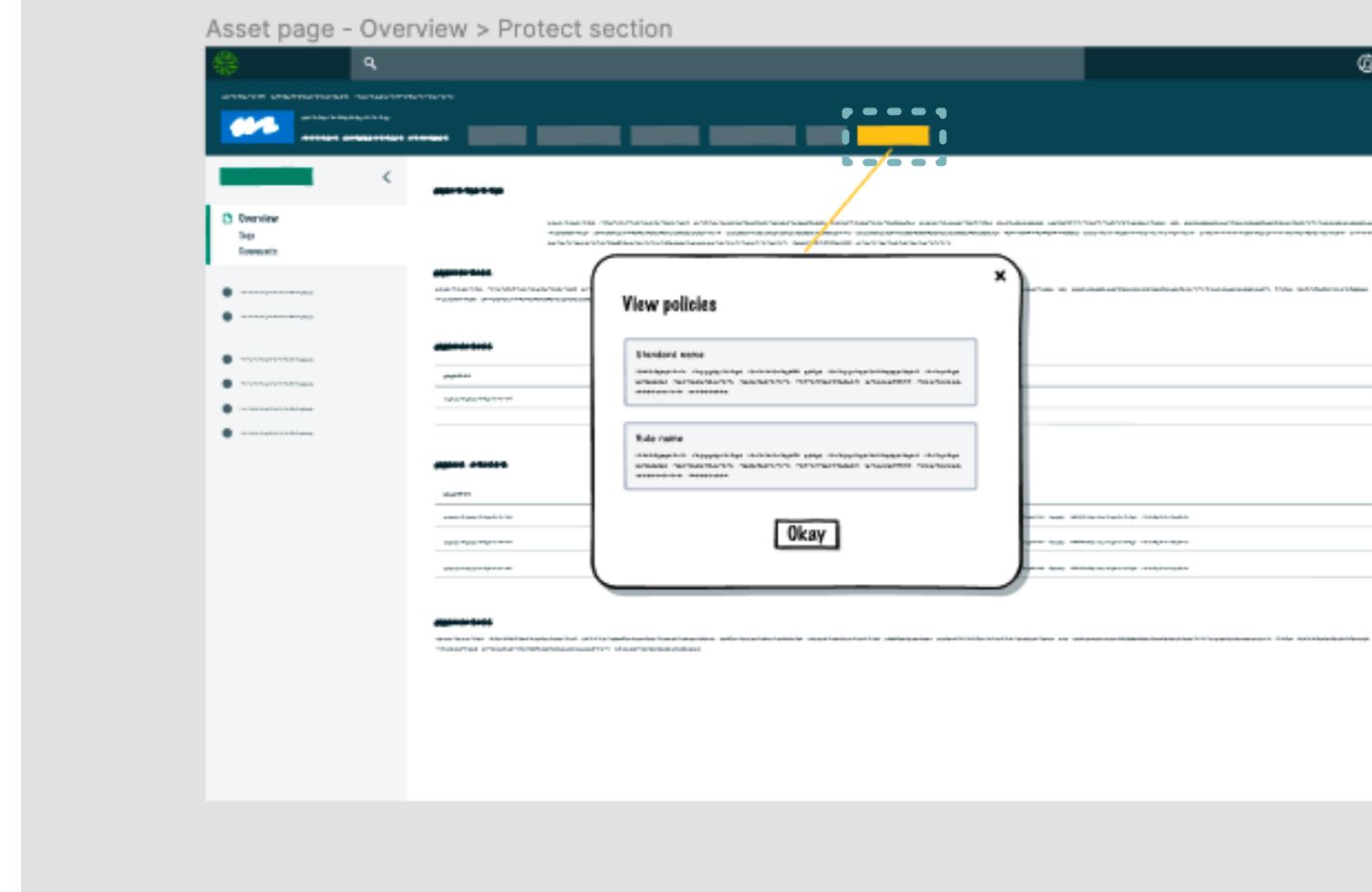
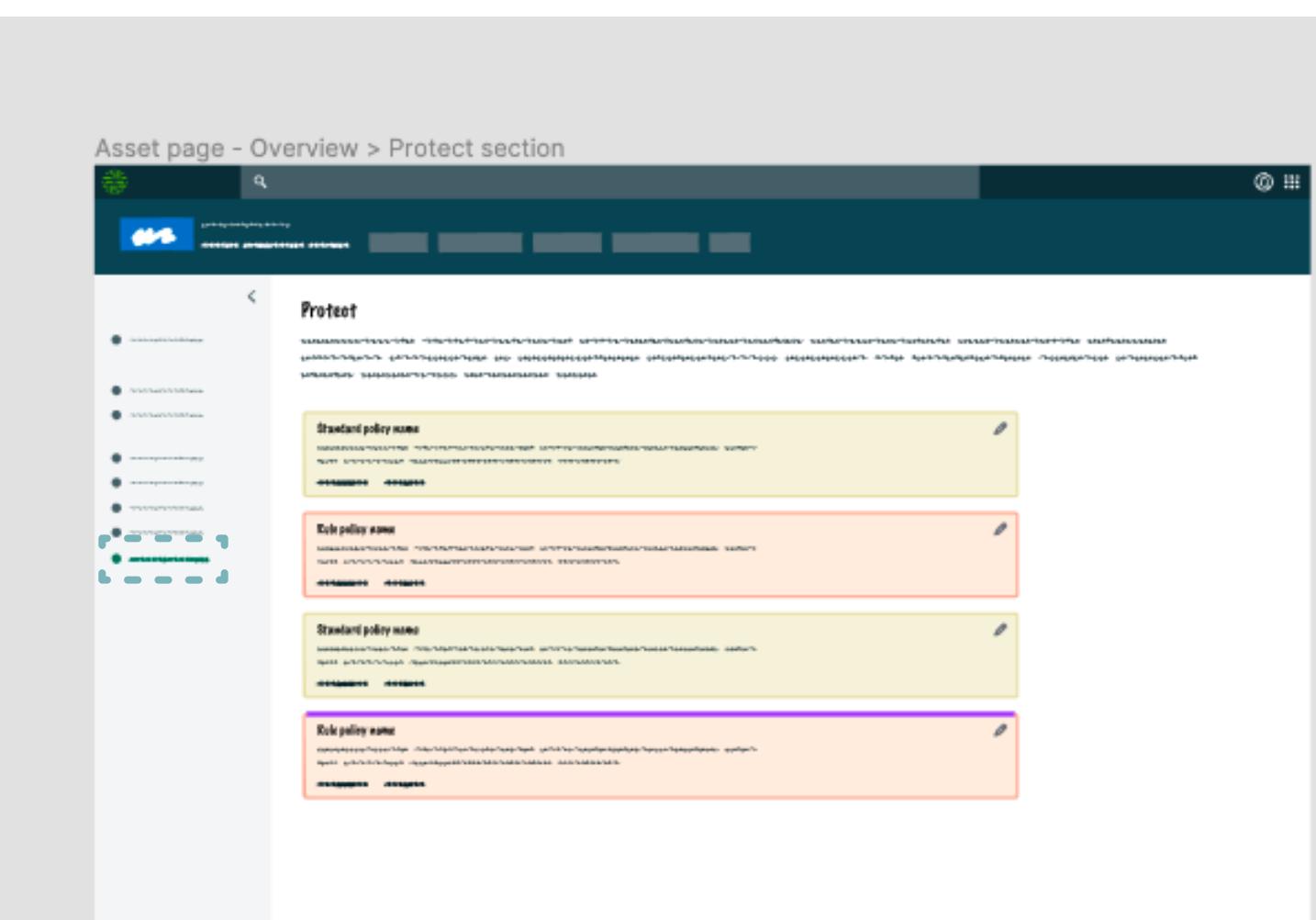
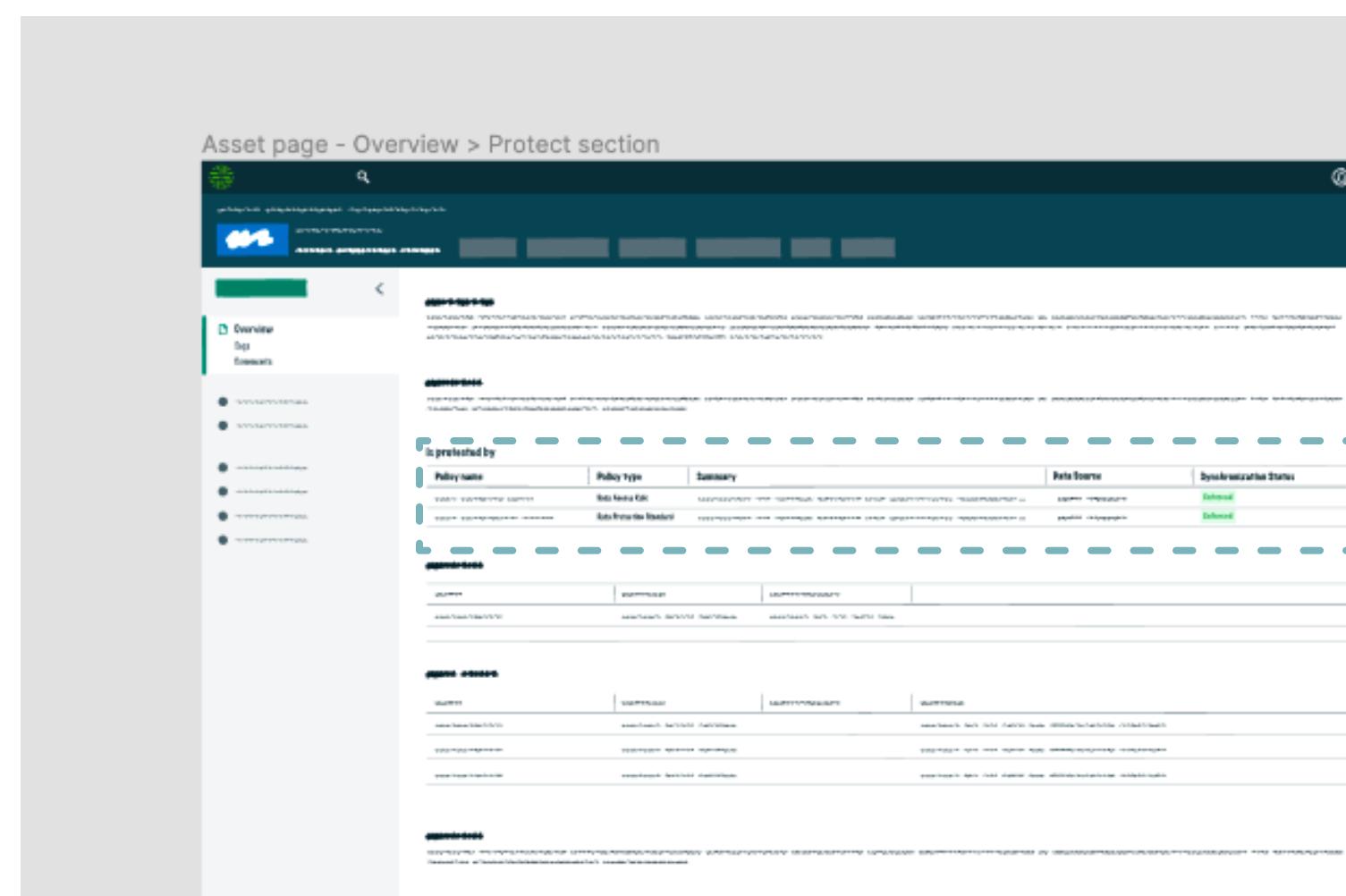
Discussing new Asset page design w/ Sepol & Lingcoco 09/20/2012
policy to run an asset, see next place in Overview screen
config via interface
New Design - 2020 Q4
use of key features in Protect?
Role based
Page definitions

