Privacy guide

A guide to complying with privacy laws in Australia

Sep 2026

justice connect

Contents

Part 1 4

Introduction 5

Why privacy matters 5

Privacy laws in Australia 7

Recent privacy laws developments 8

Proposed reforms 8

Privacy and fundraising 9

Privacy and private ancillary funds 9

Part 2 10

Information protected by privacy laws 11

Personal information 11

Sensitive information 13

Health information 14

Other protected information 15

Part 3 16

When privacy laws apply 17

Sources of privacy law obligations 17

Australian Privacy Principles (APPs) 18

State and territory privacy laws 23

Health privacy laws 24

Part 4 26

Privacy obligations 27

Privacy policies 27

Rules for collecting information 29

Collecting personal information 29

Collecting sensitive and health information 30

© 2026 Justice Connect. This information was last updated in September 2026 and does not constitute legal advice, full disclaimer and copyright notice at www.nfplaw.org.au/disclaimer.

Collection notices 31
Consent 33
Unsolicited information 36
Storing and protecting information 37
Health information 40
Using and disclosing information 41
Automated Decision Making 43
Direct marketing 44
Access to and correcting personal information 46
Cross-border disclosure of personal information 48
Children's Online Privacy Code 50
Comparison of Commonwealth and State and Territory Privacy Principles 51
Part 5 **55**
Notifiable Data Breaches scheme 56
What the Notifiable Data Breaches scheme is 57
Organisations which must comply with the NDB scheme 57
What kind of data breaches require notification? 59
Unauthorised access, unauthorised disclosure and loss 59
The process for responding to data breaches 61
Step 1: Contain 62
Step 2: Assess 62
Step 3: Notify 67
Step 4: Review 71
Declaration of an eligible data breach by the Minister 73
Declaration of an emergency by the Minister 74
Part 6 **78**
Practical compliance tips and permitted situations 79
Practical compliance tips 79
Permitted situations 81
Part 7 **84**
Privacy enforcement, penalties and ongoing obligations 85
Regulatory action under the Privacy Act 85
Statutory tort for serious invasions of privacy 87
Doxxing offences 89
Ongoing privacy obligations 90

Part 1

Introduction

Introduction

This part covers:

- why privacy matters
- what this guide covers
- privacy laws affecting not-for-profit organisations
- recent privacy law developments
- privacy issues in fundraising
- privacy issues for private ancillary funds

This guide is for not-for-profit organisations in Australia that want to understand their obligations under privacy laws.

Disclaimer

This guide provides information on privacy laws for community organisations. This information is intended as a guide only and is not legal advice. If you or your organisation has a specific legal issue, you should seek legal advice before deciding what to do.

Please refer to the full disclaimer that applies to this guide.

Why privacy matters

Not-for-profit organisations often collect, use, store and disclose personal information about clients, service users, members, donors, employees, volunteers and other people. Privacy obligations can arise under legislation, funding agreements, service contracts and other arrangements.

Some of this information may be personal information, sensitive information or health information, all of which can attract additional legal protections.

Your organisation should consider privacy obligations whenever it:

- recruits and manages staff or volunteers
- delivers services
- raises funds
- communicates with members or supporters
- stores records
- uses cloud services or third-party software
- uses artificial intelligence tools, or
- responds to a data breach

© 2026 Justice Connect. This information was last updated in September 2026 and is not legal advice; full disclaimer and copyright notice at www.nfplaw.org.au/disclaimer.

Understanding your organisation's privacy obligations can help you handle personal information lawfully, transparently and respectfully, protect the people your organisation works with, reduce legal and regulatory risks, and maintain community trust.

Note – community expectations

The Office of the Australian Information Commissioner's (**OAIC**) *Australian Community Attitudes to Privacy Survey 2026* highlights the importance Australians place on privacy and their expectations that organisations will protect personal information and respond appropriately to privacy incidents.

Organisations should consider community expectations alongside their legal obligations.

Questions for your organisation

This guide will help your organisation consider:

- What information is protected by privacy laws?
- Which privacy laws apply to your organisation?
- What obligations apply when collecting, storing, using and disclosing personal information?
- Does your organisation need a privacy policy?
- What should you do if a data breach occurs?
- What practical steps can you take to improve privacy compliance?

About this guide

The guide has seven parts:

Part 1.	**Introduction**
Part 2.	**Information protected by privacy laws**
Part 3.	**When privacy laws apply**
Part 4.	**Privacy obligations**
Part 5.	**The Notifiable Data Breaches scheme**
Part 6.	**Practical compliance tips and permitted situations**
Part 7.	**Privacy enforcement, penalties and ongoing obligations**

Caution

Privacy laws can be complex and may apply differently depending on your organisation's structure, activities, contracts and the information it handles. You should seek legal advice for specific situations.

Privacy laws in Australia

Privacy regulation operates at both Commonwealth and state or territory level.

A not-for-profit organisation may need to comply with:

- the *Privacy Act 1988* (Cth), including the Australian Privacy Principles
- state and territory privacy legislation
- health privacy legislation
- privacy obligations under contracts or funding agreements

An organisation may need to comply with more than one set of privacy obligations at the same time.

The Commonwealth Privacy Act generally operates alongside state and territory privacy legislation rather than replacing it.

This guide describes obligations under the following legislation, collectively called **privacy laws**:

Privacy Laws
Commonwealth *Privacy Act 1988* (Cth) (**Privacy Act**) which includes the Australian Privacy Principles (**APPs**)
Australian Capital Territory *Information Privacy Act 2014* (ACT) *Health Records (Privacy and Access) Act 1997* (ACT)
New South Wales *Privacy and Personal Information Protection Act 1998* (NSW) *Government Information (Public Access) Act 2009* (NSW) *Health Records and Information Privacy Act 2002* (NSW)
Northern Territory *Information Act 2002* (NT)
Queensland *Information Privacy Act 2009* (QLD)
Tasmania *Personal Information Protection Act 2004* (Tas)
Victoria *Privacy and Data Protection Act 2014* (Vic) *Health Records Act 2001* (Vic)
Western Australia *Privacy and Responsible Information Sharing Act 2024* (WA) *Information Commissioner Act 2024* (WA)

South Australia doesn't currently have a legislative scheme for privacy law. But note, in South Australia an administrative direction on handling personal information binds the public service (PC012- Information Privacy Principles (**IPP**s) Instruction).

Recent privacy laws developments

Privacy law in Australia has changed significantly in recent years.

The *Privacy and Other Legislation Amendment Act 2024* (Cth), introduced a range of reforms, including:

Reform	Start date
Clarification that organisations must implement appropriate technical and organisational measures (reasonable steps) to protect personal information	In effect since **11 December 2024**
New OAIC enforcement powers and increased penalties	In effect since **11 December 2024**
A framework for recognising countries and binding schemes that provide privacy protections substantially similar to the APPs, to assist organisations disclosing personal information overseas	In effect since **11 December 2024.** Organisations should review current legislation and OAIC guidance to determine whether any countries or binding schemes have been recognised under the framework.
Criminal doxxing offences	In effect since **11 December 2024**
Statutory tort for serious invasions of privacy	In effect since **10 June 2025**
New transparency requirements for certain automated decision-making processes that require privacy policies to disclose information about the use of automated processes to make decisions	To start on **10 December 2026**
Children's Online Privacy Code framework	To be developed and registered by **10 December 2026**

Several of these reforms are discussed in more detail later in this guide.

Proposed reforms

The Australian Government is also considering further reforms to the Privacy Act.

Draft proposals released for consultation in 2026 include potential changes to:

- the definition of personal information
- rules governing the collection, use and disclosure of personal information
- direct marketing requirements
- data breach notification requirements
- data retention and destruction obligations
- information-handling practices, and
- certain individual privacy rights

These proposals have not been enacted and may change before any legislation is passed. This guide explains the law as it exists at the time of publication.

Privacy and fundraising

If your organisation is subject to privacy laws and collects, stores, uses or discloses personal information as part of its fundraising activities, it should ensure those activities comply with applicable privacy obligations.

When fundraising, organisations should:

- explain how personal information will be used
- tell people if their information may be shared with others
- provide opt-out mechanisms where required
- only use personal information for fundraising purposes where permitted by law

For information about the fundraising laws that apply in each state and territory see our fundraising resources

Privacy and private ancillary funds

Details of charities registered with the Australian Charities and Not-for-profits Commission (**ACNC**) can generally be viewed on the ACNC Register.

Because registration information can become publicly available, private ancillary funds should consider whether publication of donor information may reveal a donor's identity.

Note

If publication of information such as a donor's name, address, ABN, governing rules, annual information statement or financial reports is likely to identify a donor, the fund may be able to apply to have identifying information withheld under the *Australian Charities and Not-for-profits Commission Regulation 2013* (Cth).

Part 2

Information protected by privacy laws

Information protected by privacy laws

This part covers:

- personal information
- sensitive information
- health information
- other protected information

Privacy laws do not protect all information held by an organisation.

Instead, privacy laws focus on particular categories of information, especially information that relates to identifiable individuals.

Understanding what information is protected is an important first step in understanding your organisation's privacy obligations. Different rules may apply depending on the type of information involved.

This guide focuses on three important categories of information:

1.	**personal information**
2.	**sensitive information**
3.	**health information**

The way privacy laws apply to your organisation will depend on both the type of information involved and whether the relevant privacy laws apply to your organisation. Part 3 of this guide explains when privacy laws apply.

Personal information

Personal information is the foundation of Australian privacy law.

Many privacy obligations only arise if information falls within the legal definition of personal information.

What is personal information?

Under the Privacy Act, personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Personal information can be:

- true or false
- written, verbal, visual or electronic
- recorded or unrecorded

Personal information may include, a person's name, address, telephone number, email address, date of birth, photographs or video recordings where a person is identifiable, membership, donor, volunteer or client records, financial information, internet protocol (**IP**) addresses in some circumstances, online identifiers and location information, opinions about an identifiable person.

When is a person reasonably identifiable?

Whether someone is reasonably identifiable depends on the circumstances.

Relevant factors include:

- the nature and extent of the information
- how the information was obtained
- what other information is available to the organisation
- whether the information can realistically be linked to a particular individual.

Information that would not identify a person on its own may become personal information when combined with other information.

Example

A charity holds a database of membership numbers. The numbers alone may not identify individual members. However, because the charity can match the numbers with names in its membership records, the members are reasonably identifiable and the information is likely to be personal information.

Information about deceased people

Under the Privacy Act, information about a deceased person is generally not personal information.

However:

- some state and territory laws continue to protect certain information about deceased people, and
- information about a deceased person may also reveal information about a living person

For example, information about an inherited medical condition may constitute personal information about a living relative.

What is not personal information?

Personal information generally does not include:

- anonymous information
- aggregated information that does not identify individuals
- properly de-identified information that is not reasonably capable of re-identification
- information about a company or other organisation that does not identify an individual

Example

A not-for-profit publishes a report stating that 40% of survey respondents were volunteers and 60% were service users. If no individual can be identified from the data, the information is not personal information.

Practical examples

Photographs and videos can be personal information where a person is identifiable from the image or recording. Organisations should consider how photographs and videos are collected, used and published.

Personal information can include information collected through websites, applications and digital platforms, including some online identifiers and location information.

Tip

The definition of personal information is broad. If there is a realistic possibility that information could identify a person, directly or indirectly, it is prudent to treat the information as personal information unless you are confident it falls outside the definition.

Sensitive information

Sensitive information is a special category of personal information.

Because it can reveal particularly private aspects of a person's life, stricter privacy protections generally apply.

What is sensitive information?

Sensitive information includes information or an opinion about a person's:

- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual orientation, preferences or practices
- criminal record

Health information is also considered sensitive information under federal privacy law.

Certain biometric and genetic information may also constitute sensitive information.

Why does sensitive information matter?

Privacy laws generally impose stricter rules on the collection, use and disclosure of sensitive information.

For example, consent is often required before sensitive information can be collected, unless an exception applies.

Caution

Your organisation should identify whether information is personal information, sensitive information or health information before collecting it. Different legal requirements may apply to each category.

Health information

Health information is generally afforded a higher level of protection under Australian privacy laws.

What is health information?

Health information includes information or an opinion about a person's:

- physical health
- mental health
- disability
- future health needs or health preferences
- use of health services
- bodily donations
- genetics

Health information can relate to a person's past, present or future health.

Examples of health information may include:

- medical reports
- pathology results
- counselling records
- appointment records
- disability information
- prescriptions
- health care identifiers collected in connection with providing health services
- information collected to provide a health service

In some circumstances, information that would not ordinarily be considered health information becomes health information because of the context in which it is collected.

For example, a person's religion, sexuality or date of birth may constitute health information where it is collected as part of providing a health service.

Health privacy laws

In addition to the Privacy Act, specific health privacy legislation applies in:

- New South Wales
- Victoria
- the Australian Capital Territory

Part 3 of this guide explains when these laws may apply.

Tip

If your organisation provides health services or collects health information, consider whether Commonwealth, state or territory health privacy obligations apply. If you are unsure, consider obtaining legal advice.

Other protected information

Other categories of information may also be subject to specific legal protections.

This guide does not deal with these categories in detail.

Examples of other protected information may include:

- tax file number information
- credit information
- electoral roll information
- surveillance information
- certain criminal history information.

Tax file numbers

Special rules apply to tax file number information.

Organisations that collect or hold tax file numbers should ensure they understand the applicable legal requirements.

Credit information

Strict legal requirements apply to information about a person's credit history and creditworthiness.

Caution

If your organisation handles credit information, you should obtain legal advice. The legal requirements are complex and extend beyond the scope of this guide.

Part 3

When privacy laws apply

When privacy laws apply

This part of the guide covers:

- the main sources of privacy law obligations
- when the Australian Privacy Principles apply
- exemptions from the Australian Privacy Principles
- state and territory privacy laws
- health privacy laws

Once you have identified that your organisation collects, uses, stores or discloses personal information, the next step is to determine which privacy laws apply.

This part of the guide focuses on the three main sources of privacy law obligations that affect not-for-profit organisations.

Privacy-related obligations can also arise under funding agreements, government contracts and other arrangements. These obligations are discussed where relevant throughout this guide.

Caution

More than one privacy regime can apply at the same time. For example, an organisation providing services under a government contract may need to comply with both the APPs and applicable state or territory privacy laws.

Sources of privacy law obligations

A not-for-profit organisation may be required to comply with one or more privacy law regimes.

The three main sources of privacy law obligations are:	
Australian Privacy Principles (APPs) under the Privacy Act	The APPs are the privacy obligations contained in the Privacy Act. They regulate how organisations collect, use, disclose, store and secure personal information.
State and territory privacy laws	State and territory privacy laws generally apply to government agencies and public sector bodies. In some circumstances, they may also apply to organisations providing services to government or handling government information.
Health privacy laws	Additional privacy obligations apply to health information in some jurisdictions. These obligations may operate alongside the APPs and other privacy legislation.

Note

The federal privacy regime generally operates alongside state and territory privacy laws rather than replacing them. An organisation may need to comply with multiple privacy law regimes at the same time.

Australian Privacy Principles (APPs)

The APPs are the main privacy obligations under the Privacy Act.

If the APPs apply to your organisation, they regulate how your organisation collects, uses, stores, discloses and otherwise handles personal information.

