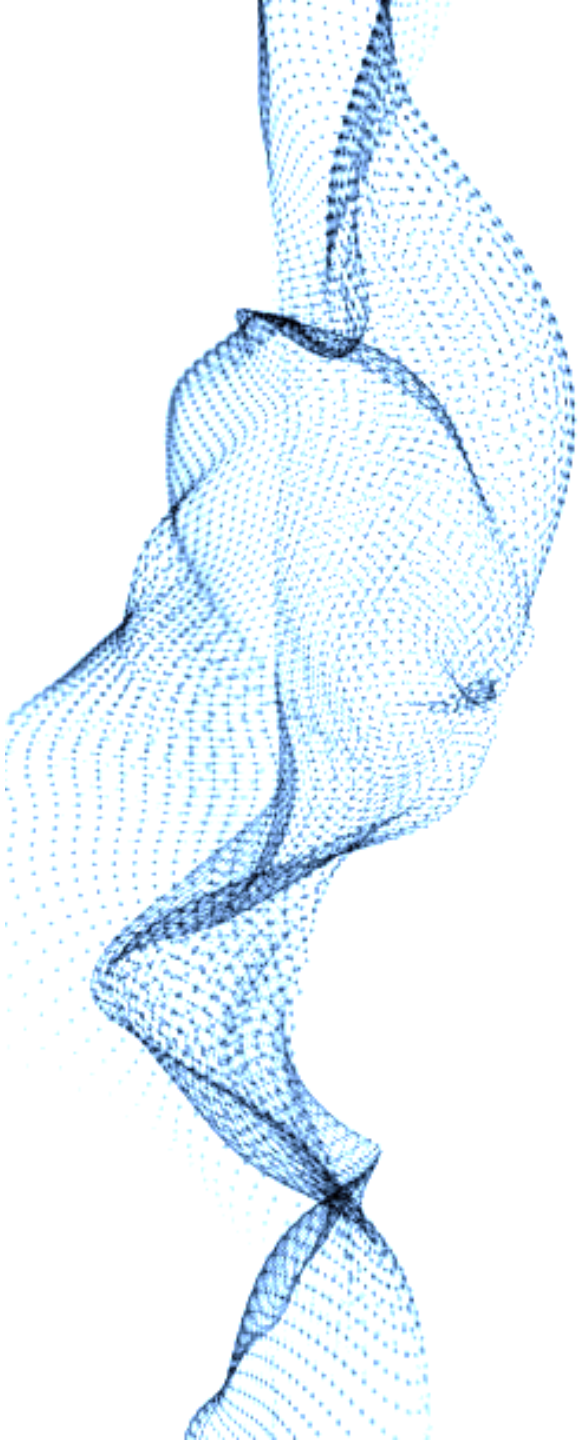
Understanding Privacy

Privacy risks

1. Over-retention of data
2. Secondary use of data
3. Cloud/Globalisation of data
4. Technologies that use data (eg ML/AI)
5. Modelling that uses PII data
6. Increasing digital basis to life (eg scope creep)
7. Lack of privacy by design (eg new products)
8. Lack of privacy compliance (eg existing products, new laws, new markets)
9. Undefined lawful basis for processing, assumption of rights by vendors



What is Privacy?

Rights and responsibilities

- ✓ Legal/regulatory obligations for organization's collecting data
- ✓ Rights to individuals to access their personal information

Information handling

- ✓ What, when, how, where, how for data processing and storage
- ✓ Standards for data governance and accountability for data protection

