Australian Government

Fair Work OMBUDSMAN

# Privacy Management Plan 2025-2027

Version 1.0

November 2024

# Document Management

## Version History

| Version | Date | Author | Revision Comments |
|---|---|---|---|
| V0.1 | 18112024 | | Initial Draft |
| V1.0 | 22112024 | | Final version for submission to Accountability Sub-Committee |
| V1.1 | | | Version for publication |

Approvals

| Name | Role | Date |
|---|---|---|
| Nicola Forbes | Director Information Governance | |
| Rebecca Price | Executive Director Corporate Services | |
| | Accountability Sub-Committee | |

# Table of Contents

# 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 Office of 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 using the OAIC's *Interactive PMP Explained* resource to guide 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 will 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.

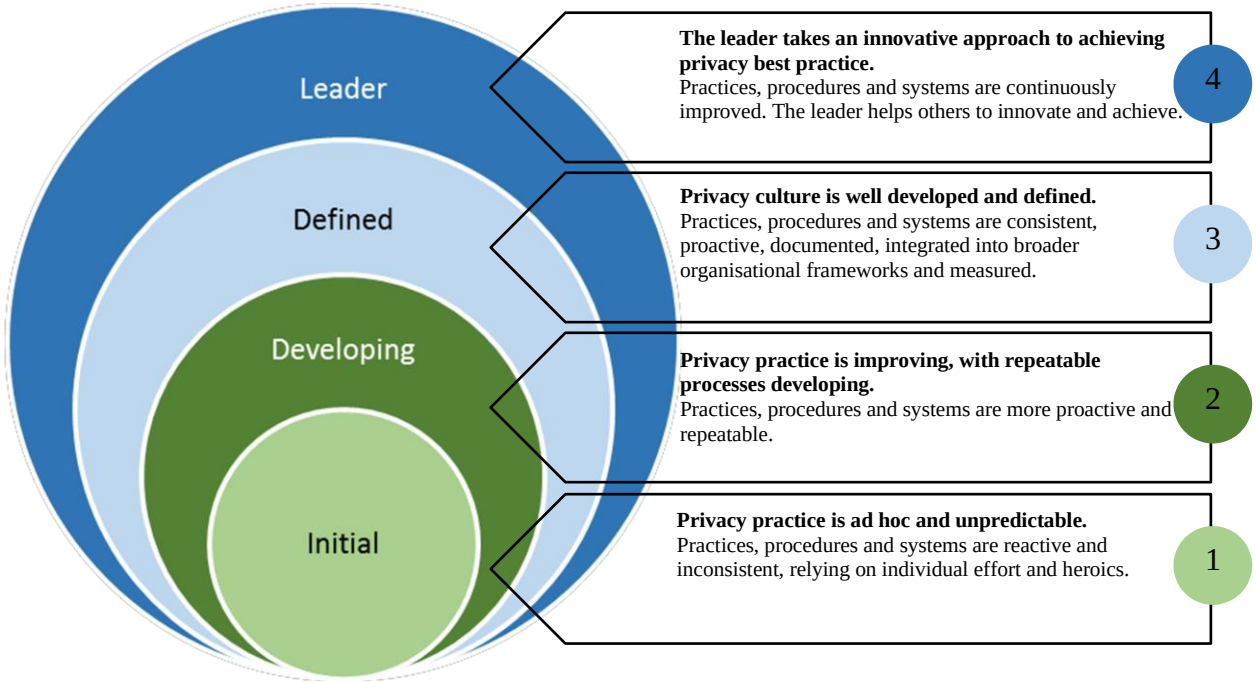
## Privacy Risk Profile

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. Additionally, the Fair Work Legislation Amendment (Closing Loopholes) Act 2023 will introduce a criminal offence to the Fair Work Act 2009 for employers who intentionally fail to pay employee entitlements. This will result in the FWO holding allegations of criminal conduct and criminal history 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.<br><br>The Fair Work Legislation Amendment (Closing Loopholes) Act 2023 introduces a criminal offence to the Fair Work Act 2009 for employers who intentionally fail to pay employee entitlements. The offence will commence as early as 1 January 2025. The FWO will be responsible for investigating contraventions of the offence and for referring matters to the Commonwealth Director or Public Prosecutions or the Australian Federal Police for consideration and potential prosecution. |
| 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.<br><br>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).<br><br>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. From 1 January 2025 the FWO will also hold information related to the criminal offence function, including criminal histories and allegations of criminal behaviour. |

