Australian Government
Office of the Australian Information Commissioner

The Australian Government Agencies Privacy Code

Seminar

OAIC

Welcome to the seminar

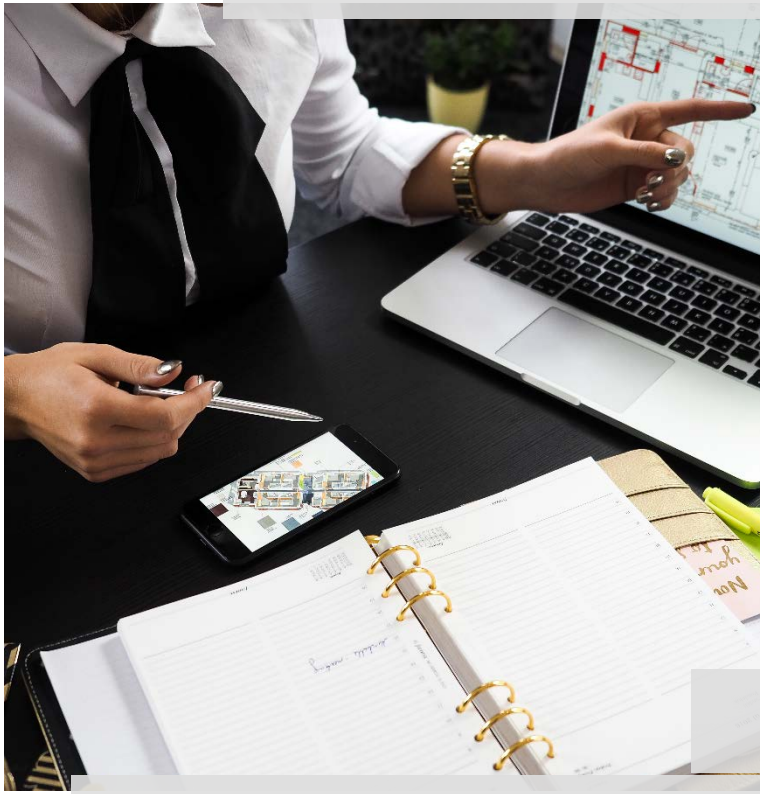
- Thank you to those that engaged with us in the development of the *Privacy (Australian Government Agencies — Governance) APP Code 2017* (Privacy Code)
- This event is an opportunity to showcase and discuss a variety of resources being developed to assist you with the implementation of the Code before 1 July 2018
- We will also be hearing from agency representatives on what action they currently take to meet some of the key privacy governance mechanisms formalised by the Code.

Privacy governance – supporting data innovation

- Demonstrating a commitment to transparency and accountability in personal information management is essential in realising the Australian Government's goals for data — because of the role this plays in building public trust in data use.

- Only 33% of Australians are comfortable with government agencies sharing personal information. 86% considered the secondary use of personal information as *misuse*

- However, there is the potential for broad public support for data use which promises a public benefit — where accountability and transparency in privacy protection is assured.



Building community confidence in data use – the Code requirements

- The 2017 Australian Community Attitudes to Privacy Survey found that the public sector was ranked third in net trustworthiness in personal information management – behind the health and financial sectors.

The Code requirements include:

- Having a privacy management plan
- The role of the Privacy Officer
- The role of a Privacy Champion
- Conducting a Privacy Impact Assessment (PIA) for ‘high privacy risk’ projects
- Keep a register of PIAs
- Privacy education or training for staff.

An ethos of privacy by design

- The Privacy Code supports compliance with Australian Privacy Principle (APP) 1.2, which requires entities to implement technical and organisational measures to demonstrate compliance with the Privacy Act

- The principles of the Act must be integrated throughout your agency – in other words, you must develop a culture of *privacy by design*
- The Code is a key tool in achieving this – and aligns with international expectations.

International expectations in privacy governance

- The Code requirements are mirrored in jurisdictions around the world
- The European Union's General Data Protection Regulation (GDPR) includes requirements to:
  - Have a Data Protection Officer (DPO)
  - Conduct Data Protection Impact Assessments (DPIA)
  - Train and educate staff on privacy matters
  - Review internal processes to ensure compliance
  - Report certain data breaches to affected individuals and supervisory authority.

Preparing for the Code's obligations

- Most of you will be well-prepared to implement the Code requirements. The resources we will present today will further assist you in implementing the Code:
  - The Privacy Self-Assessment Tool (PSAT) and Privacy Management Plan template
  - The Privacy Officer Toolkit
  - A self-assessment checklist
  - Privacy training.

