SafeTrack

OneSolution Inc.

Privacy Impact Assessment

SafeTrack

The Next Generation Privacy-Focused Location Tracking and Timeline Service

Part 1 – Program background and details

Program	SafeTrack -The Next Generation Privacy-Focused Location Tracking and Timeline Service		
Organisation	Onesolution Inc		
PIA Drafter	Thanuka Thathsara Rathanayke	Email	s8145860@live.vu.edu.au
Program Manager	Thanuka Thathsara Rathanayke	Email	s8145860@live.vu.edu.au
Privacy Officer		Email	
Date Completed	24/07/2024		

Description of the program and parties

Overview

SafeTrack is an advanced location tracking and timeline that is being designed and proposed by Onesolution Inc. to offer you the best tracking solutions. Latest technological features in the tool will also guarantee customers give permission to monitor the movement of family members or employees or assets with the highest privacy and data security. The SafeTrack product supports the company's general objective of offering excellent, simple to use, and safe location-based services at Onesolution Inc. SafeTrack was a project that originated from the lack of proper efficient and private tracking solutions within the personal safety and logistics and workforce

Purpose and Objectives

SafeTrack has been developed to provide an optimal location tracking service for users with one of the focuses consisting of privacy protection and the secure storage of users' data. It was developed as a solution to the rising complications in data management and protection alongside the demand for better location tracking services. Key objectives include:

- Provide accurate and real time data to the users
- Ensure security and protection to the collected and stored data of the users
- Provide access to control data to the users
- Enhancing operational efficiency for businesses.

SafeTrack is dedicated to revolutionizing the way of location data collection and usage, To implement enhanced security measures that exceed the existing field's standards.

Fit Within Organizational Objectives

Primarily focusing on such concepts as innovation and users' trust, SafeTrack complies with the objectives of OneSolution Inc. As an organization prioritizing privacy and security, SafeTrack additionally contributes to the improvement of the company's image as the provider of the safest technologies.

Program Operation

SafeTrack consists of several key components:

- **Mobile Application:** SafeTrack mobile app collects location data via GPS, Wi-Fi triangulation, and Bluetooth beacons.
- **Backend Systems :** Data sent to the SafeTrack servers , processes and stores securely.
- **User Interface :** Users can manage their data and through the SafeTrack app conveniently

It must be noted that the program involves different departments of OneSolution Inc. , such as information technology, security, legal, and clients' support departments. The Chief Privacy Officer is the one who has a managerial responsibility of the program, as well as the observance of the different privacy laws and policies. SafeTrack communicates with other organizational systems, for instance, customer base and analytical tools to boost offer utility.

Key milestones include:

- **Development :** Development and testing of SafeTrack platform including the SafeTrack App
- **Pilot Launch :** Launch to selected group initially and optimize according to their feedbacks
- **Full Launch :** Release the service to the public
- **Ongoing Updates :** Regular updates and improvements based on user feedback and technological advancements

Personal information is directly collected from the users during registration on SafeTrack site and while using the mobile app. This concerning personal information involves items like names, address, and the email address among other things.

Duration and Implementation Timeframes

SafeTrack is currently an active project and goes through constant evolution and enhancement phases. The pilot is planned for the six months, following which a full launch will be made. The plan to update the application regularly and incorporate new features is plausible after the experiments' launch.

Technical Platform and Services

SafeTrack uses a highly secure technical platform, incorporating:

- **End-to-End Encryption:** Secures the data when it is being transferred from one network to another, or when the data is stored.
- **Blockchain Technology:** Ensures that there is a record of auditing of data usage as well as alterations.
- **Differential Privacy:** Preserves user's identity while data is being processed.
- **Zero Trust Architecture:** Ongoing authentication to user identity and the authorization to access the information.

They make SafeTrack functioning secure and safeguarding users' data possible.

Expected Benefits

SafeTrack offers significant benefits, including:

- Enhanced user safety through reliable location tracking.
- Improved operational efficiency for businesses.
- Stronger user trust due to advanced privacy and security measures.
- Compliance with privacy regulations, reducing legal risks.

Involvement of Third Parties

SafeTrack works with several third-party service providers, like the storage of cloud and map services. Basically these third parties are useful in offering basic services and the ones who deal with personal data are under legal obligation observing data protection laws. This means that all the third-party providers recognize the Privacy and Data Protection Act 2014 (PDP Act) and other related acts of laws on the recognition of privacy.

