Australian Government | TAX PRACTITIONERS BOARD

Privacy and securing personal information

Presented by Debra Anderson, Board member, Tax Practitioners Board

What we will cover today

- ✓ *Privacy Act 1988*
- ✓ What is personal information
- ✓ Information lifecycle
- ✓ Securing personal information
- ✓ Securing tax file numbers
- ✓ Notifiable Data Breaches Scheme
- ✓ Questions

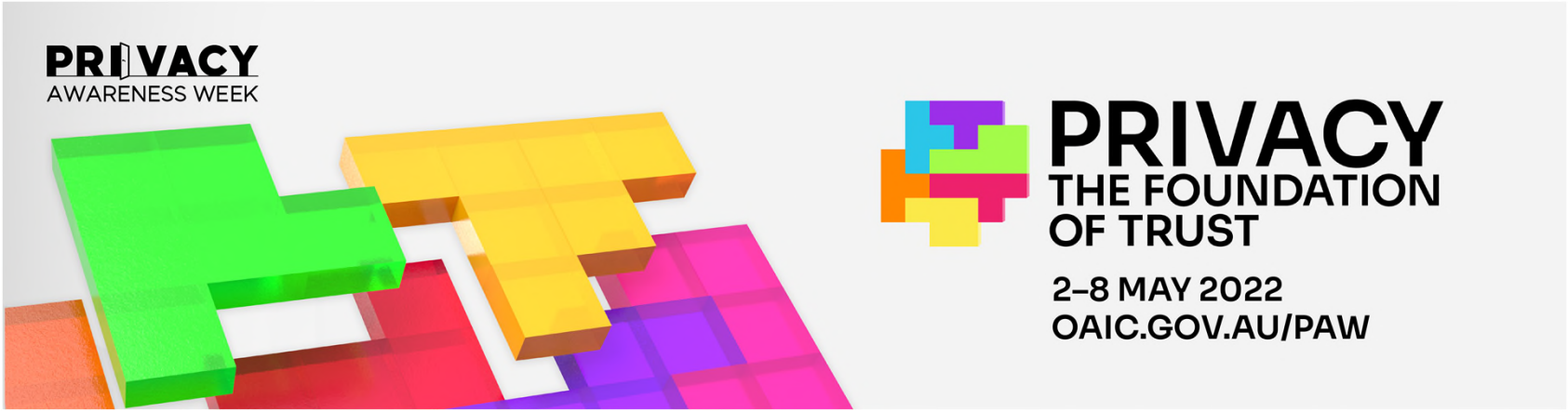
Access the presentation slides : tpb.gov.au/webinar-hub

Meet your presenter

- Debra Anderson
- Board Member
- Tax Practitioners Board

Privacy Awareness Week

- We are proud supporters of Privacy Awareness Week (PAW).
- PAW is an annual event to promote and raise awareness of the importance of protecting personal information.
- It is led by the Office of the Australian Information Commissioner (OAIC).



PRIVACY ACT 1988

Privacy Act 1988

- The *Privacy Act 1988* (Privacy Act) regulates how personal information is handled.
- The Privacy Act includes 13 Australian Privacy Principles (APPs).
- The Privacy Act also regulates the privacy component of:
  - the consumer credit reporting system
  - tax file numbers
  - health and medical research.

Privacy Act

Under the Privacy Act an APP entity must:

- Protect personal information from:
  - theft
  - misuse
  - interference
  - loss
  - unauthorised access
  - modification
  - disclosure.
- Take reasonable steps to destroy or de-identify personal information when it's no longer needed.

What is personal information?

- Personal information is any information where you can reasonably identify an individual.
- It doesn't matter if the information or opinion is true or what form it is recorded in.
- Personal information may include:
  - name
  - address and telephone number
  - date of birth
  - medical records
  - bank details
  - employment details
  - photos and videos.

