



# TANGO

## PEC USAGE DOCUMENT

✉ September 2024

Digital Technologies Acting as  
Gatekeepers to Information and  
Dataflows

Ahsan Mukhtar, Sakshyam Panda,  
Manos Panaousis

## Table of Contents

<b>Table of Figures .....</b>	<b>2</b>
<b>1. Introduction .....</b>	<b>3</b>
<b>2. Getting Started .....</b>	<b>4</b>
Form Description: .....	4
User Interaction: .....	4
Form Submission Process: .....	4
<b>3. Authentication .....</b>	<b>7</b>
1. Registration.....	7
User Inputs.....	7
2. Logging In .....	8
<b>4. Project Creation .....</b>	<b>10</b>
1. Assessments .....	10
1. Application Assessment Page .....	10
2. AI Assessment Page.....	11
3. Dataflow and AI Privacy Threat Generation.....	13
2. Data flow selection .....	13
<b>5. Dashboard .....</b>	<b>17</b>
1. Application Dashboard .....	17
2. AI Dashboard.....	18
3. Mitigations .....	18
4. Details Page .....	20

# Table of Figures

Figure 1: DPIA Need Assessment Form .....	5
Figure 2: DPIA need Assessment form submit button.....	5
Figure 3: DPIA App/AI Assessment Form .....	6
Figure 4: Registration Page .....	8
Figure 5: Login page .....	9
Figure 6: Application Assessment Page.....	10
Figure 7: AI Assessment Page .....	12
Figure 8: Data Flow selection page .....	13
Figure 9: DPIA Form .....	14
Figure 10: DPIA Selection Page .....	15
Figure 11: Application Assessment Project Card .....	17
Figure 12: AI Assessment Project Card.....	18
Figure 13: Mitigations Page .....	18
Figure 14: Search for mitigations .....	19
Figure 15: Filter Mitigations .....	19
Figure 16: Mitigations Checklist .....	20
Figure 17: Threats Details Table .....	20
Figure 18: Threats associated to a Impact Category.....	21
Figure 19: Web Charts for each impact category.....	22
Figure 20: Mitigation Checklist Popup .....	22
Figure 21: Project Control button .....	23

# 1. Introduction

The Tango project is meant to develop a solution for secure, trustworthy and environmentally sustainable data management system. Tango enables its users to analyse their Apps and products for potential threats and gives mitigation suggestions according to the user requirements.

This guide offers a comprehensive walkthrough of Tango's key features and functionalities. We will cover everything from registering an account and logging into the system, to navigating the Dashboard, creating Apps and AI projects, and managing the associated data flows.

Additionally, Tango empowers users to manage their projects with ease. From viewing and updating project details to deleting unnecessary projects and printing reports, the platform is designed for efficiency and transparency. This document provides a detailed step-by-step guide, including screenshots, to help you fully utilize all aspects of the platform, ensuring an optimal experience as you interact with your data in a responsible and sustainable manner.

## 2. Getting Started

Upon arriving at the Tango platform, users are greeted with a **DPIA Need Assessment Form** modal, as seen below.

### Form Description:

The modal prompts users to select one or both of the following options:

1. **Application Scenario:** Leads to the **Application Scenario Form**.
2. **AI Scenario:** Leads to the **AI Scenario Form**.

### User Interaction:

- **Single Selection:** If the user selects either **Application Scenario** or **AI Scenario**, they are redirected to the respective form.
- **Multiple Selections:** If both options are selected, the user will be shown the **Application Scenario** form first, followed by the **AI Scenario** form.

### Form Submission Process:

1. **Form Completion:** Once the user completes the selected form(s), they will be automatically redirected to the **Login Page**.
2. **User Authentication:**
  1. If the user already has an account, they can log in using their credentials.
  2. If the user is new, they must proceed to register.
3. **Post-Login/Registration:**

After logging in or registering, users are directed to the relevant assessment page:

1. Users who initially selected **Application Scenario** are redirected to the **App Assessment** page.
2. Users who selected **AI Scenario** are redirected to the **AI Assessment** page.

Upon completing the form and successfully logging in or registering, users will be seamlessly redirected to the appropriate assessment pages based on their initial selection from the modal form.

The user must select either one or both options

DPIA Need assessment forms  
Please select either one or both options.

Application Scenario

AI Scenario

Submit

Figure 1: DPIA Need Assessment Form

The submit button is enabled after the options are selected

DPIA Need assessment forms  
Please select either one or both options.

Application Scenario

AI Scenario

Submit

Figure 2: DPIA need Assessment form submit button

General Data Protection Regulation (GDPR) mandates that organisations dealing with sensitive data must perform a data protection impact assessment (DPIA) to ensure compliance. Let's assess if you require to perform a DPIA:

Do your data processing activities include profiling or making automated decisions about individuals, which could impact their rights and freedoms?\*

Yes ←  
 No

Could the data processing result in high risks to the rights and freedoms of individuals such as identity theft, financial fraud, reputation damage, fraud, discrimination or other social or economic disadvantage?\*

Yes ←  
 No

Does the data processing involve sensitive data or data of a highly personal nature such as health information, racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data, or data concerning a person's sex life or sexual orientation?\*

Yes ←  
 No

**Submit** ←

The user must fill entire form to proceed

Figure 3: DPIA App/AI Assessment Form

## 3. Authentication

### 1. Registration

After selecting and submitting the appropriate form (either **Application Scenario** or **AI Scenario**) from the landing page modal, users who do not have an account are redirected to the **Registration Page**.

