Privacy guide

A guide to complying with privacy laws in Australia

Mar 2025

justice connect

Contents

Part 1 5

Introduction 6

Why you should consider your organisation's responsibilities under Privacy Laws 6

What this guide covers 7

What are the Privacy laws? 8

Recent changes to the Privacy Laws 9

Privacy issues when fundraising 10

Privacy laws and private ancillary funds 10

Part 2 12

What information is covered by Privacy Laws? 13

What is 'personal information'? 13

What is sensitive information? 14

What is 'health information'? 15

Other categories of confidential information 15

Part 3 17

Is your organisation subject to Privacy Laws? 18

Federal Privacy Laws: Australian Privacy Principles (APPs) 19

Exemptions to the APPs 22

State and territory Privacy Laws and Principles 24

Health Privacy Laws 25

Part 4 27

What are your organisation's obligations under Privacy Laws? 28

An organisation's privacy policy 28

Rules for collecting information 30

Collecting personal information 30

Collecting sensitive and health information 31

Things you are obliged to tell the person providing information 32
Getting consent 33
Unsolicited information 35
Storing personal information 35
Security measures 35
Other recommended action 37
Health information 37
Using or disclosing information 38
Automated Decision Making 38
Direct marketing 39
Access to and correcting personal information 40
Disclosing across borders 40
Children's Online Privacy Code 41
Comparison of Commonwealth and State and Territory Privacy Principles 42
Part 5 **46**
Notifiable Data Breaches scheme 47
What is the Notifiable Data Breaches scheme? 48
What organisations must comply with the scheme? 48
What kind of data breaches require notification? 49
What is unauthorised access, disclosure or loss? 50
The process for responding to data breaches 51
Containing a data breach 52
Assessing suspected data breaches 53
How is an assessment done? 53
When are data breaches likely to result in serious harm? 53
Exceptions to the requirement to notify 55
Notification 56
Data breaches involving more than one organisation 59
Reporting data breaches to other authorities 60
Reviewing the incident 60
Declaration of an eligible data breach by the Minister 61
Declaration of an emergency by the Minister 62
Penalties for not complying with the scheme 62
Part 6 **64**
Practical tips for compliance and 'permitted situations' 65
Practical compliance tips 65

Exceptions for ‘permitted situations’ 66
Part 7 **70**
Rights of action and penalties under Privacy Laws 71
What happens if your organisation doesn’t comply with Privacy Laws? 71
Interference with the privacy of an individual 71
Tort of serious invasion of privacy 72
Defences to the tort of serious invasions of privacy 74
Doxxing offences 74
Ongoing obligations 75

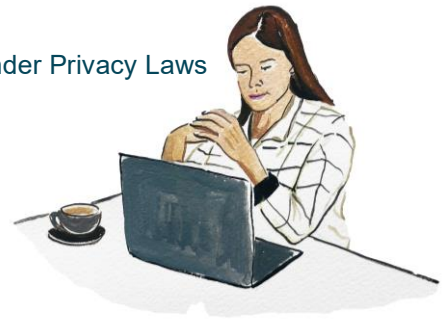
Part 1

Introduction

Introduction

This part:

- why you should consider your organisation's responsibilities under Privacy Laws
- what this guide covers
- what are the Privacy Laws?
- recent changes to the Privacy Laws
- privacy issues when fundraising
- privacy laws and private ancillary funds



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

Disclaimer

This guide provides information on privacy laws, including the Notifiable Data Breaches scheme, 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 you should consider your organisation's responsibilities under Privacy Laws

If you work for a not-for-profit organisation, it's likely that you or your colleagues collect, use, store or disclose information about people – for example, when you deliver services or gather new membership information.

This information will often be classified as 'personal information' under Privacy Laws and may include 'sensitive information' or 'health information'. 'Sensitive information' and 'health information' are subcategories of personal information that require special treatment.

You must consider your organisation's responsibilities under Privacy Laws when you deal with personal information. This includes when you:

- engage and manage employees and volunteers
- advertise your products and services
- fundraise and communicate with members and the public, or
- store and manage records

Note

Handling personal information in a lawful, transparent and respectful way is an important part of building the trust of the people your organisation works with, as well as avoiding any legal consequences of a data breach, including financial penalties.