Even if your organisation is not legally required to comply with the APPs, they provide a useful framework for good privacy practice.

You can read the full text of the APPs on the Office of the Australian Information Commissioner (**OAIC**) website.

When do the APPs apply?

The APPs do not apply to every not-for-profit organisation.

An organisation must comply with the APPs if it falls within one or more of the categories below.

An organisation must comply with the APPs if it:
• has an annual turnover of more than $3 million in any financial year since 2002
• provides a health service (even if providing a health service is not its primary activity)
• trades in personal information (for example, by buying or selling a mailing list)
• is a contracted service provider under a Commonwealth contract
• is a credit reporting body
• operates a residential tenancy database
• is a reporting entity for the purposes of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
• is an employee association registered or recognised under the *Fair Work (Registered Organisations) Act 2009* (Cth)
• conducts protected action ballots
• is a business prescribed by the *Privacy Regulation 2013*
• is related to a body corporate that meets one of the above criteria, or
• has voluntarily opted into the Privacy Act

Annual turnover

Many not-for-profit organisations determine whether the APPs apply by reference to annual turnover.

As a general rule, organisations with annual turnover exceeding $3 million must comply with the APPs.

Health services

An organisation may be required to comply with the APPs even if its annual turnover is less than $3 million if it provides a health service.

The concept of a health service is broad and may extend beyond traditional medical treatment.

Depending on the circumstances, organisations providing counselling, disability support, rehabilitation programs, wellbeing services, childcare services or other health-related services may be providing a health service.

Commonwealth contracts

Organisations providing services under Commonwealth Government contracts may be required to comply with the APPs even where they would otherwise be exempt.

Privacy obligations may also arise under funding agreements, service agreements and other contractual arrangements, regardless of whether the Privacy Act applies directly.

Trading in personal information

The APPs apply where an organisation trades in personal information.

This may occur where personal information is bought, sold or exchanged for a benefit.

The Office of the Australian Information Commissioner (**OAIC**) has published a checklist to help you decide if your small business must comply with the Privacy Act

Note – organisation

The term 'organisation' is defined broadly under the Privacy Act and includes bodies corporate, partnerships, trusts and other unincorporated associations.

Not-for-profit organisations structured as trusts, unincorporated associations, incorporated associations, co-operatives, companies limited by guarantee and Indigenous corporations can all fall within the definition.

Organisations that are not otherwise covered by the APPs may choose to opt into the Privacy Act. Once they do so, they are generally treated as an organisation for the purposes of the Privacy Act.

For more information on opting in and out see the Office of the Australian Information Commissioner (**OAIC**)'s website.

What are the APPs?

The APPs establish standards for how organisations handle personal information.

The APPs are summarised below.

APP	Subject
APP 1	**Open and transparent management of personal information.** Requires APP entities to manage personal information in an open and transparent way.
APP 2	**Anonymity and pseudonymity.** Requires individuals to have the option of not identifying themselves, or of using a pseudonym, in appropriate circumstances.

APP 3	**Collection of solicited personal information.** Regulates when personal information may be collected.
APP 4	**Dealing with unsolicited personal information.** Regulates how organisations deal with personal information they receive without requesting it.
APP 5	**Notification of the collection of personal information.** Requires organisations to notify individuals about certain matters when collecting personal information.
APP 6	**Use or disclosure of personal information.** Limits the circumstances in which personal information may be used or disclosed.
APP 7	**Direct marketing.** Regulates the use and disclosure of personal information for direct marketing purposes.
APP 8	**Cross-border disclosure of personal information.** Regulates disclosure of personal information to overseas recipients.
APP 9	**Adoption, use or disclosure of government related identifiers.** Restricts use of identifiers such as Medicare numbers and passport numbers.
APP 10	**Quality of personal information.** Requires reasonable steps to ensure personal information is accurate, up-to-date and complete.
APP 11	**Security of personal information.** Requires reasonable steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure.
APP 12	**Access to personal information.** Gives individuals a right to access personal information held about them, subject to limited exceptions.
APP 13	**Correction of personal information.** Requires organisations to correct personal information in certain circumstances.

The APPs are discussed in more detail throughout this guide.

Examples of when the APPs apply

Example 1: organisation with annual turnover above $3 million

You run a charity that recorded annual turnover of more than $3 million in its most recent financial year. **The APPs apply.**

Example 2: sponsorship arrangement

You run a theatre company with annual turnover below $3 million. As part of a sponsorship arrangement, you provide a customer or supporter list to a sponsor organisation. **The APPs apply.**

Example 3: Commonwealth-funded services

You run a not-for-profit organisation with annual turnover below $3 million that delivers services under a Commonwealth Government funding contract. **The APPs apply** in relation to information handled under that contract.

Examples of when the APPs may apply

Example 1: sporting club

You run a sporting club with annual turnover below $3 million. The club operates programs and facilities designed to improve members' fitness and health. Depending on the circumstances, the club may be providing a health service. **The APPs may apply.**

Example 2: disability support organisation

You run a not-for-profit organisation with annual turnover below $3 million that collects information about disabilities, diagnoses and medical needs in order to provide support services. **The APPs may apply** because the organisation may be providing a health service.

Example 3: related body corporate

You are part of a group structure and your organisation is related to a body corporate that is required to comply with the APPs.

The APPs may apply, even if your organisation's annual turnover is less than $3 million.

Example of when the APPs don't apply

You run a local sporting club that collects participants' names and contact details and has annual turnover of $120,000. Provided none of the other criteria apply, **the APPs will generally not apply.**

Exemptions to the APPs

Even where the APPs would otherwise apply, exemptions may apply in some circumstances.

The exemptions discussed below are those most likely to be relevant to not-for-profit organisations.

Caution

Exemptions are often narrower than organisations expect. An exemption from the APPs does not necessarily mean there are no privacy obligations. State and territory privacy laws, contractual obligations, health privacy laws and other legal duties may still apply.

Employee records exemptions

The employee records exemption applies where:

- information forms part of an employee record, and
- the organisation's handling of that information is directly related to a current or former employment relationship

The exemption does not generally apply to volunteers, contractors, unsuccessful job applicants, or employees of related entities.

The exemption means that some activities involving employee records are not regulated by the APPs.

However, it does **not** create a general exemption from privacy obligations. State and territory privacy laws may still apply to some employee information, particularly health information.

The exemption also does not apply to the statutory tort for serious invasions of privacy, or criminal doxxing offences.

Example

A prospective employer contacts your organisation seeking information about a former employee.

Information forming part of the employee's employment record may fall within the employee records exemption. However, information outside the employment record, or information unrelated to the employment relationship, may not be covered by the exemption.

Caution

Employee records that are exempt from the APPs may be subject to special requirements under the *Fair Work Act 2009* (Cth). If you are not sure about your obligations in handling employee records, you should get legal advice.

Commonwealth contract exemption

An organisation may become subject to the APPs because it provides services under a Commonwealth Government contract.

Where this is the only reason the APPs apply, the organisation may only be required to comply with the APPs in relation to activities connected with that contract.

Example

A not-for-profit organisation with annual turnover below $3 million provides:

- a privately funded youth program, and
- services under a Commonwealth Government funding contract

The APPs may apply to information handled under the Commonwealth-funded program, but not necessarily to information handled under the privately funded program.

If information is handled across both programs, the position can become more complex and legal advice may be required.

Political exemption

Work carried out on behalf of a registered political party or political representative may be exempt where the activity relates to an election, a referendum, participation in the political process, or activities connected with those purposes.

This exemption is unlikely to apply to most not-for-profit organisations.

Other exemptions

Other exemptions exist under the Privacy Act, including exemptions that apply in limited circumstances to:

- journalists and media organisations
- local councils and state or territory government agencies
- some information sharing between related organisations

These exemptions are generally less relevant to community organisations and are not discussed in detail in this guide.

Caution

If your organisation intends to rely on an exemption, consider obtaining legal advice. Exemptions can be complex and may apply differently depending on the circumstances.

State and territory privacy laws

The APPs are not the only privacy laws that may affect a not-for-profit organisation.

Each Australian state and territory has its own privacy regime, although the nature and scope of those regimes differ.

State and territory privacy laws generally apply to government agencies and public sector organisations, including government departments, local councils, courts and police services. In some circumstances, they may also apply to organisations that provide services to government or handle government information under a contract or other arrangement.

If your organisation provides services to a state or territory government agency, you should review the relevant contract carefully to determine whether state or territory privacy obligations apply.

State and territory Information Protection Principles (IPPs)	
ACT	*Information Privacy Act 2014* (ACT) sets out 13 Territory Privacy Principles (**TPP**) in Schedule 1
NSW	*Privacy and Personal Information Protection Act 1998* (NSW) sets out 12 Information Protection Principles (New South Wales IPPs) in Part 2, Division 1
NT	*Information Act 2002* (NT) sets out 10 Information Privacy Principles in Schedule 2
Qld	*Information Privacy Act 2009* (QLD) sets out 13 Queensland Privacy Principles (**QPP**) in Schedule 3
SA	Part II of the administrative instruction, PC012 – Information Privacy Principles Instruction provides a set of Information Privacy Principles
Tas	*Personal Information Protection Act 2004* (Tas) sets out 10 Personal Information Protection Principles in Schedule 1
Vic	*Privacy and Data Protection Act 2014* (Vic) sets out 10 Information Privacy Principles in Schedule 1
WA	*Privacy and Responsible Information Sharing Act 2024* (WA) sets out 11 Information Privacy Principles in Schedule 1. Some rights relating to access and correction of information are dealt with under the *Freedom of Information Act 1992* (WA)

Caution

State and territory privacy laws operate alongside the Commonwealth privacy regime. Compliance with the APPs does not necessarily mean that your organisation has satisfied all state or territory privacy obligations.

Health privacy laws

NSW, Victoria and the ACT each have their own specific Health Privacy Laws:	
ACT	*Health Records (Privacy and Access) Act 1997* (ACT)
NSW	*Health Records and Information Privacy Act 2002* (NSW)
Vic	*Health Records Act 2001* (Vic)

Your organisation may need to comply with health privacy legislation, in addition to any obligations under the Privacy Act, if it operates in the ACT, New South Wales or Victoria and:

- provides a health service, or
- collects, holds or uses health information

These requirements may apply even where health services are not the organisation's primary activity.

Health service providers

The concept of a health service provider is broad and extends beyond hospitals and medical practices.

Depending on the circumstances, a health service provider may include:

- public and private hospitals
- medical practitioners
- pharmacists
- allied health professionals
- mental health professionals
- counsellors
- disability support services
- complementary therapists, including naturopaths and chiropractors
- gyms and weight-management services
- childcare centres
- private schools

If your organisation collects, holds or uses health information, you should consider whether additional health privacy obligations may apply.

Tip

Organisations often underestimate the breadth of activities that may constitute a health service. If there is uncertainty about whether your organisation provides a health service, consider obtaining legal advice.

Examples of when health privacy laws apply

Example 1

Your organisation is contracted to provide health services within Victoria's publicly managed prison system. **The applicable health privacy legislation will apply**.

Example 2

Your organisation operates a supervised injecting facility and records the names of people using the service. **The applicable health privacy legislation is likely to apply.**

Example of when health privacy laws don’t apply

Your organisation provides basic first aid at music festivals on a completely anonymous basis and does not collect or retain personal information about the people receiving assistance. **The health privacy legislation is unlikely to apply.**

Part 4

Privacy obligations

Privacy obligations

This part of the guide covers:

- privacy policies and collection notices
- collecting, using and protecting personal information
- consent and direct marketing
- access to and correction of personal information
- overseas disclosure of personal information
- emerging privacy obligations, including automated decision-making and children's online privacy protections

If your organisation collects, holds, uses or discloses personal, sensitive or health information, and privacy laws apply to your organisation, you need to understand the obligations that apply to that information.

The Australian Privacy Principles (**APPs**) establish the core privacy obligations under the *Privacy Act* 1988 (Cth) (**Privacy Act**). They set the minimum standards for handling personal information at the Commonwealth level and regulate how organisations collect, use, store, disclose, secure and manage personal information.

Many state and territory privacy regimes contain similar principles, although there are differences. A comparison of the Commonwealth and state and territory privacy principles is included later in this part of the guide.

This part of the guide explains the practical obligations most commonly encountered by not-for-profit organisations, including privacy policies, collection notices, consent, information security, direct marketing, access requests and cross-border disclosure.

Privacy policies

If the APPs apply to your organisation, you must have a clearly expressed and up-to-date privacy policy.

A privacy policy explains how your organisation handles personal information. It demonstrates transparency and helps individuals understand what information your organisation collects, how it is used and what rights they have in relation to that information.

Under APP 1, your organisation must take reasonable steps to make its privacy policy available free of charge and in an appropriate form. In practice, this usually means publishing the policy on your organisation's website and providing it on request.

What must a privacy policy include?

A privacy policy must include information about:	
• the kinds of personal information your organisation collects and holds	☐
• how your organisation collects and holds personal information	☐

• the purposes for which the information is collected, held, used and disclosed	☐
• how an individual may access personal information held about them	☐
• how an individual may seek correction of personal information held about them	☐
• how an individual may make a complaint about a breach of the APPs or an applicable privacy code and how your organisation will deal with that complaint	☐
• whether your organisation is likely to disclose personal information to overseas recipients, and	☐
• if practical, the countries in which those overseas recipients are likely to be located	☐

Additional information the OAIC encourages organisations to include

The OAIC also encourages organisations to consider including information about:

- categories of individuals whose personal information is collected and retained
- practices relating to children and other vulnerable individuals
- who may access personal information and under what circumstances
- any exemptions that apply to the organisation
- information retention and destruction practices
- how the organisation reviews and updates its privacy policy

Privacy policies and technology

Privacy policies should accurately reflect the way your organisation collects, uses and stores personal information.

When reviewing a privacy policy, organisations should consider whether it appropriately addresses:

- cloud-based services
- third-party service providers
- overseas storage or processing of information
- online platforms and applications
- AI tools or automated decision-making processes
- current data breach response practices

Note

Organisations that use automated decision-making processes may need to update their privacy policies before the new automated decision-making transparency requirements start on **10 December 2026**. This is discussed later in this part of the guide.

Tips for privacy policies

- **Do not copy another organisation's privacy policy.** A policy should reflect your organisation's actual practices and legal obligations.
- **Use clear, plain English.** A privacy policy should be easy for individuals to find, read and understand.
- **Avoid making promises you may not be able to keep.** Statements such as 'we will never disclose your information without your consent' may be inaccurate because privacy laws contain exceptions that permit or require disclosure in some circumstances.
- **Include sufficient detail.** A short policy is not necessarily a compliant policy.
- **Review the policy regularly.** Privacy practices, technology and legal requirements can change over time.
- **Make the policy easy to access.** A clear website link and downloadable version are generally good practice.
- **Ensure consistency.** Privacy policies, collection notices, consent forms and internal procedures should align with each other and with your organisation's actual practices.

A privacy policy is not the same thing as a collection notice.

A privacy policy explains your organisation's overall approach to handling personal information, whereas a collection notice explains a particular collection of personal information. Collection notices are discussed later in this part of the guide.

Rules for collecting information

Collecting personal information

APP 3 regulates the collection of personal information.

As a general rule, an organisation should only collect personal information where it is reasonably necessary for one or more of its functions or activities.