#### User Inputs

To create a new account, users must fill in the following details:

1. **Username:** Enter a unique username (e.g., "i.e Alex"). This is required and must be 150 characters or fewer, using letters, digits, and symbols (@/.+/-/\_).
2. **Email Address:** Provide a valid email address (e.g., "xyz@gmail.com").
3. **Organisation Name:** Specify your organisation (if applicable).
4. **Password:** Create a secure password. Tango requires that your password meets the following criteria:
  - It must contain at least 8 characters.
  - It cannot be a commonly used password or entirely numeric.
5. **Confirm Password:** Re-enter the password for confirmation

Once all fields have been filled out, click on the **Register** button to complete the registration process. After successfully registering, the user will be redirected based on their initial scenario selection:

- If **Application Scenario** was selected, they will be taken to the **App Assessment** page.
- If **AI Scenario** was selected, they will be taken to the **AI Assessment** page.

If the user already has an account, they can click on the **Sign in now** link to be redirected to the **Login Page** instead.

**Sign in to Tango**

Username\*  
i.e Alex

Email address  
i.e xyz@gmail.com

Organisation  
No Org

Password\*  
Enter Password

- Your password can't be too similar to your other personal information.
- Your password must contain at least 8 characters.
- Your password can't be a commonly used password.
- Your password can't be entirely numeric.

Confirm Password

Enter the same password as before, for verification.

**Register**

Have an account? [Sign in now](#)

Figure 4: Registration Page

## 2. Logging In

Once a user has either registered an account or previously created an account, they are directed to the **Login Page**. This is where users authenticate themselves to access the Tango platform's features.

### User Inputs:

To log in, the user must enter the following information:

- **Username:** Enter the username that was provided during registration (e.g., "i.e Alex").
- **Password:** Enter the password that was set during registration.

After entering these details, click on the **Sign In** button to log into your account. If the user doesn't have an account yet, they can click the **Sign up now** link below the login form to be redirected to the registration page. If the user forgets their password, a **Forgot Password** link may also be available (if applicable), allowing them to reset it.

### Expected Outcome:

Upon successfully logging in, the user will be redirected to the appropriate page based on their initial selection from the modal:

- **App Assessment Page** if they chose the **Application Scenario**.
- **AI Assessment Page** if they chose the **AI Scenario**.

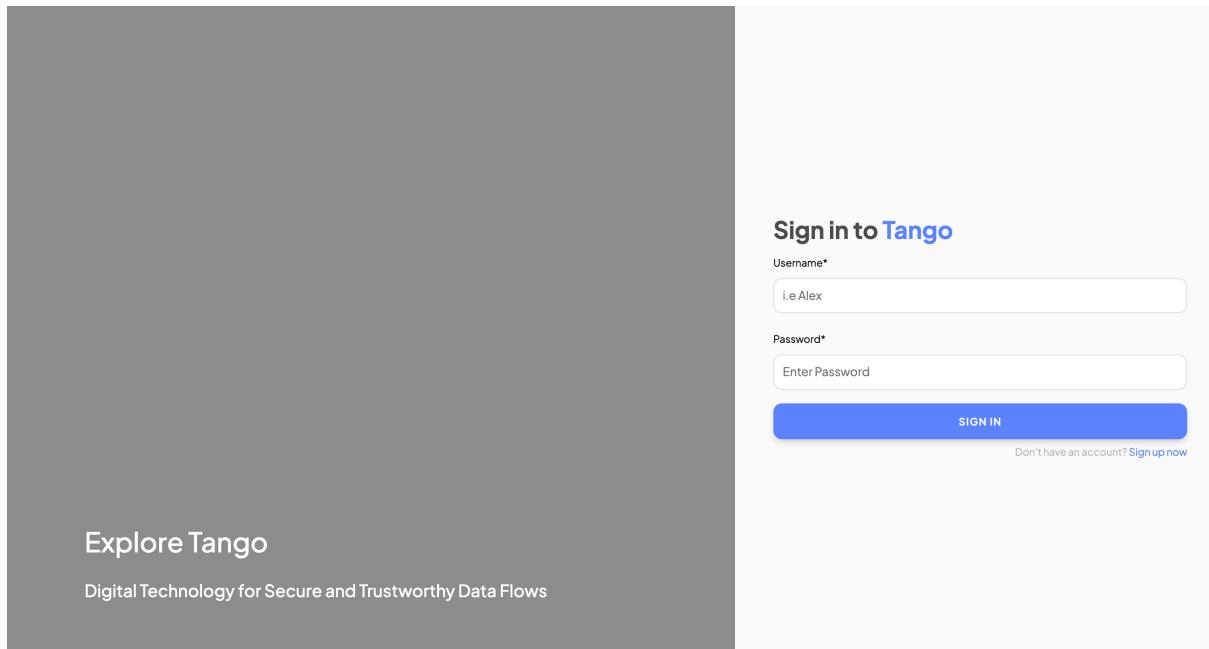


Figure 5: Login page

## 4. Project Creation

### 1. Assessments

Based on the scenario the user selected earlier (either **Application Scenario** or **AI Scenario**), they will be directed to the relevant assessment form to provide detailed information about their project. Each form captures specific data about the user's app or AI-based application and follows a similar structure but with different required fields.

