NUS
National University
of Singapore

NPS2001D Milestone 2

A0258448N Ngoh Pek Suan, Nikki
A0252779M Adam Seah Jun Hui
A0252754B Jackson Yeong Hong Han
A0254813E Seck Miao Zhen Christabel

Data required for app to function:

<u>External entities</u>

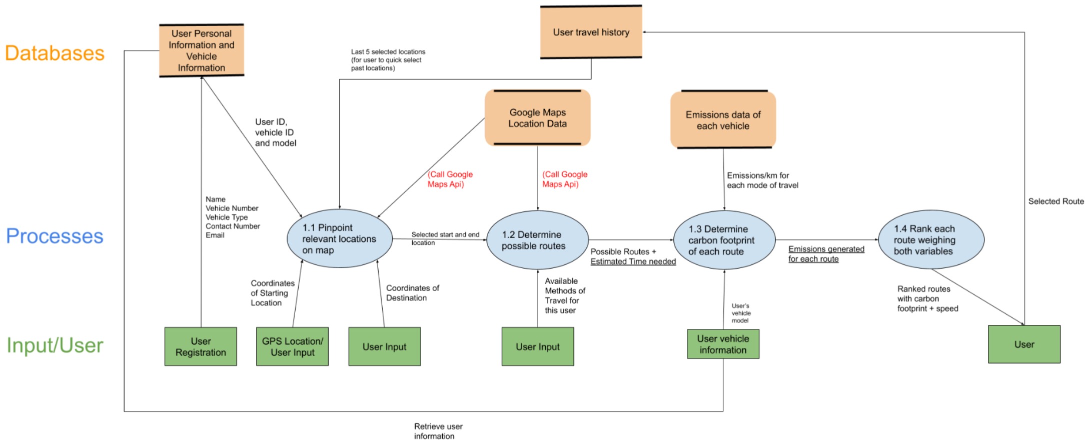
- End user
- Current GPS location input

<u>Data stores (see spreadsheet)</u>

- User contact information
- User vehicle information
- User travel history
- Geographical database of all locations
- Database of public transport routes, roads, electric car stations etc.
- Emissions data of each vehicle

<u>Data processes</u>

- Register new user
- Add / update user contact information
- Add / update vehicle information
- Add travel history
- Starting location & Destination query (pinpointing relevant locations)
- Determine possible routes
- Determine carbon footprint of each route
- Ranking routes


Databases
Processes
Input/User
User Personal Information and Vehicle Information
User travel history
Last 5 selected locations (for user to quick select past locations)
Google Maps Location Data
Emissions data of each vehicle
User ID, vehicle ID and model
(Call Google Maps Api)
(Call Google Maps Api)
Emissions/km for each mode of travel
Selected Route
Name
Vehicle Number
Vehicle Type
Contact Number
Email
1.1 Pinpoint relevant locations on map
Selected start and end location
1.2 Determine possible routes
Possible Routes + Estimated Time needed
1.3 Determine carbon footprint of each route
Emissions generated for each route
1.4 Rank each route weighing both variables
Coordinates of Starting Location
Coordinates of Destination
Available Methods of Travel for this user
User's vehicle model
Ranked routes with carbon footprint + speed
User Registration
GPS Location/ User Input
User Input
User Input
User vehicle information
User
Retrieve user information

Issues related to data privacy and security and how we intend to curb them:

Data Collection: Our programme only gathers the necessary information needed. User security and privacy are our top priorities, and we make sure that no unnecessary data is collected. The data we collect is solely used to provide tailored transportation recommendations based on the user's profile. This includes important information including route preferences, trip histories, and location data. Before collecting any sensitive personal information, especially data like addresses and phone numbers, we will ensure user consent has been obtained. Users have the autonomy to decide whether or not to participate in data collection. After data is collected, we offer users the option to anonymize or pseudonymous their personal data, mitigating the risk of identification in the event of a data breach. Furthermore, all private user information is encrypted both during transit and in storage to prevent unauthorised access by third parties. Transparency is also very important to us. We are open about our data collection methods, giving users a clear picture of what information is gathered, how it is put to use, and who it may be shared with. Our dedication to transparency assures users that they are in control over their personal information.

Data Usage: Data collected by our app is utilised solely to enhance the app's recommendation algorithm and improve the overall user experience. We adopt stringent guidelines for data minimization, gathering just the necessary amount of relevant information required for the target purposes. To safeguard user privacy, we refrain from collecting or unnecessary personal data, such as identification numbers or travel histories from family members. In addition, we believe it is crucial to respect user's preferences. We provide users with control over their data usage, including options to manage access permissions, such as allowing the app to access their cameras and real-time location. Most importantly, we do not engage in the sale or sharing of user data with third parties for marketing or advertising purposes.

Data Sharing: User data security and privacy are our top priorities, and we enforce strict guidelines when it comes to sharing it. User data will not be shared with companies or third-party services without the explicit consent of the user. All data sharing activities will be conducted in full compliance to mandatory privacy regulations, ensuring that users' rights are protected. Before any data sharing is performed, careful consideration is given to anonymizing or pseudonymizing the data to minimise the chance of individual identification while allowing third parties to perform insightful analysis. In addition we will verify that these companies have robust systems such as data encryption and unauthorised restricted access in place to safeguard the integrity and confidentiality of the data. Furthermore, the data sharing agreements will include clauses that require immediate notification in the case of unauthorised access or data breach.

Risk Assessment Matrix

	Mild	**Moderate**	**Severe**
Near Certain	Low	High	High
Likely	Low	Moderate	High
Unlikely	Low	Low	Moderate

Data Risks

Risk	**Likelihood**	**Severity**	**Mitigation Strategy**
Unauthorised Access	Likely	Severe	Implement strong authentication and access controls such as 2FA. Regularly audit access logs to monitor suspicious activity. Encrypt sensitive data at rest and in transit using end-to-end-encryption.
Data Breach	Likely	Severe	Employ robust encryption mechanisms such as Advanced Encryption Standard (AES) to protect user's data. Implement intrusion detection systems to detect and respond to breaches promptly. Regularly update security protocols and conduct security audits.
Data Misuse	Unlikely	Moderate	Implement strict data access controls and user permissions. Regularly review and update privacy policies and user agreements on data sharing. Educate users about safe data practices and provide tools for data management and deletion.

GitHub Link: https://github.com/ChristabelSeck/Milestone-2-Dataset-Submission