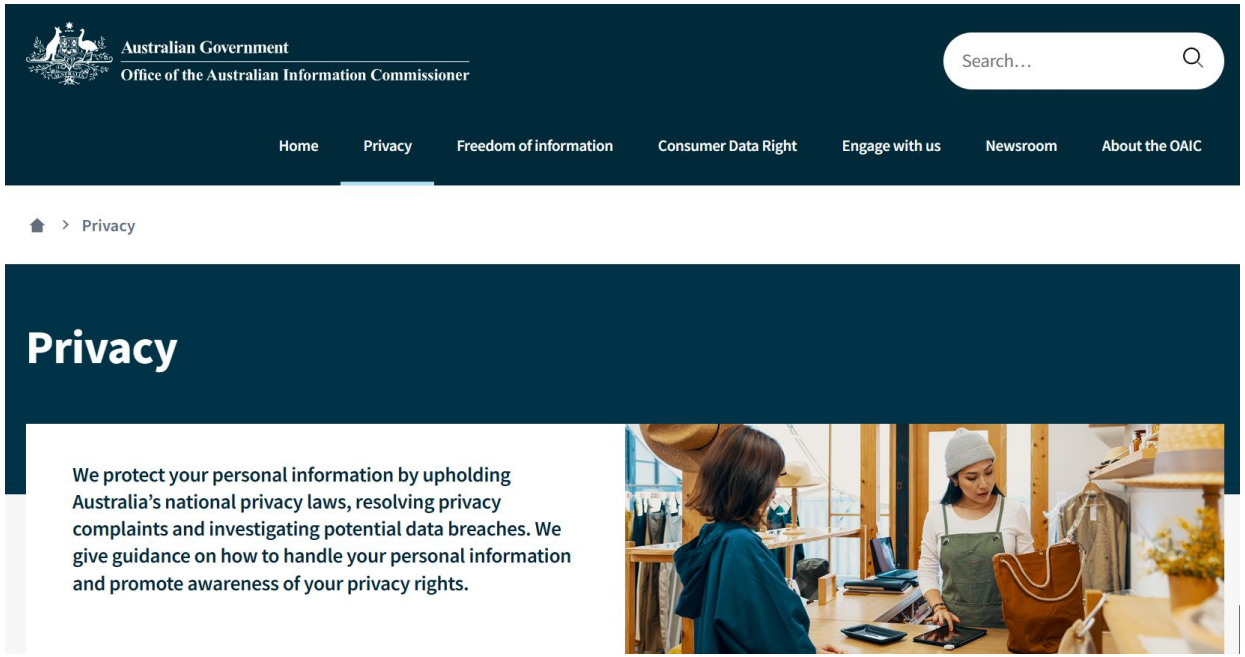
ough

Australian Legislation

Australia – Privacy Act

Privacy Act 1988 was introduced to promote and protect the privacy of individuals and to regulate how Australian Government, agencies and organisations handle personal information.

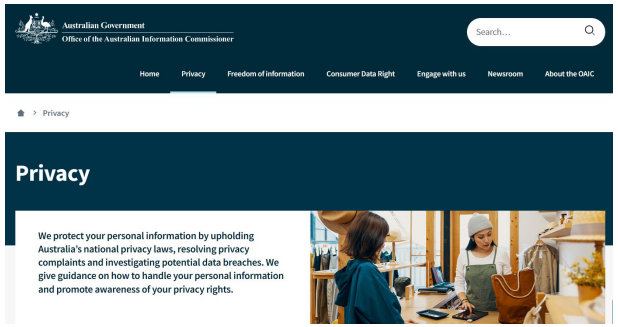
www.oaic.gov.au/privacy



Australia – Privacy legislation

- **Privacy Amendment (Enhancing Privacy Protection) Act 2012** introduced Australian Privacy Principles (APPs) and changes to the definition of "personal information" to include sensitive information such as health and financial information.
- **Privacy Amendment (Privacy Alerts) Act 2014** introduced mandatory data breach notification requirements for entities to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) of any serious data breaches.
- **Privacy Amendment (Notifiable Data Breaches) Act 2016** expanded the mandatory data breach notification requirements to apply to all entities covered by the Privacy Act, regardless of their size or turnover.
- **Privacy Amendment (Public Health Contact Information) Act 2020** introduced temporary amendments to the Privacy Act in response to the COVID-19 pandemic, allowing government entities and health officials to collect and use personal information for contact tracing purposes.

Australian Privacy Principles - Guidelines



www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines

- Chapter 1: APP 1 Open and transparent management of personal information →
- Chapter 2: APP 2 Anonymity and pseudonymity →
- Chapter 3: APP 3 Collection of solicited personal information →
- Chapter 4: APP 4 Dealing with unsolicited personal information →
- Chapter 5: APP 5 Notification of the collection of personal information →
- Chapter 6: APP 6 Use of disclosure of personal information →
- Chapter 7: APP 7 Direct marketing →
- Chapter 8: APP 8 Cross-border disclosure of personal information →
- Chapter 9: APP 9 Adoption, use or disclosure of government related identifiers →
- Chapter 10: APP 10 Quality of personal information →
- Chapter 11: APP 11 Security of personal information →
- Chapter 12: APP 12 Access to personal information →
- Chapter 13: APP 13 Correction of personal information →

Australian Privacy Principles

Principle	Title	Purpose
APP 1	Open and transparent management of personal information	Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.
APP 2	Anonymity and pseudonymity	Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.
APP 3	Collection of solicited personal information	Outlines when an APP entity can collect personal information that is solicited such as when reasonably necessary or directly related to the organisation's activities . It applies higher standards to the collection of sensitive information.
APP 4	Dealing with unsolicited personal information	Outlines how APP entities must deal with unsolicited personal information.