Australian Government
Office of the Australian Information Commissioner

Implementing the Code: how the OAIC can help

Melanie Drayton
Assistant Commissioner, Regulation and Strategy

OAIC

Multi-faceted approach

- Australian Government Agencies Privacy Code checklist
- Privacy Officer toolkit
- Privacy Officer training
- Privacy Management Plan template
- Privacy Self-Assessment Tool
- Privacy eLearning course
- Privacy Impact Assessment resource
- Ongoing ‘community of practice’

Code checklist

Question	Y/N	Agency Details/documentation	OAIC Resources
1 – Privacy management plan (section 9 of Code)			
Does your agency have a privacy management plan?		*E.g. We have created a privacy management plan, available at [link].*	The OAIC has developed a Privacy Management Plan template and a Privacy Self-Assessment Tool, to assist agencies assess their current privacy practices and set privacy goals and targets to maintain or improve these practices.
Does your privacy management plan identify specific, measurable privacy goals and targets and set out how your agency will meet its compliance obligations under APP 1.2?		*E.g. We have used the OAIC's Privacy Self-Assessment Tool to identify our privacy goals and targets for the coming financial year. This has been incorporated into our privacy management plan.*	
2 – Privacy Officer (section 10 of Code)			
Does your agency have a Privacy Officer?		*E.g. The Privacy Officer in the Corporate Services Branch is our designated Privacy Officer.* *The Privacy Officer's duties and functions are outlined in a position description for the role, available at [link].*	The OAIC has developed a Privacy Officer Toolkit to assist Privacy Officers to understand and perform their responsibilities.
Has your agency advised the OAIC of your Privacy Officer and their contact details?		*E.g. On 6 December 2017, we advised the OAIC of the name and contact details of our Privacy Officer via email.*	

Privacy Officer toolkit

OAIC

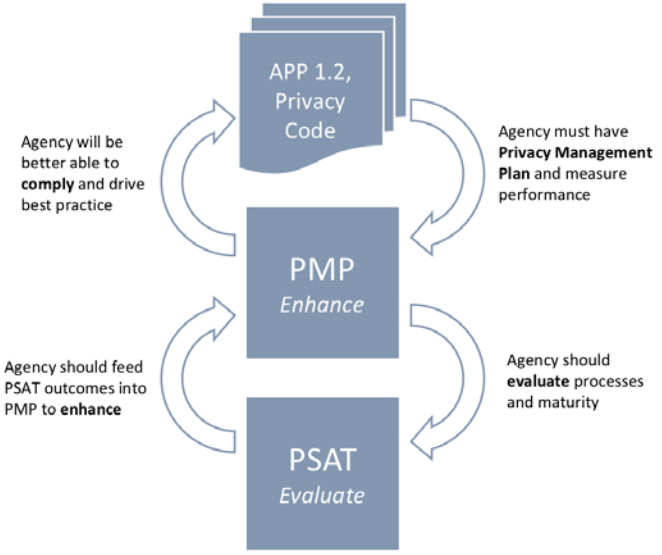
Privacy Management Plan (PMP)

- A Privacy Management Plan is a document that identifies specific, measurable privacy goals and targets and sets out how an agency will meet its compliance obligations under APP 1.2
- An agency must measure and document its performance against its PMP at least annually (Section 9 of the Code)

Using the PMP Template

Lifting Maturity – Privacy Self-Assessment Tool and Privacy Management Plan template

- Reduce the likelihood of mistakes that are embarrassing for the agency or harmful for individuals
- Create and embed a culture that respects people and treats personal information as a valuable asset
- Enhance the capability, efficiency and accountability of agencies through better privacy processes
- Build community trust and confidence through the personal information handling practices of agencies



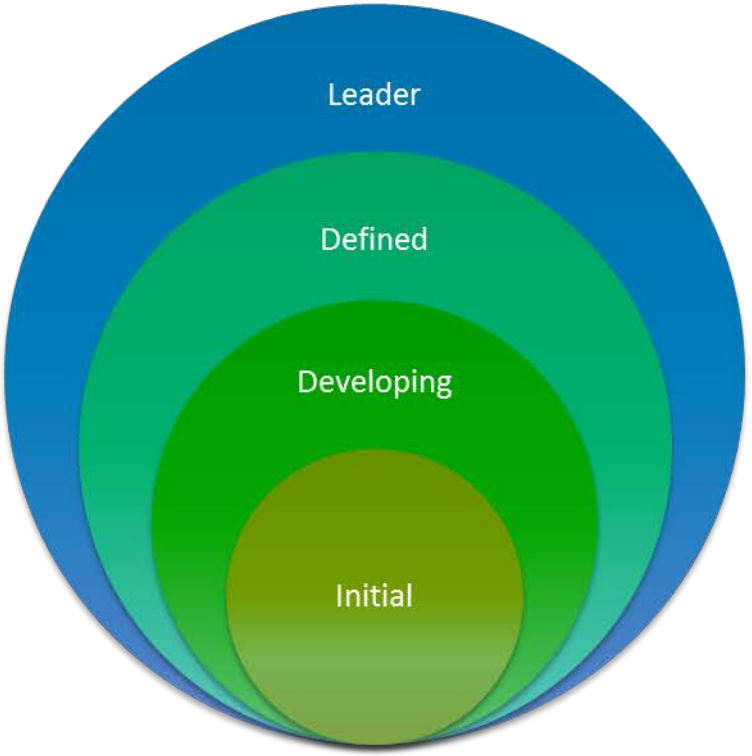
What is PSAT?