Questions for your organisation to consider

This guide helps your not-for-profit organisation understand its Privacy Law obligations by considering the following questions:

- What kinds of information do Privacy Laws cover?
- Is the information your organisation collects and holds covered by Privacy Laws?
- What kinds of information do Privacy Laws cover?
- How do you apply the Privacy Law requirements to your not-for-profit organisation?

What this guide covers

The guide has seven parts:

Part 1.	**Introduction**
Part 2.	**What information is covered by Privacy Laws?**
Part 3.	**Is your organisation subject to Privacy Laws?**
Part 4.	**What are your organisation's obligations under Privacy Laws?**
Part 5.	**The Notifiable Data Breaches scheme**
Part 6.	**Practical tips for compliance and 'permitted situations'**
Part 7.	**Rights of action and penalties under Privacy Laws**

Caution

The information in this guide is of a generic nature only and should not be relied on as specific advice. Rather, it provides an overview of the Commonwealth and state and territory laws on privacy. The content is also subject to change.

Privacy Laws are complex and not always easy to apply in practice. You should seek your own legal and other advice for any question, or for any specific situation or proposal, before making any final decision.

What are the Privacy laws?

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.

Note, however, in South Australia:

- an administrative direction on handling personal information binds the public service (PC012- Information Privacy Principles (**IPPs**) Instruction)

Recent changes to the Privacy Laws

The *Privacy and Other Legislation Amendment Act 2024* (Cth), which passed both houses of the Australian Parliament on 29 November 2024, has introduced the following changes to the Privacy Act:

Meaning of 'reasonable steps'	• clarification that the 'reasonable steps' that must be taken to protect the security of personal information includes implementing 'technical and organisational measures', covered in part 4 of this guide: What are your organisation's obligations under Privacy Laws? • effective since **11 December 2024**
Automated decision-making	• a new requirement for privacy policies to disclose information about the use of automated processes to make decisions, covered in part 4 of this guide: What are your organisation's obligations under Privacy Laws? • to start on **10 December 2026**
Children's Online Privacy Code	• a framework for a Children's Online Privacy Code, covered in part 4 of this guide: What are your organisation's obligations under Privacy Laws? • to be developed and registered by **10 December 2026**
Whitelisting countries for disclosure overseas	• ministerial powers to 'whitelist' countries that provide substantially similar privacy protections, to assist entities disclosing personal information overseas, covered in part 4 of this guide: What are your organisation's obligations under Privacy Laws? • effective since **11 December 2024**, but a list of 'whitelist' countries has not yet been published
Tort for serious invasions of privacy	• a new statutory cause of action (tort) for serious invasions of privacy, covered in part 7 of this guide: Rights of action and penalties under Privacy Laws • to start by **10 June 2025**
OAIC civil powers and penalties	• new civil powers for the Office of the Australian Information Commissioner (**OAIC**) to issue infringement notices and compliance notices, and to impose civil penalty orders for non-compliance for three levels of interference with the privacy of an individual, covered in part 7 of this guide: Rights of action and penalties under Privacy Laws • effective since **11 December 2024**

A new doxxing offence has also been introduced under the Criminal Code (effective since **11 December 2024**). This is covered in part 7 of this guide: Rights of action and penalties under Privacy Laws

Privacy issues when fundraising

If your organisation is subject to federal Privacy Laws and is collecting, using, storing or disclosing personal information as part of, or in connection with, its fundraising activities, **you will need to make sure your fundraising activities comply with the Privacy Laws**. (See part 3 of this guide: Is your organisation subject to Privacy Laws?)

When fundraising, you must:

- notify donors, volunteers, clients and others that you intend to use the personal information you collect from them for fundraising purposes from the start
- If you share your donor lists with other organisations, make sure that you explain who their information might be passed to
- always offer donors who support fundraising campaigns a choice about receiving information on non-fundraising activities or new campaigns from the start, and
- provide a prominent, simple opt out option in all fundraising communications

If you haven't notified a person that their personal information might be used for fundraising purposes, don't use it for those purposes unless:

- you first obtain consent, or
- an exception applies (for example, for non-sensitive personal information, the fundraising purpose is related to the primary purpose and the person would reasonably expect you to use the information in that way)

Note

Always consider the capacity of children, young adults, or people with compromised capacity when obtaining consent.

