Privacy Impact Assessment

For

ANUOK

Prepared by Date	Grace Bannister-Tyrrell, Security, Facilities and Services Division 29 September 2021

1. Executive summary/introduction

This Privacy Impact Assessment provides a summary of the data used by the ANUOK app.

2. Project description

ANUOK is the ANU's official safety and wellbeing app. The app provides users with safety tools and information about the University's safety and wellbeing initiatives. It is not designed to operate outside of existing security infrastructure or act as an independent source of safety and wellbeing information.

3. Threshold assessment

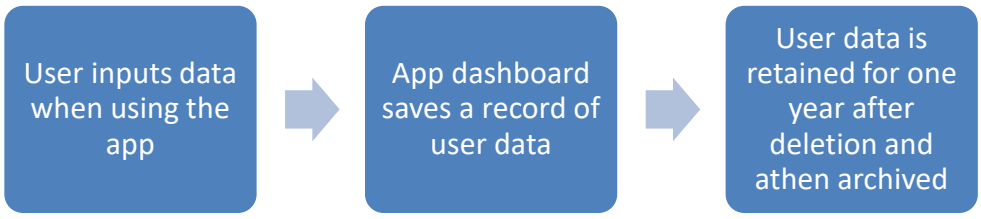
ANUOK collects user data for certain features within the app (e.g. WorkAlone) which creates the requirement for a Privacy Impact Assessment.

4. Consultation with stakeholders

The following stakeholders were consulted in preparing this PIA:

- App Armor (developer hosting the ANUOK app)
- ANU Security Management
- ANU Senior Privacy Officer

5. Information flows



5.1 Data collection

What personal information is captured?

Users submit the following information when using the app:

- Name (certain features only)
- Phone number (all app users and emergency contacts nominated for WorkAlone sessions)
- Location (certain features only)

How will the personal information be collected?

Users must input personal data for certain features (e.g. name, phone number/s and location for WorkAlone). This information is recorded in the app dashboard for operators to access to fulfil support requirements for these features. All outbound calls made from the app are made from the user's device, making use of the user's phone number. All other features do not require users to provide identifying information. The user opts-in to providing the information in return for accessing the feature(s).

5.2 Data management

How will the personal information be stored?

All app data is stored securely in the AppArmor cloud on Microsoft Azure, located in US Data Centres Azure US East 1 and East 2. Data is encrypted at rest at AES 256 and in-transit at TLS 1.2. The app data is accessible to ANU via the dashboard - its specific location depends on the feature (e.g. incident reports are in the incident reporting page, "walk" data is in the Walk History page, etc).

How will the personal information be secured/protected?

The developer App Armor utilises a number of features on Microsoft Azure, including Azure upstream attack pattern detection, automated IP blocking and other tools made internally by AppArmor. They also conduct quarterly vulnerability scanning of their systems via a third party provider and semi-annual penetration testing.

Who will have access to the personal information?

Only ANU staff who have been granted access to the app management dashboard will have access to personal information collected by the app – this consists of nominated staff in ANU Security and ACE only.

How can individuals request access to and/or correction of their personal information?

Any requests for access to personal information stored by the app must be made to ANU Security. Data cannot be corrected as it is only a record of information provided by the user during previous engagement with the app. Users can update their information when they next use the feature of the app.

When will the personal information be deleted/destroyed?

When data is deleted from the dashboard, it is initially flagged as "deleted" and not erased which allows time to reverse any changes. Data is subsequently archived after one year.

6. Privacy management

#	Privacy Impact	Impact treatment Plan
1	Personal information will be collected without a clear purpose, which could increase the risk of unauthorised uses and disclosures.	Users must enter personal information in order for this data to be registered by the app. All personal information collected is retained for (period of time) and accessible only to those granted access to the dashboard. Use of the app is optional.
2	Consent for collection, use or disclosure of information may not be valid.	Users are directed to provide personal information only when it relates to a feature within the app that they seek to deploy. Use of these features in the app is optional butwill not be able to engage with that feature if information is not provided.
3	Individuals may be surprised or upset by a secondary use or disclosure, resulting in privacy complaints and/or negative publicity.	Operators with access to user data are approved to only access that information within the context of facilitating the app's functions. Any unauthorised secondary use or disclosure of personal information would result in disciplinary procedures for those involved.

4	The organisation or agency does not have basic information security standards in place.	Access to the app dashboard is restricted to approved operators and is password protected.
5	Individuals are not able to easily access and correct their personal information.	Users are not able to correct personal information registered through the app, as this information only records data provided by users during previous sessions. Requests for access to personal data can be made at any time to ANU Security.
6	Poor quality information may lead to inappropriate decisions that have a negative impact on the individuals concerned.	As all information is provided by users, any negative outcome resulting from poor quality information would only affect the user's experience of the app in that singular instance. There are no ongoing consequences resulting from poor quality information.

7. Conclusion/recommendations

The information collected via the ANUOK app is managed in accordance with ANU privacy requirements.

Data is collected directly from the user, who opts in to providing their personal information to access the features of the ANUOK app. Use of the app is voluntary.

Staff handling personal information will complete the ANU Privacy Awareness training in Pulse.

Facilities and Services to seek advice from University Records about the appropriate retention period for data collected on the ANUOK App, and to liaise with the vendor to update retention and deletion processes to align with the requirements.

This PIA remains a living document and will be reviewed, and updated as required, should the information handling practices of ANU and/or App Armor change.

Approved by	Roxanne Missingham University Librarian/ANU Privacy Officer Email: Privacy@anu.edu.au Phone: 02 6125 5467
Signature	
Date	19 October 2021