Australian Government

Fair Work OMBUDSMAN

FWO Privacy Management Plan 2022-2024

Version 1.1

July 2022

Visual style realignment:DB-810535/3.0

Document Management

Version History

Version	Date	Author	Revision Comments
V0.1	20072022		Initial Draft
V1.0	26072022		Final version for submission to Accountability Sub-Committee
V1.1	09092022		Version for publication

Approvals

Name	Role	Date

Table of Contents

Table of Contents 3

Background 2

What is a Privacy Management Plan? 2

Privacy Risk Profile 2

Maturity Framework 4

Privacy Maturity Assessment Outcomes 5

Goals for improvement – privacy maturity actions 16

Background

What is a Privacy Management Plan?

The Australian Government Agencies Privacy Code requires agencies to have a privacy management plan (PMP).

A PMP is a strategic planning document in which the Fair Work Ombudsman (the FWO):

- identifies its privacy goals and maturity targets, and
- sets out how it will meet its compliance obligations under the Australian Privacy Principles.

The FWO developed this PMP with reference to the OAIC's *Interactive PMP Explained* resource for guidance on how it identified compliance gaps and opportunities to improve maturity.

This PMP builds on actions taken by the FWO since the introduction of the Australian Government Agencies Privacy Code in 2018 to increase its privacy maturity and describes steps the FWO should take to continue working towards its maturity targets. When reviewing its privacy performance, the FWO will return to this PMP and use it to assess how well it has met and delivered its privacy targets.

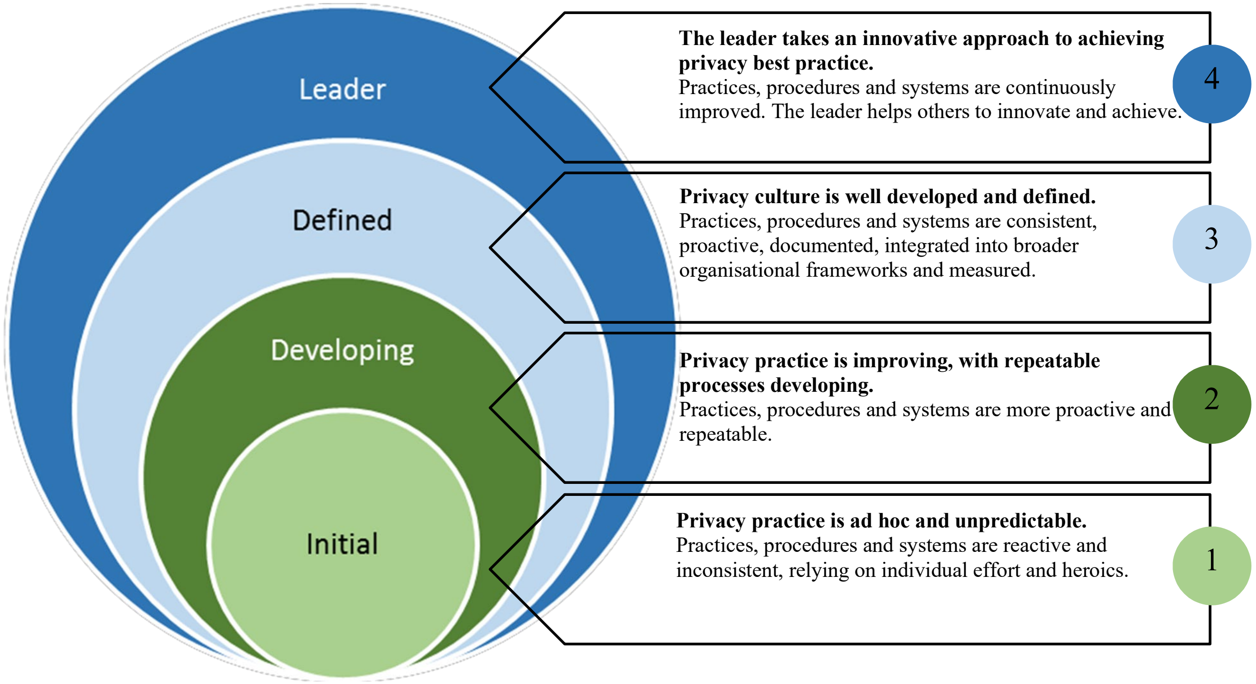
Privacy Risk Profile

When preparing this PMP, the FWO considered various matters relevant to its privacy risk profile and determined that it has a high privacy risk-profile. The FWO provides complex public services to individuals and handles a significant amount of personal information. The table below outlines the risk factors taken into consideration when determining the privacy risk profile of the FWO.