Tip

It's a good idea to only allow staff access to client information on a 'need to know' basis. For example, make sure that people involved in getting donor memberships don't have routine access to personal information that may be kept on client databases, and put checks and balances in place to protect the security of personal information.

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

Privacy laws and private ancillary funds

Details of charities registered with the Australian Charities and Not-for-profits Commission (**ACNC**) can be viewed by the public on the ACNC Register. Registration with the ACNC is a prerequisite for a charity to access certain Commonwealth tax benefits. For this reason, although charity registration is voluntary, most not-for-profits that are charitable organisations register with the ACNC.

Charities that are private ancillary funds may reveal the personal information of individual donors on the ACNC Register. An ancillary fund is a fund that links donors with an organisation that has deductible gift recipient status.

Note

If your organisation is a private ancillary fund and you are concerned that publication of a donor name, ABN, contact details, governing rules, financial reports or annual information statement is likely to result in the identification of the donor, you can apply to have identifying information withheld under the *Australian Charities and Not-for-profits Commission Regulation 2013* (Cth) before registration.

Part 2

What information is covered by Privacy Laws?

What information is covered by Privacy Laws?

This part covers:

- personal information
- sensitive information
- health information
- other categories of information

Generally, Privacy Laws do not regulate or apply to all the information your organisation collects or deals with.

So, the first step in understanding your obligations under Privacy Laws is to determine whether the information you hold, or want to collect, falls into one of the following categories:

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

Privacy Laws apply to these categories in different ways. The way that Privacy Laws apply to your organisation also depends on the size and type of your organisation (discussed further in part 3 of this guide: Is your organisation subject to Privacy Laws?).

What is 'personal information'?

'Personal information' is information or an opinion about an identified person (or a person who is 'reasonably identifiable').

Personal information can be:

- true or false
- verbal, written or photographic, or
- recorded or unrecorded

Personal information includes a person's name, address, contact details (such as telephone number or email), date of birth, gender, and internet protocol (IP) address.

When will someone be 'reasonably identifiable'?

Whether someone is 'reasonably identifiable' from the information you hold depends on:

- the nature and extent of the information
- how the information was received, and
- whether it's possible for you to identify the person from resources you hold (including other information available to you)

Deceased people don't have 'personal information' under federal Privacy Laws. But, under some state and territory laws, a deceased person's personal information may still be protected for a period. Also, where information about a deceased person includes information about a living person (for example, if a deceased person with children has an inheritable medical condition) this information may form personal information about the living person.

Personal information doesn't include:

- anonymous information
- aggregated information (for example, data that reflects trends without identifying the sample)
- de-identified information not reasonably capable of re-identification, or
- information about companies or other entities which does not identify individuals

Example

Consider a car licence plate. Most people can't identify the owner of a car simply from the registration number. So, to most people, knowing a car's licence plate number wouldn't make the car owner 'reasonably identifiable'.

But if you work for a car registration agency, you may be able to identify the owner of the car because you have access to other information. Holding information about the car registration would make the person 'reasonably identifiable' to you from the information you hold. In these circumstances, the registration number would be considered personal information.

Tips

- The definition of 'personal information' is very broad and covers photographs of people where they are identifiable. If you plan to take photographs of your event for use in any material (such as your website or in brochures or newsletters), you should arrange notification forms for the people who appear in the images. These forms should explain the purpose of the photographs and how you plan to use them, in addition to the other notification requirements discussed in part 4 of this guide: What are your organisation's obligations under Privacy Laws?
- While information about companies is not covered by Privacy Laws, it might be covered by confidentiality laws. For information on confidentiality- see our guide to intellectual property

What is sensitive information?

'Sensitive information' is a special category of personal information and is subject to stricter legal requirements for collection, storage, use and disclosure.

Under Privacy Laws, information is 'sensitive information' if it is or 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 preferences or practices, or
- criminal record

Health information (discussed further below), including genetic information and many aspects of biometric information are also considered ‘sensitive' information’ under the federal Privacy Laws.

Caution

Your organisation needs to distinguish between different types of personal information to make sure you deal with each type as required by law.