Australian Privacy Principles

Principle	Title	Purpose
APP 5	Notification of the collection of personal information	Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters.
APP 6	Use or disclosure of personal information	Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.
APP 7	Direct marketing	An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

Australian Privacy Principles

Principle	Title	Purpose
APP 8	Cross-border disclosure of personal information	Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.
APP 9	Adoption, use or disclosure of government related identifiers	Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.
APP 10	Quality of personal information	An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

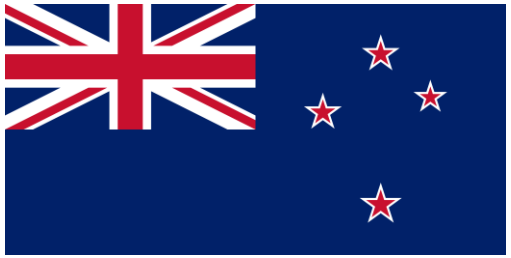
Australian Privacy Principles

Principle	Title	Purpose
APP 11	Security of personal information	An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from un-authorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.
APP 12	Access to personal information	Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.
APP 13	Correction of personal information	Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

International Legislation

European law - GDPR

1. General Data Protection Regulation 2018 covers personally identifiable information (PII)
2. Protects personal data and privacy of European citizens for transactions that occur in Europe or other countries (ie Internationally).
3. Affects all organisations that operate in, sell goods or monitor the behaviour of individuals in any European country.
4. Provide expanded rights for individuals to erase or object to data over and above Australian Privacy laws



New Zealand – Privacy laws

1. Recognises that an individual has the right to access their personal information held by a company or organisation.

2. Recognises the international privacy obligations including the OECD Guidelines and International Covenant on Civil and Political Rights.

Privacy Policies

Privacy policy elements

Purpose - describes the organization's policy regarding the personal information of all organization stakeholders in compliance with the law

Scope – lists stakeholders and personal information policy applies to

Applicable Legislation – specifies Privacy Act 1988, it's 13 Australian Privacy Principles and any regulations

Definitions – explains key terms

Responsibility – lists key stakeholders and their responsibilities

Policy Statement – outlines the policy

- Collection of personal information (sensitive information, method of collection, notification)
- Use and disclosure of personal information (direct and/or indirect marketing)
- Quality of personal information (unsolicited personal information)
- Security of personal information
- Transparency of information handling
- Access to and correction of personal information (access, correction, refusal, costs and charges),
- Unique identifiers, anonymity and pseudonymity
- Cross-border data flow

Communication – details steps undertaken such as announcements, notifications, publications, digital distribution

Implementation – details steps undertaken such as publication, inductions, training sessions


PROTECT
INFORMATION
SECURITY
CYBER
ONLINE
WEB
HACKER
ACCESS
SYSTEM
DATA BREACH
INTERNET
PASSWORD
THIEF
DATABASE
FRAUD
INFORMATION
CONFIDENCE
DIGITAL
ATTACK
01001001
HACKER
ACCESS
WEB

What is a data breach?

A data breach occurs when personal information (PII) held by an organisation is subject to un-authorised access or disclosure, or is lost

Eligible data breaches

Criteria 1 – Un-authorised access to personal information, un-authorised disclosure of personal information or loss of personal information has occurred:

- **Un-authorised access** – personal information is accessed by someone who is not permitted to have access. This may be an employee, an independent contractor or an external third party such as a hacker.
- **Un-authorised disclosure** – information is made accessible or visible to others outside the organization either intentionally or unintentionally.
- **Loss** – accidental or inadvertent loss of personal information, in circumstances where it is likely to result in un-authorised access or disclosure.

Eligible data breaches

Criteria 2 – The data breach is likely to result in serious harm to one or more individuals.

- **Serious harm** - includes serious physical, psychological, emotional, financial or reputational harm.

- Examples may include identity theft, significant financial loss by an individual, threats to an individual's physical safety, loss of business or employment opportunities, humiliation, damage to reputation or relationships, workplace or social bullying or marginalization.

arborough

Eligible data breaches

Criteria 3 – The organization with the data breach has not been able to prevent the likely risk of serious harm with remedial action.