Hence, SafeTrack has been designed with innovative technologies and the inclusion of strong privacy features to create a new generation secure location tracking solution provider – OneSolution Inc.

.

Scope of this privacy impact assessment

Areas Covered by This PIA

SafeTrack this Privacy Impact Assessment (PIA) covers the program from the setup-development stage of the program, the using and maintaining stage of the program. The assessment includes:

- **Data Collection:** Examination of the methods and technologies used to collect location data, such as GPS, Wi-Fi triangulation, and Bluetooth beacons.
- **Data Transmission:** Assessment of the security measures in place to protect data as it is transmitted from user devices to SafeTrack servers.
- **Data Storage:** Evaluation of the storage solutions and encryption protocols used to secure user data at rest.
- **Data Usage:** Analysis of how collected data is processed, used to provide services, and displayed to users through the application.
- **Data Deletion:** Review of the mechanisms and policies for secure data deletion and user control over their data.

Areas Not Covered by This PIA

This PIA does not cover:

- **Third-Party Integrations:** Specific integrations with third-party applications or services that may be developed in the future will require separate PIAs.
- **External Legal Compliance:** Compliance with specific international laws outside the jurisdictions explicitly mentioned (such as specific regional privacy laws not covered under GDPR or PDP Act) is not covered and will require additional assessments.

Nature and Stage of Development
SafeTrack is an ongoing program with multiple stages:

- **Initial Development and Pilot Phase:** Currently, the program is in the development phase, with a pilot launch planned for the next six months.
- **Full Launch and Ongoing Operations:** Post-pilot, the program will transition into full operational status with regular updates and enhancements.

Due to the dynamic nature of the program being proposed, the extent of this PIA applies to the entry implementing stage, pilot test and stabilization phase. Any future changes or development of the application and/or the additional functional will also require its own PIA.

Public Interest Determinations and Arrangements

At this time, SafeTrack does not fall under any public interest determinations or information usage arrangements. Should such determinations or arrangements be made in the

Other Relevant PIAs

It is therefore to be noted that this particular PIA is aimed to span only the core aspects of SafeTrack. As the program evolves, additional PIAs will be conducted for:

- **New Features:** In this respect, it is essential to identify any major new developments or alterations in procedures for data management.
- **Third-Party Integrations:** Right now it is integrated with other services or applications only indirectly, through the GUI of the browser.

This way, two types of checks are employed: overall PIAs for the entire program to be launched and incremental PIAs for each stage of the program.

Multiple Parties Involved

The SafeTrack program involves several key parties:The SafeTrack program involves several key parties:

- **OneSolution Inc. :** A body serving as the main governing and implementing agency of SafeTrack.
- **Cloud Service Providers (CSPs):** Third-party service companies who handles secured storage and analysis of data.
- **Security Consultants:** People outside of the organization to examine and suggest the best security measures within the company.

Specifically, this PIA determines OneSolution Inc. ’s privacy requirements and conduct data handling for itself and its direct CSPs. New PIAs will be carried out in the event that there are other third-parties to integrate or partner with.

Legal authority

OneSolution Inc. is authorized to collect, use, and disclose personal information under the following legislation:

- **Privacy and Data Protection Act 2014 (PDP Act):** Meeting state-level privacy standards that are mandatory to be adhered to.
- **General Data Protection Regulation (GDPR):** The other concern for purchasing the system is to ensure the organization adheres to the international policies of data protection and privacy.

The following acts act as the legal provisions that OneSolution Inc. uses to process personal information relating to the SafeTrack program. Furthermore, OneSolution Inc. applies all the other related laws which includes Charter of Human Rights and Responsibilities Act 2006 of Victoria, and Victoria Data Sharing Act 2017.