What is ‘health information’?

‘Health information’ is generally afforded a higher level of protection under Privacy Laws.

‘Health information’ includes information or opinions about a person’s:

- physical and mental health
- disability (at any time)
- health preferences (including future provision of health services)
- use of health services
- bodily donations (for example, blood, organs), and
- genetics

Examples of ‘health information’ include:

- notes on a person’s symptoms or diagnosis and treatment
- specialist reports or test results
- appointment and billing details
- dental records
- a person’s healthcare identifier when it’s collected to provide a health service
- prescriptions and other pharmaceutical purchases, and
- any other personal information (such as information about a person’s sexuality, religion, date of birth, gender) collected to provide a health service

Other categories of confidential information

The following types of information are also protected. This guide does **not** cover these types of information.

- ‘spent convictions’ (old, minor criminal convictions)
- tax file numbers (extreme care must be taken with tax file numbers as special rules apply)
- electoral roll information
- surveillance information, and
- credit history

If you deal with this kind of information and are not aware of the particular privacy requirements that apply to your organisation, you should get a privacy lawyer's advice.

Caution

Strict legal requirements apply to the handling of information about a person's credit worthiness.

If your organisation deals with credit information, it should get advice on complying with these obligations.

Part 3

Is your organisation subject to Privacy Laws?

Is your organisation subject to Privacy Laws?

This part covers:

- the sources of Privacy Laws
- who Privacy Laws apply to

Once you have established that the information you collect, store, use or disclose may be considered 'personal', 'sensitive' or 'health' information, you need to work out which (if any) Privacy Laws apply to your organisation.

A not-for-profit organisation may be governed by one or more laws that make up the Privacy Laws.

Three separate sources of law make up the Privacy Laws:

1.	The Australian Privacy Principles (**APPs**) under federal Privacy Laws
2.	Applicable state and territory Privacy Laws (for example, government records and industry specific legislation)
3.	Applicable state and territory health privacy legislation (**Health Privacy Laws**)

Caution

Your organisation may have to comply with more than one set of privacy obligations listed above.

For example, an organisation that has a contract with a Victorian Government agency may need to comply with the APPs as well as the State Privacy Laws.

You will need to make sure your practices are consistent with all the Privacy Laws that apply to your organisation. If you're not sure, you should get legal advice.

The federal legislation is generally not intended to override state and territory privacy legislation but to operate alongside it.

Organisations that meet the criteria set out below must comply with Privacy Law obligations.

Federal Privacy Laws: Australian Privacy Principles (APPs)

The APPs are legal obligations under federal Privacy Laws.

The APPs are summarised below and are discussed in more detail throughout this guide.

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

The APPs set out requirements about how organisations may collect, use, disclose and store information.

The principles are considered best practice for privacy, so even if your not-for-profit organisation is not legally bound by the APPs, it's a good idea to follow them.

State and territory privacy laws largely replicate the APPs, but there are some differences.

In the following two tables, we've summarised

- each APP, and
- the criteria for determining whether your organisation is required to comply with the APPs

What is an 'APP entity'?

An 'APP entity' is an agency or organisation to which the APPs apply for the purposes of the Privacy Act.

Summary of the APPs

APP	Subject
APP 1	**Open and transparent management of personal information** Requires that APP entities manage personal information in an open and transparent way. This enhances the accountability of APP entities for their personal information handling practices and can build community trust and confidence in those practices.
APP 2	**Anonymity and pseudonymity** Provides that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.
APP 3	**Collection of solicited personal information** Distinguishes between an APP entity collecting solicited personal information (APP 3) and receiving unsolicited personal information (APP 4).
APP 4	**Dealing with unsolicited personal information** Outlines the steps an APP entity must take if it receives unsolicited personal information. Unsolicited personal information is personal information received by an entity that has not been requested by that entity.

