



# Privacy Impact Assessment Tool

May 2020

<b>Privacy Impact Assessment Tool.....</b>	<b>2</b>
<b>Part 1: Plan the PIA .....</b>	<b>3</b>
Description of the project and parties.....	3
Scope of this privacy impact assessment.....	3
Stakeholder identification and consultation .....	4
Map information flows.....	4
<b>Part 2: Privacy impact analysis and compliance check.....</b>	<b>5</b>
Privacy impact analysis .....	5
Ensuring compliance.....	5
APP 1 — Open and transparent management of personal information .....	5
APP 2 — Anonymity and pseudonymity .....	7
APP 3 — Collection of solicited personal information.....	8
APP 4 — Dealing with unsolicited personal information.....	11
APP 5 — Notification of the collection of personal information .....	11
APP 6 — Use or disclosure of personal information .....	13
APP 7 — Direct marketing.....	15
APP 8 — Cross-border disclosure of personal information.....	16
APP 9 — Adoption, use or disclosure of government related identifiers .....	17
APP 10 — Quality of personal information .....	17
APP 11 — Security of personal information.....	18
APP 12 — Access to personal information .....	22
APP 13 — Correction of personal information .....	23
Other considerations .....	24
<b>Part 3: Privacy management — addressing risks.....</b>	<b>25</b>
Summary of risks and recommendations.....	26
<b>Part 4: Respond and review .....</b>	<b>Error! Bookmark not defined.</b>
Respond to recommendations .....	<b>Error! Bookmark not defined.</b>
Sign-off .....	<b>Error! Bookmark not defined.</b>
Update PIA if required .....	<b>Error! Bookmark not defined.</b>
<b>Further information.....</b>	<b>Error! Bookmark not defined.</b>
Other OAIC resources .....	<b>Error! Bookmark not defined.</b>
Other resources .....	<b>Error! Bookmark not defined.</b>
Disclaimer.....	<b>Error! Bookmark not defined.</b>

# Privacy Impact Assessment Tool

A privacy impact assessment (PIA) is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

The Office of the Australian Information Commissioner (OAIC) has developed this tool to assist Australian Privacy Principle (APP) entities conduct a PIA, report its findings and respond to recommendations. Entities are encouraged to take a flexible approach and adapt this tool to suit the size, complexity and risk level of their project. The term 'project' covers the full range of activities and initiatives that may have privacy implications.

This tool should be used in conjunction with the OAIC's [Guide to undertaking privacy impact assessments](#) and [PIA eLearning course](#). Additional resources are also listed below.

<b>Name of project</b>	Indoor Radon Survey
<b>Name of entity</b>	Australian Radiation Protection and Nuclear Safety Agency
<b>Date</b>	29 April 2025
<b>PIA version number</b>	1
<b>PIA Drafter</b>	<b>Name:</b> Cameron Lawrence
<b>Project Manager</b>	<b>Name:</b> Cameron Lawrence
<b>Has the Privacy Officer of your entity been consulted in the drafting of this PIA?</b>	Yes
<b>Privacy Officer</b>	<b>Name:</b> Laura Antoniazzi

# Part 1: Plan the PIA

## Description of the project and parties

Australia published the results of a nation-wide survey of  $^{222}\text{Rn}$  (radon) concentrations and gamma dose rate levels in Australian homes in 1990 (Langaroo et al 1990). In comparison with some other countries the indoor radon concentrations in Australian homes are generally quite low, average of  $12 \text{ Bq/m}^3$  from the 1990 survey (Langaroo et al 1990). Only several areas around Australia were identified as having radon concentrations between  $20 - 25 \text{ Bq/m}^3$  which is  $10 - 12.5\%$  of the reference level of  $200 \text{ Bq/m}^3$ . These include some suburbs of Canberra, Eastern Perth, Orange, Goulburn, Bathurst and Wagga Wagga.

Although radon levels in Australia are generally low compared to other countries, there are still areas and buildings where radon concentrations can exceed recommended safety levels. Changes in housing construction and living conditions since the last indoor radon survey can significantly impact radon exposure in homes. Modern energy-efficient construction techniques, such as improved insulation and airtight buildings, can inadvertently increase indoor radon levels by reducing ventilation and trapping radon inside. The more energy efficient homes are generally located in newer developments that have not been subject to significant radon surveys.

ARPANSA has not performed a survey of this type since its predecessor, Australian Radiation Laboratory (ARL), completed the work in the late 1980's that resulted in the publication of the nation-wide survey report (Langaroo, 1990). There have been significant changes in communication methods since the last survey and ARPANSA is interested in determining the best current processes to be able to complete this type of work through a pilot program. The main aim of a survey will be to define how ARPANSA can engage with the public to complete a survey of the type performed in the late 1980's.