Risk Factor	Agency response
Functions and activities	The *Fair Work Act 2009* sets out the functions and responsibilities of the FWO. This includes providing education, assistance, advice and guidance to employees and employers, outworkers, outworker entities and organisations, promoting and monitoring compliance with workplace laws, inquiring into and investigating breaches of the Act, taking appropriate enforcement action and performing our statutory functions efficiently, effectively, economically and ethically.
Privacy influence and trust	The FWO relies on the trust of employees and employers to achieve its purpose. The role of the FWO is to promote compliance with Australian workplace relations laws by employees or employers through advice, education and (where necessary) enforcement, which necessarily includes investigation. In promoting cooperative workplace relations and compliance with the FW Act, the FWO relies on the supply of information and cooperation from employees and employers. Importantly, this includes encouraging parties to work with the FWO and to remedy breaches (as part of promoting cooperative workplace relations between employers and employees). Any loss of trust and confidence in the FWO leading to a reduction in the types and quantity of information supplied could reduce the ability of the FWO to detect and deal with issues of non-compliance. This could potentially lead to an increase in the costs of monitoring and enforcing compliance as well as the FWO's ability to effectively and efficiently conduct its operations.
Amount of personal information handled	The FWO collects, handles and manages a large quantity of personal information provided by employees, employers and their legal representatives. Personal information is collected through online and phone enquiries, requests for assistance, investigation and litigation.
Sensitivity of personal information handled	The FWO may hold sensitive information about individuals including information about an individual's employment rights and entitlements, racial or ethnic origin, trade union membership, sexual orientation and health information. By exception, the FWO may also hold information related to alleged criminal matters such as sexual harassment or bullying in the workplace.

Maturity Framework

The Maturity Framework requires the FWO to assess its maturity across four maturity levels. The maturity levels are shown in the following diagram:



The leader takes an innovative approach to achieving privacy best practice. Practices, procedures and systems are continuously improved. The leader helps others to innovate and achieve.

Privacy culture is well developed and defined. Practices, procedures and systems are consistent, proactive, documented, integrated into broader organisational frameworks and measured.

Privacy practice is improving, with repeatable processes developing. Practices, procedures and systems are more proactive and repeatable.

Privacy practice is ad hoc and unpredictable. Practices, procedures and systems are reactive and inconsistent, relying on individual effort and heroics.

The attributes for each maturity level within the Maturity Framework are described in detail in Appendix 1: *Privacy Program Maturity Assessment Framework* of the OAIC's *Interactive Privacy Management Plan*.

Privacy Maturity Assessment Outcomes

This PMP has been prepared using an assessment of the FWO's privacy maturity, the results of which are recorded in the table below. An asterisk (*) next to an attribute name means that it is a 'compliance attribute' and that the FWO must have a minimum maturity level of 'Developing' to comply with the Privacy Act or the Australian Government Agencies Privacy Code.

This PMP provides a high-level overview of steps the FWO will take to reach the specified target levels. Target levels will be reconsidered as part of the review period, including consideration of elevating target levels once existing targets are substantially reached.

Governance & Culture				
Attribute	**Current Level**	**Target Level (for current plan)**	**Rationale/Commentary**	**Steps to maintain or reach target level**
Privacy Champion*	**Defined**	**Leader**	The FWO has a designated Privacy Champion (Executive Director Corporate Services) who promotes a culture of privacy that values and protects personal information and supports the integration of privacy practices, procedures and systems into broader organisational frameworks.	The Privacy Champion continues to leverage privacy resources and best practice approaches to raise awareness of privacy risks and issues at the Executive level.