APP 5	**Notification of the collection of personal information** Requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters.
APP 6	**Use or disclosure of personal information** Outlines when an APP entity may use or disclose personal information. The intent is that an entity will generally use and disclose an individual's personal information only in ways the individual would expect or where one of the exceptions applies.
APP 7	**Direct marketing** An organisation must not use or disclose the personal information that it holds about an individual for the purpose of direct marketing.
APP 8	**Cross-border disclosure of personal information** APP 8 and section 16C create a framework for the cross-border disclosure of personal information. The framework generally requires an APP entity to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs and makes the APP entity accountable if the overseas recipient mishandles the information
APP 9	**Adoption, use or disclosure of government related identifiers** An organisation must not adopt, use or disclose a government related identifier unless an exception applies.
APP 10	**Quality of personal information** Requires an APP entity to take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete. It also requires an APP entity to take reasonable steps 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.
APP 11	**Security of personal information** Requires an APP entity to take active measures to ensure the security of personal information it holds, and to actively consider whether it is permitted to retain personal information.
APP 12	**Access to personal information** Outlines an APP entity that holds personal information about an individual must, on request, give that individual access to the information (APP 12.1).
APP 13	**Correction of personal information** Outlines that an APP entity must take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.

Summary of the criteria for determining whether an organisation is required to comply with the APPs

An organisation must comply with the APPs if it falls into any of the following categories:

- it has an annual turnover of more than $3 million in any financial year since 2002
- it provides a health service (which is broadly defined) to a person (even if the organisation's primary activity is not providing that health service)
- it trades in personal information (for example, buying or selling a mailing list)
- it is a contracted service provider under a Commonwealth contract (for example, an aged care provider or a disability services provider under a Commonwealth agreement)
- it is a credit reporting body
- it operates a residential tenancy database
- it is a reporting entity for the purposes of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
- it is an employee association registered or recognised under the *Fair Work (Registered Organisations) Act 2009* (Cth)
- it is a business that conducts protection action ballots
- it is a business prescribed by the *Privacy Regulation 2013*
- it is related to a body corporate (for example, a subsidiary) that meets any of the above criteria (even if your not-for-profit itself does not), or
- it has opted into the Privacy Act (choosing to comply, despite not meeting any of the above criteria)

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'

'Organisation' is defined broadly under the Privacy Act to include individuals, bodies corporate, partnerships, trusts and other unincorporated associations.

Not-for-profit organisations that are unincorporated associations and trusts also fit into the definition of 'organisation'. 'Bodies corporate' includes many common legal structures in the not-for-profit sector, such as incorporated associations, co-operatives, companies limited by guarantee and indigenous corporations.

Organisations that are not covered by the APPs can 'opt in' to be bound by the APPs. They are then 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.

Examples of when the APPs apply

- ✓ You run a charity that recorded an annual income of $3 million in its most recent Annual Report. **The APPs apply to you.**
- ✓ You are a club with an annual turnover of less than $3 million, but your club has a program or facilities to assist members with injuries or improve fitness and health. It's probably providing a health service, especially if it hires a health professional. **The APPs apply to you.**
- ✓ You are a theatre company with an annual turnover of less than $3 million, but you enter into a sponsorship deal and, as part of that sponsorship deal, you pass your customer list to the sponsor corporation (ie. in exchange for the sponsorship benefit). **The APPs apply to you.**
- ✓ You are a not-for-profit organisation that provides childcare services or activities. While you have an annual turnover of less than $3 million per year, you collect, use and store information about children's allergies, disabilities and medical needs (ie. health information). **The APPs apply to you.**
- ✓ You are a subsidiary of a not-for-profit organisation and have an annual turnover of less than $3 million in Australia. Your not-for-profit organisation is part of a larger global network of not-for-profits. Your parent organisation (incorporated in the US under a different legal entity) has an annual turnover of over $3 million. You provide information about your members, donors or volunteers to your parent not-for-profit organisation. **The APPs apply to you.**
- ✓ You are a not-for-profit organisation that has an annual turnover of less than $3 million. You obtain funding from the Commonwealth Government to run a specific program and you enter into an associated funding contract. **The APPs apply to you.**

Example of when the APPs don't apply

- ✗ You are a sporting club that collects the names and addresses of team participants. You earn $120,000 in annual revenue. Provided you don't fall into any of the other categories listed above**, the APPs don't apply to you.**

Exemptions to the APPs

There are exemptions to the APPs.

Once you've considered whether your not-for-profit organisation is required to comply with the APPs under the 'threshold' criteria (set out above), you need to work out whether your organisation, or particular information it handles, falls into an exemption category.