Stakeholder consultation

Consultations have been conducted with:Consultations have been conducted with:

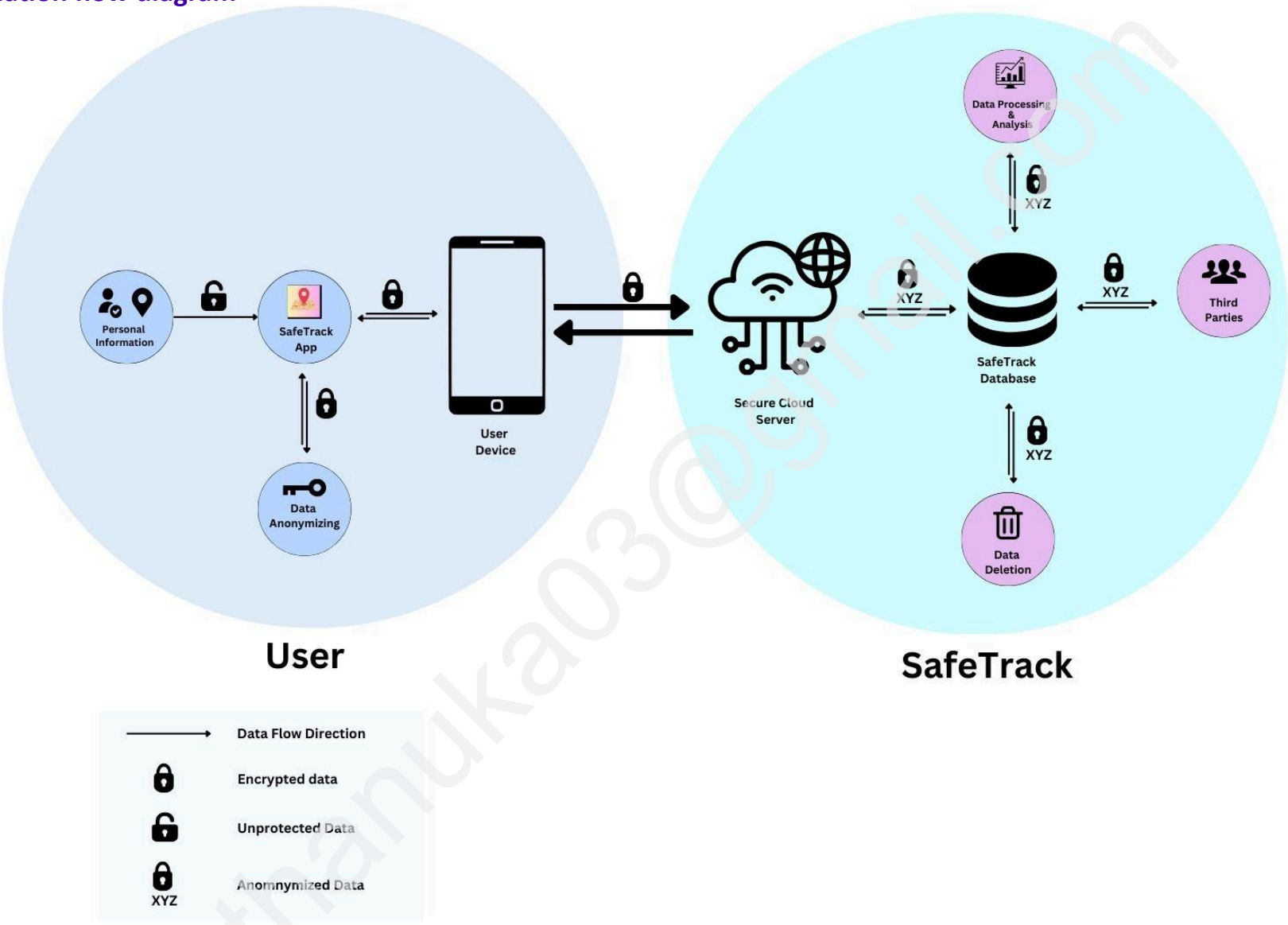
- **Internal Stakeholders:** Adding IT, security, legal, and customer support departments as the members of OneSolution Inc.
- **External Stakeholders:** Web site users who volunteered to test new versions of a site, privacy concern individuals, and Independent security experts.

The latter has been accomplished by incorporating the results of such consultations into the program improvements aimed to strengthen privacy and security approaches within the context of corresponding higher education programs.

Community Expectations

The process of consultation and feedback has been incorporated during the development of SafeTrack. This aspect has enabled the development of the program features and provisions of the privacy policies based on the community attitudes and expectations. Measures have been taken to successfully reach out to users and maintain the trust since people's trust is much important ShouldTrack will have in the future.