Members of the public living in areas of interest will be able to register their interest to participate in the survey. This will require them to provide personal information namely, name, address, email and phone number, to be able to register. As the work is discrete it is intended that the personal information will be archived within 12-24 months and retained as a Commonwealth record. Personal information will be maintained in a register hosted on the ARPANSA systems and be accessible only to staff involved with the work.

## Scope of this privacy impact assessment

This privacy impact assessment is limited to the radon survey work only. This discrete survey will collect the name, address, email and phone numbers of people interested in hosting a radon monitor in their homes for a period of approximately 12 months. This personal information is the minimal amount of information that is required to identify individuals and the means to contact them for the distribution and collection of the monitoring equipment. Sensitive information is not being collected in this project.

The work is small scale involving a few hundred individuals hosting radon monitors in their homes for up to 12 months. There is no involvement by other organisations or agencies and the

personal information will not be shared externally to the agency or even outside of the team involved with the work.

## Stakeholder identification and consultation

Internally at ARPANSA the Office of the CEO will be assisting with the development of the webpage registration and communications. The Personal Radiation Monitoring Service (PRMS) will provide and analyse the radon monitoring devices while the Modelling, Assessment and Emergency Preparedness Section will coordinate the survey and provide the assessment and report.

Externally members of the public who are interested in hosting a radon monitor will be able to register that interest and communicated to if they are to receive a monitor. They'll be provided details about the program and what they need to do to deploy and return the monitor. They will be provided with their monitors result and a summary of the results from the program.

This PIA will be available to those who have registered interest in the program. Given the small scale of the project our assessment indicates that the work does not require further consultation, and the PIA does not need further distribution.

## Map information flows

The following information is intended to be collected:

- Name
- Home address
- Postal address (if different)
- Email address
- Phone number

The information will be provided via a registration page on the ARPANSA website and stored internally on ARPANSA secured systems. The registrations will be filtered and people whose homes are in areas with elevated radon potential will be selected to host a monitor. The information for those who registered and were not selected will be archived. Monitors and information will be provided to those selected and follow up communications will be made throughout the program, for the return of the monitors and distribution of results. The information obtained from the program will be used to draft a report and the data, including the personal information, will be archived as a Commonwealth record.

The process will be as follows:

Registration of Interest → Selection of homes → Communicate selection → Send monitors → Communicate through survey → Collect monitors → Send results → Develop report → Archive information

Information collected during the program will only be accessed by ARPANSA staff working on the program, this includes PRMS, OCEO and ANRDR team members.

## Part 2: Privacy impact analysis and compliance check

### Privacy impact analysis

Understanding the flow and usage of personal information within the project is crucial to protecting individuals' privacy. The project will involve the collection, use, and disclosure of personal information such as names, addresses, email addresses, and phone numbers. This data will be securely stored on ARPANSA's systems and will only be accessible to authorised staff.

#### Positive Privacy Impacts:

- Enhanced protection of personal information through secure storage and limited access to authorised personnel only.
- Transparency with individuals about how their data will be used and the purpose of data collection.
- Regular communication with participants ensures they are informed about the status and outcomes of the project.

#### Negative Privacy Impacts:

- Risk of data breaches or unauthorised access to personal information, although mitigated by secure storage practices.
- Potential discomfort or concern among participants regarding the collection and use of their personal data.

#### Risk Mitigation Strategies:

- Implementing stringent security measures to protect stored data.
- Clearly communicating the purpose and scope of data collection to participants to build trust and transparency.
- Providing participants with the option to withdraw from the program at any time.

Overall, the project must balance the need for collecting personal information with the imperative to protect individuals' privacy. By adhering to privacy laws and maintaining transparency, the project can align with community expectations and values regarding privacy.

### Ensuring compliance

#### APP 1 — Open and transparent management of personal information

APP entities must have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way.

**Have reasonable steps been taken to implement practices, procedures and systems that will ensure compliance with the APPs and any binding registered APP code for the purposes of the project?**

*See the OAIC's [Privacy Management Framework](#) for the steps the OAIC expects you to take to meet your obligations under APP 1.2. Agencies should also consider their obligations under the Privacy (Australian Government Agencies – Governance) APP Code 2017. Consider whether any adjustments or additions need to be made to your practices, procedures and systems for the purposes of this project.*

ARPANSA has a privacy policy that is compliant with the APPs. This outlines the practices, procedures and systems ARPANSA has in place that will apply to this survey program.

