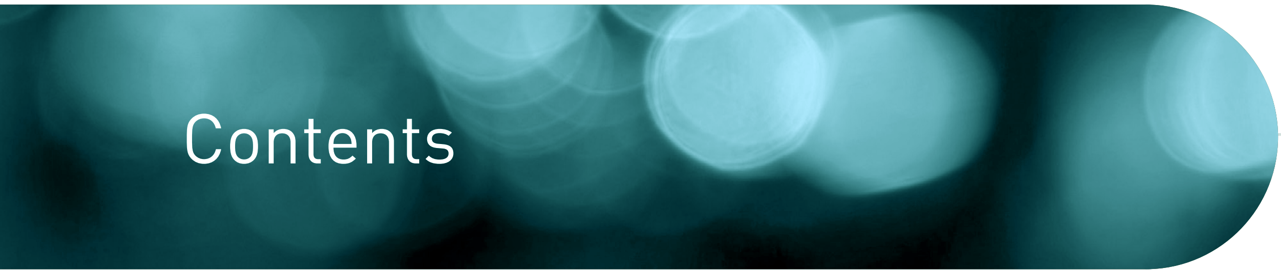
Australian Government
Attorney-General's Department

Privacy Management Plan

1 December 2018 | 31 December 2019

ISBN: 978-1-920838-66-9 (Online)

Use of the Coat of Arms



Contents

Background

What is a Privacy Management Plan?

A Privacy Management Plan (**PMP**) is a document that identifies specific, measurable privacy goals and targets and sets out how the Attorney-General's Department (the department) will meet its compliance obligations under Australian Privacy Principle 1.2. The department must measure and document its performance against its privacy management plan at least annually.

Before developing a PMP, every agency will need to understand the current state of their privacy practices. The department has developed this PMP with reference to the OAIC's Interactive PMP Explained resource for guidance on how to identified compliance gaps and opportunities to improve maturity.

What are the next steps?

This PMP describes the actions that the department must take in order to meet its privacy compliance obligations and maturity targets for the year following the PMP's commencement date (specified below). The department must take steps to achieve these actions and to record how it has done so.

This PMP should be kept up to date over the course of the year. In the recommended review period (specified below), the department should return to this PMP and use it to assess how well it has met and delivered its privacy targets.

The department should start the review process early enough to develop a strong PMP that can be endorsed by management and put into place by the start of the next year (for example, on 1 July). By completing this process in a timely way, the department will be best placed to highlight priority activities for the coming year to senior management and seek the resources it will need to undertake them.

About this PMP

Agency name	The Attorney-General's Department
PMP commencement date	11 December 2018
PMP end date	Following commencement, this PMP will operate until Thursday, 31 December 2019.
Recommended review period	1 October 2019 to 31 December 2019
PMP review date	1 October 2019

Privacy risk profile

In the course of preparing this PMP, the department has considered various matters relevant to its privacy risk profile. The details of these considerations are provided below for reference.

Privacy risk profile rationale

The department has a medium privacy risk profile. An agency with a medium risk profile provides some public services but handles less personal information, or which influences the privacy practices of other agencies.

The department collects and holds a broad range of personal information, including 'sensitive information', in records relating to:

- individuals participating in programs and initiatives
- the management of grants, contracts and funding agreements for both individuals and organisations
- Royal Commissions
- criminal matters and case work, including extradition and mutual assistance
- legal advice provided by internal and external lawyers, and
- employment and personnel matters for staff and contractors.