Information flow diagram



Part 2 – Privacy analysis

The part identifies the privacy elements and risks the program. The PIA Guide provides guidance on responding to the questions. The right column indicates the relevant section of the PIA Guide. Some questions may not be relevant or applicable. The response should be noted as N/A where this occurs.

The assessment includes prompts to assist identifying the program's elements and risks. There may exist elements or risks beyond each prompt, and each question should be given a broad interpretation. Identified privacy risks should be listed in Part 3. The PIA Guide contains examples of privacy risks that may arise.

Identify the information elements

	Question	*Response*
1	**Does the program involve personal information?** *List each piece of personal information that is involved in the program.*	Yes • Anonymized identifiers(Name,age,address,email) • 3rrWi-Fi triangulation data, cellular data)
2	**Does the program involve other information that has the potential to identify individuals?** *This may include information that does not appear to be personal information at first glance, but which could identify individuals based on the context of the project or how the program uses the information.* *Describe this other information and explain how it could potentially identify individuals within the context of the program.*	Yes. Encrypted and anonymized location data could potentially identify individuals if the encryption is compromised or if combined with other data sources. Even anonymized location data can reveal patterns that may identify individuals based on their movements and frequent locations.
3	**Does the program involve sensitive information (as defined under Schedule 1 of the PDP Act)?** *Describe the type(s) of sensitive information that is involved in the program (if any), and how the collection or use of the sensitive information is authorised either by the PDP Act or other legislation.*	No. The program does not explicitly collect sensitive information such as racial or ethnic origin, political opinions, or religious beliefs.
4	**Does the program involve health information?** *If the answer is yes, please refer to the Health Records Act 2001 or consult with the Health Complaints Commissioner in relation to health information (and where applicable, the Office of the Australian Information Commissioner).*	No.
5	**Does the program involve information that has previously been de-identified?** *Describe the type(s) of de-identified information that is involved in the program (if any), and the potential for re-identification.*	Yes. The location data collected is de-identified through anonymization and encryption techniques before being stored. Potential for re-identification: Low, due to the use of strong encryption and differential privacy techniques.

Collection of personal information

6	**Is all the personal information collected necessary for the program?** *Explain why all the information collected is necessary for the program.*	Yes. The anonymized identifiers and location data are essential for providing the tracking and timeline services while ensuring user privacy.
7	**Does the organisation need to collect information that identifies an individual for the purposes of the program, or can individuals remain anonymous?**	Individuals can remain anonymous. The program uses anonymized identifiers instead of personal identifiers.
8	**If individuals can remain anonymous, will the organisation be collecting indirect identifiers, such as demographic information?**	No. The organization does not collect indirect identifiers; it focuses solely on anonymized location data.

Method and notice of collection

9	**How will the personal information be collected?** *Describe the means by which the information will be collected. If personal information is collected via a third party platform, explain whether the platform will also be collecting that information*	Directly from users' devices through on-device data processing. Data is collected using GPS, Wi-Fi triangulation, and cellular data. Anonymized and encrypted before transmission to SafeTrack's servers.
10	**Is the personal information collected directly from the individual?**	Yes. The information is collected directly from users' devices with their consent.
11	**Will the individual be notified about the collection of their personal information?** *Describe the steps taken to provide notice to the individual OR explain why notice will not be provided to the individual. Include a link or attach collection notices where appropriate.*	Yes. Users are informed during the registration process and through the app's privacy policy and terms of service.
12	**Will any personal information about the individual be collected indirectly from another source?** *Describe how and from which other sources the personal information will be collected.*	No. All personal information is collected directly from users' devices.

13	**Will the individual be notified that their personal information has been collected from another source?** *Describe the steps taken to provide notice to the individual OR explain why notice will not be provided to the individual. Include a link or attach collection notices where appropriate.*	N/A. No personal information is collected from another source.

Unique identifiers

14	**Will the program assign a unique identifier or collect a unique identifier assigned by another organisation to adopt as the organisation's own?** *Describe the unique identifier, the purpose for assigning or collecting it, and how this is authorised by either the PDP Act or other legislation.*	Yes. The program assigns anonymized identifiers to users for tracking purposes. Authorization: The process adheres to privacy laws by ensuring identifiers are anonymized and encrypted.
15	**Does the program require an individual to provide a unique identifier?** *Explain why or how the provision of a unique identifier is necessary for the program.*	Yes. The unique identifier is necessary to anonymize and track users while maintaining privacy.