When collecting personal information, your organisation should:

- only collect personal information that is reasonably necessary for its functions or activities
- collect personal information by lawful and fair means
- collect personal information directly from the individual wherever reasonable and practicable
- allow individuals to remain anonymous or use a pseudonym where lawful and practicable
- notify individuals about why the information is being collected
- tell individuals if the information may be used for direct marketing purposes

Practical considerations

Before collecting personal information, consider:

- Why is this information needed?
- Is it reasonably necessary for our organisation's activities?
- Could we achieve the same purpose with less information?
- Have we clearly explained why we are collecting the information?
- Does the collection involve sensitive information or health information?

Organisations should avoid collecting personal information simply because it may be useful in the future.

Tip

Collecting less personal information generally reduces privacy risks, cyber security risks and the potential impact of a data breach.

Example – facial recognition technology

In 2024, the OAIC found that Bunnings Group Limited interfered with individuals' privacy through its use of facial recognition technology.

The OAIC found that:

- the collection of individuals' facial information was not reasonably necessary in the circumstances
- less privacy-intrusive alternatives were available, and
- customers were not adequately notified that their personal information was being collected

The decision demonstrates the importance of ensuring that personal information is only collected where it is reasonably necessary and that individuals are adequately informed about the collection.

More information

Commissioner Initiated Investigation into Bunnings Group Ltd (Privacy) [2024] AICmr 230 (29 October 2024)

OAIC media release 19 November 2024: Bunnings breached Australians' privacy with facial recognition tool

Collecting sensitive and health information

Sensitive information and health information are subject to stricter privacy requirements than other forms of personal information.

As a general rule, your organisation must obtain the person's consent before collecting sensitive information or health information unless an exception applies.

Your organisation must not collect sensitive information or health information unless:

- the individual consents to the collection, and
- the information is reasonably necessary for one or more of your organisation's functions or activities

Exceptions

There are limited circumstances in which sensitive information may be collected without consent.

These include:

- certain permitted situations under the Privacy Act (discussed in Part 6), and
- a specific exception for some not-for-profit organisations

Exception for some not-for-profit organisations

Certain not-for-profit organisations may collect sensitive information without consent where:

- the organisation engages in cultural, recreational, political, religious, philosophical, professional, trade or trade union activities

- the information relates to the organisation's activities, and
- the information relates only to members of the organisation, or people who have regular contact with the organisation in connection with its activities

Examples

Examples of situations where this exception may apply include:

- a religious organisation collecting information about members' religious beliefs
- a trade union collecting information about a member's political views
- a community organisation collecting information about a person's disability to provide support services, provided the organisation is not providing a health service

Caution

This exception is narrower than many organisations realise.

- The information must relate to the organisation's activities.
- The information must relate to members or people with regular contact with the organisation.
- The exception does not automatically apply simply because an organisation is a not-for-profit organisation.
- Information about family members or relatives will not usually fall within the exception unless they also have regular contact with the organisation.

Best practice

Regardless of whether consent is required, your organisation should:

- only collect information that is reasonably necessary for its activities
- collect information by lawful and fair means
- collect information directly from the individual wherever practical
- limit access to people who genuinely need the information
- explain why the information is being collected and how it will be used

Collection from third parties

Health information should generally be collected directly from the individual concerned.

However, collection from a third party may be permitted in limited circumstances, including:

- emergencies where information is collected from family members or carers
- referrals between health service providers

Where information is collected from a third party, organisations should generally notify the individual that the information has been collected, unless an exception applies or notification is not reasonably practicable.

Collection notices

When an organisation collects personal information, it must take reasonable steps to ensure the individual is aware of certain information about the collection.

This requirement comes from **APP 5**.

In practice, organisations often comply with APP 5 by providing a **collection notice** (sometimes called a privacy notice).

A collection notice explains why personal information is being collected, how it will be used and other information the individual needs to know at the time of collection.

A collection notice is different from a privacy policy.

- A privacy policy explains your organisation's overall approach to handling personal information.
- A collection notice explains a specific collection of personal information.

Depending on the circumstances, a collection notice may be provided:

- on a paper or online form
- before a person registers for a service or event
- before a donation is made
- when someone subscribes to communications
- when information is collected by phone
- when information is collected through an online platform, application or website

What information must be provided?

When your organisation collects personal information (or as soon as reasonably practicable afterwards), it must take reasonable steps to ensure the individual is aware of:

- your organisation's identity and contact details
- the fact that the information has been collected (if the individual is not already aware)
- whether collection is required or authorised by law, and if so, the relevant law or authority
- the purpose of the collection
- the main consequences if the information is not collected
- any person or organisation to whom the information may be disclosed
- circumstances in which disclosure may be required or authorised
- how the individual can access and correct their personal information
- how they can make a privacy complaint
- whether the information is likely to be disclosed overseas and, where practicable, the countries involved.

Collection notices and modern technology

When preparing collection notices, organisations should also consider whether they need to explain:

- use of cloud-based services
- disclosure to third-party service providers
- overseas storage or processing
- use of AI tools
- use of automated decision-making processes
- website tracking tools and online platforms

The collection notice should accurately reflect how personal information will actually be handled.

Tip

Collection notices should be written in clear, plain English and presented at the point information is collected. Important privacy information should not be hidden in lengthy terms and conditions.

Collection notices and consent

Providing a collection notice does not necessarily mean consent has been obtained.

In some cases, privacy laws require consent in addition to notification. This is particularly relevant when collecting sensitive information or health information.

Consent is discussed in the next section.

Example

A not-for-profit organisation asks people to complete an online registration form for a community event.

The registration form contains a short collection notice explaining:

- who is collecting the information
- why the information is being collected
- whether photographs may be taken at the event
- whether event updates or fundraising communications may be sent
- where the organisation's privacy policy can be found

This is an example of a collection notice being used to help meet APP 5 notification requirements.

Consent

Consent is an important concept in privacy law and is required in some circumstances, particularly when collecting sensitive information and health information.

However, consent is **not always required** to collect, use or disclose personal information. For example, organisations can often collect non-sensitive personal information without consent where the collection is reasonably necessary for the organisation's functions or activities and the other requirements of the APPs are met.

When is consent required?

As a general rule, your organisation must obtain consent before collecting sensitive information or health information, unless an exception applies.

Consent may also be required in other situations under privacy laws or where your organisation relies on consent as the basis for a particular use or disclosure of information.

Note

Obtaining consent does not remove the need to comply with other privacy obligations. For example, your organisation must still comply with requirements relating to collection, notification, security and access to information.

What makes consent valid?

Whether express or implied, valid consent requires that the individual:

- is adequately informed before giving consent
- gives consent voluntarily
- gives consent that is current and specific
- has the capacity to understand and communicate the consent

Consent can be express or implied. However, organisations should be cautious about relying on implied consent, particularly where sensitive information or health information is involved.

Consent does not need to be in writing, but organisations should keep an appropriate record of consent wherever possible.

Examples of evidence of consent may include:

- a signed form
- an online tick box
- an email response
- a recorded verbal agreement

Express and implied consent

Express consent occurs where the individual clearly communicates their agreement, either verbally or in writing.

Implied consent may arise from a person's conduct and the surrounding circumstances.

Privacy regulators generally:

- caution against inferring consent solely from a person's failure to opt out, and
- expect organisations to ensure consent is genuinely informed and voluntary

Because implied consent can be harder to establish, organisations should consider whether express consent is more appropriate, particularly when handling sensitive information.

Collection notices and consent

Providing a collection notice does not necessarily mean consent has been obtained.

A collection notice helps satisfy notification obligations under APP 5. Consent serves a different purpose and may be required in addition to notification.

For example, a collection notice may explain that health information will be collected and used to provide support services. The organisation may still need the individual's consent before collecting that health information.

Continuing consent

Consent is not always permanent.

Just because an individual consented to one activity does not mean they have consented to every future use, disclosure or processing of their information.

Your organisation should consider whether consent remains:

- current
- appropriate
- sufficiently specific to the activity being undertaken

This may become important where:

- services change
- technology changes
- information will be used in a new way
- information will be disclosed to additional recipients

Withdrawal of consent

Individuals should be able to withdraw consent where consent is the basis on which information is being handled.

The process for withdrawing consent should be easy and accessible.

Where relevant, organisations should explain any consequences of withdrawing consent. For example:

- a service may no longer be available, or
- the organisation may not be able to continue using information for a particular purpose

Capacity to consent

Before relying on consent, consider whether the individual has capacity to provide it.

Relevant questions may include:

- Is the person under 18 years of age?
- Do they understand what they are consenting to?
- Is there an illness, disability or impairment affecting their ability to provide informed consent?
- Is the person temporarily unable to make or communicate a decision?
- Can the person understand the language being used?

In some situations, it may be appropriate to involve:

- a parent or guardian
- a person authorised to make decisions on the individual's behalf
- an interpreter or other support person

Caution

Always ensure the individual, or the person authorised to act on their behalf, understands what they are consenting to and can communicate their decision.

Good practice tips

- Use clear, plain language when seeking consent.
- Consider whether the individual has capacity to give consent, particularly if the individual is a child or has impaired decision-making capacity.
- Avoid bundling multiple different consents together where possible.
- Keep records of consent.
- Review consent practices when introducing new technologies or services.
- Consider using a ‘double opt-in’ process for electronic communications, where individuals confirm their consent through a follow-up email or message.
- Inform users when significant changes are made to privacy practices or the privacy policy.

For more information, see the Office of the Australian Information Commissioner’s (OAIC) webpage ‘Consent to the handling of personal information’.

Unsolicited information

Sometimes an organisation receives personal information that it did not actively seek or request. This is known as **unsolicited information**.

APP 4 regulates how organisations deal with unsolicited personal information, including sensitive information and health information.

Examples of unsolicited information may include:

- a job application sent when there is no advertised vacancy
- personal information included in a complaint or enquiry that your organisation did not request
- information provided by a third party without your organisation asking for it

What should your organisation do?

If your organisation receives unsolicited personal information, the first question is whether it could have lawfully collected the information under APP 3.

In particular, consider:

- is the information reasonably necessary for one or more of your organisation's functions or activities?
- if the information is sensitive information or health information, could your organisation have collected it consistently with the APPs?

If your organisation could have collected the information

If the information could have been lawfully collected, your organisation may retain it.

The information must then be handled in accordance with the applicable privacy laws, including requirements relating to:

- collection notices
- storage and security
- use and disclosure
- access and correction

Where required, your organisation should also take reasonable steps to notify the individual about the collection of their information.

If your organisation could not have collected the information

If your organisation could not have lawfully collected the information, it must take reasonable steps to destroy or de-identify it, provided it is lawful and reasonable to do so.

Before destroying or de-identifying information, consider whether there is any legal obligation to retain it. If you are unsure, seek legal advice.

Commonwealth records

Different rules apply to Commonwealth records.

A Commonwealth record generally must not be destroyed and must instead be managed in accordance with the *Archives Act 1983* (Cth).

Organisations managing Commonwealth records should ensure they understand any record-keeping obligations that apply.

Caution

Do not automatically delete unsolicited information. First consider whether there is any legal requirement to retain the information and whether it may constitute a Commonwealth record or another record subject to retention requirements.

Example

A person sends their CV to your organisation even though there is no advertised position.

The individual has relevant skills and may be suitable for future opportunities.

Provided your organisation could have lawfully collected that information, it may retain the CV and consider the person for future roles. However, the information must then be handled in accordance with privacy laws, including any applicable notification obligations.

Practical tips

- Train staff, volunteers and contractors to recognise unsolicited personal information.
- Establish clear procedures for assessing whether unsolicited information can be retained.
- Do not retain personal information indefinitely simply because it might be useful one day.
- If information is retained, ensure it is covered by your organisation's privacy and information management practices.
- Keep records of any decisions to destroy or de-identify information.
- Consider whether your procedures adequately address unsolicited personal information received through email, online contact forms and social media.

Storing and protecting information

Once personal information has been collected, your organisation must take steps to protect it.

APP 11 requires organisations to take reasonable steps to protect personal information from:

- misuse
- interference
- loss
- unauthorised access
- unauthorised modification, and
- unauthorised disclosure

The *Privacy and Other Legislation Amendment Act 2024* (Cth) clarified that these reasonable steps include both **technical measures** and **organisational measures**.

What amounts to a reasonable step will depend on the circumstances, including:

- the nature and sensitivity of the information
- the amount of information held
- the risk of harm if the information is compromised
- the size and resources of the organisation
- the technologies and security measures available

Privacy protection is broader than cyber security. Organisations should consider both technical safeguards and organisational practices that protect information throughout its lifecycle.

Reasonable security measures

Your organisation should consider implementing a combination of organisational and technical safeguards.

Organisational measures

Depending on your organisation's activities and resources, consider:

- appointing a person responsible for privacy and information security
- developing privacy, information security and data retention policies
- training staff, volunteers and contractors
- limiting access to information on a need-to-know basis
- enforcing document retention and destruction procedures
- requiring personnel to return information and remove access when they leave the organisation
- keeping paper files and portable devices secure
- implementing procedures for reporting and escalating privacy incidents
- maintaining data breach and cyber incident response plans

Tip

The more people who can access personal information, the greater the risk of unauthorised access or disclosure.

Review access permissions regularly and limit access to people who genuinely need the information to perform their role. For example, staff involved in donor recruitment or membership administration should not routinely have access to client records unless access is required for their work.

Technical measures

Depending on your circumstances, consider:

- multi-factor authentication
- strong passwords or passphrases
- regular software and security updates
- encryption of sensitive information
- access controls for files, systems and databases
- audit logs and monitoring
- secure backups and recovery processes
- secure email practices, including using the BCC field where appropriate
- secure destruction of electronic records
- measures that reduce the amount of personal information available if a breach occurs

Storing information in the cloud

Many not-for-profit organisations use cloud-based services to store and manage information.

Cloud services can offer significant operational benefits, but they also create additional privacy and security considerations.

If your organisation uses cloud-based storage or other third-party technology providers, it should understand:

- where personal information is stored
- whether information may be transferred overseas
- who can access the information
- how the provider secures information
- how privacy incidents are identified and reported

- whether information is retained after the contract ends
- how information can be securely deleted or returned

Under APP 8, organisations that disclose personal information overseas may be responsible if the overseas recipient mishandles the information.

Working with third-party providers

Before engaging a cloud provider, software provider, fundraising platform, AI provider or other service provider that handles personal information, consider:

- the provider's privacy and security practices
- whether the provider complies with applicable privacy laws
- whether the provider uses subcontractors
- where information is stored or processed
- whether the provider can use your organisation's data for its own purposes
- what incident response obligations apply

Where appropriate, contracts should address:

- privacy compliance
- confidentiality
- security measures
- incident reporting obligations
- access controls
- retention and destruction of information
- return of information when the arrangement ends

Caution

Outsourcing the storage or handling of personal information does not necessarily transfer privacy responsibility. Your organisation may remain accountable for how personal information is handled by a service provider.

Cross-border storage and processing

If personal information is stored or processed overseas, your organisation should ensure that appropriate protections are in place.

This issue is discussed further under **Cross-border disclosure of personal information** later in this part of the guide.

Accuracy and retention of information

APP 10 requires organisations to take reasonable steps to ensure that personal information they collect, use or disclose is:

- accurate
- up to date
- complete, and
- relevant to the purpose for which it is being used or disclosed

Organisations should also review whether they still need the personal information they hold.