#### 1. Application Assessment Page

If the user selected **Application Scenario**, they will be directed to the **Application Assessment Page** where they need to fill in the following details:

- **Project Name:** Name of the project being assessed.
- **Date of Assessment:** Enter the date of this assessment.
- **Use Case Scenario:** Select the use case that best fits the project.
- **Explain broadly what the project aims to achieve:** Provide a high-level explanation of the project's goals.
- **Type of Processing Involved:** Describe what kind of data processing the app will involve.
- **Summarize why you identified the need for DPIA:** Detail why this project requires a Data Protection Impact Assessment (DPIA).

Once these fields are filled in, the user can submit the form.

The user must fill entire form to proceed

Project Name\*

Use Cases Scenario\*

Explain broadly what project aims to achieve\*

What type of processing is involved? You may find it helpful to refer or link to other documents, such as project proposal.\*

Summarise why you identified the need for DPIA.\*

Logout

Submit

Figure 6: Application Assessment Page

## 2. AI Assessment Page

If the user selected **AI Scenario**, they will be redirected to the **AI Assessment Page** where they must provide details such as:

- **Project Name:** Name of the AI-related project.
- **Date of Assessment:** The date of this assessment.
- **Use Case:** Choose the relevant use case for the AI application.
- **Describe the scenario where AI will be used:** Provide details about how AI is utilized in the project.
- **Primary Purpose of AI System:** Explain the main goal of the AI component.
- **Implementation:** Select whether the AI system is predictive or generative.
- **Types of Data Processed:** Identify the type of data being processed by the AI system (e.g., Personally Identifiable Information, Financial Data, etc.).
- **Beneficiaries of the AI systems:** Who are the primary users or beneficiaries of the system (e.g., General Public, Businesses, Governments).
- **Outcome of the system:** Explain the expected outcome of the system and its methods to achieve the outcome.
- **Effects of the outcome:** Explain the impacts of the outcome on its users or its beneficiaries.
- **Outcome Accessibility:** Is the outcome shared with third parties?
- **Nature of Data Sharing:** Explain the involvement of the third parties and the type of data being shared externally.

Once the form is completed, the user can submit it for processing.

The user must fill entire form to proceed.

AI Assessment

Project Name\*

Date of Assessment\*  dd/mm/yyyy

Use case\*

Describe the scenario where you plan to use AI.\*

Briefly describe the primary purpose of the AI system\*

Implementation\*  
 Predictive  
 Generative

What types of data does the AI system process to achieve its purpose?\*  
 Personally Identifiable Information  
 Financial Data  
 Special Categories of Personal Data  
 Non-Sensitive Data

Who are the primary users or beneficiaries of the AI system?\*  
 General Public  
 Specific Consumer Segments  
 Businesses  
 Government Agencies  
 All

Briefly describe the expected outcomes or outcomes of the AI system and how it is achieved\*

How do these outcomes directly impact the beneficiaries?\*

Are the outcomes of AI system shared with or accessible to third parties?\*  
 Yes  
 NO

**Submit**

Figure 7: AI Assessment Page

Click on submit after filling the form

### 3. Dataflow and AI Privacy Threat Generation

Upon submitting either form, the system generates **Dataflows**—which represent potential threats or vulnerabilities the application might face:

- For **Application Assessments**, only Dataflows are generated.
- For **AI Assessments**, the system generates both **Dataflows** and **AI Privacy Threats**.

This generation process can take up to 10 seconds, during which the user will see a loading screen.

Once the backend has generated the Dataflows (and AI privacy threats for AI assessments), the user is redirected back to the same page, where they can review and select the data flows that align best with the requirements and threats faced by their application.

## 2. Data flow selection

After completing the assessment form and submitting it, the user is directed to the **Data Flow Selection Page**. This page allows users to select from a list of newly generated data flows or reuse previously created data flows from other projects.

#### Data Flow Options:

Users can choose from the following:

1. **Newly Generated Data Flows:** These data flows are automatically created by the system based on the details provided in the previous assessment form.
2. **Create New Data Flows:** Users can manually create new data flows if the automatically generated ones do not meet their needs.
3. **Reuse Existing Data Flows:** Users can also select data flows they've previously created for other projects.

The screenshot shows a user interface for selecting data flows. At the top, there's a summary for 'Ahsan' dated 'Sept. 25, 2024'. A callout box says 'Click on fill the DPIA form'. Below, a section titled 'Select required Dataflows' contains two checked checkboxes: 'Sensor Data Collection' and 'Vehicle To Infrastructure Communication'. A tooltip for 'Sensor Data Collection' is visible, explaining its purpose for autonomous vehicles.