Reasonably identifiable

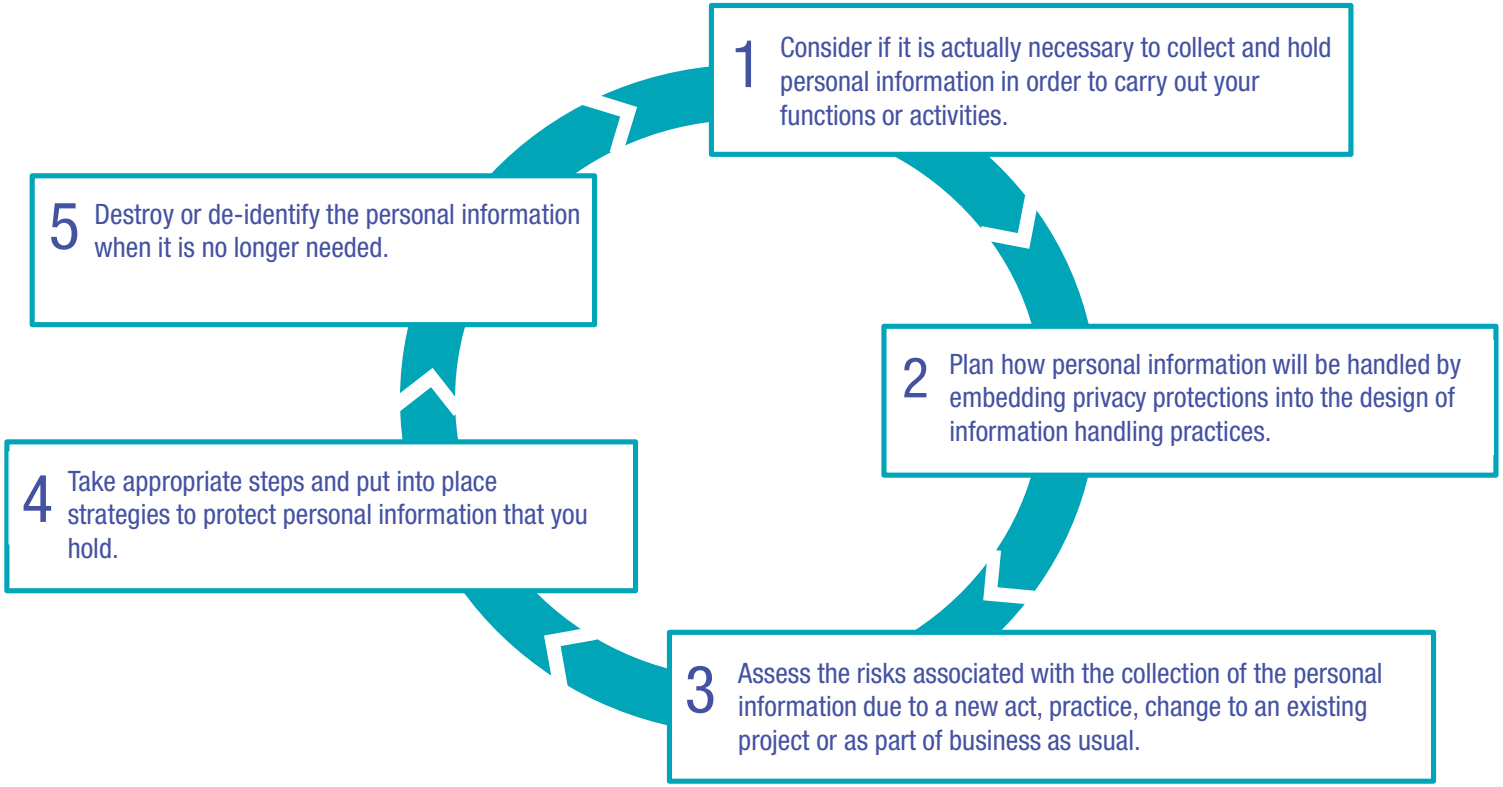
To determine if an individual is ‘reasonably identifiable’ will depend on:

- the nature and amount of information
- the circumstances of its receipt
- who will have access to the information
- other information either held or available
- whether it is possible for the individual or entity that holds the information to identify the individual
- if the information is publicly released.

INFORMATION LIFECYCLE

Information lifecycle

If you handle personal information, you must consider how you will:



1. Consider whether to collect personal information

- The first step in managing the security of personal information is to ask whether the collection of personal information is reasonably necessary to carry out your functions or activities.
- If it is, you should then consider if it should be collected.
- Personal information that is not collected or is not stored can’t be mishandled.

2. Privacy by design

- Privacy should be incorporated into your business planning, staff training, priorities, project objectives and design processes.
- You should design your personal information security measures with the aim to:
  - prevent the misuse, interference, loss or unauthorised accessing, modification or disclosure of personal information
  - detect privacy breaches
  - be ready to respond to potential privacy breaches in a timely and appropriate manner.
- An important element of ‘privacy by design’ is to integrate privacy into your risk management strategies.

3. Assessing the risks

- Assessing the security risks to personal information is also an important element of ‘privacy by design’.
- You can assess your personal information security risks by conducting:
  - a privacy impact assessment (PIA)
  - an information security risk assessment; and
  - regular reviews of your personal information security controls.

