COMMONWEALTH OMBUDSMAN

USER RESEARCH TO INFORM THE DEVELOPMENT OF A 2020-2025 CHANNEL MANAGEMENT STRATEGY

PRIVACY IMPACT STATEMENT

August 2020

Privacy Impact Assessment Report – Contents

Introduction:
Role of the OAIC and purpose of a Privacy Impact Assessment.

PRIVACY IMPACT ASSESSMENT

Role of OAIC

Note: The *Privacy Act 1988* (Privacy Act) gives the Information Commissioner (IC) a power to direct an agency to provide a PIA to the OAIC, if the Commissioner considers that a proposed activity or function of the agency might have a significant impact on the privacy of individuals (s 33D Privacy Act).This includes when the agency proposes to engage in a new activity or function, or substantively change an existing activity or function e.g., a substantive change to the system that delivers an existing function or activity.

What is a Privacy Impact Assessment (PIA)?

A Privacy Impact Assessment (PIA) is a systemic assessment of a project that may have privacy implications. The term project includes:

- policy proposal
- new or amended legislation
- new or amended program. system or database
- new methods or procedures for service delivery or information handing
- changes to how information is stored

that the PIA identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating adverse impacts. It will go beyond assessing the project's risk of non-compliance with privacy legislation and identify controls to mitigate the risk.

This PIA will also consider the broader privacy implications and risks, including whether the planned uses of personal information in the project will be acceptable to the community.

This PIA should be prepared with reference to the Commonwealth Ombudsman's Privacy Impact Assessment Guidelines (attached to the Privacy Policy)

User research to inform the development of a 2020-2025 Channel Management Strategy

The Ombudsman is seeking to develop a channel management strategy (the strategy) for the Office to guide our contact management/service delivery approach for the next 5 years and to inform supporting business process and technology requirements.

The strategy will focus on effective use of our engagement channels for customer centric service delivery and better use of technology to enhance our performance, resulting in meaningful and efficient access to our services.

1. Threshold Assessment

a) Will any personal information be collected? If yes, record a brief description of the personal information that will be collected, used or disclosed (such as name, address, date of birth, health information etc.).

In order to identify user experiences and needs, the Ombudsman will need to disclose the personal details of complainants to a third party user research company, Portable. The following complainant information will be disclosed:

- Complainant first and last name
- Complainant telephone number and email
- Complainant location (postcode)
- The manner in which the complainant contacted the Commonwealth Ombudsman.
- Complaint type; whether complaint is classified as Consumer (Industry) or Parliamentary (CMEB including ACT).

This data will be used by Portable to invite complainants to attend interviews and/or workshops to gain an in-depth understanding of how and when Ombudsman clients want and need to engage and explore what their needs are from Ombudsman channels.

Any personal data obtained by Portable will be recorded, stored and anonymised by Portable.

As personal information will be disclosed by the Ombudsman and personal information will also be collected and used by Portable, a Privacy Impact Assessment is required.

2. Plan the PIA.

General Description

Name of Program: User research to inform the development of a channel management strategy	
Date: August 2020- October 2020	
Name of Section/Branch: Not applicable	
PIA Drafter: Stephany Leggett	
Email: stephany.leggett@ombudsman.gov.au	Phone: (08) 7088 0628
Program Manager: Fran Jensen	
Email: fran.jensen@ombudsman.gov.au	Phone: (07) 3228 9921

Definition – Project: For the purpose of this document, the term project is intended to cover the full range of activities and initiatives that may have privacy implications including:

- policy proposals,

- new or amened legislation, programs, activities, systems or databases,
- new methods or procedures for service delivery or information handling
- changes to how information is stored

3. Describe the Project

A PIA needs a broad 'big picture' description of the project. It should be kept fairly brief.

The Ombudsman is seeking to understand how best to support its clients to engage with the Ombudsman to make and resolve complaints. Key complaint areas include, but are not limited to, Parliamentary complaints about Commonwealth agencies, Industry complaints about private health providers, VET student loans, overseas student complaints, the postal industry, and the ACT Ombudsman.