[Privacy Policy | ARPANSA](#)

**Do you have an APP privacy policy which:**

- **is clearly expressed, understandable and up-to-date**
- **covers the matters listed in APP 1.4**
- **is freely available at no cost (for example, on your website).**

*Identify the document(s) and provide a link where available or include as an attachment to this PIA. See the OAIC's [Guide to developing an APP privacy policy](#) for more information.*

ARPANSA has a privacy policy the is compliant with the APPs

[Privacy Policy | ARPANSA](#)

**Will the APP privacy policy need to be updated to reflect a new collection, use or disclosure of personal information for the purposes of this project?**

*Your analysis under APP 3 and APP 6 should inform whether updates to your entity's APP privacy policy are required (see below).*

The privacy policy will not need to be updated for this work.

**Are there procedures and systems in place for handling privacy inquiries and complaints?**

*Identify the process (internal and external) for making a privacy inquiry or complaint, including who is responsible for complaint handling. Is it visible, comprehensive and effective?*

The privacy policy outlines these procedures and systems.

## APP 2 — Anonymity and pseudonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter, unless an exception applies.

**Will individuals have the option of not identifying themselves or of using a pseudonym? If not, explain why it is impracticable for you to deal with individuals who have not identified themselves or who have used a pseudonym.**

*Describe how individuals will be provided with the option of not identifying themselves or of using a pseudonym. Alternatively, explain why it is impracticable for you to deal with individuals who have not identified themselves (for example, if you need to deliver purchased goods to an individual, you may need to know their name if the individual needs to sign for delivery). See Chapter 2 of the APP Guidelines for more information about when it may be impracticable to deal with an individual who is not identified.*

The program requires that monitors be mailed to participants so while it is possible that they could use a pseudonym it is impractical for the program to not request the names of people participating (no anonymity).

**Are you required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves?**

*Identify the law that requires or authorises you to deal with identified individuals.*

There is no requirement for the program to only deal with individuals who have identified themselves (shown identification).

**Are there categories of individuals affected by the project who are likely to seek to interact with your entity anonymously or using a pseudonym?**

*For example, an individual may prefer to deal anonymously or pseudonymously with you for various reasons including to access services (such as counselling or health services) without this becoming known to others, or to keep their whereabouts secret from a former partner or family member.*

People who may only want to engage with the program using a pseudonym and they can register with that alternative name. As monitors and results must be mailed to individuals it is not possible to engage with the program anonymously. The option of providing a pseudonym as opposed to an individual's full legal name will be explicitly advised when collecting the personal information on our website (i.e. at the time of collection). It is then the individual's choice as to whether they provide ARPANSA with their full legal name or use a pseudonym.

## **APP 3 — Collection of solicited personal information**

Any personal information collected (other than sensitive information) must be reasonably necessary for (or if your entity is an agency, reasonably necessary for, or directly related to) one or more of the entity's functions or activities.

An APP entity must not collect sensitive information about an individual unless one of the exceptions listed in APP 3.3 or APP 3.4 applies.

Personal information can only be collected by lawful and fair means.

Personal information about an individual must only be collected from the individual unless one of the exceptions in APP 3.6 applies.



**If you are an agency, is the information being collected necessary for, or directly related to, one or more of your functions or activities?**

**If you are an organisation, is the information being collected necessary for one or more of your functions or activities?**

*List each item of personal information that will be collected (eg. name, date of birth, address) and explain why each item is necessary for one or more of your functions or activities. This should be a very granular assessment. You should clearly and specifically describe the relevant function or activity and why each item of personal information is reasonably necessary for (or, for agencies, directly related to) that specific function or activity. You should only collect the minimum amount of personal information that is necessary for the relevant function or activity ('data minimisation').*

*Data minimisation is an important concept that can help reduce the privacy impacts for individuals that may be associated with your project. Minimising the amount of data that you collect can also help to mitigate security risks. For example, collecting more personal information than is necessary may increase the risk of harm to an individual in the event of a data breach, which could also trigger your notification obligations under the Notifiable Data Breach scheme. Holding large amounts of personal information may also increase the risk of unauthorised access by internal or external sources. Security issues are considered further below under APP 11.*

*Also consider whether your APP privacy policy will need to be updated if the project will involve a new collection of personal information and record this under APP 1 above.*



**Privacy risk:** If some personal information is not reasonably necessary for the project, there may be a risk of over collection. For example, it may not be necessary to collect all personal information on an individual's driver licence when the purpose of collection is to verify the individual's age.