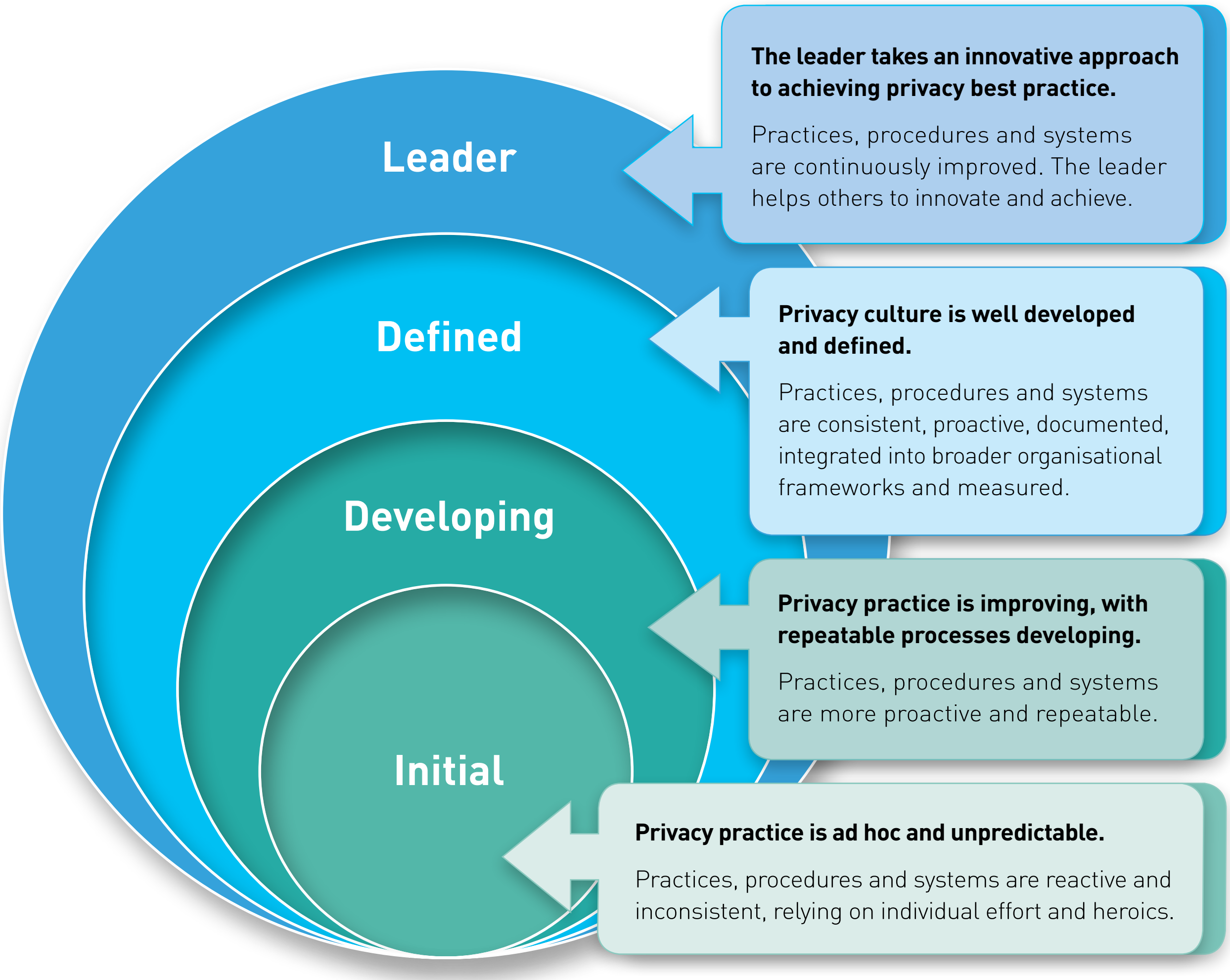
The department's role also involves influencing the privacy practices of other agencies. In particular, the department is responsible, on behalf of the Attorney-General, for administering several key pieces of legislation relevant to personal information. This includes:

- the *Privacy Act 1988*, which regulates the handling of personal information about individuals
- the *Public Interest Disclosure Act 2013*, which underpins the scheme to encourage and protect 'whistleblowers', and
- the *Freedom of Information Act 1982*, which facilitates access to government documents, but includes exemptions for certain documents, including to protect personal privacy.

The department is also routinely consulted on privacy policy implications of government policy proposals and draft legislation developed by other agencies.

Current state

The Maturity Framework requires the department 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*.

