PRIVACY AWARENESS WEEK

15–21 MAY 2016

#2016PAW

www.oaic.gov.au/paw

Introduction to the Australian Privacy Principles & the OAIC's regulatory approach

Privacy Awareness Week 2016

Office of the Australian Information Commissioner (OAIC)

- Independent Australian Government statutory authority
- The Australian Privacy Commissioner and staff regulate Australia's *Privacy Act 1988*

What does the Privacy Act cover?

- Information privacy
- Australian Privacy Principles (APPs)
- Privacy Act contains provisions that deal with:
  - ‘personal information’
  - ‘sensitive information’ (such as health information)
  - tax file numbers
  - credit information
- Commissioner’s regulatory powers

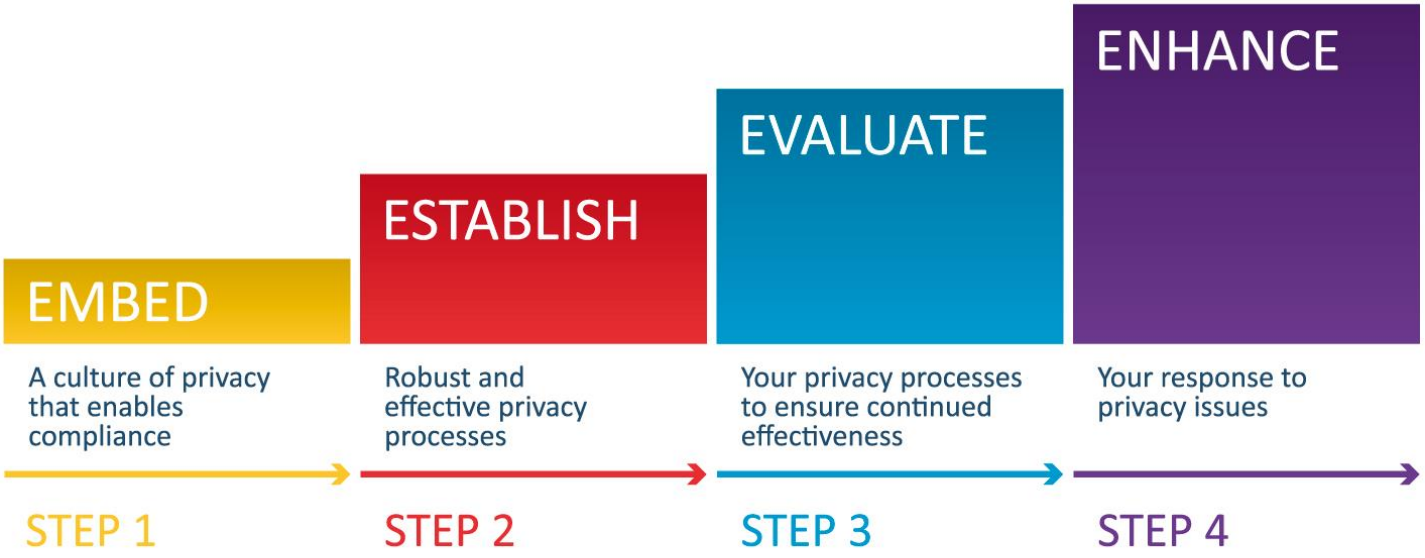
Australian Privacy Principles

- 13 APPs
  - Principles apply to government agencies and private sector organisations (referred to as 'APP entities')
  - Structured to reflect the information life cycle — planning, collection, use and disclosure, quality and security, access and correction
  - APP Guidelines

APP 1 — Open and transparent management of personal information

- Take reasonable steps to implement practices, procedures and systems to ensure compliance with APPs
- Privacy policies must be clearly expressed and up-to-date
- OAIC's *Guide to developing a privacy policy*

Privacy management framework



APP 2 — Anonymity and pseudonymity

- Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym
- Doesn’t apply if identification is required by law or it is impracticable

APP 3 — Collection of personal and sensitive information

- Covers collection of personal information and sensitive information
- Collection must be ‘reasonably necessary’ for one or more of an APP entity’s functions or activities
- Additional obligations apply to sensitive information

APP 4 — Dealing with unsolicited personal information

If an APP entity receives unsolicited personal information, it must:

- Assess whether it could have collected the information under APP 3
- If not, destroy or de-identify that information

But different rules apply to Commonwealth records

APP 5 — Notification of collection

- Outlines **what** an APP entity must tell an individual and **when**
- Includes:
  - Who the entity is and how to contact it
  - The purpose(s) of the collection
  - Usual disclosures to third parties
  - Complaint handling process
  - Likely overseas disclosure

APP 6 — Use or disclosure

Can only use or disclose personal information for:

- Purpose for which it was collected, or
- Secondary purpose if an exception applies

APP 7 — Direct Marketing

- Only use or disclose personal information for direct marketing purposes if certain conditions are met
- Opt-out option
- Direct marketing of sensitive information requires consent

APP 8 — Cross border disclosure

- Before disclosing personal information overseas, reasonable steps must be taken to ensure that the overseas recipient does not breach the APPs
- The APP entity will be accountable for a breach of the APPs by an overseas recipient
- Subject to exceptions
- OAIC's *Sending personal information overseas*

APP 9 — Adoption, use or disclosure of government related identifiers

- Prohibits an organisation from adopting, using or disclosing a government related identifier
- Number, letter, symbol used to identify an individual, e.g. Medicare #
- Exceptions include where the adoption, use or disclosure is required or authorised by law

APP 10 — Quality

- An APP entity must take reasonable steps to ensure personal information it collects, uses or discloses is:
  - accurate
  - up-to-date
  - complete
  - relevant
- Must also take reasonable steps to ensure that personal information is relevant for the purpose of the use or disclosure

APP 11 — Security

- Must take reasonable steps to protect personal information held from misuse, interference and loss, and from unauthorised access, modification or disclosure
- Obligation to destroy or de-identify personal information in certain circumstances
- OAIC's *Guide to securing personal information*

APP 12 — Access to personal information

- An APP entity must provide an individual with access to the personal information they hold about them, unless a specific exception applies

APP 13 — Correction of personal information

An APP entity must take reasonable steps to correct personal information to ensure it is accurate, up-to-date, complete, relevant and not misleading, if:

- the entity is satisfied it needs to be corrected, or
- the individual requests correction.

OAIC's regulatory powers

- Powers to:
  - Promote privacy compliance
  - Handle complaints and conduct investigations
  - Enforcement powers
- OAIC's *Privacy regulatory action policy*

Promoting privacy compliance

- Approve enforceable codes
  - Code obligations apply in addition to the APPs
  - Developed by entities (on their own initiative or on request) or by the Commissioner
- Privacy performance assessments
- Direct an agency to give the Commissioner a privacy impact assessment

Privacy impact assessment (PIA)

- A systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact
- Consider conducting PIAs as a matter of course for projects that involve personal information.
- OAIC's *Guide to undertaking privacy impact assessments*

Complaints and investigations

Privacy powers to investigate an alleged interference with privacy include powers to:

- investigate a matter following a complaint by an individual
  - Can decline a complaint for certain reasons, or refer to an alternative complaint body
  - Otherwise, must attempt to conciliate the complaint
- investigate on the Commissioner's own initiative (a ‘CII’)

Enforcement powers

Enforcement powers, that range from less serious to more serious, include powers to:

- Accept an enforceable undertaking
- Make a determination following a complaint or CII
- Bring proceedings to enforce a determination
- Apply to the court for an injunction
- Apply to the court for a civil penalty order for a breach of a civil penalty provision

Minimising complaints/investigations

- Create and implement privacy management plan
- Consult OAIC guidance
- PIA for new information handling practices
- Manage customer/client expectations
  - Clear APP privacy policy
  - Clear APP 5 notice
- Staff training and awareness — OAIC's *ten tips for protection customers' personal information*
- Robust IDR process
- Data breach notification — OAIC's *Data breach notification guide*

Need further information?

- Visit our website: www.oaic.gov.au
- OAIC resources
- Sign up for OAICnet newsletter via the website
- Follow us on Twitter @OAICgov

PRIVACY AWARENESS WEEK

15–21 MAY 2016

#2016PAW

www.oaic.gov.au/paw

www.oaic.gov.au/paw