ARPANSA has been established under the Australian Radiation Protection and Nuclear Safety Act (1998), the object of the Act and the main aim of ARPANSA is "to protect the health and safety of people, and to protect the environment, from the harmful effects of radiation."

Radon can accumulate in buildings, particularly in areas with high radon potential, posing a health risk due to association with lung cancer. Understanding radon and its potential risks is crucial for maintaining public health.

An updated radon survey of new Australian homes built in areas of high radon potential will add to the existing extensive survey data ARPANSA already has and enable us to assess the risks in these areas for new homes. This work is well within the primary function of ARPANSA to protect the health and safety of people from the harmful effects of radiation.

In order to perform an effective survey and communicate directly with individuals who will host monitoring equipment it is reasonable to collect names, addresses and contact details to deliver monitors, results and advice to these individuals.

**For the collection of sensitive information, can you rely on any of the exceptions in APP 3.3 or APP 3.4?**

*Explain which exception you are relying on for the collection of any sensitive information. For example, has the individual consented or is the collection required or authorised by or under an Australian law or a court/tribunal order?*

No sensitive information will be collected for the course of this program.

**Will the information be collected by lawful and fair means?**

*Describe the means by which personal information will be collected.*



**Privacy risk:** Your method of collection may be 'unfair' if it involves intimidation, deception or is unreasonably intrusive. For example, it would usually be unfair to collect personal information covertly without the knowledge of the individual (however, this will depend on the circumstances).

Information will be provided with consent via an online application form. There will be a collection notice provided at the time of collection of the personal information, with detailed information regarding the program.

**Will the personal information be collected from the individual concerned? If not, do any of the exceptions in APP 3.6 apply?**

*Describe how, and from which other sources, the personal information will be collected. Also, explain which exception you are relying on to collect personal information about the individual from another source.*



**Privacy risk:** There may be a risk of the information being inaccurate, out-of-date or incomplete if collected from another source.

Information will be collected directly from the individuals.

**If the collection of personal information will be outsourced, will measures be in place to ensure compliance with APP 3 and prevent over collection of information?**

*Describe how you will ensure that any third party that collects personal information on your behalf complies with APP 3 (for example, by entering an enforceable contractual arrangement).*

Information will be collected directly by ARPANSA.

## APP 4 — Dealing with unsolicited personal information

Where an APP entity receives unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 will apply to that information. If the information could not have been collected under APP 3, and the information is not contained in a Commonwealth record, the APP entity must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.

### **Are there practices, procedures and systems in place for dealing with the receipt of unsolicited personal information that will ensure compliance with APP 4?**

Unsolicited information could be provided by individuals who register interest on behalf of other individuals without their knowledge. ARPANSA may become aware of this when they reach out to selected individuals to host a monitor. To mitigate the chances of this occurring, the privacy collection notice will advise that individuals must provide their information only and not the information of third parties.

The same information could have been received if the individual had registered themselves, i.e. it could have been collected under APP 3.

As the information will be a Commonwealth record it cannot be destroyed but will be archived.

## APP 5 — Notification of the collection of personal information

An APP entity that collects personal information about an individual must take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of the matters listed in APP 5.2.

An APP entity must provide notification before, or at the time it collects personal information. If this is not practicable, notification should be provided as soon as practicable after collection.

### **Consider each of the matters listed in APP 5.2. Will steps be taken to notify the individual of each matter? If steps are not being taken in relation to a matter, is it reasonable not to notify the individual?**

*Describe the steps taken to notify the individual OR explain why steps are not being taken. Include a link or attach collection notices where appropriate.*

Individuals will be notified and consent to ARPANSA collecting their personal information during the registration process. A privacy collection notice will be on the front page of the registration form and therefore an individual would need to read and consent to the collection of their personal information, prior to registering.

A link to the registration process will be provided once the form has been finalised.

**If personal information is collected from another source, will the individual be notified? What steps will be taken to notify of each of the APP 5.2 matters?**

*Describe the steps taken to notify the individual OR explain why steps are not being taken. Include a link or attach collection notices where appropriate.*



**Privacy risk:** If you are collecting personal information from another source, there may be a risk that an individual is not aware that you have collected their personal information. Ensure that any third-party notifies, or makes an individual aware, of the relevant APP 5 matters on your behalf (such as through an enforceable contractual arrangement).

As identified in APP 4 the only identified way in which personal information could be provided is from another individual registering on behalf of someone else without their consent.

The intention of the program is to communicate to all registered individuals whether they will be hosting a monitor or not and therefore each individual will become aware that their information has been provided. If another individual's information has been provided by a third party and they do not wish to be part of the program, ARPANSA has the ability to remove them from the program. Their details may still be in a Commonwealth record and therefore will be dealt with in accordance with the Archives Act.