Privacy maturity assessment outcomes

This PMP has been prepared using an assessment of the department'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 department 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 department 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
Privacy Champion*	Developing	Leader	The department has a designated Privacy Champion.
Privacy Values	Developing	Defined	There is a connection between the department's values and respecting and protecting personal information. This connection is understood by staff. The department has information and resources relating to privacy on both the intranet and the internet. The department has also undertaken activities to enhance privacy awareness, such as holding a Privacy Awareness Week.
Privacy Officer*	Developing	Leader	The department has designated a Privacy Officer. The Privacy Officer is undertaking a review of the department's existing privacy practices, procedures and systems to ensure that they are integrated into broader departmental frameworks.
Management & Accountability	Developing	Defined	The department has assigned responsibility for privacy compliance and privacy management to a dedicated Privacy Unit. The Privacy Unit, which reports to the department's Privacy Officer, is responsible for handling enquiries and complaints, and responding to requests for access and correction. To ensure that privacy management and accountability are well understood across the department, the department will continue to build on these resources.
Awareness	Developing	Defined	Departmental staff view privacy as a positive and valuable part of business, and have knowledge of and access to departmental policies and expectations. The department is working to continue to build on staff awareness and a privacy culture.

Privacy Strategy			
Attribute	Current Level	Target Level (for current plan)	Rationale/Commentary
Privacy Management Plan*	Developing	Defined	The department has developed this PMP which includes measures for addressing any known privacy compliance gaps. In addition, the Privacy Unit is available to provide advice and respond to privacy related queries from a practical perspective. The department will continue to develop the PMP and will ensure senior management and staff are aware of the plan and its objectives.
Inventory of Personal Information*	Developing	Defined	The department collects, uses and discloses a range of personal information, including sensitive personal information. When collecting personal information, the department advises individuals of the possible uses of that information. Personal information is stored on the departmental Content Manager database, and access to individual documents and files is restricted to officers with a need to access or use that information. The department is in the process of developing an inventory of personal information it holds.
Data Quality Processes*	Developing	Defined	The department is taking steps to define the processes it uses to monitor and improve the quality of personal information it holds.
Information Security Processes	Developing	Defined	The department has a security-aware, and information security-aware culture. The department has policies regarding collection, access to, use and disclosure of personal and other types of information. The Privacy Unit and the Departmental Security Unit work together to promote privacy awareness and compliance.

Privacy Processes

Attribute	Current Level	Target Level (for current plan)	Rationale/Commentary
External Privacy Policy & Notices*	Developing	Defined	Privacy messaging is regarded as an important part of the department's operations. Areas that collect personal information provide privacy notices which comply with the Australian Privacy Principles and the Australian Government Agencies Privacy Code. Privacy information is available on the department's intranet and internet. Privacy standards that can be expected from the department and the reporting mechanism for the department's performance against these standards are outlined in its Client Service Charter.
Internal Policies & Procedures	Developing	Defined	The department will undertake a review of the existing privacy policies and procedures to ensure they are comprehensive, compliance focused and appropriately operationalised. The department will also take steps to improve awareness of, and compliance with, these policies and procedures.
Privacy Training*	Developing	Defined	Privacy training is included in mandatory annual security training. Training is generic, but provides an opportunity for staff to ask questions and seek clarification about specific issues. The Privacy Unit will investigate opportunities to raise awareness within the department.
Privacy Impact Assessments*	Developing	Defined	Privacy Impact Assessments (PIA) are prepared by line areas for projects that carry a privacy risk. Privacy assessment is also undertaken for all proposed legislative amendments. The Privacy Unit will investigate opportunities to raise awareness within the department of the tools available for those undertaking a PIA.

Privacy Processes *continued*

Attribute	Current Level	Target Level (for current plan)	Rationale/Commentary
Dealing with Suppliers	Developing	Defined	While some assessment is undertaken, there may be inconsistency across line areas. Third party contracts include confidentiality, secrecy and privacy requirements. The Privacy Unit will investigate options to raise the department's awareness of processes which can be applied consistently where a third party may have access to personal information through procurement processes.
Access & Correction*	Developing	Defined	The Privacy Unit is responsible for access and correction requests. The Privacy Unit is reviewing current processes and policies to ensure they are comprehensive and up to date. The department receives very few requests of this nature.
Complaints & Enquiries	Developing	Defined	Complaints and enquiries can be made through the External Feedback portal or direct to the Privacy Unit.