Quality of personal information

16	**What steps will the organisation take to ensure the personal information collected is accurate, complete, and up to date?**	• Regular data audits • User verification processes • Automated error detection mechanisms

Security of personal information

17	**Are there security measures in place (existing or intended) to protect the personal information collected and used for this program?** *List the policies, procedures, or controls that the organisation implements to protect personal information. Please indicate how these measures will be governed. Include links or attachments where appropriate*	Yes. Policies and Controls: • End-to-End Encryption (E2EE) • Multi-Factor Authentication (MFA) • Role-Based Access Control (RBAC) • Regular security audits and penetration testing • Data anonymization and differential privacy techniques
18	**Where and how will personal information be stored?** *Describe the format in which the personal information will be stored (e.g. electronic, hard copy etc.) and where it will be stored (e.g. internally, external provider, cloud, third party platform etc.)*	Format: Electronic, encrypted database Storage: Secure servers, possibly using a cloud provider with stringent security measures External provider usage: Only if they meet the high security and privacy standards set by SafeTrack
19	**Who will have access to the personal information?** *Describe the positions that will have access how access is gained or controlled, and whether it is logged.*	Access: Limited to authorized personnel based on RBAC Controlled through authenticated sessions and logged access Positions: System administrators, data privacy officers

20	**Has a separate security risk assessment been completed?** *If so, please refer to or attach a copy of the assessment to this PIA. If not, OVIC suggests a security risk assessment is completed.*	Yes. Security Risk Assessment: A comprehensive risk assessment has been conducted, addressing potential vulnerabilities and mitigation strategies.

Primary and additional uses and disclosures of personal information

21	**Is the personal information (including any sensitive information) involved in this program used or disclosed for the main or primary purpose for which it was collected?** *Describe what personal information will be used or disclosed, and for what purposes.*	Yes. • Personal information is used for location tracking and timeline services. • Disclosure: Only to the user or authorized individuals as per the user's consent.
22	**Does the program use or disclose personal information (including sensitive information) for a new or additional purpose other than the original purpose of collection?** *Describe the new/additional purpose for the use or disclosure of the information and explain how it is authorised, by either the PDP Act or other legislation. If relying on IPP 2.1(a), explain how the secondary use or disclosure is related to the primary purpose of collection.*	No. The program strictly uses personal information for the primary purpose of location tracking and timeline services.
23	**Will the individual be notified of the additional use(s) of their personal information?** *Explain how the individual will be given notice of the secondary use(s) of their information, or why notice of the secondary use will not be provided.*	N/A. There are no additional uses of personal information beyond the primary purpose.

Transfer and sharing of personal information

24	**Will any personal information be shared outside of the organisation?** *Describe:* • *what information will be shared;* • *with whom the information will be shared;* • *the frequency of the disclosure;* • *how the information will be shared; and* • *how the disclosure is authorised by either the PDP Act or other legislation.* *Identify whether any information sharing agreements are or will be in place.*	No. Personal information is not shared outside the organization unless explicitly authorized by the user.
25	**Will any personal information be transferred outside Victoria?** *Describe what information will be transferred, to whom the information will be transferred, in which jurisdiction the information will be stored, and how the information will be transferred. Explain how the transfer is authorised by either the PDP Act or other legislation.*	Possibly, depending on the storage solutions used (e.g., cloud storage). • Information: Encrypted location data and anonymized identifiers • Transfer: To cloud servers that may be located outside Victoria but within jurisdictions compliant with privacy laws. • Authorization: Ensured by compliance with the PDP Act and other relevant legislation.