The main exemption categories relevant to not-for-profit organisations are summarised below.

Employee records exemptions

If an employer handles information that is part of an employee record that is directly related to a person's current or former employment relationship, the employer's conduct is exempt from the APPs.

This exemption does not apply (and so the APPs may still apply) if the information is about:

- former job applicants (who were not employed)
- contractors
- volunteers, or
- employees of related entities (for example, subsidiaries)

Note – this exemption might not extend to records of an employee's (after-hours) behaviour on social media while employed by your organisation, or other records not related to the person's employment with your organisation. This exemption will also not apply to the tort for serious invasions of privacy and doxing offences.

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.

Note

Despite the employee records exemption under federal Privacy Laws, state and territory Privacy Laws may still apply to certain employee information.

In particular, the Health Privacy Laws may apply to private sector organisations, including to not-for-profits that handle health information (including employees' health information).

Example

You are contacted by a prospective employer of a former employee asking for personal information related to their employment record with your organisation. This information is subject to the employee records exemption.

However, during the conversation, the prospective employer asks if you noticed any unusual activity on the employee's social media accounts during their employment. It's unclear if this is covered by the APPs. Err on the side of caution when disclosing information regarding former employees – stick to what is in the employee's official record.

Government contractors' exemption

If an organisation is required to follow the APPs only because it has a contract with government, the organisation is only required to follow the APPs for personal information that it manages in relation to activities under that contract.

Example

Your not-for-profit organisation has an annual turnover of $1.2 million and is not normally bound by the APPs. Your group provides free after school care for refugee children, and also has a contract with the Federal Government to provide English language classes to adult migrants. The personal information you collect, use and disclose in relation to the government-funded English language program is protected by the APPs, but the personal information you manage for the privately-funded after school care program may be exempt.

If an organisation is required to do something under a government contract that is inconsistent with the APPs, an exemption applies so that the terms of the government contract can be met.

Example

You are a not-for-profit halfway house contracted by a state government to assist in rehabilitating juvenile offenders. You are required to disclose information regarding possible offences by residents under the terms of your contract, despite it conflicting with an APP. This information is subject to an exemption to the APPs and may be disclosed.

Political exemption

If you work on behalf of a registered political party or representative (with their authority), the work you do for them will be exempt from the APPs if the purpose of the work is connected with:

- an election
- a referendum
- the party or representative's participation in the political process, or
- facilitating acts or practices of the political party for the purposes of any of the above

Other exemptions

Other exemptions exist, but are not usually relevant to community organisations, for example:

- local councils or state or territory governments or authorities (these entities are exempt from the APPs and are usually subject instead to state and territory Privacy Laws)
- journalism exemption (this only applies when an organisation adopts other media privacy standards), and
- an exemption from some APPs for transfers of information between related organisations

Caution

If your organisation is required to comply with the APPs, and you're not sure whether the information you deal with might fall into one of the exempted categories discussed here, you should get legal advice.

State and territory Privacy Laws and Principles

Australian state and territory information privacy principles (**IPPs**) apply to their respective government agencies (including public sector agencies, local councils, courts, state police, etc.) except where the Health Privacy laws apply. The state and territory IPPs may also apply to organisations that contract with the relevant state or territory government.

State and territory 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. In addition, some privacy principles (dealing with access to information and correction of information) are covered by the *Freedom of Information Act 1992* (WA)

Health Privacy Laws

New South Wales, Victoria and the Australian Capital Territory each have their own specific Health Privacy Laws. The Health Privacy Laws apply a higher standard of protection to certain health information.

The state and territory Health Privacy Laws are set out in the following legislation:	
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 be required to comply with Health Privacy Laws (in addition to federal Privacy Law) if you operate in New South Wales, Victoria or the Australian Capital Territory and:

- you are a health service provider, or
- you collect, hold or use health information (described in part 1 of this guide)

Health service providers

A health service provider may be a public or private organisation including:

- traditional health service providers (such as public or private hospitals, day surgeries, medical practitioners, pharmacists and allied health professionals)
- complementary therapists (such as naturopaths and chiropractors)
- gyms and weight loss clinics, and
- childcare centres and private schools

If you think your organisation may collect, hold or use health information, we recommend you get legal advice to understand your organisation's obligations.