If personal information is no longer required, organisations must take reasonable steps to destroy or de-identify it, unless:

- the information forms part of a Commonwealth record, or
- another law requires the information to be retained

Tip

Keeping personal information longer than necessary increases privacy and cyber security risks. A documented information retention and destruction process can help reduce those risks.

For more information about how to store personal information securely and overseas transfers of information, see the OAIC guidance to securing personal information and the OAIC guidance on cross-border disclosure of personal information.

Health information

Health information often attracts additional privacy obligations.

If your organisation holds health information, you may need to comply with:

- the APPs
- applicable state or territory health privacy laws, and
- other state or territory privacy laws that apply to your organisation

The specific obligations depend on the nature of the organisation, the information collected and where the organisation operates.

What does it mean to hold health information?

Your organisation will generally be considered to hold health information if it possesses, or has control over, a paper or electronic record that contains health information.

My Health Record

Organisations participating in the My Health Record system must comply with:

- the *My Health Records Act 2012* (Cth), and
- the *Healthcare Identifiers Act 2010* (Cth)

These laws regulate how information in a person's My Health Record may be collected, used and disclosed.

Access to health information

People whose health information is held by an organisation may have rights relating to that information.

Depending on the circumstances and applicable laws, organisations may be required to help individuals understand:

- why the information is being stored
- how the information was collected
- what health information is held
- their rights to access the information, and
- how they can seek correction of that information

State and territory health privacy laws

As discussed in part 3 of this guide, additional health privacy legislation applies in:

- New South Wales
- Victoria
- the Australian Capital Territory

These laws may impose obligations beyond those contained in the APPs.

Tip

Health information is often subject to stricter privacy protections than other forms of personal information. If your organisation collects, stores or uses health information, it is important to understand all applicable privacy obligations.

In addition, state and territory privacy obligations may apply where information has a sufficient connection to a particular jurisdiction. For example, obligations may arise because information relates to a state government contract, a state-based service or an individual receiving services in that jurisdiction.

Using and disclosing information

Using information for the purpose it was collected

APP 6 regulates when an organisation can use or disclose personal information.

As a general rule, personal information should only be used or disclosed for the purpose for which it was collected. This is sometimes called the **primary purpose**.

The primary purpose will depend on the circumstances.

For example:

- a donor's contact details may be collected to process a donation and communicate with the donor
- a volunteer's personal information may be collected to manage the volunteer relationship
- a client's information may be collected to provide services

Tip

Organisations should be clear about why they are collecting personal information before they collect it. Clearly identifying the primary purpose makes it easier to determine whether a later use or disclosure is permitted.

Example

A conservation organisation collects personal information from people who sign up to receive email updates about rainforest protection. The organisation tells the individuals that their information will be used to provide updates and information about its work.

As a general rule, the organisation may use the information for those purposes because they are the purposes for which the information was collected.

Using information for a secondary purpose

A **secondary purpose** is a purpose that is different from the primary purpose for which the information was collected.

An organisation may only use or disclose personal information for a secondary purpose if an exception applies.

The most common exceptions are set out below.	
Consent	An organisation may use or disclose personal information for another purpose if the individual has consented. Consent should be informed, current and specific to the relevant use or disclosure.
Reasonable expectation	An organisation may use or disclose personal information for a secondary purpose where: • the individual would reasonably expect the use or disclosure, and • the secondary purpose is related to the primary purpose If the information is sensitive information, the secondary purpose must be directly related to the primary purpose.
Required or authorised by law	An organisation may use or disclose personal information where a law permits or requires the use or disclosure. Examples include some reporting obligations, law enforcement requests and circumstances discussed later in this guide under **Permitted situations**.

Example

A not-for-profit organisation collects email addresses from people who sign up to receive updates about rainforest conservation.

The organisation cannot later use those email addresses to promote an unrelated commercial venture unless:

- the individual has consented, or
- another exception applies

Government-related identifiers

Additional restrictions apply to government-related identifiers.

Government-related identifiers include identifiers such as:

- Medicare numbers
- passport numbers
- driver's licence numbers

APP 9 limits when these identifiers can be adopted, used or disclosed.

Organisations should take particular care when collecting and storing government-issued identifiers.

Caution

Just because your organisation lawfully holds a government-related identifier does not mean it can use it for any purpose it chooses.

Automated Decision Making

Recent amendments to the Privacy Act introduced new transparency requirements relating to certain automated decision-making processes.

From **10 December 2026**, some organisations will be required to include information about automated decision-making processes in their privacy policies.

These requirements were introduced by the *Privacy and Other Legislation Amendment Act 2024* (Cth).

When do the automated decision-making requirements apply?

The requirements apply where:

- an organisation has arranged for a computer program to make a decision, or do a thing that is substantially and directly related to making a decision
- the decision could reasonably be expected to significantly affect the rights or interests of an individual, and
- personal information about that individual is used in the operation of the computer program

All three requirements must be satisfied before the automated decision-making provisions apply.

What is a decision?

For these purposes, a decision includes both making a decision and failing or refusing to make a decision.

A decision may affect a person's rights or interests whether the outcome is beneficial or adverse.

Examples of decisions that may significantly affect a person's rights or interests include decisions about:

- entitlement to a service or benefit
- eligibility for financial assistance or a grant
- access to a significant support service
- employment or volunteer opportunities
- contractual rights or obligations.

What information must be included in the privacy policy?

If the automated decision-making requirements apply, the privacy policy must include information about:

- the kinds of personal information used in the operation of the computer program, and
- the kinds of decisions for which the computer program makes, or substantially and directly supports, the decision-making process

Automated decision-making and AI

Not all automated decision-making involves artificial intelligence, and not all uses of artificial intelligence will trigger the automated decision-making requirements.

However, some AI systems may be captured where:

- they use personal information, and
- they make or substantially support significant decisions affecting individuals

Organisations using AI tools should understand how those tools influence decisions and whether the automated decision-making requirements apply.

Example

A not-for-profit organisation uses software that analyses personal information about applicants and automatically determines eligibility for a significant support program.

Because personal information is used by the system and the decision may significantly affect an individual's interests, the automated decision-making requirements may apply.

Example

A staff member uses a generative AI tool to assist with drafting a newsletter.

Although personal information may be processed by the tool, it is unlikely that the automated decision-making requirements apply because the tool is not making, or substantially and directly supporting, a decision that significantly affects an individual's rights or interests.

Preparing for the requirements

Organisations should consider:

- identifying systems that use personal information to make or support decisions
- understanding what decisions those systems influence
- assessing whether those decisions could significantly affect individuals
- reviewing privacy policies before 10 December 2026
- reviewing the use of AI tools and other automated technologies
- ensuring there is appropriate human oversight of important decisions

Tip

Although these requirements do not become enforceable until 10 December 2026, organisations should begin identifying automated decision-making processes now so that privacy policies and governance arrangements can be updated in time.

More information

The OAIC has published guidance to help organisations understand and apply the new transparency requirements for automated decision-making. This includes a fact sheet, flowchart and updated guidance on when the requirements apply and what information must be included in a privacy policy.

See the OAIC's New resources on transparency for use of AI and automated decision-making.

Direct marketing

Many not-for-profit organisations use personal information to communicate with donors, members, volunteers, clients and supporters.

These communications may include fundraising appeals, newsletters, event invitations, membership campaigns and other promotional activities. Under privacy law, these types of communications may constitute direct marketing.

Direct marketing is regulated by **APP 7**. Other laws, including the *Spam Act 2003* (Cth) and the *Do Not Call Register Act 2006* (Cth) may apply.

Direct marketing using sensitive information

Sensitive information, including health information, receives a higher level of protection under privacy law.

An organisation may only use or disclose sensitive information for direct marketing where the individual has consented to that use or disclosure.

Because sensitive information can reveal highly personal matters, organisations should be cautious about using it in fundraising or other direct marketing activities.

Direct marketing using personal information

An organisation may use or disclose non-sensitive personal information for direct marketing where all of the following apply:

- the organisation collected the information directly from the individual
- the individual would reasonably expect the organisation to use or disclose the information for direct marketing
- the organisation provides a simple way for the individual to opt out of receiving direct marketing communications, and
- the individual has not opted out

Example

A charity collects email addresses from supporters who sign up through its website to receive updates about its environmental conservation work. The collection notice explains that the charity will send newsletters, campaign updates and fundraising communications.

In these circumstances, supporters would generally expect to receive those communications, provided the charity also offers a simple way to unsubscribe.

Where the individual would not reasonably expect direct marketing

Sometimes an organisation wants to use personal information for direct marketing even though:

- the information was originally obtained from a third party, or
- the individual would not reasonably expect the information to be used in that way

Additional requirements apply in these circumstances.

Generally, an organisation must either obtain the individual's consent or demonstrate that obtaining consent would be impracticable. The organisation must also provide a simple opt-out mechanism and draw attention to that mechanism in each direct marketing communication.

The individual must not have previously opted out.

Opt-out mechanisms

Individuals who do not wish to receive direct marketing communications must be able to stop those communications easily.

An opt-out process should be clear, simple and easy to use.

Examples include:

- an unsubscribe link in an email
- a reply option for a text message
- a communication preferences page
- a dedicated email address for opt-out requests

Tip

Organisations should keep records of unsubscribe requests and ensure they are actioned promptly.

The Spam Act

The *Spam Act 2003* (Cth) applies to many commercial electronic messages, including emails, text messages and instant messages.

Not-for-profit organisations are generally required to comply with the Spam Act.

The Spam Act usually requires:

- consent from the recipient
- clear identification of the sender
- a functional unsubscribe facility

Registered charities may benefit from limited exemptions in some circumstances, but organisations should not assume that a charity exemption automatically applies to all communications.

Caution

Compliance with APP 7 does not necessarily mean compliance with the Spam Act. Organisations should consider both legal regimes when sending electronic communications.

The Do Not Call Register Act

Organisations conducting telephone-based fundraising or promotional campaigns should also consider the *Do Not Call Register Act 2006* (Cth).

This Act regulates certain telemarketing calls and faxes and may affect how an organisation contacts individuals by telephone.

Direct marketing and privacy documentation

An organisation's privacy practices should be consistent across its:

- privacy policy
- collection notices
- consent processes
- fundraising and marketing activities

Individuals should be told how their information will be used and should not be surprised by the communications they receive. Clear collection notices and accurate privacy policies can also help reduce privacy complaints and maintain community trust.

Access to and correcting personal information

Privacy laws give individuals important rights in relation to their personal information.

These rights include:

- the right to request access to personal information held about them, and
- the right to seek correction of personal information that is inaccurate, incomplete, out of date, irrelevant or misleading

These rights are reflected in **APP 12** and **APP 13**.

Accessing personal information (APP 12)

As a general rule, if an individual requests access to personal information held about them, an organisation must provide access.

Access should generally be provided in the manner requested by the individual, where this is reasonable and practicable.

An organisation should respond to access requests within a reasonable period.

Providing access

When responding to an access request, an organisation should take care not to inadvertently disclose another person's personal information.

For example, a document may contain information relating to multiple individuals. In those circumstances, some information may need to be removed or redacted before access is provided.

Refusing access

An organisation may refuse access in limited circumstances.

Examples include where:

- providing access would pose a serious threat to the life, health or safety of an individual
- providing access would unreasonably impact another person's privacy
- the request is frivolous or vexatious
- providing access would be unlawful

If an organisation refuses access, it must provide the individual with written notice that explains:

- the reasons for the refusal (unless it would be unreasonable to do so), and
- the mechanisms available to complain about the decision

Charges

An organisation must not charge a person for making an access request.

However, an organisation may charge for providing access to the information, provided the charge is not excessive.

Tip

Establishing a documented process for responding to access requests can help ensure requests are handled consistently and within a reasonable timeframe.

Example

A former volunteer asks a not-for-profit organisation for a copy of the personal information it holds about them. The organisation identifies volunteer records, contact details and correspondence relating to that individual.

Unless an exception applies, the organisation will generally be required to provide access to that information.

Correcting personal information (APP 13)

Organisations should take reasonable steps to ensure that the personal information they hold is accurate, up to date, complete, relevant and not misleading.

Individuals also have a right to request correction of their personal information.

Requests for correction

If an individual requests correction of personal information, or if the organisation is otherwise satisfied that the information is inaccurate, out of date, incomplete, irrelevant or misleading, the organisation must take reasonable steps to correct the information.

If the individual requests it, the organisation must also take reasonable steps to notify any other APP entity to which it previously disclosed the information that the correction has been made.

Refusing to correct information

An organisation may refuse a correction request in some circumstances.

If it does so, it must provide the individual with written notice explaining:

- the reasons for the refusal, and
- how the individual can make a complaint

The organisation must also take reasonable steps, if requested by the individual, to associate a statement with the information indicating that the individual believes the information is inaccurate, out of date, incomplete, irrelevant or misleading.

Charges

An organisation must not charge an individual:

- for making a correction request
- for correcting personal information, or
- for associating a statement with personal information

Example

A donor advises a charity that their address has changed and requests that its records be updated.

The charity should take reasonable steps to update the donor's personal information and ensure that future communications are sent to the correct address.

Tip

Regularly reviewing personal information and providing simple mechanisms for people to update their details can improve compliance with APP 10 and APP 13 while reducing administrative burden.

Cross-border disclosure of personal information

Many not-for-profit organisations use technology platforms, service providers and cloud-based systems that store or process information outside Australia.

In these circumstances, personal information may be disclosed to an overseas recipient.

APP 8 regulates cross-border disclosure of personal information.

When does APP 8 apply?

Before disclosing personal information to an overseas recipient, an organisation must generally take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to that information.

This obligation commonly arises when organisations:

- use cloud-based storage services
- engage overseas service providers

- use software or technology platforms hosted overseas
- use overseas fundraising or donor management platforms
- disclose personal information to overseas affiliates or partners
- use AI or other digital services that process information overseas

Accountability for overseas disclosures

If an organisation discloses personal information to an overseas recipient and APP 8 applies, the organisation may remain accountable for certain acts or practices of the overseas recipient.

This means that outsourcing the handling of personal information does not necessarily transfer responsibility for privacy compliance.

Exceptions

APP 8 contains several exceptions.

One exception applies where an organisation reasonably believes that:

- the overseas recipient is subject to a law or binding scheme that provides protections that are substantially similar to the APPs, and
- there are mechanisms available to enforce those protections

Other exceptions may also apply in limited circumstances.

Because these exceptions can be complex, organisations should consider obtaining legal advice where large volumes of personal information are disclosed overseas or where sensitive information is involved.

Recent developments

Amendments made by the *Privacy and Other Legislation Amendment Act 2024* (Cth) allow countries or binding schemes to be recognised where they provide privacy protections that are substantially similar to the APPs.

This is intended to make it easier for organisations to identify overseas jurisdictions that provide an appropriate level of privacy protection when personal information is disclosed overseas.

Organisations should review current legislation and OAIC guidance before relying on this exception.

Practical steps

Before disclosing personal information overseas, an organisation should consider:

- where the information will be stored or processed
- whether overseas providers have appropriate privacy and security measures
- whether contractual protections are in place
- whether the organisation's privacy policy accurately describes the disclosure
- whether the disclosure involves sensitive information or health information
- whether individuals have been appropriately informed about the disclosure.