Figure 8: Data Flow selection page

After selecting the required Dataflows (at least one) the user can click on “Next” button or “DPIA Form” button. Both will redirect them to a DPIA requirements form. This form captures more User Application Details required for accurate generation of threats and their mitigation for the user.

### DPIA Form:

The DPIA form has six sections, which are as follows:

- 1. Nature:** Capturing the nature of data collected.
- 2. Scope:** Scope or the types of data collected by the user for their application.
- 3. Context:** Details on why the data collected is important for their application.
- 4. Purpose:** Further details on why the dataset is necessary and its use.
- 5. Consultation:** Has the user taken in consultation regarding the nature of their collected dataset and if so who are they and at what frequency are they consulted.
- 6. Necessity:** What is the necessity of your project.

The screenshot shows the TANGO Privacy Enhancing Component interface. On the left, there's a sidebar with options like Dashboard, App Assessment (which is selected), AI Assessment, Need for DPIA, Navigate to PAT, and Logout. The main area shows a user profile for 'Ahsan' from 'Sept. 25, 2024' with the identifier 'svsfwefwefwg'. To the right, a large orange box contains a list of six sections: 1. Nature, 2. Scope, 3. Context, 4. Purpose, 5. Consultation, and 6. Necessity. Each section has a green circular icon next to it. Above this list, a callout box with a blue border and white text says 'Fill all selections of the DPIA form'. Below the list, there's a section titled 'Project Consultation' with a text input field containing placeholder text about seeking consultation with stakeholders. There's also a dropdown menu for asking processors for assistance. Further down, there are sections for selecting internal stakeholders (with 'Technical Team' checked) and providing the frequency of consultation with them (with 'Regulatory Authority' checked). There's also a section for external stakeholders and their consultation frequency. At the bottom right, a blue button labeled 'Next →' is highlighted with a callout box that says 'Click next to proceed'.

Figure 9: DPIA Form

The user will fill each section of the form and click on **Next** button and if they want to go back to a previous section they can navigate using the **Prev** button at the bottom. The form has auto saving functionality so if the user want to leave the form half-filled and come back later they can navigate back to the form from the **Dashboard** page. This will be discussed in more detail in later sections.

After filling all the sections the user will be redirected back the Data flow selection page where they can submit it to the backend for processing.

Ahsan  
Sept. 25, 2024  
svvsfwefwefwg

Select at least one existing or newly created Dataflow \*

Sensor Data Collection New  
Autonomous vehicles continuously collect data from various sensors like LIDAR, RADAR, cameras, and GPS to perceive their surroundings, detect obstacles, and navigate through the environment. [Read more](#)

Vehicle To Infrastructure Communication New  
Autonomous vehicles communicate with traffic signals, road signs, and other infrastructure components to receive updates about traffic conditions, road works, and other relevant information for... [Read more](#)

Autonomous Cars  
Autonomous vehicles collect real-time data from various sensors, including LIDAR, cameras, GPS, and IMU, to perceive their environment and detect obstacles, road signs, and traffic... [Read more](#)

**Create New +** **DPIA Form** **Submit**

Figure 10: DPIA Selection Page

## Backend Processing:

When the user submits their data flows:

- A **cronjob** starts running on the backend to generate associated threats for each selected data flow.
- Each threat is categorized into one of four **Privacy Impact Categories**:
  - Identity theft and financial fraud
  - Unauthorized access to personal and sensitive data
  - Interception of communication
  - Vehicle tracking and location history access.
- For each privacy impact category, the backend generates the following metrics:
  - **Legal, Financial, and Reputation costs**: Assessed as **Low, Medium, or High**.
  - A **Privacy Score**: Scored between **0** and **100** for each Privacy Impact Category.
- The cronjob also generates mitigation suggestions for each threat.

### **Redirection and Notifications:**

After submitting the DPIA form, the user is redirected to the **Dashboard** page, where the project status may be tagged as "**In Progress**." A notification will pop up informing the user that the system is currently generating the **threats and scores** for the project. This process can take up to 10 minutes, but the user is free to navigate the website while the processing occurs in the background.

## 5. Dashboard

The Dashboard page has three tabs, which are as follows.

1. Application Dashboard
2. AI Dashboard
3. Mitigations

### 1. Application Dashboard

Any projects the user created from the Application Assessment page will be listed in the Application Dashboard page. The project will be shown to the user in the form of cards. Each card will have the name, type, created date and description of the projects along with a delete icon and an eye icon.

Each project may be completed or in completed depending on the status. **In-completed** status means that's either the user has not completed the form Data Flow selection stage for that project, or the backend system is currently processing the user data to generate threats for the data flows selected by the user for those projects. If the status is **completed** the user will see another options on the project card, like a **Detail** button. Clicking on the detail button will lead the user to the Details page where they can view the details of the dataflows they selected along with the threats generated and their scores and visualizations.