Examples of when Health Privacy Laws apply

- ✓ You are a contracted health service provider to Victoria's 12 publicly managed prisons. You are required to comply with the applicable Health Privacy Laws.
- ✓ You run a safe injection house that takes the names of drop-in patients. You may be required to comply with the applicable Health Privacy Laws

Example of when Health Privacy Laws don't apply

- ✗ You provide first aid at music festivals on an anonymous basis. You would not be required to comply with the Health Privacy Laws.

Part 4

What are your organisation's obligations under Privacy Laws?

What are your organisation's obligations under Privacy Laws?

This part covers:

- more about the APPs
- the requirements for an organisation's privacy policy
- the rules for collecting and storing information
- when an organisation may use or disclose information (including direct marketing)
- access to and correcting information, and
- the differences between state and territory Privacy Principles (**IPPs**)

If your organisation holds or wants to collect 'personal', 'sensitive' or 'health' information about a person and Privacy Laws apply to your organisation, you need to know what your organisation must do to meet its legal obligations.

The Australian Privacy Principles (**APPs**), listed in part 3 of this guide above, are legally binding principles which set the basic standard for protecting 'personal', 'sensitive' and 'health' information at the federal level.

An organisation's privacy policy

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

Your privacy policy must cover a number of things (listed below).

You must also make the policy as available as is practically possible (for example, on your website) and, if anyone asks for the policy, you must give them a copy of it (for example, by posting it to them) (**APP 1**).

It's good practice to have a copy of your privacy policy accessible either in full or as a link in the footer section of all pages on your website so it is readily available.

Things you must include in your organisation's privacy policy:	
• the kind of personal information you collect and hold	☐
• how you collect and hold that personal information	☐
• the purposes for which you collect, hold, use or disclose that personal information	☐
• how someone may access and correct the personal information you hold about them	☐
• how someone can complain about a suspected breach of privacy laws	☐
• whether you are likely to disclose the information to overseas recipients	☐
• if you are disclosing information to people overseas, the countries where those people might be (if it's practical to specify)	☐

- an explanation of the right to anonymity and pseudonymity, including how it can be accommodated in your organisation's activities ☐
- whether you use personal information for direct marketing ☐

Things that the OAIC encourages organisations to include in their privacy policy:

- whether you retain a record of personal information about all individuals (or categories of persons) of who you deal with ☐
- if you interact with and collect personal information about a vulnerable segment of the community (such as children), the criteria that will be applied and the procedure that will be followed in collecting and holding that personal information ☐
- who, other than the individual, can access personal information, and the conditions for access ☐
- any exemptions under the Privacy Act that apply to personal information held by you ☐
- your process or schedule for updating your APP Privacy Policy, and how changes will be publicised ☐
- information retention or destruction practices or obligations that are specific to you ☐

Tips for privacy policies

- **Don't copy text from another organisation's policies, because that text might:**
  - not be relevant to your organisation's handling practices
  - be drafted according to laws from states or countries different from those that apply to you
  - contain details specific to an external organisation
  - not cover all the requirements you're obliged to meet, or
  - be protected by copyright
- **Don't over-commit.** An example of promising too much could be: 'we will never disclose your information without your consent'. Failing to comply with your privacy policy can have serious consequences – overcommitting can make it difficult to avoid breaking that commitment
- **Keep it easy to read.** Draft your privacy policy in plain and simple language to help people understand the policy and avoid potential legal ambiguity
- **Include relevant detail.** Making your policy easy to consume doesn't mean that it shouldn't contain all the information users need to know
- **Keep it updated.** The ways your organisation collects and uses personal information can change, and so do technology and laws. Review your privacy policy regularly to make sure it reflects your current practices and obligations.
- **Keep it easy to access.** The best place for your privacy policy is on your website, with a clearly visible link and an easily downloadable resource. It's also a good idea to keep a hard copy in your office.

