COMMONWEALTH OMBUDSMAN

Privacy Impact Assessment

New project: policy review and creation – managing unreasonable complainant conduct and service escalations

July 2018

Privacy Impact Assessment Report – Contents

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

1. Threshold assessment 2
2. Plan the PIA 2
3. Describe the project 2
4. Identify and consult with stakeholders 3
5. Map information flows 3
6. Privacy impact analysis and compliance check 6
7. Privacy management - addressing risks 10
8. Recomendations 10
9. Sign off 10

PRIVACY IMPACT ASSESSMENT

Role of OAIC

Note: The 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. (s33D 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

Policy review and creation: managing unreasonable complainant conduct and service escalations

Description: Development of a policy on managing service escalations by complainants and review of the existing policy on managing unreasonable complainant conduct.

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.).

Yes – health information (complainant); name and contact details (representative, if any).

2. Plan the PIA.

General Description

Name of Program: Policy review and creation: managing unreasonable complainant conduct and service escalations
Date: July 2018
Name of Section/Branch: Complaints Management and Education
PIA Drafter: Shirley Tong
Email: Shirley.tong@ombudsman.gov.au Phone: 07 3228 9911
Program Manager: Shirley Tong

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 policy will assist staff to prevent, manage and respond to unreasonable complainant conduct, and provides a framework for senior managers to restrict services where appropriate. It demonstrates the Office's commitment to staff wellbeing and its objective to provide an efficient and effective complaint handling service.
- As the project is about dealing with difficult complainants, it is anticipated that much of the personal information should already have been collected by the Office as part of complaint handling / provision of advice. However, new personal information that could be collected include a person's health information (e.g. whether or not the personal has a mental illness) and the complainant's representative's name and contact details (e.g. when the Office decides that the complainant can only contact us via a representative).
- The personal information collected would be stored in Resolve.
- We may need to use the personal information in communicating with the complainant. We may sometimes need to disclose the personal information to other organisations (e.g. the police or the agency complained of).

4. Identify and consult with stakeholders

CME branch teams (Intake, Early Res, Investigations), Industry branch (Post, OSO, VSLO, PHIO), Legal team, Program Delivery branch (Defence, ACT)

Provide key privacy elements

Purpose of collecting, using and disclosing information: to assist with the management of complaints

Authority: s 8(3) Ombudsman Act 1976

Nature and sensitivity of information: may collect sensitive health information.

5. Map Information Flows

Describe and map the project's personal information flows.

VERIFICATION

Not required.

COLLECTION

The purpose of collecting information is to assist the Office to manage complaints it receives about Government agencies and other organisations under its jurisdiction.

Information will be collected from hard copy letters, over the telephone or by electronic means (ie. emails, online complaint form) from the complainant or someone acting on their behalf.

Usually collected by an invitation from us (e.g. offering review right to the complainant for placing a service restriction on them or asking the complainant to provide details of a representative). The complainant would then respond.

USE

The information will be used to handle complaints received by the Office – for example, contacting the complainant/their representative.

DISCLOSURE

Disclosure will be for the purpose of preventing harm to others. For example, alerting the agency complained of and the police to the complainant's behaviour.

The information is unlikely to be disclosed overseas.

INFORMATION QUALITY

Information collected will be updated when the Office reviews service restrictions placed on the complainant. The policy would require the Office to contact the complainant prior to a review.

It is unlikely that any updated information would be given to others outside the organisation. Within the organisation, staff who manage the complaint, and their managers would have access to the updated information.

SECURITY

Information will be stored in Resolve case management system, accessible by all staff.

RETENTION AND DESTRUCTION

Information will be retained and destroyed as per Resolve information retention practices.

ACCESS AND CORRECTION

A person can access and update information about themselves for free. The person can make a request via the Intake team or directly to the staff who is handling their complaint. The information in Resolve can be easily updated if personal information changes.

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.