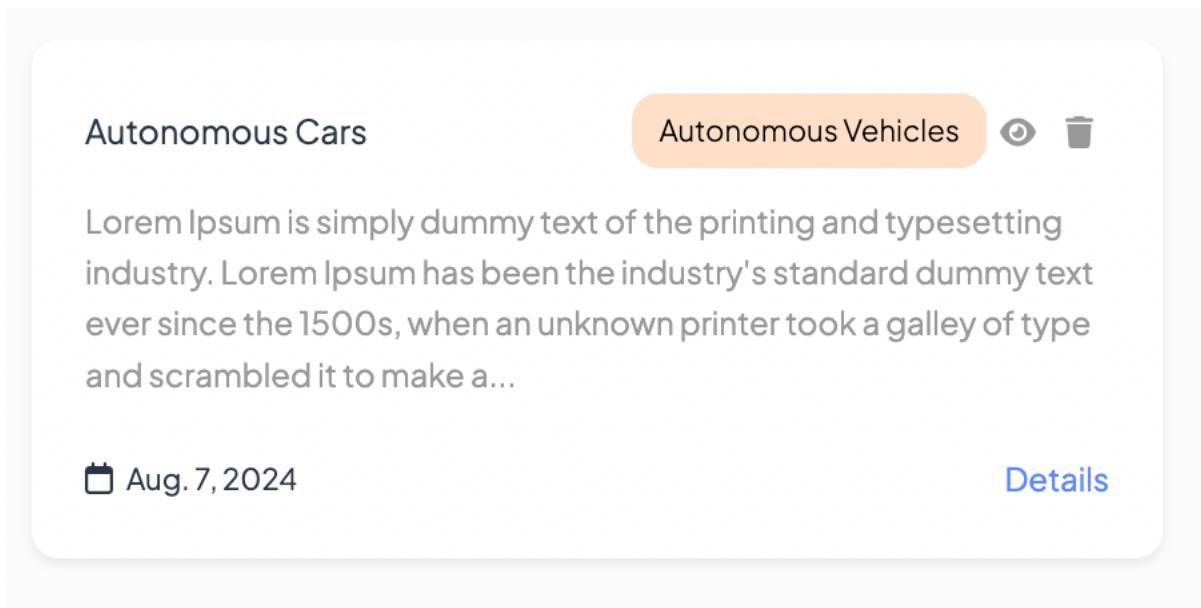


Figure 11: Application Assessment Project Card

## 2. AI Dashboard

Any projects the user created from the AI Assessment Page will be listed in the AI Dashboard page. The details of the AI Dashboard page are same as from the App Dashboard discusses above.

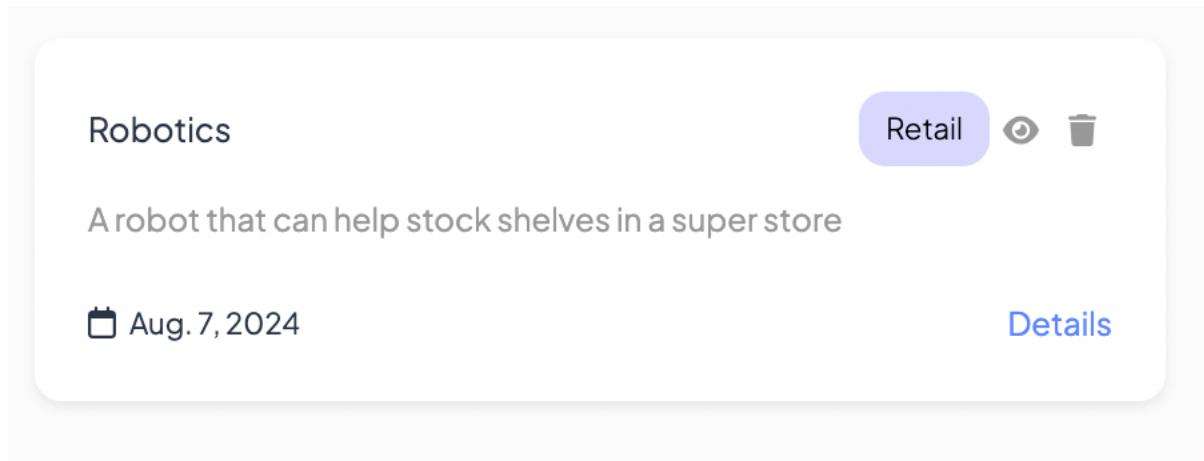


Figure 12: AI Assessment Project Card

## 3. Mitigations

The mitigations page allows the user to quickly and easily search for mitigations that were generated for their projects.

A screenshot of the Mitigations page. The top navigation bar shows "Dashboard / Projects List" and tabs for "Application Dashboard", "AI Dashboard", and "Mitigations", with "Mitigations" being the active tab. Below the tabs is a search bar with placeholder text "Search anything i.e dataflow, threat or mitigation etc" and a clear button. There are four dropdown menus labeled "Select Type", "Select Dataflow", "Select Threat", and "Select Mitigation", each with a dropdown arrow. To the right of these are "Filter" and "Clear" buttons. The main content area contains a section titled "Sensor Data Collection" with a descriptive paragraph about autonomous vehicles collecting real-time data from various sensors. Below this are three collapsed sections: "Sensor Spoofing", "Denial Of Service Attack", and "Man In The Middle Attack", each with a collapse arrow.

Figure 13: Mitigations Page

In the mitigations page they will find a search bar labelled as “**Search Anything**” to find mitigations by dataflow, threat, or mitigation name.