Governance & Culture				
Attribute	**Current Level**	**Target Level (for current plan)**	**Rationale/Commentary**	**Steps to maintain or reach target level**
Privacy Values	**Defined**	**Leader**	There is a connection between the FWO's values and respecting and protecting personal information. This connection is understood by staff. The FWO has information and resources relating to privacy on both the intranet and the internet. The FWO has also undertaken activities to enhance privacy awareness, such as holding mandatory training for staff and Privacy Awareness Week activities.	FWO Privacy Policy remains aligned with organisational functions and including during periods of legislative or organisational change.
Privacy Officer*	**Defined**	**Leader**	Privacy Officers were designated on 3 July 2018 and OAIC has been updated as these appointments have changed. A role description has been developed and approved (Roles and Responsibilities Privacy Champion and Privacy Officers). There are established practices, procedures and systems to support the obligations of the Privacy Officers and these are documented and integrated into broader organisational frameworks. There is an agency wide awareness of the Privacy Officers.	Capability framework for privacy officers.
Management & Accountability	**Defined**	**Defined**	The Privacy Team is responsible for promoting privacy awareness throughout the agency, assisting with the preparation of PIAs,	Report to Accountability Sub-Committee on PIA recommendations.

Governance & Culture				
Attribute	**Current Level**	**Target Level (for current plan)**	**Rationale/Commentary**	**Steps to maintain or reach target level**
			providing privacy advice and managing responses to suspected privacy breaches. The Director and Assistant Director of the Team act as the agency's Privacy Officers, reporting to the Executive Director overseeing the Team who is also the agency's Privacy Champion. The Team reports to the Accountability Sub-Committee – the governance committee overseeing privacy matters on privacy breaches and privacy risk and accountable to the Corporate Board.	
Awareness	**Defined**	**Leader**	Staff view privacy as a positive and valuable part of business as usual and understand the importance of maintaining the trust of employers and employees. The FWO's policies and expectations are well communicated to staff.	Focused workshop events targeting topical privacy issues as part of Privacy Awareness Week. Calendar of intranet communication stories including focused narratives.
Element score (average of attribute scores)	**3/4 (Defined)**			

Privacy Strategy				
Attribute	**Current Level**	**Target Level (for current plan)**	**Rationale/Commentary**	**Steps to maintain or reach target level**
Privacy Management Plan*	**Defined**	**Defined**	The FWO's PMP is used to guide the agency's measurement of privacy awareness, to identify compliance gaps and facilitate continuous improvement. The PMP is approved by the Accountability Sub-Committee. The PMP actions work to identify and mitigate any risks or issues raised in the preceding period.	Publish the PMP on website to provide transparency and facilitate external engagement. Investigate feasibility of an external survey to explore privacy expectations of our customers to feed into next PMP.
Inventory of Personal Information*	**Developing**	**Defined**	The FWO has documented the general categories of personal information collected, and the systems used to store it, across most areas of the agency.	Refresh of personal information holdings register to include data flows and third parties where they hold information, ownership, accountability and access for specific IT systems and databases that hold personal information and retention policies. Schedule regular review and update, including determining and reporting on update triggers (ie system change).
Data Quality Processes*	**Developing**	**Defined**	The FWO has a designated Data Governance Group which reports to the Accountability Sub-Committee and that is responsible for putting in place organisational practices to ensure data quality and relevance.	Refresh Information and Data Governance Framework. Liaise and provide input to Data Governance Group on requirements under APPs for data quality.

Privacy Strategy				
Attribute	**Current Level**	**Target Level (for current plan)**	**Rationale/Commentary**	**Steps to maintain or reach target level**
Information Security Processes	**Defined**	**Defined**	The FWO has an established information-security aware culture. The FWO has policies regarding collection, access to, use and disclosure of personal and other types of information. The FWO has an agency security advisor who is responsible for ensuring FWO complies with the Commonwealth Protective Security Policy Framework. The Information Governance Team and project teams work with IT security personnel when undertaking PIAs where privacy and information security considerations are both necessary and may intersect. The FWO has robust processes in place for reporting on privacy and information security breaches and is responsive to potential and identified breaches.	Establish regular information security / privacy team meetings on information security and privacy risks.
Element score (average of attribute scores)	**2.5 / 4 (Developing)**			

Privacy Processes				
Attribute	Current Level	Target Level (for current plan)	Rationale/Commentary	Steps to maintain or reach target level
External Privacy Policy & Notices*	Defined	Leader	Privacy messaging is viewed positively, as an opportunity to build trust and engage the public and is an important part of the agency's privacy practice. A clear, comprehensive and plain English privacy policy is provided to the public and goes beyond compliance, focusing on customer experience, openness and transparency. The FWO Privacy page and Privacy Policy are subject to regular review. Amendments to the FWO Privacy Policy require approval by the Accountability Sub-Committee. The Privacy Team assists areas that collect personal information to draft privacy notices which comply with the Australian Privacy Principles and the Australian Government Agencies Privacy Code. There is a clear link between privacy notices issued by the FWO when it collects personal information, and the privacy policy and privacy messaging is consistent and easy to locate. A privacy statement register is maintained to ensure that the FWO is aware of and can refresh all privacy statements.	Privacy statement register published on Intranet Privacy page to raise staff awareness of current privacy statements.