Where personal information is handled by third-party providers, contracts should clearly address privacy, security, access controls, incident reporting, retention and destruction of information

Example

A not-for-profit organisation uses a donor management platform hosted outside Australia. Donors' names, contact details and donation histories are stored on overseas servers.

The organisation should understand where the information is stored, what privacy protections apply, whether overseas subcontractors are involved and what contractual safeguards exist before using the platform.

Tip

If it is practicable to do so, organisations should identify in their privacy policy the countries where personal information is likely to be disclosed or stored overseas.

For more information on cross-border disclosures, see OAIC's guide to Cross-border disclosure of personal information - Chapter 8: APP 8.

Children's Online Privacy Code

Many organisations provide online services that may be accessed by children, including websites, apps, educational platforms, online communities and messaging services.

Recognising that children may require additional privacy protections, the *Privacy and Other Legislation Amendment Act 2024* (Cth) introduced a framework for a Children's Online Privacy Code (**COP Code**).

The Office of the Australian Information Commissioner (**OAIC**) is required to develop and register the Code by **10 December 2026**.

The Code is intended to strengthen privacy protections for children who use online services and to support organisations to handle children's personal information in an appropriate and transparent way.

Who will the Code apply to?

The COP Code will apply where all of the following apply:

- the entity is a provider of a social media service, relevant electronic service or designated internet service (within the meaning of the *Online Safety Act 2021* (Cth))
- the service is likely to be accessed by children, and
- the entity is not providing a health service

The OAIC may also specify particular APP entities or classes of APP entities that are required to comply with the Code.

What will the Code do?

At the time this guide was last updated, the detailed requirements of the Code had not been finalised.

However, the Code is expected to operate alongside the APPs and provide additional guidance and protections in relation to matters such as:

- collection of children's personal information
- privacy notices and transparency
- consent processes
- profiling and tracking practices
- online safety and privacy risks
- handling personal information through digital services

The OAIC is expected to publish guidance to help organisations assess whether their services are likely to be accessed by children and whether the Code applies.

What should organisations do now?

Organisations whose websites, applications or online services may be accessed by children should begin considering whether the Code could affect their activities.

This may include reviewing:

- what personal information is collected from children
- how that information is used and disclosed
- existing privacy notices and consent processes
- online features that involve profiling, tracking or personalised content

Tip

Even if a service is not specifically designed for children, the Code may still be relevant if children are likely to access it.

Comparison of Commonwealth and State and Territory Privacy Principles

The APPs and state and territory privacy principles generally address similar issues relating to the collection, use, disclosure, protection, access and correction of personal information, although there are important differences between jurisdictions.

The table below provides a high-level comparison of the APPs and comparable state and territory privacy principles. It is intended as a reference guide only and is not a substitute for legal advice or the relevant legislation.

Commonwealth	States and Territories	
APP 1 – Open and transparent management of personal information		
APP 1.1 – Organisation must be open and transparent in its management of personal information	ACT NSW NT QLD SA TAS VIC WA	TPP 1.1 IPP 6 IPP 5 QPP 1 - PIPP 5 IPP 5 -
APP 2 – Anonymity and pseudonymity		
APP 2.2 – Individuals must have the option of not identifying themselves, or of using a pseudonym (where lawful and applicable)	ACT NSW NT QLD SA TAS VIC WA	TPP 2.1 - IPP 8.1 QPP 2 - PIPP 8 IPP 8 -
APP 3 and APP 4 – Collection of personal information		
APP 3.1 and 3.2 – Information must be reasonably necessary for or directly related to your organisation's functions or activities	ACT NSW NT QLD SA TAS	TPP 3.1 IPP 8(1) IPP 1.1 QPP 3.1 - PIPP 1(1)

	VIC WA	IPP 1.1 -
APP 3.3 and 3.4 – Additional requirements in relation to 'sensitive information'	ACT NSW NT QLD SA TAS VIC WA	TPP 3.3 IPP 19(1) IPP 10 QPP 3.3 and 3.4 - PIPP 10 IPP 10 -
APP 3.5 – Must only collect by lawful and fair means	ACT NSW NT QLD SA TAS VIC WA	TPP 3.5 IPP 8(2) IPP 1.2 QPP 3.5 IPP 1 PIPP 1(2) IPP 1.2 -
APP 3.6 – Information must be collected directly from the person unless exceptions apply	ACT NSW NT QLD SA TAS VIC WA	TPP 3.6 IPP 9 IPP 1.4 QPP 3.6 - PIPP 1(4) IPP 1.4 -
APP 5 – Notification of the collection of personal information		
APP 5.1 – Organisation must take steps (if any) that are reasonable in the circumstances to notify/ensure that the individual is aware of certain matters	ACT NSW NT QLD SA TAS VIC WA	TPP 5.1 IPP 10 IPP 1.3, 1.5 QPP 5.1 IPP 2 PIPP 1(3) IPP 1.3 -
APP 6 – Use or disclosure of personal information		
APP 6.1 and 6.2 – Organisation must only use or disclose personal information for the primary purpose for which it was collected unless an exception applies	ACT NSW NT QLD SA TAS VIC WA	TPP 6.1, 6.2 IPP 17 and 18 IPP 2.1 QPP 6 IPP 8, 10 PIPP 2 IPP 2.1, 2.2 -
APP 7 – Direct marketing		
APP 7.1 – An organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies.	ACT NSW NT QLD SA TAS	TPP 7 (s 23) - - QPP 6 - -

	VIC WA	- -
APP 8 – Cross-border disclosure of personal information		
APP 8.1 – Restrictions on cross border disclosure of personal information	ACT NSW NT QLD SA TAS VIC WA	TPP 8.1 - IPP 9.1 - - PIPP 9 IPP 9.1 -
APP 9 – Adoption, use or disclosure of government related identifiers		
APP 9.1 – Restrictions on organisations adopting a government related identifier of an individual as its own	ACT NSW NT QLD SA TAS VIC WA	TPP 9 - IPP 7.2 - - PIPP 7(2) IPP 7.2 -
APP 9.2 – Restrictions on organisations using or disclosing a government related identifier of an individual	ACT NSW NT QLD SA TAS VIC WA	TPP 9 - IPP 7.3 - - PIPP 7(3) IPP 7.3 -
APP 10 – Quality of personal information		
APP 10.1 – Must take reasonable steps (if any) to ensure that the personal information it collects is accurate, up to date and complete	ACT NSW NT QLD SA TAS VIC WA	TPP 10.1 IPP 11(a) IPP 3.1 QPP 10.1 IPP 3 PIPP 3 IPP 3 -
APP 10.2 – Must take reasonable steps (if any) to ensure that the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant	ACT NSW NT QLD SA TAS VIC WA	TPP 10.2 IPP 16 IPP 3.1 QPP 10.2 IPP 9 PIPP 3 IPP 3 -
APP 11 – Security of personal information		
APP 11.1 Organisation must take reasonable steps to protect information it holds from misuse, interference and loss and unauthorised access, modification or disclosure	ACT NSW NT QLD	TPP 11.1 IPP 12 IPP 4.1 QPP 11.1

	SA TAS VIC WA	IPP 4 PIPP 4(1) IPP 4 -
APP 11.2 – If an organisation no longer requires personal information, it must take reasonable steps to destroy or de-identify the information (subject to any document retention laws)	ACT NSW NT QLD SA TAS VIC WA	TPP 11.2 IPP 12 IPP 4.2 QPP 11.2 - PIPP 4(2) IPP 4.2 -
APP 12 – Access to personal information		
APP 12.1 An organisation must on request by the individual, give the individual access to the information, subject to some exceptions	ACT NSW NT QLD SA TAS VIC WA	TPP 12.1 IPP 14 IPP 6.1 QPP 12 IPP 5 PIPP 6(1) IPP 6.1 -
APP 13 – Correction of personal information		
APP 13.1 – If an organisation is satisfied that information it holds is inaccurate, out-of-date, incomplete, irrelevant or misleading, or the individual requests the entity to correct the information, the entity must take reasonable steps correct the information.	ACT NSW NT QLD SA TAS VIC WA	TPP 13.1 IPP 15 IPP 6.3, 6.4 QPP 13 IPP 6 PIPP 6(2) IPP 6.5 -

Note

Not every state or territory privacy regime has a direct equivalent to every APP. Differences in wording do not necessarily mean organisations have different obligations. In many cases, the underlying privacy principle is substantially similar.

Part 5

Notifiable Data Breaches scheme

Notifiable Data Breaches scheme

This part of the guide covers:

- what the Notifiable Data Breaches (**NDB**) scheme is
- which organisations must comply with the scheme
- what constitutes an eligible data breach
- responding to a data breach
- notifying affected individuals and the Office of the Australian Information Commissioner (**OAIC**)
- eligible data breach declarations
- emergency declarations
- penalties for non-compliance

This part of the guide explains the Notifiable Data Breaches (NDB) scheme under the *Privacy Act 1988* (Cth) and the steps organisations should take when responding to a suspected or actual data breach.

Data breaches are an increasingly significant privacy and cyber security risk for not-for-profit organisations. Effective data breach response can help reduce harm to affected individuals and minimise legal, financial and reputational risks for an organisation.

The Office of the Australian Information Commissioner (**OAIC**) expects organisations to have appropriate practices, procedures and systems in place to protect personal information and to respond promptly and effectively when a data breach occurs.

The OAIC publishes a biannual Notifiable Data Breaches Report, which provides useful information about current breach trends and emerging risks.

State and territory mandatory notification of data breach schemes

New South Wales and Queensland have mandatory data breach notification schemes for certain public sector agencies. These schemes are separate from the NDB scheme and are not covered in this guide.

For more information, see:

- the NSW Information and Privacy Commission's guidance on the Mandatory Notification of Data Breach Scheme
- the Queensland Office of the Information Commissioner's guidance on notification under the mandatory notification of data breach scheme

Read this part of the guide alongside our fact sheet on cyber security. A data breach response will often involve both privacy and cyber security considerations.

What the Notifiable Data Breaches scheme is

The NDB scheme requires certain organisations to notify affected individuals and the OAIC when they reasonably believe an eligible data breach has occurred.

The scheme is intended to ensure that individuals can take steps to protect themselves where a data breach is likely to result in serious harm.

The NDB scheme complements the obligations under the Australian Privacy Principles (**APPs**), which require organisations to take reasonable steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure.

Only certain organisations are subject to the NDB scheme and only certain data breaches require notification.

What is an eligible data breach?

Not every data breach requires notification.

An eligible data breach occurs where:

- there is unauthorised access to, unauthorised disclosure of, or loss of personal information
- the breach is likely to result in serious harm to one or more individuals, and
- remedial action has not prevented the likely risk of serious harm

All three elements must be present before notification is required.

The NDB scheme applies to data breaches occurring on or after 22 February 2018.

Note

Recent amendments to the Privacy Act also give the Minister powers to make:

- an eligible data breach declaration, and
- an emergency declaration

These declarations can authorise the collection, use or disclosure of personal information that would otherwise not be permitted under the APPs for specified purposes. These powers are discussed later in this part of the guide.

Organisations which must comply with the NDB scheme

The Notifiable Data Breaches (**NDB**) scheme applies to organisations that are required to comply with the security obligations in **APP 11** of the *Privacy Act 1988* (Cth).

The scheme also applies to organisations that hold certain categories of information, including tax file number (**TFN**) information, credit reporting information and credit eligibility information, even if they are not otherwise APP entities.

Organisations subject to the NDB scheme

Organisations that may be required to comply with the NDB scheme include:

- businesses and not-for-profit organisations with annual turnover exceeding $3 million
- Australian Government agencies
- organisations that provide a health service and hold health information
- employee associations registered under the *Fair Work (Registered Organisations) Act 2009* (Cth)
- reporting entities under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
- Consumer Data Right accredited entities
- organisations that have voluntarily opted into coverage under the Privacy Act
- credit reporting bodies and certain credit providers
- organisations providing services to the Commonwealth under government contracts
- organisations that trade in personal information

As discussed in part 3 of this guide, some organisations with annual turnover below $3 million may still be subject to the Privacy Act and, consequently, the NDB scheme.

Organisations that hold TFN information

The NDB scheme also applies to organisations that hold TFN information.

Examples may include employers and organisations that assist individuals with employment or other services that require the collection of TFNs.

These organisations are often referred to as **TFN recipients**.

Note

A TFN recipient may have notification obligations under the NDB scheme even if it is not otherwise subject to the APPs.

For more information about protecting TFN information, see the OAIC's guidance on the Privacy (Tax File Number) Rule 2015.

Organisations that outsource the storage of personal information

An organisation cannot avoid its obligations under the NDB scheme simply because it stores information with a third-party provider.

An organisation will generally be considered to hold personal information where it has possession or control of a record containing that information.

This can include situations where personal information is stored by:

- a cloud service provider
- a software provider
- an outsourced records management provider
- another third party acting on the organisation's behalf

An organisation may still hold personal information even if it does not physically possess the records.

For example, where an organisation retains the right to access, manage, amend or control personal information stored by a third-party provider, it will generally continue to hold that information for the purposes of the NDB scheme.

Example

A not-for-profit organisation uses a cloud-based client management platform operated by an external provider. The provider stores all client records on its servers, but the organisation can access, edit and manage the information through the platform.

Although the records are stored by the provider, the organisation will generally still be considered to hold the personal information and may be required to assess and respond to an eligible data breach affecting that information.

What kind of data breaches require notification?

Not every data breach triggers notification obligations under the NDB scheme.

An organisation is only required to notify affected individuals and the OAIC if it experiences, or has reasonable grounds to believe it has experienced, an eligible data breach.

As explained above, an **eligible data breach** occurs where:

- there is **unauthorised access** to, **unauthorised disclosure** of, or loss of **personal information**
- the breach is **likely to result in serious harm to one or more individuals**, and
- remedial action has not prevented the likely risk of serious harm

All three requirements must be satisfied before notification is required.

For organisations that are not APP entities but are TFN recipients, an eligible data breach only arises to the extent that TFN information is involved in the breach.

Note

The Minister also has powers to make:

- an eligible data breach declaration, and
- an emergency declaration

These declarations can authorise the collection, use or disclosure of personal information that would otherwise not be permitted under the APPs for certain purposes. They are discussed later in this part of the guide.

Unauthorised access, unauthorised disclosure and loss

The first element of an eligible data breach is that there has been unauthorised access to, unauthorised disclosure of, or loss of personal information.

Unauthorised access occurs when personal information is accessed by someone who is not permitted to access it.

This can include access by an employee, a volunteer, a contractor, a service provider, or an external malicious actor such as a hacker.

Example – unauthorised access

Sandra volunteers for an organisation that provides support services to LGBTIQ+ people. The organisation stores information about people who have used its services and restricts access to that information to certain employees.

Sandra becomes curious about whether one of her friends has used the service and searches the organisation's records without authorisation.

This is an example of unauthorised access.

Unauthorised disclosure occurs when personal information is made accessible or visible to another person outside the organisation, whether intentionally or accidentally.

Examples – unauthorised disclosure

Example 1 – Michael works for a large not-for-profit organisation that supports veterans' families. A journalist contacts him seeking information about a well-known person believed to be a client of the organisation. Michael confirms that the person is a client and provides contact information from the organisation's records. This is unauthorised disclosure.