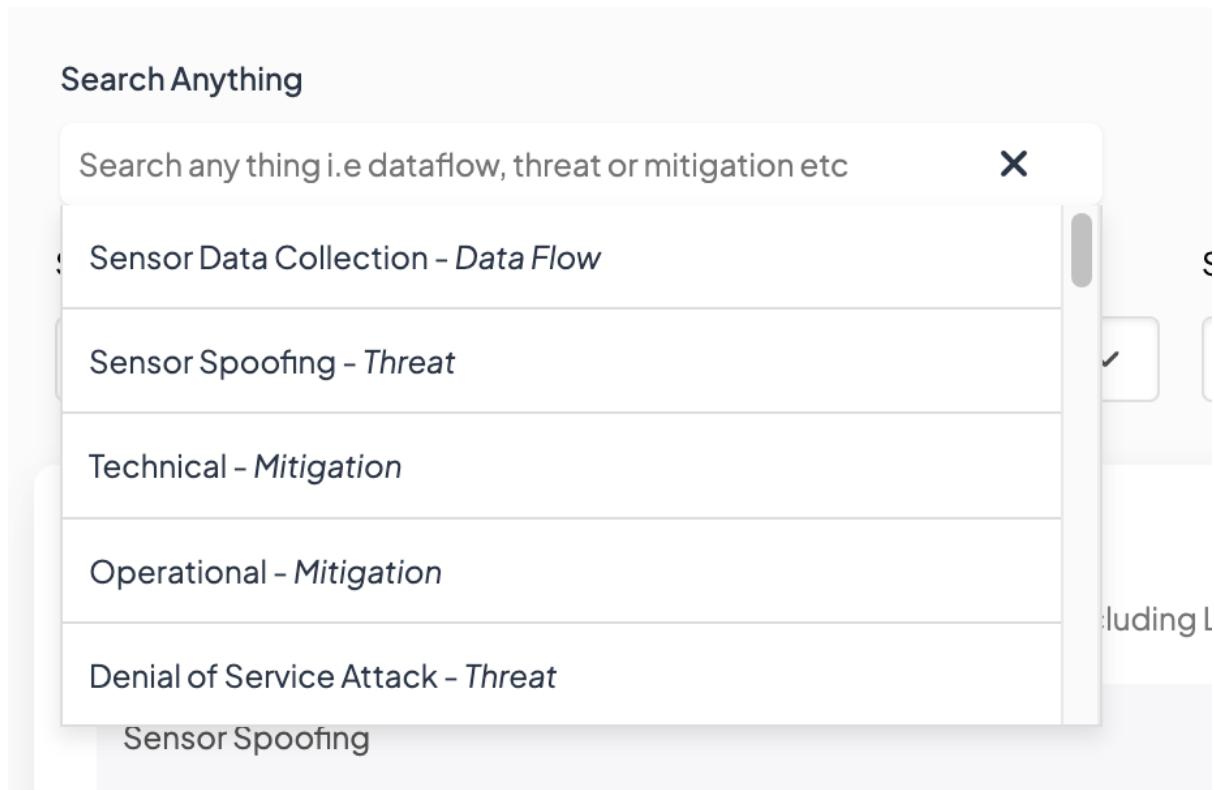


Figure 14: Search for mitigations

The user will also find a set of filters in the mitigations tab. They can use these filters to find filter mitigations using Type, Dataflow, Threat and mitigations name. Each filter they select, further limits the scope of the filter for example selecting the type i.e selecting type App will only list the dataflows that come under App.

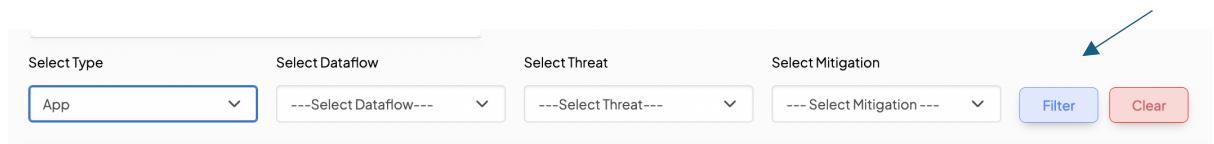


Figure 15: Filter Mitigations

When the user clicks on the filter button, depending on their filter criteria the user will see a list of data flows, their threats and the suggested mitigations related to those threats. The user may select or de-select the mitigations they have implemented as a checklist.

Sensor Data Collection

Autonomous vehicles collect real-time data from various sensors, including LIDAR, cameras, GPS, and IMU, to perceive their environment and detect obstacles, road signs, and traffic signals.

**Sensor Spoofing**

An attacker generates false sensor signals or alters the real signals, causing the autonomous vehicle to make incorrect decisions. This could involve spoofing GPS coordinates or feeding incorrect data to LIDAR and cameras.

**Technical**

- Use cryptographic techniques to authenticate and verify sensor data integrity. (Mitigation)
- Implement sensor fusion to cross-verify data from multiple sources.

**Operational**

- Regularly update and patch sensor firmware to address known vulnerabilities.
- Conduct thorough testing and validation of sensor data under various scenarios.