## APP 6 — Use or disclosure of personal information

An APP entity can only use or disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies, such as where the individual has consented to the use or disclosure of the information.

Note that APP 6 does not apply to organisations using or disclosing personal information for the purpose of direct marketing (refer to APP 7), or government related identifiers (refer to APP 9).

### **Does the project use or disclose personal information (including sensitive information) for a secondary or additional purpose?**

*Describe the secondary purpose and explain how it is authorised, by either asking the individual to consent, or by applying one of the exceptions to the requirement for consent in APP 6.2. Also consider whether your APP privacy policy will need to be updated if the project will involve a new use or disclosure of personal information and record this above under APP 1.*

The personal information collected during the survey will not be used for any other purpose than to communicate with individuals involved with the survey.

There is no secondary or additional purposes for the use of personal information.

### **If you are an agency, is it possible that personal information may be used or disclosed because it is reasonably necessary for an enforcement related activity? If so, are procedures in place to ensure a written note of the use or disclosure is made in compliance with APP 6.5?**

There is no identified possibility for personal information collected to require disclosure to an enforcement agency.

**Will the individual be notified of any additional use(s) or disclosure of their personal information?**

*Explain how the individual will be given notice of the secondary use(s) or disclosure of their information, or why notice is not required (eg. additional notice may not be required if the proposed use or disclosure is consistent with the notice originally provided at the point of collection).*



**Privacy risk:** If relying on APP 6.2(a) to use or disclose personal information for a secondary purpose, but your project involves a new way of handling personal information, there may be a risk that individuals would not reasonably expect their personal information to be used for the new purpose. Carefully consider whether additional notification is required.

There is currently no identified secondary or additional purpose for the personal information other than in relation to the survey, primary purpose.

If during the course of the project an additional use for disclosure of the information is identified then notification will be given and consent sought.

**If you're disclosing personal information to another entity (eg. if you are outsourcing some of your functions, or as part of an ongoing data sharing arrangement), will measures be put in place to protect the information and will compliance with APP 6 be monitored?**

*Describe the measures (such as an enforceable contractual arrangement or other information sharing agreement) that will be put in place to ensure compliance with APP 6 and protect the personal information that is being disclosed/shared. If no measures will be put in place, explain why (for example, the disclosure is a once-off and permitted by one of the exceptions under APP 6).*

Not applicable for this program.

## APP 7 — Direct marketing

An organisation must not use or disclose personal information for the purpose of direct marketing unless an exception applies, such as where the individual has consented. APP 7 may also apply to an agency in the circumstances set out in s 7A of the Privacy Act.

**Do any of the exceptions permitting the use or disclosure of personal information for the purpose of direct marketing as set out in APP 7.2 or APP 7.3 apply?**

There is no intention to disclose personal information collected for this program for any marketing purposes. The exemptions are not applicable.

**If sensitive information is to be used or disclosed for the purpose of direct marketing, will the individual be asked to consent? Consider APP 7.4.**

No sensitive information is being collected and there is no intention of disclosing any information for the purpose of direct marketing.

**If you are a contracted service provider for a Commonwealth contract, is the use or disclosure necessary to meet an obligation under the contract? Consider APP 7.5.**

Not applicable.

**If use or disclosure of personal information for the purpose of direct marketing is permitted under APP 7, will individuals be given the opportunity to request not to receive direct marketing communications?**

Not applicable.

**Does your organisation have any guidance or processes in place to help manage your direct marketing obligations?**

Not applicable.

**Have you considered your obligations under the *Do Not Call Register Act 2006* and the *Spam Act 2003*?**

*APP 7 does not apply to the extent that the Do Not Call Register Act 2006 and the Spam Act 2003 apply. APP 7 will still apply to the acts or practices of an organisation that are exempt from these Acts.*

Not applicable.

## APP 8 — Cross-border disclosure of personal information

Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information, unless an exception applies, such as the individual has given informed consent.

An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (see s 16C of the Privacy Act).

### **Will any personal information be disclosed to an overseas recipient?**

*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.*

The personal information collected by ARPANSA will only be used internally by ARPANSA staff involved with the program and will not be disclosed.

### **Will reasonable steps be taken under APP 8.1 to ensure the overseas recipient does not breach the APPs (other than APP 1) in relation to the information?**

*Explain the arrangements in place with overseas recipients to ensure that personal information is handled in accordance with the APPs. For example, provide details of any enforceable contractual arrangement.*

Not applicable.