- As step one, I began gathering relevant information for this feature. I jotted down the user goals and available data points.
- I used sketches to share my ideas with the Asset Pages designers. I wanted their feedback and thoughts about how Protect could be integrated. I also wanted to see how Protect would fit the Asset Page re-design that they were envisioning.

LOW FIDELITY DESIGN EXPLORATIONS



Exploring different design patterns and trigger points for PROTECT



I started working in low fidelity, exploring ideas, still thinking of questions for different stakeholders.

I discussed feasibility of the different trigger points with the developers.

DISCUSSIONS WITH DEVS & PM

Main question to be answered -
Is this data protected? Can I access this asset?
Is it masked or completely protected?

What information must appear in the policy (rule/standard) widget?
• Name
• Standard or Rule
• Groups
• Summary
• Synchronization Status
• Other assets protected
• Data Source
• Other meta data

Actions
• View
• Edit
• Delete?

This question cannot be directly answered (Collibra doesn't have a direct 1:1 mapping between Collibra and Snowflake user profiles).
It is also not possible for a user to determine (at least through Collibra) which Snowflake group they belong to.
So what can be done instead? We can show which groups are impacted by a particular rule or standard and trust that the user will be able to fill those gaps on their own.
Groups have a 1:1 mapping (Protect - DGC)

Which group does a user belong to in DGC?
Question by DGC users

Consider -
• How to verify/check the end result of a masking algorithm?
As a consumer, how am I going to see the actual data? (Preview)
• For different asset types, number of policies will change
ex. column vs. dataset
• A quick usability test - what are people interested in?

Different asset types & protection
• Direct / Indirect relations, Prescriptive paths
• Do we show/not show INDIRECT rules or standards that are applied?
• Define Direct vs. Indirect

Show all policies that are included in the prescriptive path of a certain column
Diagram for "Data set" asset page
Out of scope for now.

Direct (protect x, y, z assets not masking, filtering assets)

Author view

Non-Author view

24/10/22 Discussion with dev team:
• Good to call this out.
• Makes a lot of sense, especially since most of the users coming to Asset pages could be non-authors (data consumers). Very few will be Privacy Stewards.
• However, for Q4 '22, this feature will mostly be used by Privacy Stewards.
• So the decision is to start designing for the "author" view now and hide things later for non-author view.

Assets --> showing only related assets
• We may not / should not do this level of hand holding for this particular situation.
• In a situation such as -
I am on the asset page of a country, see that there's a policy impacting it, I want to edit this and add another country. In this case not allowing to add an unrelated asset will be irritating.

MID FIDELITY DESIGN EXPLORATIONS

Explorations to understand -

- What information needs to / can be showed here?
- What level of detail is necessary?
- Which actions are necessary, for which persona?

The image displays four separate wireframe prototypes of a 'Protect' interface, likely from a software application. Each prototype shows a different way of presenting rule information and search functionality.

- Top Left:** Shows a detailed view of a rule named "Name a long name". It includes sections for "Data Access Rule" and "Standard / Rule loong long name", both labeled "Enforced". Below these are "Summary" and "More details" sections.
- Top Right:** Shows a list of protection rules. A modal window titled "Add protection" is open, containing search fields for "All policies", "Search for a group", and "Search for asset". Below the search fields are several collapsed sections labeled "Protection name can be a long name" (under Data Protection Standards and Data Access Rules).
- Bottom Left:** Shows a list of protection rules. Each rule item has a "Name a long name" label followed by "Data Protection Standard" or "Data Access Rule", with a plus sign icon to its right.
- Bottom Right:** Shows a "Data Preview" section with a "Preview of data" placeholder. To the right, there's a "Applied protection" section with search fields for "Search for protection by user group" and "Search for assets". A note on the right side lists: "Might trigger more questions", "Data Preview will be different for each group", "In order to check if you're in this group, do this...", and "People familiar with this real data".

Based on certain decisions and priorities I further refined the design, and added more details.

These are a few UI explorations - best way to display the rule information.

SPECIFICS OF A COMPONENT - EXPLORATION & DISCUSSION

Another example of explorations, prioritization and discussions.

These low fidelity designs gave me a chance to do frequent check-ins with the development team, and keep them informed about my direction. It proved to be a quick and efficient way to work.

Around this time, I stopped working on this project.

The image displays three wireframe prototypes of a user interface for managing data access rules. The top prototype shows a 'Data Access Rule' screen with a 'Role name' field set to 'Enforced'. The middle prototype shows a 'Name a long name' screen with the same 'Enforced' status. The bottom prototype shows a 'Standard / Rule is long long name' screen with the same 'Enforced' status. To the right of these prototypes is a screenshot of a comment card from a platform like Slack or Microsoft Teams. The card has a pink header with the text 'Should you be allowed to Edit a policy from this page?'. It features a profile picture of a user named 'Koen Van Geert' and a timestamp '7 days ago'. The message content reads: 'Yes, I believe this is a requirement. We will follow the same rules that only administrators or authors can edit the rule'. At the bottom of the card is a 'Reply' button.

Is this status necessary here?
OR
Should only Enforced policies appear here?
Someone other than a Privacy Steward may not fully understand this status.

- Author / Non-author cases
- Q4 --> for Privacy Stewards, managing protections i.e. Author view

THANK YOU !