Example 2 – Sandeep sends an email containing client information to an incorrect email address. Although the disclosure was accidental, it is still an example of unauthorised disclosure.

Example 3 – Carrie-Anne accidentally includes a link to a client database in a public webpage, making the information available online. This is also an example of unauthorised disclosure.

Loss occurs when personal information is lost in circumstances where unauthorised access or unauthorised disclosure is likely.

Example – loss

Anthea downloads payroll information, including employee names and tax file numbers, onto an unencrypted USB device. On her way home from work she loses the device and cannot locate it.

This is an example of the loss of **personal information** and **TFN information**.

A loss of information will not necessarily be an eligible data breach. For example, where information is strongly encrypted and unlikely to be accessed or disclosed, notification obligations may not arise.

Tax file number information

For TFN recipients, an eligible data breach only arises to the extent that TFN information is involved.

TFN information is information that links a person's tax file number with their identity.

Examples may include:

- a document containing a person's name and TFN
- records that allow a person's identity to be connected with a TFN

Where a data breach does not involve TFN information, the NDB scheme may not apply to a TFN recipient.

However, organisations should still consider whether notification is appropriate in the circumstances.

The next step: assessing serious harm

Once an organisation has identified unauthorised access, unauthorised disclosure or loss of personal information, the next question is whether the breach is likely to result in serious harm to one or more individuals.

This assessment is critical because not every data breach is an eligible data breach requiring notification.

The next section explains how organisations should assess suspected data breaches and determine whether the serious harm threshold has been met.

The process for responding to data breaches

The OAIC expects organisations to have practices, procedures and systems in place to identify, report and respond to suspected data breaches.

A data breach response plan is a documented process that sets out:

- the steps to be taken following a suspected or actual data breach
- who is responsible for managing the response
- how decisions will be made and documented
- when notifications will be given
- how lessons learned will be implemented

Tip

Put data breach response procedures in place before a breach occurs and review them regularly.

See the OAIC's Data breach preparation and response guidance which recommends that organisations prepare for data breaches before they occur and review their response procedures regularly.

The OAIC's four-step response process

The OAIC recommends a four-step approach to responding to data breaches.

Step	Action
1. Contain	Stop the breach from continuing or escalating and preserve evidence.
2. Assess	Investigate what happened, identify the information affected and assess the risk of harm.
3. Notify	Notify affected individuals and the OAIC where notification is required.
4. Review	Review the incident and identify improvements to reduce the risk of future breaches.

Every data breach is different and these steps may overlap or occur at the same time

For example, it may be necessary to notify affected individuals before an assessment has been fully completed if there is an immediate risk of serious harm.

Step 1: Contain

Once an organisation becomes aware of a suspected or actual data breach, it should act immediately to limit the impact of the breach.

The appropriate containment measures will depend on the nature of the incident.

Examples may include:

- stopping the unauthorised activity
- shutting down affected systems
- changing passwords or access credentials
- revoking access privileges
- recovering information that has been disclosed accidentally
- disabling compromised accounts

Note

While containing a breach, organisations should take care not to destroy evidence that may assist in understanding how the incident occurred and whether further action is required.

At this stage an organisation may:

- suspect that an eligible data breach has occurred and begin an assessment, or
- reasonably believe that an eligible data breach has occurred and move directly to notification

Step 2: Assess

If an organisation becomes aware of reasonable grounds to suspect that an eligible data breach may have occurred, it must promptly assess the situation.

The purpose of the assessment is to determine whether:

- unauthorised access, disclosure or loss of personal information has occurred
- the breach is likely to result in serious harm to one or more individuals, and
- notification is required

Timeframe for assessment

An assessment must be completed as quickly as possible.

The Privacy Act requires organisations to take all reasonable steps to complete the assessment within **30 days** after becoming aware of reasonable grounds to suspect an eligible data breach.

Organisations should not unnecessarily delay assessments while waiting for management, executive or board discussions.

If an assessment cannot be completed within 30 days, it is prudent to document the reasons.

Conducting an assessment

Although the Privacy Act does not prescribe a specific assessment methodology, the OAIC recommends a **three-stage process**:

Initiate the assessment process – Identify person or team responsible for the assessment and establish a process for investigating the incident

Investigate the matter – Gather relevant information about the suspected breach. Questions may include: What happened? What information was affected? Who may have accessed the information? Can remedial action be taken? What harm could result?

Evaluate the breach – Consider the available information and determine whether the incident is an eligible data breach. The assessment and reasons for the decision should be documented.

Tip

If there is uncertainty about whether unauthorised access or disclosure has occurred, organisations should take a cautious approach and carefully consider the risks to affected individuals rather than focusing solely on whether information can be proven to have been extracted or misused.

When are data breaches likely to result in serious harm?

An organisation is only required to notify affected individuals and the OAIC if a data breach is likely to result in serious harm to one or more individuals.

Whether serious harm is likely must be assessed from the perspective of a reasonable person in the organisation's position who is properly informed and has considered the information available at the time of the assessment.

The phrase "likely to result in serious harm" is not specifically defined in the Privacy Act. In practice, it means that the risk of serious harm is more probable than not.

Serious harm may include physical harm, psychological or emotional harm, financial harm, reputational harm, identity theft, fraud, humiliation or distress.

Organisations should assess the likelihood of serious harm holistically, having regard to both the nature of the information involved and the circumstances of the breach.

Factors to consider

The NDB scheme sets out a number of factors that an organisation should consider when assessing whether a breach is likely to result in serious harm.

Factor	Example of lower risk	Example of higher risk
The kind of information involved and its sensitivity	A person's name, without other identifying information	Health information, such as information about a person's HIV status

Whether the information is protected by security measures and whether those measures could be overcome	Strongly encrypted information protected by multi-factor authentication	Unencrypted information or information protected only by basic security measures
The people who have obtained, or who could obtain, the information	Accidental access by a trained employee who reports the incident immediately	Public disclosure or access by malicious actors such as hackers
The nature of the potential harm	Information that is already publicly available	Identity theft, financial loss, threats to physical safety, reputational damage or serious embarrassment

No single factor is determinative. Organisations should consider all relevant circumstances.

Additional considerations

The following questions may also assist when assessing whether serious harm is likely:

- **Does the breach affect vulnerable individuals?**

  The impact of a breach may vary depending on the circumstances of the people affected.

  For example, a list of names and addresses may present a greater risk where it includes people who are vulnerable or at risk of harm.

- **How many people are affected?**

  The greater the number of individuals affected, the greater the likelihood that at least one individual may experience serious harm.

  The OAIC has indicated that where a breach affects a large number of people, organisations should carefully consider whether the serious harm threshold has been met, even where the risk to each individual appears relatively low.

- **What information could be inferred?**

  Organisations should consider not only the information that has been disclosed, but also what additional information could be inferred from it.

  For example, information linking a person to a particular medical condition, support service or sensitive activity may increase the likelihood of serious harm.

  Similarly, the disclosure of multiple pieces of personal information together can significantly increase risk.

- **Is the information adequately protected?**

  If the information was encrypted, anonymised or otherwise protected so that it is unlikely to be accessed or understood by an unauthorised person, the likelihood of serious harm may be reduced.

  For example:

  – information that is securely encrypted and cannot reasonably be decrypted may present a lower risk

  – information that has been remotely deleted before it could be accessed may also present a lower risk

- **How long ago did the breach occur?**

  The length of time between the breach and its discovery may be relevant.

  A longer period may increase the likelihood that information has been accessed, copied or misused.

For example, if a malicious actor has had access to a compromised mailbox for several months, there may have been greater opportunity to gather information and use it for fraudulent purposes.

- **Who has obtained, or may obtain, the information?**

  Organisations should consider who has access to the information and how likely it is that the information will be misused.

  For example, where a breach appears to specifically target personal information for criminal purposes, the likelihood of serious harm may be greater than where information was accidentally disclosed to a trusted recipient who immediately deletes it.

Note

Organisations are not expected to contact affected individuals to determine their personal circumstances before assessing whether serious harm is likely. The assessment should be based on the information reasonably available to the organisation at the time.

Taking a cautious approach

Data breaches are often complex and organisations may not immediately have all relevant information.

The OAIC encourages organisations to:

- take a cautious approach where there is uncertainty
- consider all relevant risks and circumstances
- avoid focusing solely on whether information has been copied or extracted
- recognise that unauthorised access alone may result in an eligible data breach

For example, a malicious actor may be able to view information, take screenshots or otherwise misuse information without leaving evidence that data was copied or downloaded.

The role of remedial action

Even where serious harm appears likely, notification may not be required if effective remedial action prevents the risk of serious harm.

The next section explains when remedial action may remove the obligation to notify under the NDB scheme.

Exceptions to the requirement to notify

An organisation may not need to notify affected individuals or the OAIC if it takes effective remedial action in time.

The purpose of remedial action is to reduce or remove the risk of serious harm arising from the data breach.

Where remedial action prevents the likelihood of serious harm, the breach will not be an eligible data breach and notification will not be required.

When can remedial action prevent notification?

Remedial action must be effective enough to ensure that serious harm is no longer likely to result from the breach.

The effectiveness of remedial action will depend on the circumstances, including:

- the nature of the information involved
- who may have accessed the information
- how quickly the organisation responds
- whether the information remains accessible
- whether the risk of misuse has been eliminated

If remedial action only removes the risk of serious harm for some affected individuals, the organisation may still need to notify those individuals who remain at risk.

Note

The fact that an organisation has taken remedial action does not automatically mean notification is unnecessary. The organisation must still assess whether serious harm remains likely.

Example – lost device

Fernando's smartphone contains personal information and falls out of his pocket while travelling to work. The phone is protected by a PIN and, shortly after discovering it is missing, Fernando asks the organisation's IT team to remotely delete the information stored on the device. The IT team is confident that the information was deleted before anyone could gain access to it.

In these circumstances, it may be reasonable to conclude that serious harm is no longer likely and notification may not be required.

Example – information inadvertently published online

While updating the organisation's website, Madeleine accidentally publishes a document containing personal information.

As soon as she becomes aware of the error, she removes public access to the document, confirms the information is not accessible elsewhere on the website, and clears website caches to minimise the likelihood of further access.

Following an assessment, the organisation concludes that serious harm is no longer likely. Notification may not be required.

Documenting remedial action

Where an organisation decides that notification is not required because remedial action has removed the risk of serious harm, it should document:

- the nature of the breach
- the remedial action taken
- the assessment process
- the reasons for concluding that serious harm is no longer likely

Keeping clear records may assist if the organisation's response is later reviewed by the OAIC.

Tip

Even where notification is not legally required, organisations should consider whether affected individuals would benefit from being informed of the incident so that they can take steps to protect themselves.

Step 3: Notify

If an organisation reasonably believes that an eligible data breach has occurred, it must notify **both**:

- the OAIC, and
- affected individuals

Notification should occur as soon as practicable after the organisation has completed its assessment and formed a reasonable belief that an eligible data breach has occurred.

In some circumstances, it may be appropriate to notify affected individuals before containment or assessment activities have been fully completed. For example, an organisation may decide that urgent notification is necessary so affected individuals can take immediate steps to protect themselves from serious harm.

Notification requirements

Where notification is required, an organisation should:

- contain the breach, so far as reasonably practicable
- prepare a notification statement
- provide the notification statement to the OAIC
- notify affected individuals

The notification statement forms the basis of both the OAIC notification and communication with affected individuals.

Preparing the notification statement

An organisation may prepare its notification statement in a format that suits the circumstances of the breach, provided that it includes the information required by the Privacy Act.

The notification statement must contain:
The identity and contact details of the organisation The notification should clearly identify the organisation responsible for the notification. Where an organisation is commonly known by a trading name or service name, it should consider using the name most likely to be recognised by affected individuals. The notification should also include appropriate contact details. Depending on the circumstances, this may include a dedicated email address, a dedicated telephone number, a specific contact person or team
A description of the data breach The description should provide enough information to help affected individuals understand the nature of the incident and assess the potential consequences. Depending on the circumstances, this may include when the breach occurred, when the breach was discovered, how the breach occurred, who may have obtained access to the information, steps taken to contain or remediate the breach. The OAIC does not generally expect organisations to identify specific individuals who obtained access to the information unless that information is necessary to help affected individuals understand the risks they face.
The kinds of personal information involved in the breach The notification should describe the categories of personal information affected. Examples may include names, addresses, telephone numbers, email addresses, dates of birth, financial information, government-related identifiers, health information. If sensitive information, health information, tax file number information, financial information or identity documents are involved, the notification should clearly state this.

Recommendations about the steps affected individuals should take in response to the breach

The notification must include recommendations about the steps affected individuals should take in response to the breach.

The recommendations should be practical and tailored to the circumstances.

For example: changing passwords, enabling multi-factor authentication, contacting a financial institution, replacing compromised identity documents, monitoring accounts for suspicious activity.

If specialist advice is needed to determine appropriate recommendations, the organisation should obtain that advice before issuing the notification.

Tip

The notification should focus on information that helps affected individuals understand the breach and take steps to protect themselves.

Notifying the OAIC

Organisations can notify the OAIC using the online Notifiable Data Breach form.

The OAIC may also make alternative notification arrangements where appropriate.

Organisations should ensure that the information provided to the OAIC is accurate and reflects the facts known at the time of notification.

Notifying affected individuals

The NDB scheme provides flexibility in how individuals are notified.

The appropriate notification method will depend on factors such as the number of people affected, the contact information available, the urgency of the risk, the resources available to the organisation.

The Privacy Act provides three notification options:	
Option 1 **Notify all affected individuals**	Where an organisation cannot identify which individuals are likely to be at risk of serious harm, it should notify all affected individuals. Notification may be given using one or more methods, including: email, telephone, SMS, post, in-person communication. The organisation should consider which method is most likely to ensure affected individuals become aware of the notification and understand its contents..
Option 2 **Notify only individuals at risk of serious harm**	Where an organisation can identify which individuals are likely to be at risk of serious harm, it may notify only those individuals. This approach may reduce costs and minimise unnecessary notifications. However, organisations should be confident that they can accurately identify all individuals who are at risk.
Option 3 **Publish a notification**	If neither of the first two options is practicable, an organisation may publish a copy of the notification statement. In these circumstances, the organisation must: • publish the statement on its website (if it has one), and • take reasonable steps to publicise the contents of the statement

The objective is to maximise the likelihood that affected individuals will become aware of the breach.

Examples of additional publicity measures may include social media announcements, online advertising, media releases, notices through regular communication channels.

Note – Making a notification statement available on a website without taking further steps to publicise it may not be sufficient to satisfy the notification requirements.

The OAIC has indicated that a published notification statement should generally remain available for a reasonable period. In many cases, six months will be appropriate.

Example – notifying only individuals at risk of serious harm

A website is compromised for a two-day period and a malicious actor obtains information entered by users during that time.

Following its investigation, the organisation concludes that only individuals who logged into the website during the affected period are likely to be at risk of serious harm.

The organisation may notify those individuals rather than every user of the website.

Protecting privacy during notification

When preparing notifications, organisations should take care not to disclose additional personal information.

For example, a notification should not identify affected individuals or include personal information that is unnecessary to explain the breach.

The purpose of notification is to provide affected individuals with the information they need to understand the breach and take steps to reduce the risk of harm.