3. Assessing the risks

Privacy impact assessment

- A PIA is a written assessment that identifies the privacy impacts of a proposal and sets out recommendations for managing, minimising or eliminating those impacts.
- Generally, a PIA should:
  - describe the personal information flows in a proposal
  - analyse the possible privacy impacts of those flows
  - assess the impact on the privacy of individuals
  - explain how those impacts will be eliminated or minimised.
- A PIA can assist you to identify any personal information security risks and the reasonable steps you could take to protect it.

3. Assessing the risks

Information security risk assessment

- An information security risk assessment is generally more specific than a PIA.
- The findings of a PIA and information security risk assessment should inform the development of your risk management and information security policies, plans and procedures.
- Once the risks have been identified, you should then review your information security controls to determine if they are adequate in mitigating the risks.

3. Assessing the risks

Human error

- Threats to personal information can be internal or external as well as malicious or unintentional.
- Privacy breaches can arise as a result of human activity or events such as natural disasters.
- Human error is regularly claimed as the cause of privacy incidents – entities should assume human error will occur.
- PIAs, information security risk assessments and regular reviews will enable you to design practices, procedures and systems to deal with human error and minimise its effect.

4. Taking appropriate steps

- Once your entity has collected and holds personal information, you need to consider what appropriate security measures are required to protect the personal information.
- This will need to be considered for all of your entity's acts and practices.

Privacy breach example

- An investigation into a business found boxes of unsecured personal records being stored in a garden shed.
- The business advised the Privacy Commissioner that the records were transferred so that renovations of the business could occur.
- The garden shed door was locked with padlocks.
- The Commissioner found the business didn’t take reasonable steps to protect the personal information, some of which was also sensitive information.

5. Destroy or de-identify personal information

- Entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed.
- This requirement doesn't apply where the personal information is contained in a 'Commonwealth record' or where the entity is required by law or a court/tribunal order to retain the personal information.
- Destroying or permanently de-identifying personal information that you no longer need is an important risk mitigation strategy.

CIRCUMSTANCES THAT AFFECT ASSESSMENT OF REASONABLE STEPS

Circumstances that affect assessment of reasonable steps

- What qualifies as reasonable steps depends on the circumstances, including:
  - the nature of your entity
  - the amount and sensitivity of the personal information held
  - the possible adverse consequences for an individual in the case of a breach
  - the practical implications of implementing the security measure, including the time and cost involved.

TIPS TO PROTECT PERSONAL INFORMATION

Tips to protect personal information

Don’t leave privacy to chance

- Understand information handling processes and procedures.
- Only collect the information you need.
- Access personal information on a need-to-know basis.
- Keep personal information secure.
- Familiarise yourself with your data breach response plan.

TAX FILE NUMBER SECURITY

Tax file number security

- The TFN Rule regulates the:
  - collection
  - storage
  - use
  - disclosure
  - security; and
  - disposal of individuals' TFN information.

NOTIFIABLE DATA BREACHES SCHEME

Notifiable Data Breaches Scheme

- The Notifiable Data Breaches (NDB) scheme is an amendment to the *Privacy Act 1998*.
- It requires organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach.
- The notice must include recommendations about the steps to be taken.

Complying with the NDB scheme

- Have procedures for assessing a suspected breach.
- Ensure you have procedures and systems in place to secure a client's personal information.
- Be prepared to conduct quick assessments of suspected data breaches.
- Provide training to relevant employees.
- Keep up to date with developments.

What to do in the event of a data breach

If you have experienced a breach you should:

- contact the ATO on 1800 467 033
- advise any of your affected clients
- contact your software provider
- take steps to secure your information
- contact the Office of the Australian Information Commissioner (oaic.gov.au)

HELPFUL RESOURCES

Helpful resources

- The Australian Privacy Principles guidelines.
- The Privacy Regulatory Action Policy.
- Guide to undertaking privacy impact assessments.
- Data breach preparation and response — a guide to managing data breaches.
- Notifiable Data Breaches scheme resources.
- De-identification and the Privacy Act.
- Privacy fact sheet 6: Protecting your tax file number information.

Questions

Stay in touch


tpb.gov.au


tpb.gov.au/contact


1300 362 829
(Mon-Fri 9am-5pm AEST)


facebook.com/TPB.gov


linkedin.com/tax-practitioners-board


twitter.com/TPB_gov_au


youtube.com/TPBgov

Disclaimer

The information included in this webinar is intended as a general reference for users. The information does not constitute advice and should not be relied upon as such.

While the Tax Practitioners Board (TPB) makes every reasonable effort to ensure current and accurate information is included in this webinar, the TPB accepts no responsibility for the accuracy or completeness of any material contained in this webinar and recommends that users exercise their own skill and care with respect to its use.

Links to other websites may be referenced in this webinar for convenience and do not constitute endorsement of material on those sites, or any associated organisation, product or service.