The Ombudsman is seeking a human-centred design approach to identifying user experiences and needs. In order to obtain this, personal information that has been collected by the Commonwealth Ombudsman from past complainants, will be provided to Portable. This information (with a minimum sample size of 25 complainants) will enable them to undertake research into how and when Ombudsman clients want and need to engage and explore what their needs are.

These research outcomes will be used to inform the development of a channel management strategy. Staff and internal stakeholders, as well as some external stakeholders, will need to also be engaged in the development of the channel management strategy.

The channel management strategy will seek to put forward high-level principles to ensure that channel engagement aligns with the Ombudsman's strategic direction and technology strategy.

4. Identify and consult with stakeholders

The key stakeholders for this project are:

- Commonwealth Ombudsman- project owner
- Portable- conduct research and collection and management of complainant's personal information
- The complainants whose information will be disclosed
- Internal Commonwealth Ombudsman staff who are invited to participate in research

Provide key privacy elements

1. The Commonwealth Ombudsman will provide personal information to Portable for the purposes of conducting research to seek an understanding of how best to support complainants to engage with the Office to make and resolve complaints.

2. Any data disclosed by the Commonwealth Ombudsman or collected by Portable is only to be used for the purposes of this project.

3. The password protected document with complainant personal information will be accessible to recruiters working on behalf of Portable to recruit participants for this project. This information will only be used to invite participants to participate in this project.

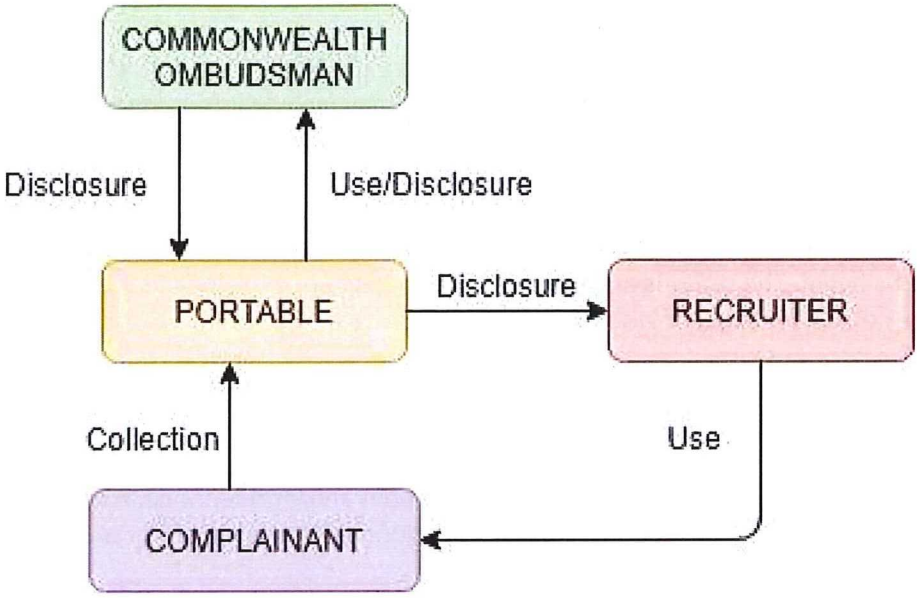
4. Portable will collect data from participating complainants regarding their experience in contacting and engaging with the Commonwealth Ombudsman. This may contain sensitive information, such as health conditions. Informed consent will be obtained from participants, both written and verbal, at the commencement of research activities. Information will be provided to participants about how the data gathered in the research will be used and stored.

   Any personal data obtained by Portable will be recorded, stored and anonymised by Portable. Participant contact information and other personal details will be stored in a Google Drive project folder with access permissions restricted to the core project team within Portable.

5. Portable will provide final research findings to the Commonwealth Ombudsman. Findings reported to the Ombudsman will be de-identified and based on aggregated data.

5. Map Information Flows

Describe and map the project's personal information flows.



VERIFICATION

A complainant will be identified by recruiters on behalf of Portable using the disclosed personal information provided by the Commonwealth Ombudsman.

The Commonwealth Ombudsman will not be required to verify identities as any information provided by Portable will be anonymised as part of aggregated data.

COLLECTION

The Commonwealth Ombudsman will not be required to collect any additional personal information for this project. Information that will be provided to Portable is existing collected information obtained in the course of performing the Ombudsman's functions and role.

