

# Ethical consideration

## Data Privacy and Security

**Data Collection and Storage:** This project collects user's speech and hand gesture data during the process of visual recognition and speech recognition. The collected data does not include sensitive information such as facial data and is stored in two recognition modules. User's gesture information is used for visual recognition to track objects, while speech information is solely used for analysis and text command generation.

**Data Protection:** The data collected in this project will not be retained for an extended period and exists only within the system for a single use. Only development and testing personnel have access to the data.

**User Consent:** Users will be informed before using this project, and their continued use will be considered as consent for data collection.

## Fairness and Bias

**Data Bias:** The project utilizes large-scale models such as GPT-3.5, making it unlikely to encounter data bias situations.

**Equality:** The system is capable of handling diverse speech patterns, accents, languages, and facial features to ensure diversity and inclusivity.

## Transparency and Explainability

**Transparency:** The project goes through three processes - voice-to-text conversion using GPT-3.5, sentence standardization, and keyword extraction, combined with visual recognition information to generate ROS2 commands for controlling the robotic arm.

**Explainability:** User speech is transformed into text by GPT-3.5, followed by semantic analysis to extract command keywords. The scene captured by the camera undergoes visual recognition to identify objects within the field of view. Finally, information from both modules is integrated to generate ROS2 commands.

**User Control:** Users have clear control over the robotic arm's operation, including the right to cancel commands.

**Failure Explanation:** When the system is unable to complete a command, it will prompt the user and explain the reason.

## Security

**Robotic Arm Safety:** The operation of the robotic arm is secure and does not pose a danger to users or the surrounding environment. This includes safety thresholds, collision detection, and emergency stop functions.

**Remote Control Security:** Communication for remote control of the robotic arm is secure and not susceptible to malicious attacks or interference.

## User Education and Engagement

**User Education:** Users are required to read the user manual, install the necessary environment, and become familiar with the operating procedures before using the system.

**User Feedback:** Users have the option to provide feedback and opinions to the developers.