Data breaches involving more than one organisation

Personal information is often held or managed by more than one organisation.

For example, organisations may share personal information under outsourced service arrangements, cloud service agreements, IT support agreements, Commonwealth government contracts, joint ventures, shared service arrangements.

Where personal information is jointly held and a data breach occurs, more than one organisation may have obligations under the NDB scheme.

Jointly held personal information

If a data breach affects personal information that is jointly held by two or more organisations, each organisation may have an interest in the breach and responsibility for ensuring that the requirements of the NDB scheme are met.

However, where the breach relates solely to jointly held personal information, only one organisation needs to comply with the notification requirements on behalf of all affected organisations.

This means that one organisation may assess the suspected breach, prepare the notification statement, notify the OAIC, and notify affected individuals.

If that organisation properly complies with the notification requirements, the other organisations will generally also be taken to have complied.

Deciding who will notify

The NDB scheme does not prescribe which organisation must undertake the assessment or notification process.

The organisations involved should reach agreement as quickly as possible about who will assess the breach, who will communicate with affected individuals, who will liaise with the OAIC, how information about the breach will be shared.

Even where one organisation takes responsibility for notification, the other organisations may still choose to undertake their own assessment of the incident.

Tip

The OAIC has indicated that the organisation with the most direct relationship with affected individuals will often be best placed to notify those individuals. However, the most appropriate arrangement will depend on the circumstances of the breach and the relationship between the organisations.

Note

If no organisation undertakes the required notification, each organisation may be at risk of failing to comply with the NDB scheme.

Information that may be included in notifications

The organisation responsible for notification may decide to include information about the other organisations involved in the breach. Whether this is appropriate will depend on the circumstances.

Relevant considerations may include:

- the relationship between the organisations
- whether affected individuals are familiar with the other organisations
- whether identifying the other organisations will help affected individuals understand the breach and its consequences

In some situations, it may be sufficient to describe the nature of the relationship rather than identifying every organisation involved.

Example

A not-for-profit organisation uses an external IT provider to host and manage a client database. A cyber security incident results in unauthorised access to personal information held in the database. Because both organisations hold or control aspects of the personal information, the breach may affect both organisations.

The organisations agree that the not-for-profit organisation will assess the incident, notify affected individuals and notify the OAIC because it has the direct relationship with the affected clients. Provided the notification requirements are properly met, the NDB scheme generally does not require both organisations to notify separately.

Planning ahead

Where personal information is shared between organisations, it is good practice to address data breach responsibilities before a breach occurs. Organisations should consider including provisions in contracts that deal with incident reporting, breach assessment, notification responsibilities, cooperation during investigations, information-sharing arrangements.

Reporting data breaches to other authorities

In addition to notifying affected individuals and OAIC, organisations should consider whether a data breach triggers any other legal, regulatory or contractual reporting obligations.

Whether additional notifications are required will depend on the nature of the information involved, the organisation's activities and any contractual arrangements that apply.

Examples of other authorities that may need to be notified include:

- the Australian Taxation Office (**ATO**), where tax file number information is involved
- the Australian Digital Health Agency, where information held in the My Health Record system is involved
- government agencies under funding agreements or service contracts
- industry-specific regulators with reporting requirements that apply to the organisation

Organisations should also consider whether notification is required under funding agreements, service agreements, procurement contracts, insurance policies, outsourced service arrangements. Keep a record of all regulators, government agencies and other authorities notified about the breach.

Example

A not-for-profit organisation experiences a data breach involving tax file number information collected as part of an employment assistance program.

In addition to assessing its obligations under the NDB scheme, the organisation may need to seek guidance from the Australian Taxation Office regarding the handling of the affected tax file number information.

Example

A health service provider participating in the My Health Record system experiences a data breach involving information contained in a person's My Health Record.

The organisation may need to notify the OAIC under the NDB scheme and should consider whether guidance or reporting to the Australian Digital Health Agency is also required.

Step 4: Review

Once an organisation has contained, assessed and responded to a data breach, it should review the incident to understand what happened and reduce the likelihood of a similar breach occurring in the future.

The OAIC encourages organisations to treat data breaches as an opportunity to strengthen their privacy, information handling and cyber security practices.

A review should occur regardless of whether the incident resulted in an eligible data breach or required notification under the NDB scheme.

Reviewing the incident

The purpose of a review is to identify:

- how the breach occurred
- whether the organisation's response was effective
- whether existing controls and procedures were adequate
- what improvements can be made to prevent similar incidents

Organisations should document the outcomes of the review and any actions that will be taken in response.

Questions to consider

When reviewing a data breach, an organisation should consider:

- How did the breach occur?
- Could the breach have been detected earlier?
- Were the organisation's response procedures effective?
- Were notification obligations identified and addressed promptly?
- Were staff aware of their responsibilities?
- Are changes required to systems, policies or procedures?
- Are additional privacy or cyber security controls needed?

Learning from the incident

A data breach can highlight weaknesses in organisational practices and systems.

Depending on the circumstances, the review may lead to:

- a security review
- additional staff training
- updates to policies and procedures
- improvements to access controls
- implementation of new technical safeguards
- changes to information retention and destruction practices
- updates to contracts with service providers

Organisations should ensure that any identified improvements are implemented and monitored.

Managing emerging privacy risks

Work environments, technologies and privacy risks continue to evolve.

Many organisations now operate in hybrid or remote work environments and use cloud-based systems, online platforms and third-party service providers to manage personal information.

These changes can create new privacy and information security risks.

Examples include:

- increased remote access to systems and information
- use of personal devices for work purposes
- reliance on cloud-based services
- greater use of automated systems and AI tools
- increased exposure to cyber security threats

Organisations should regularly review whether their privacy and security practices remain appropriate for their operating environment.

Privacy impact assessments

Where new technologies, programs or processes involve the handling of personal information, organisations should consider undertaking a privacy impact assessment.

A privacy impact assessment can help identify privacy risks before they result in a breach and assist organisations to implement appropriate safeguards.

The OAIC has published guidance Assessing privacy risks in changed working environments: privacy impact assessments to assist organisations.

Tip

A data breach review should focus not only on what went wrong, but also on whether existing practices can be improved. Lessons learned from a single incident can significantly strengthen an organisation's overall privacy and cyber security posture.

Example

A not-for-profit organisation experiences a data breach after an employee accidentally emails personal information to the wrong recipient.

Following its review, the organisation identifies several improvements, including additional staff training, clearer procedures for handling personal information, technical controls to reduce the risk of emails being sent to incorrect recipients.

Although the breach was caused by human error, the review enables the organisation to reduce the likelihood of similar incidents occurring in the future.

Declaration of an eligible data breach by the Minister

Recent amendments to the *Privacy Act 1988* (Cth) give the Minister the power to make a declaration of an eligible data breach. The purpose of a declaration is to help organisations share information where necessary to protect affected individuals and prevent or reduce harm arising from the misuse of personal information following a significant data breach.

A declaration may authorise the collection, use or disclosure of personal information that would otherwise not be permitted under the Australian Privacy Principles (**APPs**). This allows organisations and other entities to share information where necessary to respond to risks arising from an eligible data breach.

While these declarations are unlikely to apply to most data breaches experienced by not-for-profit organisations, they may become relevant following a major cyber security incident or large-scale data breach.

Purpose of a declaration

Following a significant data breach, organisations may need to share personal information quickly to help protect affected individuals.

For example, information sharing may assist with preventing fraud or identity theft, responding to cyber security incidents, limiting financial loss, reducing emotional or psychological harm, preventing further misuse of personal information.

A declaration can provide a legal basis for this information sharing.

Example

A not-for-profit organisation experiences a cyber security incident that results in unauthorised access to clients' names, dates of birth and financial information.

The compromised information is then used to attempt identity theft and fraud.

A declaration may permit the organisation to disclose relevant information to financial institutions so that additional monitoring and protective measures can be implemented for affected individuals.

Circumstances in which a declaration may be made

The Minister may only make a declaration for specified purposes related to preventing or reducing harm arising from the misuse of personal information following unauthorised access to, or disclosure of, that information.

These purposes include:

- preventing cyber security incidents, fraud, scam activity or identity theft
- responding to cyber security incidents, fraud, scam activity or identity theft
- responding to the consequences of cyber security incidents, fraud, scam activity or identity theft
- addressing malicious cyber activity
- reducing financial, emotional, psychological or physical harm arising from a data breach

Information contained in a declaration

A declaration will specify matters such as:

- the kinds of personal information covered by the declaration
- the entities, or classes of entities, that may collect, use or disclose that information
- the entities, or classes of entities, to whom the information may be disclosed
- the purposes for which the information may be collected, used or disclosed

When an organisation may rely on a declaration

An organisation may be able to collect, use or disclose personal information under a declaration where:

- it reasonably believes an individual may be at risk because of the eligible data breach
- the collection, use or disclosure is for a purpose specified in the declaration
- the information falls within a category covered by the declaration, and
- the relevant entities are covered by the declaration

Note

A declaration does not remove an organisation's obligations under the Notifiable Data Breaches scheme. An organisation must still assess, contain and notify eligible data breaches where required.

Declaration of an emergency by the Minister

The *Privacy Act 1988* (Cth) also gives the Minister the power to make an emergency declaration.

The purpose of an emergency declaration is to facilitate the sharing of personal information during a disaster or emergency where information sharing is necessary to protect individuals, coordinate responses or provide assistance.

Like a declaration of an eligible data breach, an emergency declaration may authorise the collection, use or disclosure of personal information that would otherwise not be permitted under the Australian Privacy Principles (**APPs**).

While most not-for-profit organisations are unlikely to rely on an emergency declaration regularly, organisations involved in disaster relief, emergency response, community recovery, health services or humanitarian assistance should be aware of these powers and their potential application during a major emergency or disaster.

Purpose of an emergency declaration

During an emergency or disaster, organisations may need to share personal information quickly to assist affected individuals or support emergency response efforts.

For example, information sharing may assist with:

- locating people who are missing, injured or at risk
- providing medical treatment, health services or emergency assistance
- coordinating disaster response activities
- informing family members or other responsible persons
- facilitating access to financial or humanitarian assistance

An emergency declaration provides a legal framework for this information sharing where timely action is required.

Example

Following a major bushfire, a community organisation is assisting people displaced by the emergency.

An emergency declaration may permit personal information to be shared between government agencies, emergency services and support organisations to help identify affected individuals and coordinate support services.

Circumstances in which an emergency declaration may be made

The Minister may make an emergency declaration where it is necessary to respond to an emergency or disaster.

Circumstances may include activities aimed at:

- identifying individuals who are, or may be, injured, missing or deceased because of the emergency or disaster
- identifying individuals who are, or may be, otherwise affected by the emergency or disaster
- assisting affected individuals to obtain medical treatment, health services, repatriation services or other support
- assisting individuals at risk of being affected by the emergency or disaster
- supporting law enforcement activities relating to the emergency or disaster
- coordinating or managing the emergency response
- informing responsible persons about matters affecting individuals involved in, or affected by, the emergency or disaster

Information contained in an emergency declaration

An emergency declaration will specify matters such as:

- the kinds of personal information covered by the declaration
- the entities, or classes of entities, that may collect, use or disclose that information
- the entities, or classes of entities, to whom the information may be disclosed
- the purposes for which the information may be collected, used or disclosed

When an organisation may rely on an emergency declaration

An organisation may be able to collect, use or disclose personal information under an emergency declaration where the collection, use or disclosure is authorised by the declaration and is for a purpose specified in the declaration.

Whether a declaration applies will depend on its terms and the organisation's role in responding to the emergency or disaster.

Regulatory action and penalties under the NDB scheme

If an organisation fails to comply with the Notifiable Data Breaches (**NDB**) scheme, the Office of the Australian Information Commissioner (**OAIC**) has a range of regulatory powers available to investigate the breach and require corrective action.

In some circumstances, non-compliance with the NDB scheme may also result in significant civil penalties.

The OAIC's powers include:

- **Apply to a court for a civil penalty order for a breach of a civil provision**

  The maximum penalty for serious or repeated interferences with privacy is the greater of:

  – $50 million

  – three times the value of any benefit obtained from the conduct (where that value can be determined), or

  – 30% of the organisation's adjusted turnover during the relevant period where the benefit cannot be determined

  Depending on the circumstances, a serious failure to comply with the NDB scheme may contribute to a finding of a serious or repeated interference with privacy.

- **Accept an enforceable undertaking and commence proceedings to enforce it**

  An organisation may agree to implement remedial measures, improve its compliance practices, undertake staff training or review its information-handling procedures. If the organisation does not comply with its undertaking, the OAIC may seek enforcement through the courts.

- **Direct an organisation to prepare a notification statement and notify affected individuals**

  Where the OAIC becomes aware of a potentially eligible data breach and considers notification is required, it may direct an organisation to comply with the notification requirements of the NDB scheme.

- **Apply to the court for an injunction**

  The OAIC may seek orders to prevent conduct from continuing or recurring. For example, a court may order an organisation to stop a particular activity until appropriate privacy or security measures have been implemented.

Caution

Compliance with the NDB scheme does not mean an organisation has complied with all of its obligations under the *Privacy Act 1988* (Cth).

An organisation may still face regulatory action if it has breached other provisions of the Privacy Act, including the requirement to take reasonable steps to protect personal information.

Before directing notification

Before directing an organisation to notify affected individuals, the OAIC must generally give the organisation an opportunity to make submissions.

This allows the organisation to provide additional information about the incident, explain any actions already taken and respond to the proposed direction.

Example

In 2017, an unintentional data breach involving the Australian Red Cross Blood Service resulted in personal information being made publicly accessible.

Following an investigation, the OAIC accepted an enforceable undertaking under which the organisation committed to reviewing and strengthening its privacy and information security practices.

The OAIC did not seek penalties. In reaching its conclusions, the OAIC took into account the organisation's response to the incident, including the steps taken to contain the breach and reduce the likelihood of a similar incident occurring in the future.

Organisations that respond quickly, cooperate with regulators, take effective remedial action and strengthen their privacy practices are generally better placed to demonstrate compliance with their obligations and reduce the risk of further regulatory action.

Part 6

Practical compliance tips and permitted situations

Practical compliance tips and permitted situations

This part of the guide covers:

- practical steps organisations can take to comply with privacy laws
- permitted situations that allow personal information to be collected, used or disclosed without consent in specific circumstances

Privacy compliance is not just about having a privacy policy.

Effective privacy management requires organisations to implement appropriate governance, procedures, training and information management practices.

The *Privacy Act 1988* (Cth) also contains a number of exceptions, known as permitted situations, which allow personal information to be collected, used or disclosed without consent in certain circumstances.

Practical compliance tips

The following practical steps can help not-for-profit organisations comply with privacy laws and reduce privacy risks.

- **Conduct a privacy audit**

  Organisations should regularly review:
  - what personal information they collect
  - how information is used and disclosed
  - how information is stored and secured
  - how privacy complaints and requests are managed
  - how information is retained, destroyed or de-identified

  A privacy audit can help identify privacy risks and areas requiring improvement.

- **Appoint a privacy officer**

  Organisations should appoint a person responsible for privacy compliance.

  A privacy officer can:
  - oversee privacy policies and procedures
  - coordinate staff training
  - manage privacy complaints and requests
  - assist with privacy compliance reviews

  Consider establishing a dedicated privacy contact email address, such as privacy@[organisation].com.au.