## 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 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 (Code).

The table below details compliance or currency gaps which require action to ensure the FWO is meeting its obligations under the Code. A compliance gap indicates areas where the FWO could take steps to improve its current privacy practices. A currency gap indicates anticipated changes in the legislative, policy or technological environment which will require proactive action during the lifetime of the PMP. For the 2025-2027 years, anticipated change includes:

- the new criminal offence introduced by the Fair Work Legislation Amendment (Closing Loopholes) Act 2023
- the intention in the FWO's Corporate Plan 2024-2025 and Statement of Intent to embrace tripartism, collaboration and engagement
- the outcomes and goals outlined in the FWO's Technology Strategy 2024-2027 to develop a culture of innovation and an artificial intelligence strategy
- the Privacy and Other Legislation Amendment Bill 2024 (POLA Bill) and possible new legislation coming out of the recommendations accepted by the Government as part of the Privacy Act Review Report.

| Governance & Culture | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/Commentary** | **Compliance or Currency Gaps** |
| **1.Privacy Champion*** | **Defined** | **Defined** | 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.<br>The Privacy Champion continues to leverage privacy resources and best practice approaches to raise awareness of privacy risks and issues at the Executive level. | |
| **2.Privacy Values** | **Leader** | **Leader** | The agency's documented values clearly promote a culture of respecting and protecting personal information to build trust. The agency publicises its values including through a specifically designed page on workplace privacy.<br>The agency's PIA processes align key recommendations to the importance of managing privacy to maintain the trust of employers, employees and their legal representatives. | |
| **3.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, | **Compliance gap:** Privacy Officer positions are located within the FOI Team. FOI timeframes impact the hours that can be dedicated to privacy. This limits the ability of the team to proactively engage |

| Governance & Culture | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/Commentary** | **Compliance or Currency Gaps** |
| | | | procedures and systems to support the obligations of the Privacy Officer and these are documented and integrated into broader organisational frameworks. There is an agency wide awareness of the Privacy Officers. | with business areas to improve their privacy practices. |
| **4.Management & Accountability** | **Defined** | **Defined** | The FWO has a defined management and accountability framework. The Privacy Team is responsible for promoting privacy awareness throughout the agency, assisting with the preparation of PIAs, 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. | |

| Governance & Culture | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/Commentary** | **Compliance or Currency Gaps** |
| **5.Awareness** | **Defined** | **Leader** | FWO 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 release of the annual Privacy Breach Report is accompanied by a communications campaign. Privacy Awareness Week includes a seminar on a topical privacy issue. | **Compliance gap:** There is a general awareness of the value of privacy. This does not always translate into an awareness of how to embed privacy obligations into business practices. |
| **Element score (average of attribute scores)** | **3.2/4 (Defined)** | | | |

| Privacy Strategy | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/Commentary** | **Compliance or Currency Gaps** |
| **6.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.<br>The PMP is published on the FWO's website to provide transparency and facilitate external engagement. | |

| Privacy Strategy | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/Commentary** | **Compliance or Currency Gaps** |
| **7.Inventory of Personal Information*** | **Defined** | **Defined** | The FWO's Personal Information Holdings Register has been updated 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. Regular review occurs in accordance with the privacy impact assessment lifecycle. | |
| **8.Data Quality Processes*** | **Developing** | **Defined** | The FWO has a designated Data Governance Group which reports to the Accountability Sub-Committee and is responsible for putting in place organisational practices to ensure data quality and relevance. There is no Documented and approved Data Governance Framework and Data Strategy. | **Compliance gap:** Individual business areas capture and manage data but there is no overall data governance framework or data strategy to drive the agency's use of data. |