- Provides agencies with a way to assess the maturity of their privacy practices against objective criteria, with four maturity levels ranging from initial to leader
- Is simple and intended to support agencies to manage their privacy programs
- Encourages a scalable, risk-based approach to privacy
- Delivers consistency through benchmarks for compliance and improvement
- Is supportive. It can help you assess your agency's strengths and weaknesses and determine how best to lift your agency's privacy performance
- Will help you identify what should be included in your privacy management plan

A scalable, risk based approach

The starting point in using PSAT is to identify the level of privacy risk your agency faces and therefore what level of privacy maturity your agency should aspire towards.

Example: A small agency that collects very little personal information can aim for a lower maturity level than a large agency that provides complex public services to individuals.

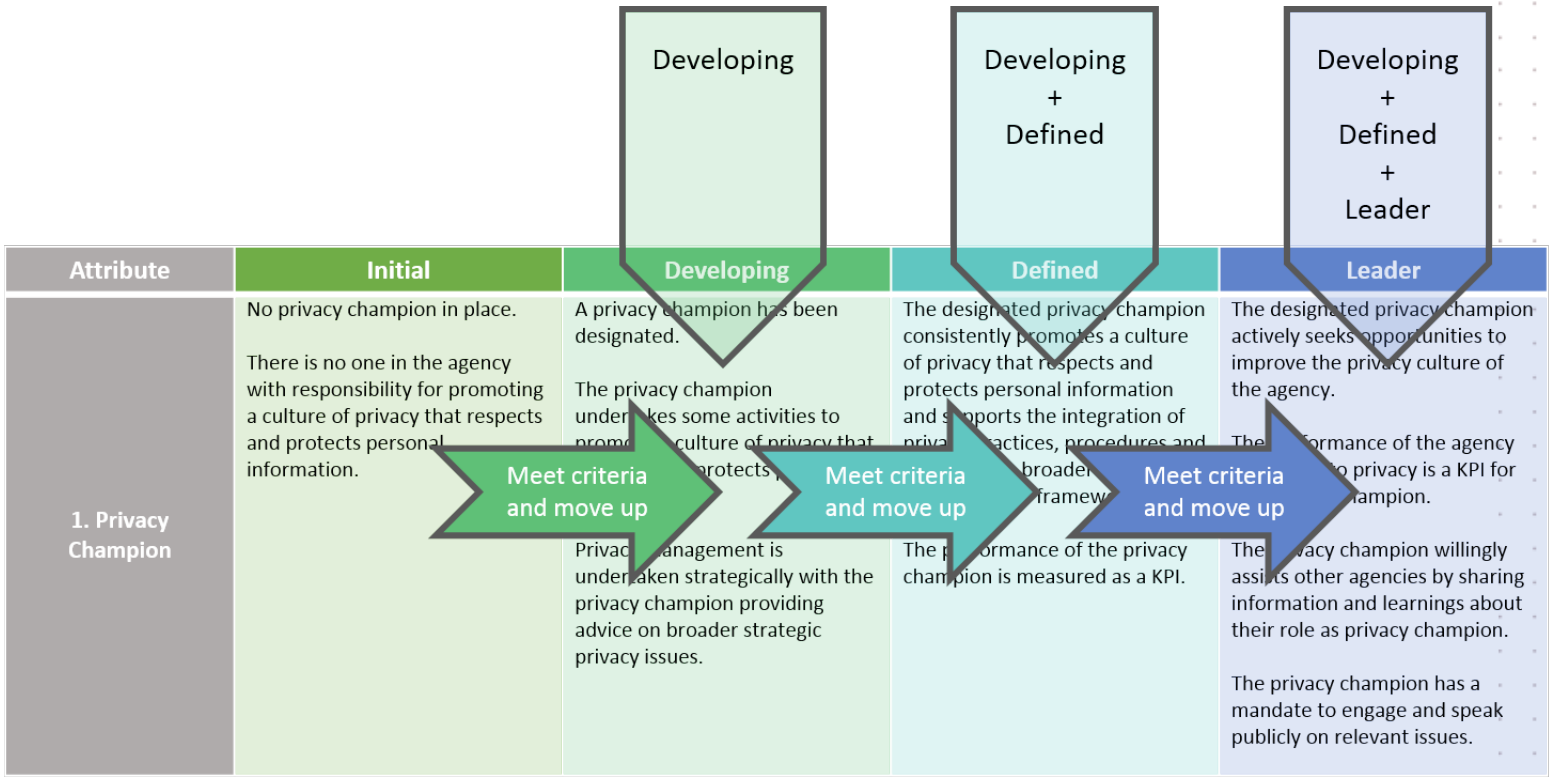


Measured against objective criteria

PSAT consists of five elements, each of which are critical tenets of good privacy practice.

Moving up the maturity scale

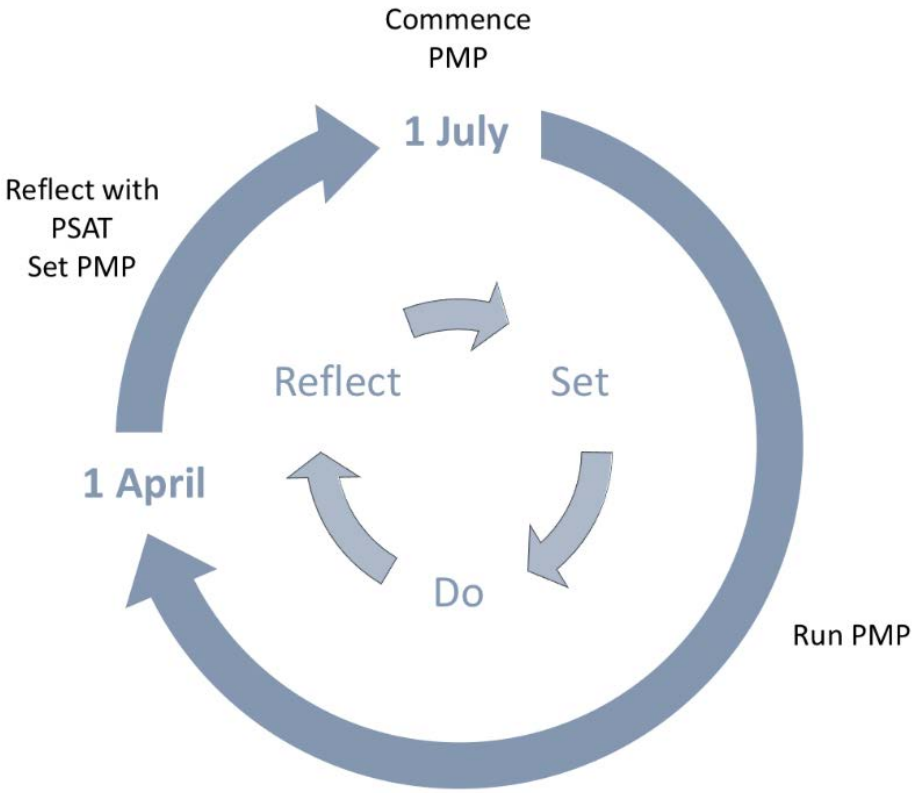
Maturity levels are cumulative. An agency will move to the next level when it has met the criteria for the level below.



Attribute	Initial	Developing	Defined	Leader
1. Privacy Champion	No privacy champion in place. There is no one in the agency with responsibility for promoting a culture of privacy that respects and protects personal information.	A privacy champion has been designated. The privacy champion undertakes some activities to promote a culture of privacy that protects personal information. Privacy management is undertaken strategically with the privacy champion providing advice on broader strategic privacy issues.	The designated privacy champion consistently promotes a culture of privacy that respects and protects personal information and supports the integration of privacy practices, procedures and broader framework. The performance of the privacy champion is measured as a KPI.	The designated privacy champion actively seeks opportunities to improve the privacy culture of the agency. The performance of the agency in relation to privacy is a KPI for the privacy champion. The privacy champion willingly assists other agencies by sharing information and learnings about their role as privacy champion. The privacy champion has a mandate to engage and speak publicly on relevant issues.