Privacy Processes				
Attribute	**Current Level**	**Target Level (for current plan)**	**Rationale/Commentary**	**Steps to maintain or reach target level**
Internal Policies & Procedures	**Developing**	**Defined**	As well as a Privacy Policy, the FWO has an existing privacy breach guide and guidance to FWO staff on undertaking Privacy Impact Assessments.	Scheduled review and refresh of internal procedures.
Privacy Training*	**Defined**	**Leader**	Online training is provided to all staff during induction and annually, by way of a compulsory module dedicated to Information Access and Privacy as part a Corporate Training program. Training is operationalised in face-to-face training at inductions and team/branch meetings upon request. High privacy risk areas receive tailored training to assist those areas to comply with the Privacy Act.	Training calendar of targeted privacy events.
Privacy Impact Assessments*	**Developing**	**Defined**	The Privacy Team has reviewed and updated the Privacy Impact Assessment process and created a new Intranet page to support staff. Opportunities for earlier engagement by project teams exist.	Internal communications on PIA process. Improve governance for monitoring of implementation of PIA recommendations.

Privacy Processes				
Attribute	Current Level	Target Level (for current plan)	Rationale/Commentary	Steps to maintain or reach target level
Dealing with Suppliers	Defined	Defined	The Information Governance Team has released a due diligence assessment tool and two toolkits on managing information as part of procurement processes. Privacy clauses have been added to the procurement manual and a workshop on privacy and procurement delivered in 2022.	Continue engagement on identifying privacy risks early in engagement lifecycle.
Privacy Management Plan*	Defined	Leader	The FWO's PMP is used to guide the agency's measurement of privacy awareness, to identify compliance gaps and facilitate continuous improvement. The PMP is approved and reviewed annually by the Accountability Sub-Committee. The PMP actions work to identify and mitigate any risks or issues raised in the preceding period.	
Access & Correction*	Defined	Defined	Information on how individuals may correct their personal information is clearly outlined on the FWO Privacy page and Privacy Policy, as well as in specific service offerings. Where appropriate, online service offerings allow the customer to easily update their own personal information. Most requests to correct or update personal information are processed within business units or through contacting the Privacy Team.	

Privacy Processes				
Attribute	**Current Level**	**Target Level (for current plan)**	**Rationale/Commentary**	**Steps to maintain or reach target level**
Complaints & Enquiries	**Defined**	**Defined**	The FWO's Privacy Policy has an established process for the management of privacy complaints and enquiries through the Privacy inbox. Where privacy complaints and enquiries are received through other channels, these are forwarded to the Privacy Team. These matters are coordinated by the Privacy Team in conjunction with the relevant business unit.	
Element score (average of attribute scores)	**4.5 (Defined)**			

Risk and Awareness				
Attribute	**Current Level**	**Target Level (for current plan)**	**Rationale/**	**Steps to maintain or reach target level**
Risk Identification & Assessment	**Defined**	**Defined**	Privacy risks are identified through Privacy Impact Assessments and through annual privacy breach reporting. Privacy risks have been incorporated into regular reporting on information risk to the Accountability Sub-Committee.	

Risk and Awareness				
Attribute	**Current Level**	**Target Level (for current plan)**	**Rationale/**	**Steps to maintain or reach target level**
Reporting & Escalation	**Defined**	**Defined**	The Privacy Team reports weekly to the Privacy Champion on emerging privacy risks and issues. The Privacy Team report to the Accountability Sub-Committee on information risks and privacy breaches.	
Assurance Model	**Defined**	**Leader**	The Privacy Team liaises where privacy risks or issues are identified within business area practices which require resolution through continuous improvement.	Document the protocol for engagement arising out of privacy complaints to ensure continuous business improvement.
Complaints & Enquiries	**Defined**	**Leader**	The FWO's Privacy Policy has an established process for the management of privacy complaints and enquiries through the Privacy inbox. Where privacy complaints and enquiries are received through other channels, these are forwarded to the Privacy Team. These matters are coordinated by the Privacy Team in conjunction with the relevant business unit.	Annual reporting on privacy complaints and enquiries to identify trends and risks
Element score (average of attribute scores)	**4.4 (Defined)**			