Risk & Assurance			
Attribute	Current Level	Target Level (for current plan)	Rationale/Commentary
Risk Identification & Assessment	Developing	Defined	Privacy compliance is integrated into a number of the department's systems, including emails (cannot be sent unless a Distribution Limiting Marker or security classification is applied) and documents (where the officer must select a privacy or security classification). In addition, line areas are encouraged to conduct a primary risk assessment where appropriate.
Reporting & Escalation	Developing	Defined	Reporting lines are clearly defined and mechanisms are in place to ensure the senior executive is briefed about privacy issues as they occur. Awareness of the department's reporting and escalation process will be achieved through raising awareness of the role of its Privacy Officer.
Assurance Model	Developing	Defined	The department undertakes appropriate action in response to incidents or breaches, which includes privacy controls (and changes as required in response to a breach), strategic oversight of privacy issues and internal audit.

Data Breach Response			
Attribute	Current Level	Target Level (for current plan)	Rationale/Commentary
Data Breach Response Plan	Developing	Defined	The department has identified preliminary processes to contain, assess, notify and prevent data breaches. The department has formalised these processes in its Data Breach Response Plan.
Data Breach Notification*	Developing	Leader	The department is committed to notification in response to all data breaches. The department is developing a plan to ensure consistent evaluation and assessment to determine whether notification is required under the legislation. Departmental officers understand and are focused on the importance of preventing harm to individuals and taking proactive steps to assist affected individuals.
Overall privacy maturity level (rounded down)			2 / 4 (Developing)

Goals for improvement

The privacy goals and targets in this section are based on the department's privacy maturity assessment outcomes. This section includes mandatory actions which the department must take in order to meet its compliance obligations under APP 1.2 (Code, s 9(2)(b)).

Compliance Actions

Where the department has identified in its privacy maturity assessment that it is at the 'Initial' level in relation to a compliance attribute, this indicates that there is a compliance gap because the department must have a minimum maturity level of 'Developing' for that attribute in order to comply with the Privacy Act or the Code. All compliance gaps must form part of this PMP and may require prompt remediation. Remediation actions are set out below.

Attribute	Remediation action	Responsible person, position or team	Due	Required resources, dependencies and/ or related documents (specify or link)
The department currently has a maturity level of Developing. As such there are no actions required for the department to be compliant under the Australian Government Agencies Privacy Code.				

Privacy Policy & Notices Actions

Remediation actions related to any gaps in the adequacy of the department's Privacy Policy (APP 1) or Privacy Notices (APP 5) are captured below.

Attribute	Remediation actions	Responsible person, position or team	Due	Required resources, dependencies and/ or related documents (specify or link)
The department currently meets its requirements to have a Privacy Policy under APP1 and relevant Privacy Notice under APP5 and the Australian Government Agencies Privacy Code.				

Maturity Improvement Actions

The table below sets out actions which the department plans to achieve in order to improve its privacy maturity. Any uncompleted actions from previous PMPs which are still relevant should also be documented in this section to ensure that they form part of the department's next PMP.

Element / Attribute	Action	Responsible person, position or team	Due	Required resources, dependencies and/ or related documents (specify or link)
Awareness raising	Undertake awareness activities to enable the department to reach its privacy target maturity levels.	Privacy Unit	Ongoing	Under Consideration
Data Breach Response Plan	The department has developed a plan to ensure consistent evaluation and assessment to determine whether notification is required under the legislation.	Privacy Unit	2018/19	nil
Inventory of Personal Information	The department will develop an inventory of personal information it holds.	Privacy Unit	2018/19	nil

Bringing the PMP together and prioritising actions

This section of the PMP identifies all compliance actions and actions for improvement, as well as who is responsible for delivery of each action, interdependencies and due dates. From here, prioritisation is a key part of establishing an achievable PMP. The department should take a risk-based approach to prioritising and timing their improvement activities.

Measure performance

It is expected that the department will review this PMP during the time in which it is active in order to document progress against the actions described above.

The table below provides a central location to track progress.

Action	Achieved	Future actions / commentary
The department will review the actions defined in this PMP on a continual basis and will update this table as required.		