When to use PSAT and complete a PMP

- We recommend that all agencies complete the PSAT and PMP process in the last quarter of each financial year
- Your PMP can be based on your completed PSAT, which will help you to understand where gaps and opportunities lie and plan for the year ahead
- Your new PMP should commence with the new financial year



Still to come

- Privacy eLearning
- Privacy Officer training
- PSAT and PMP webinar
- Privacy Impact Assessment resource

Australian Government

Office of the Australian Information Commissioner

code@oaic.gov.au

www.oaic.gov.au/privacy-law/australian-government-agencies-privacy-code/

Australian Government

Office of the Australian Information Commissioner

Q&A

OAIC

Australian Government
Office of the Australian Information Commissioner

The Notifiable Data Breaches scheme

Andrew Solomon
Assistant Commissioner, Dispute Resolution

OAIC

Data breach notification — a community expectation

- Mandatory data breach reporting has been introduced across jurisdictions around the world

- This is because of the widespread community expectation for transparency when a data breach occurs which might have a serious impact on affected individuals

  - 95% of Australian already believe they should be told about data breaches affecting their personal information.

- The Notifiable Data Breaches (NDB) scheme therefore formalises existing community expectations — and in doing so, strengthens trust in data use over time.

‘Eligible data breaches’ under the NDB scheme

- An eligible data breach occurs when three criteria are met:
  - There is unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds
  - This is *likely to result in serious harm* to one or more individuals, and
  - The entity has not been able to prevent the likely risk of serious harm with remedial action.
- ‘Serious harm’ can be psychological, emotional, physical, reputational, or other forms of harm
- Understanding whether serious harm is likely or not requires an evaluation of the context of the data breach.

What to include in a statement to the Australian Information Commissioner

Your notification to the Australian Information Commissioner must be in the form of a statement, which includes the following information:

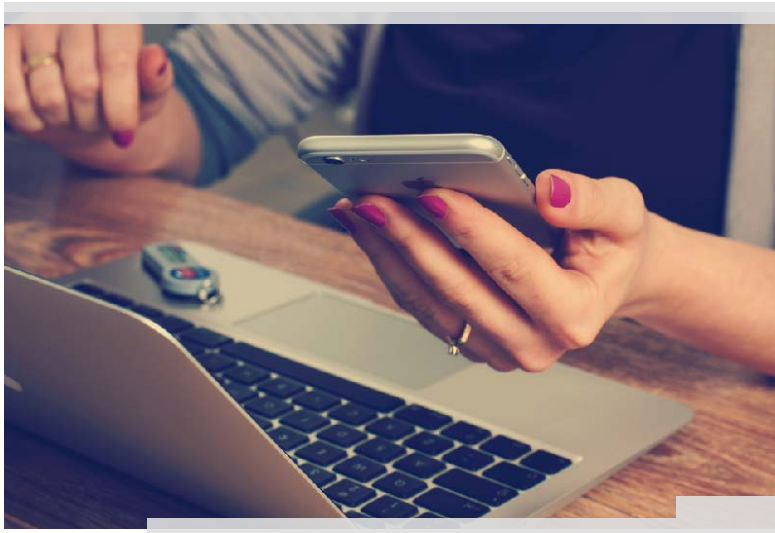
- The identity and contact details of you agency/organisation
- A description of the eligible data breach
- The kind or kinds of information involved in the eligible data breach
- What steps your agency/organisation recommends that individuals take in response to the eligible data breach.

Notifying affected individuals

You must notify any individuals that are at likely risk of serious harm as a result of a data breach.

There are three options for notification:

- Notify all individuals whose personal information is involved in the eligible data breach
- Notify only the individuals who are at likely risk of serious harm; or
- Publish your notification, and publicise it with the aim of bringing it to the attention of all individuals at likely risk of serious harm.



There is flexibility in the way you notify individuals.

If you suspect a data breach which may meet the threshold of ‘likely to result in serious harm’, you must conduct an assessment

- Generally, there is a maximum of 30 days to conduct this assessment. This begins from when you become aware of a potential breach
- Ahead of the NDB scheme, you should review your data breach response framework to ensure relevant personnel will be made aware of a breach as soon as practicable
- It is not expected that every data breach will require an assessment that takes 30 days to complete before notification occurs. You must notify as soon as practicable once you hold the belief an eligible data breach has occurred.

Visit: www.oaic.gov.au/ndb

Australian Government
Office of the Australian Information Commissioner

Panel discussion

- Andrew Rice, Attorney-General's Department
- Annette Musolino, Department of Human Services
- Lily Viertmann, Australian Bureau of Statistics
- Vidoshi Jana, Department of Immigration and Border Protection

Facilitated by Angelene Falk, Office of the Australian Information Commissioner

Australian Government
Office of the Australian Information Commissioner

Q&A

OAIC

Australian Government

Office of the Australian Information Commissioner

Thank you for attending.

OAIC