Other considerations relating to use and disclosure

26	**Does the program use or disclose a unique identifier assigned by another organisation?** *Describe the unique identifier and how it will be used or disclosed, and whether this is authorised by either the PDP Act or other legislation.*	No. SafeTrack assigns its own unique anonymized identifiers to users to ensure privacy. These identifiers are used solely within the context of SafeTrack's services and are not shared with or sourced from other organizations.
27	**Will any data matching occur as part of this program? This includes matching datasets within the program, or matching to other datasets external to the program.** *If so, explain the purpose for the data matching, what personal information will be matched and what other datasets it will be matched with, and what the combined dataset will be used for.*	No. SafeTrack does not engage in data matching with external datasets. All data processing occurs within the SafeTrack environment using encrypted and anonymized data, ensuring no external data is matched or combined
28	**Will any personal information be de-identified as part of the program?** *Describe the purpose for de-identifying personal information for the program, the method of de-identification, how the de-identified information will be used, and the potential for re-identification.*	Yes. De-identification is used to protect user privacy while providing location tracking services. On-device encryption and anonymization techniques, including differential privacy. De-identified data is used for generating statistical insights and for providing anonymized alerts and notifications. Potential for re-identification: Minimal due to strong encryption and privacy-preserving techniques.
29	**What will be done to ensure the ongoing accuracy, completeness, and currency of the personal information?** *Describe the steps that will be taken, or the measures that are in place, to ensure the ongoing integrity of the information.*	Regular data audits and validations. User verification during registration and periodic checks. Automated systems to detect and correct data errors.

Management of personal information

30	**Is there a document available to the public that sets out the organisation's policies for the management of personal information, such as a privacy policy?** *Identify the document(s) and provide a link where available or include as an attachment to this PIA.*	Yes. Privacy Policy Document: Available on OneSolution Inc.'s website with the launch SafeTrack Privacy Policy
31	**Will the document be updated to reflect the new collection or use of personal information for the purposes of this program?** *If not, explain why.*	Yes. The privacy policy will be updated to reflect the specifics of the SafeTrack program

32	**Is there a way for a person to find out the types of personal information the organisation holds about them? Can an individual find out the purposes for which it is held, and how the organisation collects, holds, uses and discloses that information?** *Describe the steps and provide links where relevant.*	Yes. Users can access information through the SafeTrack portal, which details the types of personal information held, the purposes for which it is held, and how it is collected, used, and disclosed

Access and correction of personal information

33	**How can individuals request access to, or correct their personal information?** *Identify the avenues available for individuals to request access to or correction of their personal information, and who is responsible for handling such requests.*	Users can request access or corrections through the SafeTrack portal. Customer support or the data privacy officer at SafeJourneys Inc.

Retention and disposal of personal information

34	**How long will the personal information be kept for?** *Describe any relevant retention and disposal schedules or policies, including those issued by the Keeper of Public Records or those in other legislation.*	Retention Policies: • Data retention policies will follow the guidelines issued by the Keeper of Public Records or other relevant legislation. • User-defined retention periods will be respected, and data will be deleted automatically after this period.
35	**How will personal information be destroyed once it is no longer required?** *Describe the method of destruction and explain how that method is secure.*	Secure deletion protocols such as cryptographic erasure. Ensures complete and irreversible destruction of data.
36	**As an alternative to destroying personal information, will any personal information be de-identified once it is no longer required?** *Describe the method of de-identification that will be used and the purposes to which the de-identified information will be put.*	Yes. Advanced anonymization techniques. De-identified information may be used for statistical analysis or to improve service quality without compromising user privacy.
37	**If applicable, what will happen to personal information held by third parties (such as contracted service providers, cloud storage, third party platforms etc.)?** *Describe any arrangements (for example, any contractual provisions) in relation to third parties' obligations to retain and dispose of personal information.*	Contractual provisions require third parties to follow the same retention and disposal protocols. Third parties must adhere to strict data protection and privacy standards.