| Privacy Strategy | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/Commentary** | **Compliance or Currency Gaps** |
| **9.Information Security Processes** | **Developing** | **Defined** | 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 reports on its compliance 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. Security and privacy personnel have regular briefing meetings.<br>While the agency has disposal policies, it lacks the technological means to carry out systematic and routine disposal activities. | **Currency gap:** The agency does not have the technological means to conduct systematic and routine disposal of time expired personal information to meet the requirements of the POLA Bill. |
| **Element score (average of attribute scores)** | **2.5 / 4 (Developing)** | | | |

| Privacy Processes | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/Commentary** | **Compliance or Currency Gaps** |
| **10.External Privacy Policy & Notices*** | **Defined** | **Defined** | 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.<br>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 Privacy Policy require approval by the Accountability Sub-Committee.<br>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.<br>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.<br>A privacy statement register is maintained to ensure that the FWO is aware of and can refresh all privacy statements. | |
| **11.Internal Policies & Procedures** | **Defined** | **Defined** | The FWO has internal policies and procedures relating to privacy breaches, privacy complaints and privacy impact assessments. Additionally, FWO operational manuals contain processes related to privacy. | **Currency gap:** Review internal policies to ensure they are fit for purpose to support information sharing with external stakeholders and the new criminal offence provision. |

| Privacy Processes | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/Commentary** | **Compliance or Currency Gaps** |
| **12.Privacy Training*** | **Defined** | **Defined** | Online training is provided to all staff during induction and annually, by way of a compulsory module as part a Corporate Training program. Training is operationalised in face-to-face training at inductions and team/branch meetings upon request. Bespoke training is provided for high privacy risk areas during Privacy Awareness Week. | |
| **13.Privacy Impact Assessments*** | **Defined** | **Defined** | The Privacy Team has reviewed and updated the Privacy Impact Assessment process and created a new Intranet page to support staff. Preliminary risk assessments are routinely undertaken to assess whether a PIA is required or not. | |
| **14.Dealing with Suppliers** | **Developing** | **Defined** | Third party contracts generally include Commonwealth Government terms related to privacy. | **Compliance gap:** Some business areas continue to struggle with procurement and contract management obligations. Support services are limited. **Currency gap:** Technology products and services are increasingly embedding AI into their service offerings. |
| **15.Access & Correction*** | **Defined** | **Leader** | Information on how individuals may correct their personal information is clearly outlined on the 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. Innovative | **Currency gap:** Some areas of the agency undertake manual identity checking which relies on the collection and storage of identity documentation. |

| Privacy Processes | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/Commentary** | **Compliance or Currency Gaps** |
| | | | approaches are taken to enabling access and correction, including the use of self-service portals. | |
| **16.Complaints & Enquiries** | **Developing** | **Defined** | The 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. Limited use is made of complaints and enquiry data to improve privacy practice. | **Compliance gap:** FWO does not currently report on privacy complaints and enquiries or have a mechanism to use this data to improve privacy practice. |
| **Element score (average of attribute scores)** | **2.4/5 (Developing)** | | | |

| Risk and Awareness | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/** | **Compliance or Currency Gaps** |
| **17.Risk Identification & Assessment** | **Defined** | **Defined** | Privacy risks are identified through Privacy Impact Assessments and through annual privacy breach reporting. | **Currency gap:** Innovative uses of AI, the new criminal offence and FWO's move towards tripartite processes and broader stakeholder collaboration and engagement may lead to new |