### **Alternatively, does an exception under APP 8.2 apply?**

*Explain how one of the exceptions in APP 8.2 apply to the transfer. For example, is the disclosure required or authorised by or under an Australian law or a court/tribunal order?*

Not applicable.



## APP 9 — Adoption, use or disclosure of government related identifiers

An organisation must not adopt, use or disclose a government related identifier of an individual as its own identifier of the individual unless an exception applies.

APP 9 does not apply to the handling of government related identifiers by agencies. However, agencies should still give careful consideration to any proposed creation, adoption, use or disclosure of government related identifiers and the potential privacy impacts this may have, including community expectations around how government should handle these identifiers.

### **If you are an organisation, is any planned adoption, use or disclosure of government related identifiers permitted under an exception in APP 9?**

*Describe the identifier, the purpose for adopting, using or disclosing it and how this is authorised. For example, is it required or authorised by or under an Australian law or a court/tribunal order?*

No government identifiers will be collected, used or disclosed for the program.

## APP 10 — Quality of personal information


An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.

An APP entity must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

### **What steps will you take to ensure the personal information collected is accurate, up to date and complete? Will guidance or processes be in place to ensure these steps are followed?**

Personal information will be collected directly from the individuals who register interest in the program. Communication between ARPANSA staff and the individuals who are selected to host a monitor will be used to update any personal information changes that occur throughout the program. ARPANSA staff will update the register that is held that contains the personal information.

**What steps will be taken to ensure that any personal information being used or disclosed is accurate, current, complete and relevant, having regard to the purpose of the use or disclosure? Will guidance or processes be in place to ensure these steps are followed?**

 **Privacy risk:** Carefully consider the consequences for individuals if the personal information is not accurate or up-to-date, including the kinds of decisions made using the information and the risks of using or disclosing inaccurate information.

Communications with the individuals throughout the course of the program will be used to ensure that the personal information is accurate, current, complete and relevant.

## APP 11 — Security of personal information


An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that the information is de-identified, unless an exception applies.

The OAIC's [\*Guide to Securing Personal Information\*](#) sets out the reasonable steps the OAIC expects entities to take to protect personal information.

**Are there technical security measures in place to protect the personal information that will be collected, used and/or disclosed as part of this project?**

*Describe the technical controls (such as software security, encryption, whitelisting and blacklisting, backing up, email security etc) that have been, or will be, implemented for the project, including any relevant policies and procedures. Include links or attachments where appropriate.*

 **Privacy risk:** If there are inadequate technical security measures in place, consider whether there is a risk that the information will not be properly protected, leading to misuse, interference, loss, unauthorised access, modification or disclosure. Consider the nature of the personal information collected and how valuable it would be to unauthorised users?

The register of personal information that will be collected for this program will remain hosted on ARPANSA systems and accessed only by ARPANSA staff involved with the project.

ARPANSA maintains robust security for our digital systems which in compliance with the Protective Security Policy Framework.

**Are there physical security measures in place to protect the personal information that will be collected, used and/or disclosed as part of this project?**

*Describe the physical security measures that have been, or will be implemented, for the project, including any relevant policies and procedures. Include links or attachments where appropriate.*

The ARPANSA building, where digital and hardcopies of the personal information will be kept, has adequate physical security measures in place to prevent access.  
Hardcopies of personal information will be required to create address labels to send monitoring equipment to.

**Are there access security and monitoring controls in place to protect against internal and external risks and ensure that personal information is only accessed by authorised persons?**

*Describe the access security controls (such as identity management and authentication, password practices, audit logs/trails and access monitoring) that have been, or will be, implemented for the project, including any policies and procedures. Consider who will have access to the data and ensure access is limited to those staff (or other third parties) necessary to enable your entity to carry out its functions and activities (ie. access should be strictly on a 'need-to-know' basis). Include links or attachments where appropriate.*



**Privacy risk:** Inadequate access security and monitoring controls may lead to the 'trusted insider risk', which can occur when staff mishandle personal information while carrying out their normal duties.

There are appropriate access controls in place to protect digital and hardcopy versions of the personal information. Only ARPANSA staff involved with the program will have access to the personal information register and this is controlled through digital system restrictions.

ARPANSA's Personal Radiation Monitoring Service (PRMS) will be responsible for the issue and collection of monitors and the consolidation of personal information from the program against monitoring devices. Access by PRMS is required to perform the survey and they are appropriately trained and authorised for this work.

**Have you completed a separate security risk assessment?**

*If so, please refer to or attach a copy of the assessment to this PIA.*

Not applicable for this program.