- Note: If an organisaton takes remedial action but cannot prevent the likelihood of serious harm, this constitutes an eligible data breach.

Steps to take in a data breach

1. Take immediate steps to contain the data breach by limiting further access or distribution.

2. Notify individuals at likely risk of serious harm.

3. Notify the Office of the Australian Information Commissioner (OAIC) using the Notifiable Data Breach Form.

arborough

Notifiable Data Breach Form

The information you provide should include:

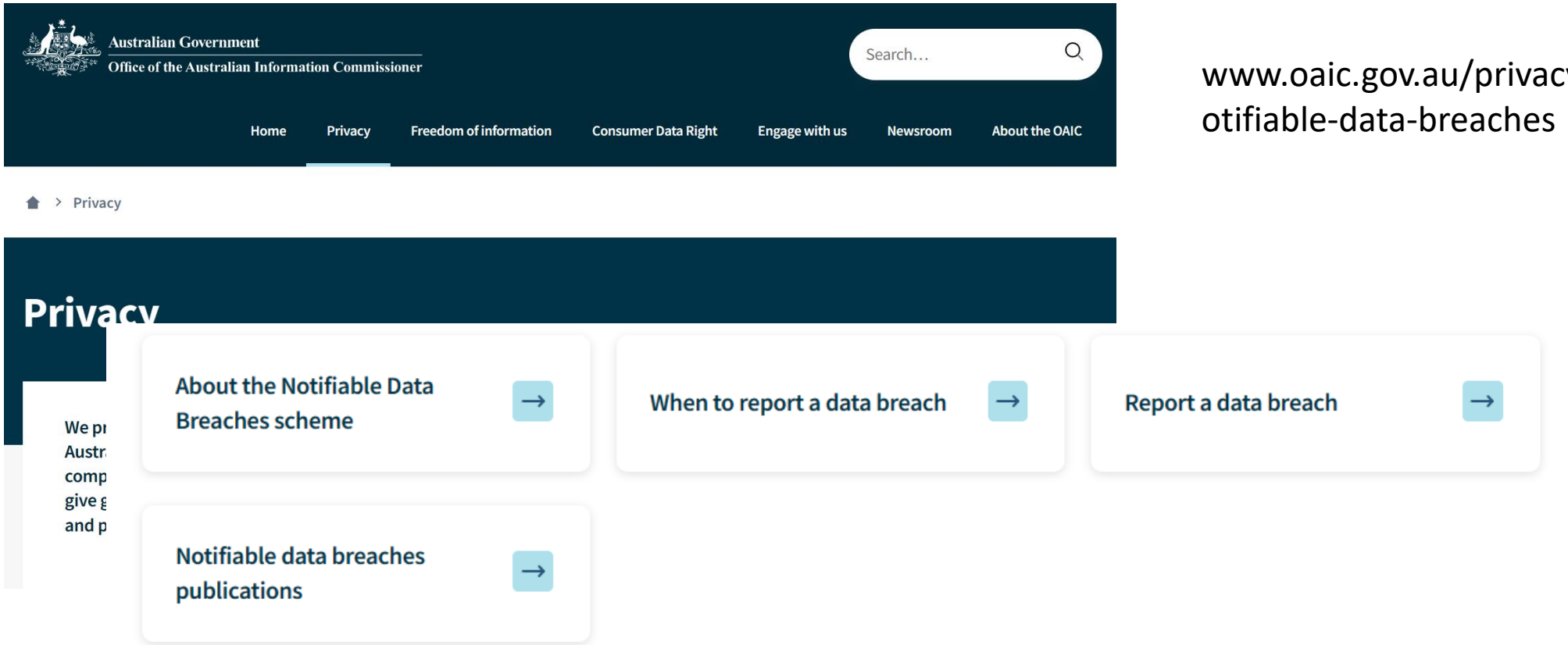
- Identity and contact details of the organisation
- Description of the data breach
- Kinds of information concerned
- Recommendations about the steps individuals should take in response to the data breach.

Consequences of Data Breaches

1. Loss of trust and diminished reputation is one consequence of data breaches.

2. Companies can be fined for data breaches. Enforces that a company has proper security in place to protect personal information.

Data Breach Guidelines



www.oaic.gov.au/privacy/notifiable-data-breaches

Any Questions?