**Denial Of Service Attack**

**Man In The Middle Attack**

Figure 16: Mitigations Checklist

## 4. Details Page

When the user clicks on the detail button from cards on Application or AI Dashboard they are redirected to the details page. The details page will list down all of their dataflows in a Accordian format which are collapsible. Each threat will be followed by a description of the threat that the user application may face, along with a table for Privacy Impact Categories.

The Privacy Impact Categories are as follows:

1. Identity theft and financial fraud.
2. Unauthorised access to personal and sensitive data.
3. Interception of communication.
4. Vehicle tracking and location access.

Privacy Impact Category	Legal Fines	Financial Costs	Reputation Costs	Privacy Score	View Threat Details
Identity theft and financial fraud	Medium	High	High	16	<button>View Details</button>
Unauthorised access to personal and sensitive data	High	High	High	27	<button>View Details</button>
Interception of communication	Medium	Medium	Medium	18	<button>View Details</button>
Vehicle tracking and location history access	High	Medium	High	32	<button>View Details</button>

Figure 17: Threats Details Table

The columns of the table will show the Legal, Financial and Reputation costs for the application rated as Low, Medium and High, along with a Privacy Score from 0-100 and a details button. When clicked on the details button. When clicked, a pop up will show the user the potential threats related to that category.

Which are as follows:

1. Dignity Loss
2. Discrimination
3. Economic Loss
4. Loss of Autonomy
5. Loss of Liberty
6. Physical Loss
7. Loss of Thrust

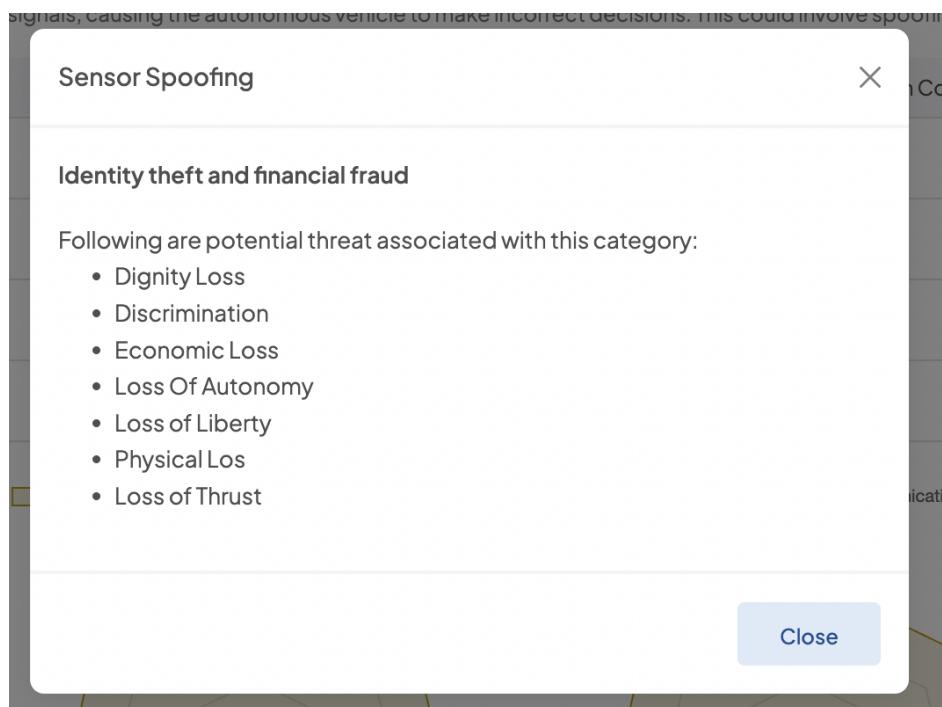


Figure 18: Threats associated to a Impact Category

The user will also see 4 web charts just below each table related to the four privacy impact categories. The colour of the chart signifies the threat level for that category. The chart will also show each potential threat level that impact category face i.e 0 - 1

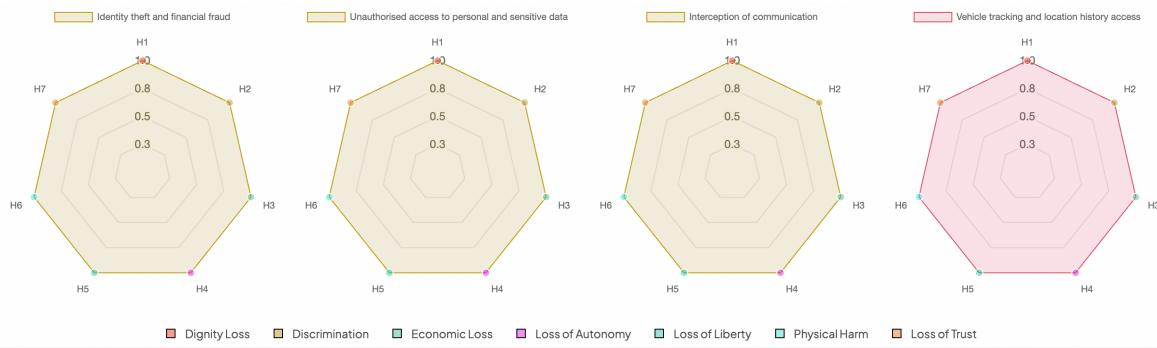


Figure 19: Web Charts for each impact category

The user will also see a “**View Mitigations**” button to the right of the threat name. Clicking on it will show a pop up list down the generated suggested mitigations for that threat. The user may select or de-select the mitigation they have implemented.