**Have you considered standards that may apply to your industry or sector? If you have decided not to adopt a widely used standard, document your reasons below.**

*You should consider using relevant international and Australian standards, policies, frameworks and guidance on information security. This includes any which are particular to your sector or industry. Australian Government agencies must apply the Attorney-General's Department's [Protective Security Policy Framework](#) and the Australian Signals Directorate's [Australian Government Information Security Manual](#).*

*You may also want to consult the [ISO/IEC 27000 series of information security management standards](#) and the [ISO/IEC 31000 series of risk management standards](#) published by both [the International Organization for Standardization](#) and the [International Electrotechnical Commission](#), parts of which have been adopted by Standards Australia.*

ARPANSA maintains a security framework in compliance with the Protective Security Policy Framework.

**If you have outsourced personal information handling as part of this project, what steps will be taken to ensure personal information is protected by third party providers?**

*Describe the measures (such as conducting due diligence on the services to be provided and contractual provisions relating to security requirements) that will be taken to ensure third party providers protect any personal information handled on your behalf.*



**Privacy risk:** Failing to conduct appropriate due diligence on the services to be provided is inconsistent with your obligations under APP 11 and can lead to an increased risk of a data breach if the third-party provider does not have adequate security measures in place.

Not applicable.

**Do you have a data breach response plan in place? If so, describe at a high level the steps that you will take in the event of a data breach or attach your response plan.**

*See the OAIC's [Notifiable data breaches](#) page which sets out information to help APP entities prepare for and respond to data breaches. You should consider whether changes to your existing data breach response plan need to be made as a result of this project.*

ARPANSA maintains a Business Continuity Framework that is designed to assist ARPANSA to manage any form of business disruption. Responses to data breaches are covered by this framework.

**If you have outsourced personal information handling as part of this project, have you considered your obligations under the Notifiable Data Breaches (NDB) scheme and how you will manage your relationship with the third party?**

*Describe how you will ensure you comply with the NDB scheme in the event a third-party provider experiences a data breach (such as including contractual terms to allocate responsibility for identifying, assessing and notifying as required).*

Not applicable

**How long will you retain the personal information collected, used and/or disclosed as part of this project?**

*Describe any relevant retention and disposal schedules or policies.*

The personal information will be archived as a Commonwealth record within 24 months of the closure of the program.

**Will personal information be destroyed or de-identified once it is no longer needed for any authorised purpose? Do any of the exceptions apply (for example, the information is part of a Commonwealth record or the APP entity is required by law or a court/tribunal order to retain the information)?**

*Explain whether an exception applies that requires you to retain the information.*

The information is a Commonwealth record and cannot be destroyed or de-identified.

**If applicable, how will personal information be destroyed once it is no longer required?**

*Describe the method of destruction and explain how that method is secure.*



**Privacy risk:** There is a risk of unauthorised disclosure if personal information is not securely and irretrievably destroyed.

Not applicable.

**If applicable, how will personal information be de-identified once it is no longer required?**

*Describe the method of de-identification that will be used and whether the de-identified information will be used for any other purpose. See the OAIC's [De-identification and the Privacy Act](#) for further information.*



**Privacy risk:** If de-identifying personal information once it is no longer required, consider whether there is a risk that the information can be re-identified.

Not applicable.

**If you have outsourced personal information handling as part of this project, what will happen to information held by third party providers?**

*Describe any arrangements (for example, any contractual provisions) in relation to third parties' obligations to retain and dispose of personal information.*



**Privacy risk:** If there are no arrangements in place relating to third parties' retention and disposal of personal information, there is a risk that personal information could be used by the third party for unauthorised purposes at the conclusion of the contract.

Not applicable.

## **APP 12 — Access to personal information**

An APP entity that holds personal information about an individual must give the individual access to that information on request unless an exception applies.

**How can individuals request access to their personal information? How will individuals be made aware of how to access their personal information?**

*Describe how individuals can request access, and who is responsible for handling such requests. If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow access to personal information held by third parties.*

The ARPANSA Privacy Policy will be made accessible to people registering for the program. The policy contains information regarding how to contact ARPANSA regarding access to their personal information.

Full disclosure on the use and retention of personal information will be provided during registration and individuals can contact ARPANSA staff involved with the program.

**Are processes in place for responding to requests from individuals to access their personal information?**

ARPANSA has processes in place to respond to requests relating to individuals access to their personal information. This is outlined within ARPANSA's publicly available Privacy Policy. The OGC maintains the privacy function and has a designated email address and phone number to answer privacy questions, concerns or complaints.

## APP 13 — Correction of personal information

An APP entity must take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. The requirement to take reasonable steps applies in two circumstances: where an APP entity is satisfied that personal information it holds is incorrect, or at the request an individual to whom the personal information relates. There are minimum procedural requirements in relation to correcting personal information.