Other considerations

38	**Who can individuals complain to if they have concerns about the handling of their personal information?** *Identify the avenues (internal and external) for making a privacy complaint, including who is responsible for complaint handling.*	Internal: Data Privacy Officer at OneSolution Inc. External: Office of the Australian Information Commissioner (OAIC).
39	**Does the organisation have a data breach response plan in place?** *If so, describe at a high level the steps that the organisation will take in the event of a data breach.*	Yes. Steps: • Immediate containment and assessment of the breach. • Notification to affected individuals and relevant authorities. • Investigation and remediation to prevent future breaches. • Data Breach Response Plan
40	**Will any training be provided to staff to ensure the appropriate collection and handling of the personal information collected for this program?** *Describe the type of training staff will receive.*	Yes. Training Type: • Privacy and data protection training. • Regular updates and refreshers. • Specific training on new technologies and protocols used by SafeTrack.
41	**Will the program be evaluated against its objectives?** *Describe who will evaluate the program, at what point in the program evaluation will occur, and how often.*	Yes. Evaluation by: Internal audit team and external privacy experts. Frequency: Regular intervals (e.g., annually) and post-major updates.
42	**Does the program comply with the organisation's other information handling or information management policies?**	Yes. SafeTrack is designed to comply with all existing information handling and management policies of OneSolution Inc.
43	**Will this PIA be published?**	Yes. The PIA will be made available to the public through OneSolution Inc.'s website.
44	**Are there any other broader privacy considerations associated with this program?**	• Continuous monitoring of emerging privacy risks. • Adaptation to changes in privacy legislation and best practices.
45	**Has the organisation's privacy officer been consulted?** *The organisation's privacy officer should be consulted.*	The privacy officer has been consulted throughout the development of SafeTrack.

Part 3 – Privacy risk assessment

This part lists any privacy risks that have been identified as part of the analysis in Part 2. Refer to **Part 3** of the PIA Guide for guidance on completing the risk assessment table.

Were any privacy risks identified in the privacy analysis completed in Part 2 of this PIA?	☐ Yes Enter each privacy risk in the risk assessment table below.	☐ No Proceed to Part 4 of this PIA.

	Description of risk	*Consequence rating*	*Likelihood rating*	*Overall risk rating*	*Accept*	*Risk management strategy*	*Residual consequence rating*	*Residual likelihood rating*	*Residual risk rating*	*Owner*
1	**1. Data Breach:** Unauthorized access to personal location data leading to privacy violations.	High	Medium	High	No	Implement end-to-end encryption, multi-factor authentication, and regular security audits. Ensure immediate response and containment procedures are in place for any data breaches.	Low	Low	Low	Chief Security Officer
	3. Inaccurate Data: Incorrect location data leading to false alerts or misuse of information.	Medium	Medium	Medium	Yes	Regularly validate data accuracy, provide users with tools to correct their data, and maintain open communication channels for reporting inaccuracies.	Low	Low	Low	Chief Data Officer
	4. Data Retention: Data being retained longer than necessary, increasing risk of exposure.	Medium	Medium	Medium	Yes	Implement automatic data deletion protocols and conduct regular audits of data retention practices. Ensure compliance with user-defined retention periods.	Low	Low	Low	Records Manager

	5. Lack of User Awareness: Users not being fully aware of how their data is used and protected.	Medium	High	High	No	Conduct regular user education and awareness campaigns, provide detailed privacy policies, and ensure easy access to information on data use and protections.	Low	Low	Low	Communications Manager

Part 4 – Action items, endorsement, document information

This part details any action items identified, endorsement of the PIA, and document information. Refer to **Part 4** of the PIA Guide for more information.

Action items

Action items identified in Parts 2 or 3 are listed here, along with the owner of the action and any timeframe within which the action needs to be completed.

	Action	*Owner*	*Timeframe*	*Completed*
1	Implement encryption for all data collected by SafeTrack to prevent unauthorized access.	IT Security Team	2 months	No
2	Conduct regular audits of data collection and storage practices to ensure compliance with privacy policies.	Compliance Officer	Quarterly	No
3	Develop and distribute a user education program about data privacy and SafeTrack's data practices.	Communicatio ns Team	1 month	No
4	Review and update the privacy policy to include new data collection and usage practices.	Legal Team	3 months	No
5	Regularly verify the accuracy and completeness of the collected data and update it as necessary.	Data Management Team	Monthly	No
6	Ensure that all data shared with third parties comply with the SafeTrack privacy policy and legal requirements.	Legal Team	Ongoing	No

Endorsement

The required endorsements for this PIA are listed below. This may include the program manager, a privacy officer, executive business owner, or any other responsible person.

Name	*Position*	*Signature*	*Date*
Thanuka Thathasara Rathnayake	PIA Drafter & Program Manager		25/01/2024
	Privacy Officer		25/01/2024

Document information

Document title	SafeTrack - A Next-Generation Privacy-Focused Location Tracking and Timeline Service
Document location	Safetrack Website
Document owner	OneSolution Inc.
Document distribution	PDF
Related documents	N/A

Next review	10/12/2024
Document version	PIA 1.1