The information that could potentially be collected in implementing the policy is collected in accordance with the Ombudsman Act in the course of the Office's complaint handling activities.

It's unlikely that the information collected would be used in the future for a different purpose. This is because the Office has a detailed and clearly defined privacy policy and procedures, which are well understood and complied with by staff through regular training.

The project therefore has acceptable privacy outcomes.

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.	*http://www.ombudsman.gov.au/privacy-policy*	*Compliant*	
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.	Usually able to manage. Exception: when it becomes impracticable to deal with a difficult complainant who wants to remain anonymous or use a pseudonym (APP 2.2(b))	*Compliant*	
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.	Purpose of collection is to manage complaints. The authority is s 8(3) of the Ombudsman Act. It fits directly with the Ombudsman's functions.	*Compliant*	

#	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.	This would not generally occur – the Ombudsman would normally have been able to collect the information under APP 3. In some cases the complainant may provide personal information about another person (e.g. someone they want us to contact). The collection of this information would be permitted under APP 3.1 – the information is reasonably necessary or directly related to the Office's complaint handling function.	*Compliant*	
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.	We can refer to the Ombudsman's privacy policy. It is unlikely that the information will be disclosed to overseas recipients	*Compliant*	
6	Principle 6 – Use or disclosure of personal information Use it for the purpose you collected it for, unless one of the exceptions applies.	Used usually for managing complaints. May disclose to the police or the agency complained of under a 'permitted general situation' (s 16A Privacy Act) – lessening or preventing serious threat to public safety or life, health or safety of an individual.	*Compliant*	

#	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)
7	Principle 7 – Direct marketing Information not to be disclosed for the purpose of direct marketing unless exceptions apply, e.g., consent.	Will not be used for direct marketing.	*Compliant*	
	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.	Unlikely to be disclosed to an overseas recipient.	*Compliant*	
9	Principle 9 – Adoption, use or disclosure of government related identifiers. Only assign unique identifiers where permitted. Agency should not disclose identifiers unless permitted.	Will not be adopting government identifiers.	*Compliant*	

#	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)
10	Principle 10 – Quality of personal information. Ensure information is accurate, up to date, complete and relevant prior to using it.	It is reasonable that the Office contacts the complainant when reviewing service restriction. The Office may also be interacting with the complainant on a periodic basis in relation to their complaint and seek to update personal information that way. Any more frequent contact to update personal information is not reasonable given that the complainant would either be on a service restriction or periodic contact is already occurring.	*Compliant*	
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.	Information will be stored in Resolve and the Office's servers. Staff have an legislative obligation under s 35 of the Ombudsman Act to keep confidentiality.	*Compliant*	
12	Principle 12 – Access to personal information People have a right to see their personal information noting exceptions apply, eg., FOI exemptions.	Personal information can be accessed free of charge by that person (except where FOI exemptions apply).	*Compliant*	

#	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)
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.	A person can correct their personal information at any time by making the request to a member of staff. As the information is stored in Resolve, corrections can be easily achieved.	*Compliant*	
14	Other privacy interests	*N/A*		

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	Staff browsing Resolve for information	Agency policy that staff	Low	Medium	Low

	unrelated to complaints they are not responsible for.	should not be browsing. This is well understood by staff. Resolve records can be audited.			
2	Information disclosed by staff not for the purpose of its collection	Staff under legal obligation to keep confidentiality Staff induction training and regular privacy training Reinforcement during information sessions about the new policy.	Low	High	Medium

8. Recommendations

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

Ref	Recommendation	Agreed Y/N
R- 01	It is recommended that the information sessions on the new unreasonable complainant conduct policy specifically address disclosure of personal information to external agencies and the police: when the disclosure is permitted and by whom.	

Signatures

LMacleod — Name of Senior Assistant Ombudsman responsible

LOUISE MACLEOD — Signature

30/11/18 — Date

Rodney Lee Walsh, Privacy Delegate

_____ — Signature

_____ — Date