Portable will collect information relating to a participant's experience with contacting and engaging with the Commonwealth Ombudsman. This may include information regarding age, location, literacy, disabilities and other barriers faced when engaging with the Office.

All participants will be provided with written project information and a consent form before interviews begin. The reasons and scope for the project are explained as well the expectations of the participants and their rights.

Staff interviews are to be conducted through the Commonwealth Ombudsman's secure video conferencing system, Cisco.

User Interviews and workshops will be conducted over Zoom and/or telephone. A web-based visual collaboration platform, Miro, may be used during these interactions and for collating and sorting research data.

A web-based audio recording and transcribing platform, Otter.ai, will be used to record research interviews in order to ensure accuracy for our research notes and to extract direct quotes from research participants to use in reports and artefacts. All audio added to the platform is automatically transcribed. Transcriptions can be edited and redacted as needed. For the purposes of this project, audio will be recorded to the team account and access will be limited to the core project team.

Any sensitive and identifiable information will be redacted from transcripts, research notes and participant quotes.

Portable will store all personal information and identifying data in a Google Drive project folder with access permissions restricted to the Portable core project team.

USE

All personal information provided to Portable is to be used solely for the purpose of conducting user research to inform the development of a channel management strategy.

Any personal information provided to recruiters acting on behalf of Portable is to be used for the sole purpose of contacting and recruiting research participants.

Complainant contact information will be provided to Portable and the information will be used to contact complainant to seek participants for this project.

Any aggregated data provided to the Commonwealth Ombudsman by Portable will be used for the purposes of informing the 2020-2015 channel management strategy to assist in improving complainant engagement.

DISCLOSURE

A database containing complainants' information will be provided to Portable. This information is only to be used for the purposes of this project.

The information will include:

- Complainant first and last name
- Complainant telephone number and email
- Complainant location (postcode).
- The manner in which the complainant contacted the Commonwealth Ombudsman.
- Complaint type; whether complaint is classified as Consumer (Industry) or Parliamentary (CMEB including ACT).

We consider that this will be a permitted disclosure under APP 6 as the secondary purpose, research to evaluate and improve our Office's services, is directly related to the primary purpose of collecting the information to handle complaints. This type of disclosure is also contemplated in our Office's privacy policy. The research that will be undertaken will help improve the way that complainants contact and engage with the Office and it would be reasonable to expect that contact information may be used in this manner.

The personal information will be provided to Portable through a password protected Excel spreadsheet. Portable will provide the protected database and associated password to recruiters with the understanding that the information is only to be used to recruit participants for this project.

Portable will provide final research findings to the Commonwealth Ombudsman. Findings reported to the Ombudsman will be de-identified and based on aggregated data.

INFORMATION QUALITY

The information provided to Portable will only consist of complainants that have lodged a complaint with the Commonwealth Ombudsman within the past 6-12 months.

This will increase the likelihood that the information provided to Portable is relevant and up-to-date.

If the provided contact information is not correct or up-to-date and the recruiter cannot verify the complaint's identity, complainant will not be given the opportunity to participate in the research.

SECURITY

The database with complainants' personal information will be provided to Portable in a password-protected document.

Data collected by Portable will be stored in a Google Drive. Any sensitive information, like participant contact details or references to the individuals matched to de-identified codes, will be isolated in a folder with stricter access permissions. This folder will be stored within the main project folder but can only be accessed by the core project team.

A web-based visual collaboration platform, Miro, may be used interviews and for collating and sorting research data. By default, projects are only accessible to the core project team. Individual boards can be made available to participants for collaboration via guest access or invitations distributed to individual user accounts. This access is obtained through the use of a unique URL. Following any collaborative session, this access will then be revoked and the URL will no longer provide access.

RETENTION AND DESTRUCTION

Any data collected by Portable will be stored and de-identified.

All participants will be assigned a unique code as a reference point in the research data and their real name will not be used. This unique code may include useful information about participant segmentation like complaint type, location or other general information. Personally-identifiable information will not be used in these unique codes.

A record of the participant codes and how they are matched to participants will be stored in a Google Drive project folder with access permissions restricted to the core project team within Portable.