| Risk and Awareness | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/** | **Compliance or Currency Gaps** |
| | | | | uses and disclosures of personal information. |
| **18.Reporting & Escalation** | **Defined** | **Defined** | The Privacy Team reports weekly to the Privacy Champion on emerging privacy risks and issues. The Privacy Team provides separate reports to the Accountability Sub-Committee on information risk and privacy breaches. | **Compliance gap:** PIA recommendations are not tracked against actions or reported to the Accountability Sub-Committee. |
| **19.Assurance Model** | **Developing** | **Defined** | Some assurance activities occur in respect of the privacy management plan, complaints and breaches. These have not been integrated into the three lines of defence model. | **Compliance gap:** Data on privacy complaints, data breaches and privacy impact assessment recommendations not integrated to identify business areas which require additional support to implement best practice and continuous improvement. |
| **Element score (average of attribute scores)** | **2.7/ 4 (Defined)** | | | |

| Data Breach Response | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/Commentary** | **Compliance or Currency Gaps** |
| **20.Data Breach Response Plan** | **Defined** | **Leader** | The FWO has a well-defined plan in place with clear and documented roles and escalation paths. Staff are aware of how to recognise a data breach and are likely to speak up. The process is integrated with other critical business functions through the SETIR form which provides for | **Currency gap:** New criminal offence may require different processes for data breaches. |

| Data Breach Response | | | | |
|---|---|---|---|---|
| **Attribute** | **Current Level** | **Target Level (for current plan)** | **Rationale/Commentary** | **Compliance or Currency Gaps** |
| | | | integrated reporting on privacy and information security risks and through corporate governance functions managing risk and assurance. The plan has been regularly tested with data breaches of varying severity, including with data breaches where the agency has collaborated at a whole of Commonwealth Government level. | |
| **21.Data Breach Notification*** | **Leader** | **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.<br>Communication is made with affected individuals when necessary. | |
| **Element score (average of attribute scores)** | **3.5 / 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 January 2025 and December 2028 and will assist the FWO to improve its privacy maturity.

| Element / Attribute | Action | Due |
|---|---|---|
| **Governance and Culture / Privacy Officer** | Create and resource dedicated Privacy Team. | February 2025 |
| **Governance and Culture / Awareness** | Annual privacy breach report communications plan | Ongoing |
| **Governance and Culture / Awareness** | PAWS seminar on privacy and the use of commercially available AI products | June 2025 |
| **Privacy Strategy /Data Quality Processes** | Develop and release Data Strategy and Data Governance Framework. | December 2025 |
| **Privacy Strategy / Information Security Processes** | Acquire and implement technological means to conduct systematic and routine disposal of time expired personal information. | December 2027 |
| **Privacy Processes /Internal policies and procedures** | Review internal policies to ensure they are fit for purpose for new criminal offence provision and to support proactive information sharing with external stakeholders as part of tripartite model. | December 2026 |
| **Privacy Processes / Working with Suppliers** | Develop an enabling service for procurement including refreshed Procurement Guidelines supported by procurement and contract management training. | December 2026 |
| **Privacy Processes / Access and Correction** | Design of new criminal implementation system to consider privacy risks and impacts | June 2025 |
| **Privacy Processes / Access and Corrrection** | Review agency processes which rely on collection of identity documentation | December 2027 |
| **Privacy Processes / Complaints and Enquiries** | Collect and analyse data on privacy complaints and enquiries. | December 2025 |
| **Risk and Awareness / Risk Identification and Assessment** | Review and refresh risk identification to include new risks. | Ongoing |
| **Risk and Awareness / Reporting and Escalation** | Build model to track and report on PIA recommendations to Accountability Sub-Committee. | June 2025 |
| **Risk and Awareness / Assurance Model** | Redesign activities of Privacy Team to support and enable business and align with three lines of defence model (control, oversight, assurance activities). | December 2026 |

| Element / Attribute | Action | Due |
|---|---|---|
| **Data Breach Response / Data Breach Response Plans** | Refresh Data Breach Response Plan for new criminal offence. | June 2025 |