- **Review and update privacy policies**

  Privacy policies should accurately reflect the organisation's information-handling practices.

Policies should be reviewed regularly and updated whenever:

- organisational practices change
- new technologies are introduced
- privacy laws change

- **Review contracts and relationships with third parties**

  Privacy obligations frequently arise through government contracts, funding agreements and service arrangements.

  Organisations should consider whether contractors, cloud providers, fundraising platforms or other third parties:

  - handle personal information on the organisation's behalf
  - require contractual privacy obligations
  - create additional privacy risks

- **Develop privacy procedures and guidance materials**

  Privacy compliance is often easier when staff and volunteers have access to practical guidance.

  Organisations should consider developing:

  - privacy procedures
  - complaint handling procedures
  - collection notice templates
  - information handling guidelines
  - data breach response procedures

- **Maintain a data breach response plan**

  A documented data breach response plan can help organisations respond quickly and effectively to privacy incidents.

  The plan should identify:

  - key decision-makers
  - reporting procedures
  - assessment and notification processes
  - communication responsibilities

- **Train staff, volunteers and contractors**

  Privacy obligations are easier to comply with when personnel understand their responsibilities.

  Training should be provided regularly and updated when procedures or legal obligations change.

- **Promote transparency**

  Privacy information should be easy to find and understand.

  Organisations should ensure that:

  - privacy policies are easily accessible
  - contact details for privacy enquiries are readily available
  - privacy complaints can be made easily

Permitted situations

The Privacy Act contains a number of exceptions that allow personal information, including sensitive information and health information, to be collected, used or disclosed without consent in specified circumstances.

These exceptions, known as **permitted situations**, are referred to in part 4 of this guide: What are your organisation's obligations under Privacy Laws? and explained in more detail below.

The permitted situations discussed below are those most likely to be relevant to not-for-profit organisations.

Permitted general situations

Situation	Applies to	Conditions
Serious threat to life, health or safety	Collection, use or disclosure of personal information or a government-related identifier	• It is unreasonable or impracticable to obtain the individual's consent, and • the organisation reasonably believes the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any person, or to public health or safety.
Unlawful activity or serious misconduct	Collection, use or disclosure of personal information or a government-related identifier	• The organisation reasonably suspects that unlawful activity, or misconduct of a serious nature, relating to its functions or activities has occurred, is occurring or may occur, and • the organisation reasonably believes the collection, use or disclosure is necessary to take appropriate action.
Locating a missing person	Collection, use or disclosure of personal information	• The organisation reasonably believes the collection, use or disclosure is reasonably necessary to assist an APP entity, body or person to locate a missing person, and • the collection, use or disclosure complies with relevant OAIC rules.
Legal claims and dispute resolution	Collection, use or disclosure of personal information	• The collection, use or disclosure is reasonably necessary for – establishing, exercising or defending a legal or equitable claim, or – a confidential alternative dispute resolution process

Permitted health situations

The Privacy Act also contains specific permitted health situations that apply to health information.

Situation	Applies to	Conditions
Provision of a health service	Collection of health information about a person receiving a health service	The information is necessary to provide the health service and either: • collection is required or authorised under an Australian law (other than the Privacy Act), or

		• collection occurs in accordance with binding professional confidentiality rules established by a competent health or medical body
Collection of third-party health information	Collection of health information about another person	• The health information forms part of the family, social or medical history of the health service recipient • Collection is necessary to provide the health service • The information is collected from the health service recipient or, where appropriate, a responsible person acting on their behalf
Disclosure to responsible persons	Disclosure of health information	• The organisation provides a health service to the individual. • The recipient is a responsible person for that individual. • The individual is incapable of giving or communicating consent. • A health practitioner reasonably believes the disclosure is necessary for care, treatment or compassionate reasons. • The disclosure is limited to what is reasonably necessary. • The disclosure is not contrary to any known wishes of the individual.
Use or disclosure of genetic information for the benefit of a family member	Use or disclosure of genetic information	• The information was obtained while providing a health service. • The organisation reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative. • The use or disclosure complies with approved National Health and Medical Research Council (**NHMRC**) guidelines. • In the case of disclosure, the recipient is a genetic relative of the individual from whom the information was obtained.
Research, statistics and health service management	Collection of health information	• The collection is necessary for research, public health or public safety activities, or the management, funding or monitoring of a health service. • The purpose cannot be achieved using de-identified information. • It is impracticable to obtain consent. • Additional legal or ethical requirements apply, including compliance with NHMRC guidelines where relevant.
Research, statistics and health service management	Use or disclosure of health information	• The use or disclosure is necessary for research or statistical activities relevant to public health or public safety.

- It is impracticable to obtain consent.
- The use or disclosure complies with approved NHMRC guidelines.
- Where information is disclosed, the organisation reasonably believes the recipient will not further disclose the information or any personal information derived from it.

The OAIC has published guides to permitted general situations and permitted health situations:

- Chapter C: Permitted general situations
- Chapter D: Permitted health situations

These resources provide additional guidance on the circumstances in which the exceptions may apply.

Caution

Permitted situations are exceptions to the general privacy rules and often involve complex legal requirements. If your organisation is unsure whether a collection, use or disclosure of personal information is permitted, consider obtaining legal advice.

Part 7

Privacy enforcement, penalties and ongoing obligations

Privacy enforcement, penalties and ongoing obligations

This part of the guide covers:

- consequences of failing to comply with privacy laws
- regulatory action and penalties under the Privacy Act
- the statutory tort for serious invasions of privacy
- doxxing offences
- ongoing privacy compliance obligations

The privacy obligations discussed throughout this guide are supported by a range of enforcement mechanisms.

Failing to comply with privacy laws can have significant consequences for both organisations and individuals.

Depending on the circumstances, non-compliance may result in:

- regulatory action by the Office of the Australian Information Commissioner (**OAIC**)
- civil penalties under the Privacy Act
- claims under the statutory tort for serious invasions of privacy
- criminal liability for doxxing offences
- reputational damage and loss of public trust

The seriousness of the consequences will depend on factors such as the nature of the information involved, the number of people affected and the steps taken by the organisation to protect personal information.

Importantly, privacy compliance is not a one-off exercise. Organisations are expected to take ongoing steps to manage privacy risks, protect personal information and respond appropriately when issues arise.

Regulatory action under the Privacy Act

Most of the obligations discussed in this guide are enforceable under the Privacy Act.

Where an organisation fails to comply with those obligations, the OAIC may investigate and take regulatory action.

An organisation may breach the Privacy Act by engaging in conduct that interferes with the privacy of an individual.

For APP entities, an interference with privacy may include:

- an act or practice that breaches an Australian Privacy Principle (**APP**), or
- an act or practice that breaches an APP code (a legally binding privacy code made under the Privacy Act that applies to particular organisations or sectors) that applies to the organisation

Recent amendments to the Privacy Act have strengthened the OAIC's regulatory powers, including powers to issue infringement notices, issue compliance notices and seek civil penalties.

Serious interferences with privacy

Some privacy breaches are more serious than others.

When deciding whether an interference with privacy is serious, a court may consider factors such as:

- the kinds of information involved
- the sensitivity of the information
- the actual or potential consequences for affected individuals
- the number of individuals affected
- whether children or vulnerable people were affected
- whether the conduct occurred repeatedly or continuously
- whether the organisation failed to implement reasonable privacy practices, procedures and systems
- any other matter the court considers relevant

Civil penalties for serious or repeated interferences with privacy

Serious or repeated interferences with privacy can attract substantial penalties.

The maximum penalty for an individual is AUD 2.5 million.

For a body corporate, the maximum penalty is the greater of:

- AUD 50 million
- three times the value of any benefit obtained from the conduct (where that benefit can be determined), or
- 30% of the body's adjusted turnover during the relevant turnover period (where the benefit cannot be determined)

The OAIC may also:

- investigate privacy practices
- conduct privacy assessments
- make determinations
- accept enforceable undertakings
- issue infringement notices and compliance notices

Civil penalties for interferences with privacy

Where an interference with privacy is not considered serious, civil penalties may still apply.

The maximum penalty is:

- AUD 660,000 for an individual, and
- AUD 3.3 million for a body corporate

Civil penalties for specific interferences with privacy

The Privacy Act also includes civil penalties for certain administrative breaches.

Examples may include:

- certain failures to comply with Privacy Act requirements
- some failures to comply with APP requirements
- submission of a non-compliant eligible data breach statement under the Notifiable Data Breaches scheme

The maximum penalty for these types of contraventions is:

- AUD 66,000 for an individual, and
- AUD 330,000 for a body corporate

Statutory tort for serious invasions of privacy

Regulatory action is not the only consequence of failing to protect privacy.

Since 10 June 2025, individuals have also had a statutory right to bring proceedings for a serious invasion of privacy. This means that, in some circumstances, an affected individual can sue the person or organisation responsible for the invasion of their privacy.

The tort applies where there has been either:

- an intrusion upon a person's seclusion, or
- a misuse of information relating to a person where they had a reasonable expectation of privacy

Importantly, an individual does not need to prove financial loss or damage in order to bring a claim.

To succeed, an individual must establish:

1. there was an invasion of privacy
2. they had a reasonable expectation of privacy
3. the conduct was intentional or reckless
4. the invasion was serious, and
5. the public interest in protecting their privacy outweighs any competing public interest

Invasion of privacy

An invasion of privacy may occur through either an intrusion upon an individual's seclusion or a misuse of information relating to the individual.

An **intrusion upon seclusion** generally involves conduct that intrudes into a person's private life, activities or private space.

Examples may include:

- entering a person's private space without permission
- monitoring a person's private activities
- listening to or recording private conversations

Misuse of information generally involves the unauthorised collection, use or disclosure of information relating to an individual.

Examples may include:

- collecting personal information without authority
- using personal information for an unauthorised purpose
- disclosing personal information without consent or another lawful basis

Note – the information does not need to be true

If a claim relates to the misuse of information, it does not matter whether the information is true or false.

A reasonable expectation of privacy

Not only does the individual need to establish there has been an intrusion, but that they had a reasonable expectation of privacy, considering all the circumstances.

Considerations include:

- the means used to invade the individual’s privacy, including any device or technology used

- the purpose of the invasion of privacy
- attributes of the individual (for example the individual's age, occupation or cultural background) in this instance a child may have a greater expectation of privacy than an adult in certain circumstances
- the conduct of the individual (for example whether the individual invited publicity or manifested a desire for privacy)
- intruding upon the individual's seclusion—the place where the intrusion occurred (for example there may be a higher expectation of privacy in a person's home than in a public place)
- misusing information that relates to the individual, considering:
  - the nature of the information (for example whether the information related to intimate or family matters, health or medical matters or financial matters)
  - how the information was held or communicated by the individual, and
  - whether and to what extent the information was already in the public domain

Intentional or reckless conduct

The tort applies only where the conduct was intentional or reckless.

Intentional conduct involves deliberately engaging in conduct that results in the invasion of privacy.

Reckless conduct occurs where a person is aware of a substantial risk that their conduct will invade another person's privacy but proceeds regardless.

Seriousness of invasion

The invasion of privacy must be serious (to discourage individuals bringing trivial claims).

When determining whether an invasion is serious, a court may consider:

- the likely offence, distress or harm to dignity caused by the conduct
- whether the defendant knew, or ought reasonably to have known, of the likely impact
- whether the conduct was deliberate or malicious

Public interest balancing

Privacy rights are important, but they are not absolute.

A court must balance the public interest in protecting privacy against competing public interests, such as:

- freedom of expression (for example, political communication and artistic expression)
- freedom of the media (for example, investigation and reporting of matters of public concern and importance)
- the proper administration of government
- open justice
- public health and safety
- national security
- the prevention and detection of crime and fraud

Example – a serious invasion of privacy

A not-for-profit organisation collects donor information as part of its fundraising activities.

An employee deliberately publishes the names and contact details of donors who made small donations and posts comments intended to shame those individuals publicly.

The affected donors expected their information to remain confidential and suffer distress and reputational harm as a result.

Depending on the circumstances, this conduct may amount to a serious invasion of privacy.

Exemptions from the tort of serious invasions of privacy

The tort does not apply in all circumstances.

Exemptions include certain conduct by:

- intelligence agencies
- law enforcement bodies
- persons under 18 years of age
- journalists and certain other persons in specified circumstances

Defences to the tort of serious invasions of privacy

A claim can be defeated by successfully arguing one of the following defences:

- the invasion of privacy was required to comply with an Australian law
- the individual (having capacity to do so) consented to the invasion of privacy
- the conduct was necessary to prevent or lessen a serious threat to life, health or safety
- the conduct was necessary to defend people or property

Time limits on when to bring a cause of action

If the individual is under 18 years of age when the invasion of privacy occurred, they have until their 21st birthday to bring a cause of action.

Otherwise, individuals must start proceedings within one year of becoming aware of the invasion of privacy, up to a maximum of three years after the invasion of privacy occurred.

Doxxing offences

Some conduct involving personal information can also have criminal consequences.

One example is doxxing, which involves exposing another person's personal information online in a manner that is menacing or harassing.

Doxxing offences were introduced into the *Criminal Code Act 1995* (Cth).

Note

The doxxing offences are not subject to the small business and journalist exemptions under the Privacy Act.

A person commits a doxxing offence if:

- they use a carriage service to publish, distribute or otherwise make information available
- the information is personal data relating to one or more individuals, and
- reasonable people would regard the conduct as menacing or harassing in the circumstances

A carriage service includes communication services such as email, text messaging, telephone services, social media platforms.

Doxxing an individual attracts a maximum penalty of six years imprisonment.

Doxxing that targets a person or group because of their race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality, national or ethnic origin attracts a maximum penalty of seven years imprisonment.

Doxxing examples

Deanonymising doxxing – Cody is annoyed by complaints made against him by a customer under a pseudonym. To get back at them, Cody reveals the person's identity online and asks people to send the customer abusive emails.

Targeting doxxing – Alice and Miles have had a falling out. To teach Miles a lesson, Alice posts Miles' address and contact details on a public social media page, with a malicious message stating that he needs to 'watch himself'.

Delegitimising doxxing – Gigi is angry at Jed, a work colleague. She decides to reveal personal messages with him to damage his reputation.

Ongoing privacy obligations

Many privacy breaches occur because organisations stop actively reviewing their privacy practices.

Privacy compliance is therefore best viewed as an ongoing governance responsibility rather than something that is addressed once and then forgotten.

The OAIC's privacy management framework identifies four steps that can help organisations maintain compliance:

Step 1.	Embed a culture of privacy that supports compliance
Step 2.	Establish a robust and effective privacy process
Step 3.	Evaluate privacy processes to ensure they remain effective
Step 4.	Enhance responses to privacy risks and issues

How an organisation implements these steps will depend on factors such as:

- its size
- its governance arrangements
- the nature of its activities
- the volume and sensitivity of the information it handles

For many not-for-profit organisations, effective privacy management will involve regular staff training, periodic review of policies and procedures, ongoing assessment of privacy risks and prompt responses to incidents when they occur.

Strong privacy governance, regular review of privacy practices and a culture of privacy awareness are often the most effective ways to reduce privacy risks and avoid the consequences discussed in this part of the guide.

justice connect