The Commonwealth Ombudsman will retain complainants personal information that was provided as part of a complaint. When no longer required, personal information is destroyed in a secure manner, or deleted, in accordance with the *Archives Act 1983 (Cth)* and the Ombudsman's Records Authority (for Commonwealth Ombudsman records), or the *Territory Records Act 2002 (ACT)* and *Territory Records (Records Disposal Schedule — Ombudsman Complaint Management Records) Approval 2011* (for ACT Ombudsman records).

ACCESS AND CORRECTION

Under the Privacy Act, complainants can request their personal information from our Office. This is outlined in our Office's privacy policy. The relevant section is also extracted here:

You can ask to see your personal information held by us. If you think that it is wrong or not up to date and/or you can ask that it be corrected. If you are speaking to an Investigation Officer or a member of the Public Contact Team you can ask them to immediately update information, such as your address or contact details if these have changed.

More formal or extensive requests should be addressed to the 'Privacy Contact Officer' and sent via:

- *land mail to GPO Box 442, Canberra ACT 2601; or*
- *email to ombudsman@ombudsman.gov.au.*

You can also call 1300 363 072 and ask to speak with a Privacy Contact Officer.

6. Privacy Impact Analysis and Compliance Check

PRIVACY IMPACT ANALYSIS

The privacy impact analysis should attempt to determine whether the project has acceptable privacy outcomes, or unacceptable privacy impacts.

All personal information provided to Portable is only to be used for the purposes of this project. The personal information provided will be limited to names, telephone numbers, postcodes, the manner in which the complainant contacted the Commonwealth Ombudsman and the type of complaint. This information will be provided in a secured password protected document.

Any personal information collected by Portable will be de-identified and stored by them in a secured Google Drive with access limited to the core project group.

No decisions that have consequences for particular individuals will be made because of the way personal information is handled. All information collected by Portable will be de-identified and any research outcomes provided to the Commonwealth Ombudsman will be based on aggregated data.

ENSURING COMPLIANCE

You will need to consider whether your project complies with each of the Australian Privacy Principles (APPs).

#	Description of the privacy principle *(These can be deleted from your final report if they're not relevant to your project)*	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
1	Principle 1 – Open and transparent management of personal information The agency must have a clearly expressed and up to date APP privacy policy about the management of personal information by the agency.	*Our Office's privacy policy is available on our website here https://www.ombudsman.gov.au/privacy-policy*		
2	Principle 2 – Anonymity and pseudonymity Individuals must have the option of not identifying themselves, or of using a pseudonym, note exceptions.to this rule apply.	*Complainants are provided with the opportunity of anonymity when lodging complaints with the Office. The information that will be provided to Portable is personal information willingly provided by complainants when contacting the Office.* *All information collected by Portable will be de-identified.*	*Complies*	
3	Principle 3 – Collection of solicited personal information Limits apply to only collect information where the information is reasonably necessary for or directly related to one or more of the agency's functions or activities.	*The information that will be provided to Portable was reasonably necessary at the time the complaint was made with our Office and related to the Ombudsman's complaint handling functions Complainants voluntarily provided this information to our Office in making a complaint.* *Portable will only collect information that is directly relevant to the research undertaken.*	*Complies*	

#	Description of the privacy principle *(These can be deleted from your final report if they're not relevant to your project)*	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
4	Principle 4 – Dealing with unsolicited personal information Determine whether or not the agency could have collected the information under APP 3. If not, where it is lawful and reasonable to do so destroy or de-identify the information.	*All information that will be collected by Portable will be essential to the outlined research.* *Any information not directly relevant will not be stored or used.*	*Complies*	
5	Principle 5 – Notification of the collection of personal information Inform the person what information you are collecting, the purpose or use of the information and how they may access or complain about the use of the information. Also inform them if the agency is likely to disclose the information to overseas recipients.	*Portable will require verbal and written consent from participants and will provide information regarding the scope of the research before any interview.*	*Complies*	