### **How can individuals seek correction of their personal information? How will individuals be made aware of how to correct their personal information?**

*Describe how individuals can seek correction of their personal information and how they will be made aware of this. If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow correction of personal information held by third parties.*

Individuals will be provided a link to the ARPANSA Privacy Policy which details how they can correct their personal information.

### **Are processes in place for responding to requests from individuals to correct personal information?**

ARPANSA has a robust process for engaging with members of the public to ensure response using our Content Manager system.

### **Are there process in place for associating a statement with personal information if a request for correction is denied?**

ARPANSA will link responses to requests to the original request in our Content Manager system.

### **Are processes in place for identifying and correcting personal information that is inaccurate, out of date, incomplete, irrelevant or misleading?**

*Describe the steps that will be taken, or the measures that are in place, to ensure the ongoing integrity of the information.*

The program will correct personal information if errors are identified in the register or individuals bring it to our attention.

## Other considerations

### **Will any training be provided to staff to ensure the appropriate collection, handling and security of the personal information as part of this project?**

*Describe the type of training staff will receive.*

ARPANSA staff involved with the program are already trained in the appropriate collection, handling and security of personal information for their roles. This program has similar requirements to their current roles.

### **Does the project comply with your entity's other information handling or information management policies?**

The survey program complies with all information handling requirements for ARPANSA.

### **Does the project recognise the risk of function creep? For example, is there an interest in using the personal information collected for the project for other purposes that might occur in the future?**

ARPANSA recognises this potential risk but has no intention to use the personal information collected for any other purpose.

ARPANSA excludes future use of this personal information.

### **Will this PIA be published?**

A link to the PIA will be provided to individuals who are selected to be engaged in the program but it is not intended to be externally published.

### **Are there any other broader privacy considerations associated with this project?**

*You might find it useful to show how the project will deal with other kinds of personal privacy not covered by the Privacy Act, such as bodily, behavioural and territorial privacy.*

*If you are an agency developing legislation or a new policy proposal with privacy impacts, consider whether any limitation on the right to privacy is reasonable, necessary and proportionate to your objective. For example, if you are developing legislation that seeks to rely on the required or authorised exception to the APPs (such as legislation authorising the use or disclosure of personal information), consider whether the proposed legislation is reasonable, necessary and proportionate to your objective. This may assist with the development of Human Rights Compatibility Statements for legislative projects.*

Not applicable.



## Part 3: Privacy management — addressing risks

Using the ARPANSA Risk Management Framework the following risks and controls have been identified and implemented for this program.

Description	Likelihood	Consequence	Rating	Controls
Privacy – Data Breach	Rare	Moderate	Low	Collected personal information to be held on ARPANSA systems. Business Continuity Framework details processes to follow in the event of a breach.
Privacy – Data mismanagement/non-compliance	Unlikely	Minor	Medium	Develop a PIA and implement requirements for data storage and access.  Personal information only to be accessed by ARPANSA staff involved with the program.
Privacy – inadequate consent	Rare	Minor	Low	Ensure consent is a requirement for registration and included in the PIA.
Privacy – Data retention	Unlikely	Minor	Medium	PIA should ensure a requirement for personal information to be retained as a Commonwealth record on completion of the project.
Comms – Poor engagement	Possible	Minor	Medium	Engage and develop comms team for a communications plan.
Comms – Failure to communicate results	Unlikely	Minor	Medium	Project closure requires reporting and communication of results.

## Summary of risks and recommendations

The Privacy Impact Assessment (PIA) for ARPANSA's Indoor Radon Survey outlines a pilot program to reassess radon levels in modern Australian homes, particularly in areas with elevated radon potential. Participants will voluntarily register to host radon monitors for up to 12 months, providing minimal personal information; name, address, email, and phone number; which will be securely stored on ARPANSA systems and used solely for survey logistics. The project complies with all Australian Privacy Principles (APPs), with no sensitive data collected or external sharing involved.

Identified privacy risks include data breach (rated low), data mismanagement or non-compliance (medium), inadequate consent (low), data retention issues (medium), poor engagement (medium), and failure to communicate results (medium). To mitigate these risks, ARPANSA will ensure secure data storage, restrict access to authorised staff, require explicit consent during registration, and archive personal data as Commonwealth records within 24 months of project completion. A communications plan has been developed to maintain participant engagement and ensure results are shared.

This PIA confirms that ARPANSA's existing privacy and security frameworks are sufficient for managing the program's privacy obligations.