Data Breach Response				
Attribute	Current Level	Target Level (for current plan)	Rationale/Commentary	Steps to maintain or reach target level
Data Breach Response Plan	**Defined**	Leader	The FWO has identified processes to contain and assess data breaches as well as notify affected individuals in appropriate cases. The FWO has formalised these processes in its Data Breach Response Plan. The Privacy Team report annually to the Accountability Sub-Committee on privacy breaches.	Testing of the Data Breach Response Plan to gauge its effectiveness against different scenarios.
Data Breach Notification*	**Defined**	Leader	The FWO is committed to notification in response to data breaches and views this as an opportunity to demonstrate trust and transparency. Clear processes are in place to evaluate and assess whether notification is necessary or desirable including under the Notifiable Data Breach Scheme. Communication is made with affected individuals when necessary.	Continuous monitoring and review of data breaches to implement appropriate mitigation measures.
Element score (average of attribute scores)	3.4 (Defined)			
Average of element scores	2.9 / 4 (Defined)			
Overall privacy maturity level	**3 / 4 (Defined)**			

Goals for improvement – privacy maturity actions

The table below summarises all actions for improvement outlined in the FWO Privacy Maturity Assessment above. These actions will take place between July 2022 and June 2024 and will assist the FWO to improve its privacy maturity.

Element / Attribute	Action	Due
Governance and Culture / Privacy Champion	The Privacy Champion continues to leverage privacy resources and best practice approaches to raise awareness of privacy risks and issues at the Executive level	Ongoing
Governance and Culture / Privacy Values	FWO Privacy Policy remains aligned with organisational functions and including during periods of legislative or organisational change	Ongoing
Governance and Culture / Privacy Officers	Capability framework for privacy officers	June 2023
Governance and Culture / Awareness	Focused workshop events targeting topical privacy issues as part of Privacy Awareness Week	Ongoing
Governance and Culture / Awareness	Calendar of intranet communication stories including focused narratives	Ongoing
Privacy Strategy / Privacy Management Plan	Publish Privacy Management Plan on website to allow for transparency and external engagement	September 2022
Privacy Strategy / Privacy Management Plan	Investigate feasibility of external survey to explore privacy expectations of our customers to feed into next Privacy Management Plan	June 2024
Privacy Strategy / Personal Information Holdings Register	Refresh of personal information holdings register to include data flows and third parties where they hold information, ownership, accountability and access for specific IT systems and databases that hold personal information and retention policies	June 2024
Privacy Strategy / Personal Information Holdings Register	Regular review and update, including determining and reporting on update triggers (ie system change)	June 2024
Privacy Strategy /Data Quality Processes	Refresh Information and Data Governance Framework	June 2024
Privacy Strategy /Data Quality Processes	Liaise and provide input to Data Governance Group on requirements under APPs for data quality	June 2023

Element / Attribute	Action	Due
Privacy Strategy / Information Security Processes	Establish regular liaison between information security and privacy teams	December 2022
Privacy Processes / External Privacy Policy and Notices	Privacy statement register published on Intranet Privacy page to raise staff awareness of current privacy statements	December 2022
Privacy Processes /Internal policies and procedures	Refresh of internal procedures	June 2024
Privacy Processes / Training	Training calendar of targeted privacy events	December 2022
Privacy Processes / Privacy Impact Assessments	Internal communications on PIA process	June 2023
Privacy Processes / Working with Suppliers	Continue engagement on identifying privacy risks early in engagement lifecycle	June 2023
Risk and Awareness / Assurance Model	Document the protocol for engagement arising out of privacy complaints to ensure continuous business improvement	June 2023
Risk and Awareness / Complaints and Enquiries	Annual reporting on privacy complaints and enquiries to identify trends and risks	June 2023
Data Breach Response / Data Breach Response Plans	Test Data Breach Response Plan to gauge its effectiveness against different scenarios.	June 2024
Data Breach Response / Data Breach Notification	Continuous monitoring and review of data breaches to implement appropriate mitigation measures	Ongoing