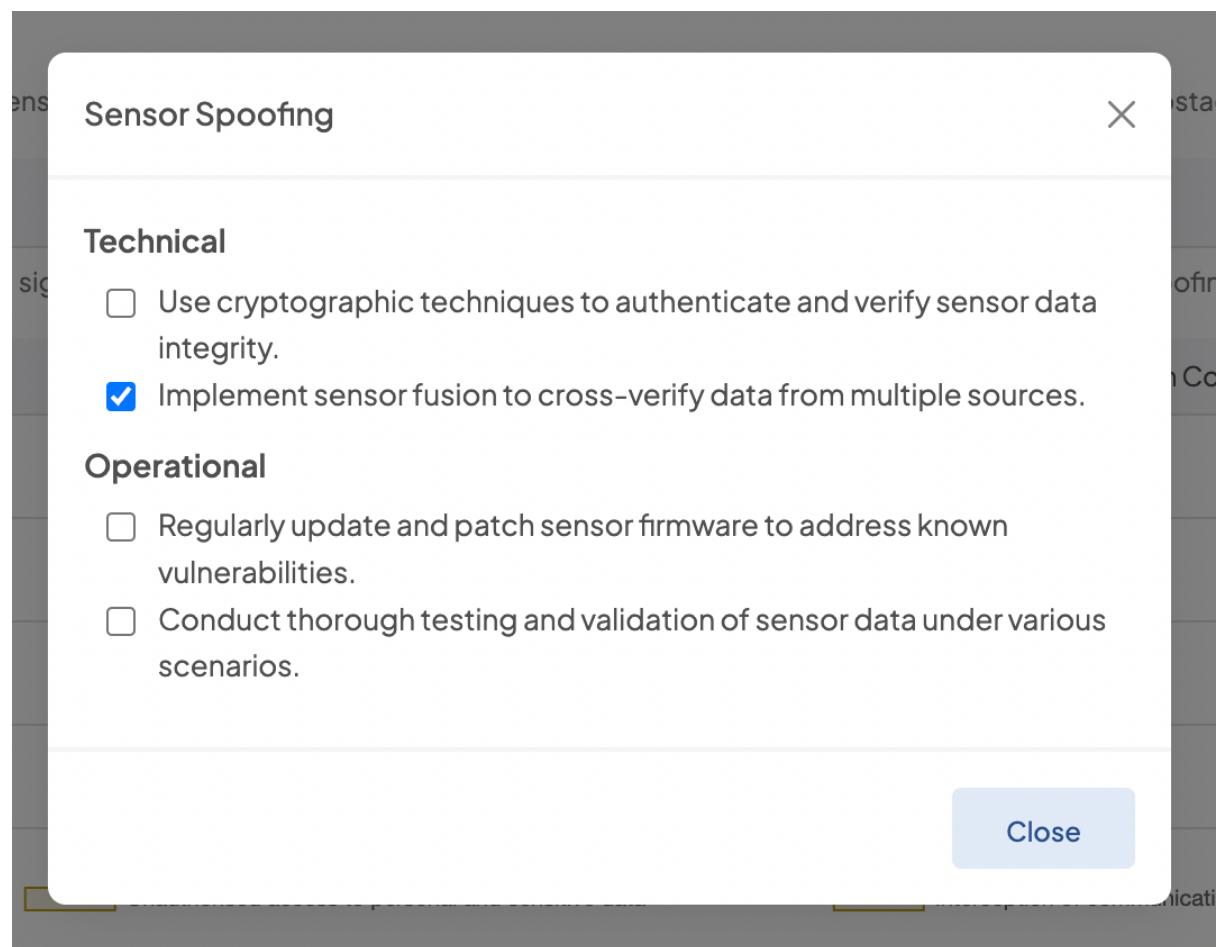


Figure 20: Mitigation Checklist Popup

The user will also see two control buttons at the top of the page, namely **Edit Dataflow** and **Delete** button. The delete button will delete the project and redirect the user back to dashboard, where as the Edit Dataflow will take the user back to Dataflow select page where can chose more dataflows or generate new ones according to their needs.

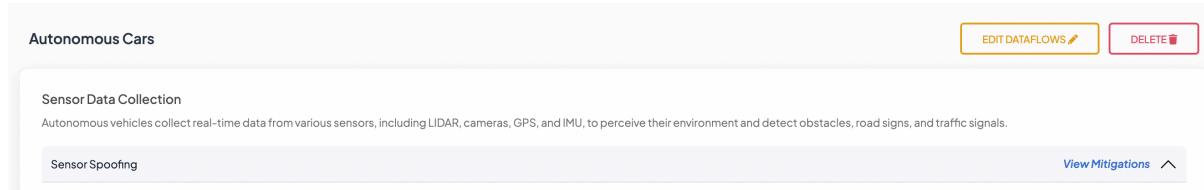


Figure 21: Project Control button