#	Description of the privacy principle *(These can be deleted from your final report if they're not relevant to your project)*	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
6	Principle 6 – Use or disclosure of personal information Use it for the purpose you collected it for, unless one of the exceptions applies.	*We consider that an exemption applies as the purpose of disclosure is directly related to the primary purpose of collection (i.e. complaint handling). In our view, disclosure to improve user experience in future complaints made to our Office would likely be reasonably expected by a complainant when they approach our Office. This is connected to the primary purpose for collection. Disclosure to a third party company for the purposes of evaluating our Office's performance and improving our Office's services to complainants is also contemplated in our privacy policy which is available on our Office's website.* *Information collected by Portable is only used for the purposes of the outlines project as agreed upon by participants.*	*Complies*	
7	Principle 7 – Direct marketing Information not to be disclosed for the purpose of direct marketing unless exceptions apply, e.g., consent.	*Information provided to Portable is only to be used for the purposes of this project.*	*Complies*	

#	Description of the privacy principle *(These can be deleted from your final report if they're not relevant to your project)*	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
	Principle 8 – Cross-border disclosure of personal information. Requirement to ensure overseas recipient does not breach APPs note exceptions apply e.g., information is subject to a law similar to APP's.	*Not applicable*	*Complies*	
9	Principle 9 – Adoption, use or disclosure of government related identifiers. Only assign unique identifiers where permitted. Agency should not disclose identifiers unless permitted.	*Not applicable*	*Complies*	
10	Principle 10 – Quality of personal information. Ensure information is accurate, up to date, complete and relevant prior to using it.	*Personal information provided to Portable will be from complainants that have contacted the Office between the last 6-12 months.*	*Complies*	
11	Principle 11 – Security of personal information. Take care of the information and protect it against loss, modification, or unauthorised disclosure and other misuse. When no longer required either destroy or de-identify it.	*All data is stored in a secure database. Information provided to Portable will be in a password protected documents.* *Any information collected by Portable will be stored in a restricted Google Drive accessible only to core project team.*	*complies*	

#	Description of the privacy principle *(These can be deleted from your final report if they're not relevant to your project)*	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
12	Principle 12 – Access to personal information People have a right to see their personal information noting exceptions apply, eg., FOI exemptions.	*Complainants can request their personal information under the privacy act from our Office as we hold their personal information.* *This is outlined in our Office's privacy policy: https://www.ombudsman.gov.au/privacy-policy*		
13	Principle 13 – Correction of personal information Agency must take steps to correct personal information held, ensure information is up to date, accurate, complete and not misleading.	*Not applicable*	*complies*	
14	Other privacy interests			

7. Privacy Management – Addressing Risks

A risk is something that could lead to the unauthorised collection, use, disclosure or access to personal information.

Use the table below to list each of the privacy risks identified and the mitigation strategies/tools that will be implemented to mitigate these. Add extra rows as required. Please specify the likelihood of the risk arising, the degree of impact it would have on individual's privacy if it occurred and an assessment (low/medium/high) of the residual risk. It may be helpful to categorise these risks into areas such as: governance, people, process, technology.

Risk Mitigation Table					
	Identified Risk	Mitigation Strategy	Likelihood	Impact	Risk Rating

1	Database containing complaint personal information is accessed by unauthorised user.	The database will be a password protected Excel spreadsheet. The password will only be provided to Portable's core project group and the recruiters working on this project. The information is only to be used for the purposes of this project.	Low	Low impact on individuals- names, personal information would become available to an unauthorised user. Possible reputational impact for Ombudsman's Office.	Low
4	Insufficient de-identification of data by Portable	Any sensitive and identifiable information will be redacted from transcripts, research notes and participant quotes by Portable. Data collected by Portable will be stored in a Google Drive. Any sensitive information, like participant contact details or references to the individuals matched to de-identified codes, will be isolated in a folder with stricter access permissions. This folder will be stored within the main project folder but can only be accessed by Portable's core project team.	Low	Medium impact- information regarding a complainant's personal circumstances and their experience in contact our Office would be made available to the Commonwealth Ombudsman.	Low

8. Recommendations

Summarise the recommendations to minimise the impact on privacy based on your risk assessment.

Ref	Recommendation	Agreed Y/N
R- 01	No recommendations made	Y
R- 02		N/A

Signatures

_____ _____

Name of Senior Assistant Ombudsman responsible Signature

_____

Date

_____

Lisa Collett, Privacy Delegate Signature

4/09/2020

Date