Rules for collecting information

Collecting personal information

Things to include in your organisation's privacy policy:

- only collect personal information reasonably necessary for your organisation's functions or activities (**APP 3**)
- only collect personal information by 'lawful and fair means'– that is, not through criminal or illegal activity, trickery or deception (**APP 3**)
- only collect personal information directly from the person it belongs to, unless it's impossible or not practical to do this (**APP 3**)
- give individuals the option of remaining anonymous or using a pseudonym, unless this is not practical, or your organisation is required by law to deal with an identified person (**APP 2**)
- tell individuals what your organisation will use their personal information for (**APP 5**)
- tell individuals if you collect personal information for the purpose of direct marketing (**APP 7**)

Tip

If you use street-based direct marketing, you may only collect personal information by lawful or fair means. You can't trick someone into telling you where they live, or how much they earn – keep your questions straight and to the point! Make sure your street representatives know their obligations regarding what information they are to collect and how they are to collect it.

Bunnings example

In 2024, the OAIC found Bunnings Group Limited breached Australians' privacy by collecting their personal and sensitive information through a facial recognition technology system.

Bunnings had been collecting individuals' personal information to protect its legitimate interests against a rising climate of theft. However, the OAIC found that:

- although convenient, facial recognition technology was not the least intrusive means to achieve the same result (ie. the invasion of privacy was disproportionate to the legitimate business interest), and
- customers were not notified when they entered the store that their personal information was being collected

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

When collecting sensitive information and health information, your organisation must get the person's consent, unless an exception applies. Consent is discussed below.

You must not collect sensitive or health information unless:

- the person specifically consents to the information being collected, and
- the information is reasonably necessary for your organisation's functions or activities

Exceptions for 'Permitted Situations' and 'Non-profit organisations'

However, sensitive information can be collected, used, or disclosed without consent in 'permitted situations'. These are listed in the Permitted Situations section in part 6 of this guide: Practical tips for compliance and 'permitted situations'.

In addition, organisations that meet the federal Privacy Law definition of a 'non-profit organisation' may collect certain types of sensitive information without consent.

'Non-profit organisation' is defined as a not-for-profit organisation 'that engages in activities for cultural, recreational, political, religious, philosophical, professional, trade or trade union purposes'.

If your not-for-profit organisation fits this definition, you may collect 'sensitive' information without consent if:

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

Examples

Circumstances where not-for-profit organisations may be entitled to collect sensitive information without consent include the following:

- a religious not-for-profit organisation collecting information about their member's views on religious or moral issues
- a trade union collecting information about a job applicant's political views, or
- a community not-for-profit organisation that assists people with disabilities collecting information about their disability, as well as diagnosis and medical reports to provide counselling and support only. (This exception would not apply if the organisation were providing any kind of health service)

Caution

- An organisation conducting activities for another purpose not related to its core purpose can't rely on this exception.
- A not-for-profit organisation can rely on the exception if there is a clear relationship between the information collected and the activity. For example, the information may relate to a fundraising activity by a not-for-profit organisation to support its cultural, recreational, political, religious, philosophical, professional, trade or trade union purpose.
- Collection of sensitive information about a relative of the member would not be covered, unless that person also had regular contact with the not-for-profit organisation.

Best practice

Regardless of whether consent is required for the collection of sensitive information, you should apply the following general rules for collecting personal information:

- only collect information reasonably necessary for your organisation's functions or activities
- collect the information by lawful and fair means
- try to collect the information directly from the person concerned
- ensure that the only persons who have access to the information in your organisation are those who require access to it, and
- tell the person the identity of your organisation and the purpose of collecting the information, as well as the other notification matters listed below under 'Things you are obliged to tell the person providing information'.

Collection from third parties

If you can't reasonably and practically collect health information from individuals themselves, you can collect it from a third party in very limited circumstances. This might include:

- in an emergency where background health information is collected from relatives, or
- where a person is referred to a medical specialist and the specialist seeks relevant information from a referring provider

Regardless of whether you collect the information directly from the person or from a third party, Privacy Laws require that you notify the person that you collected the information. However, Privacy Laws recognise it might not be reasonably practical to notify the person in some instances. For example, in an emergency situation, there may not be enough time to notify the person concerned.

Tip

Health information has a number of special protocols that must be followed, and state or territory laws may apply in addition to the federal Privacy Laws. If you manage health information, make sure you know your organisation's obligations.

Things you are obliged to tell the person providing information

When you collect personal information (or as soon as you reasonably can after collection), you must take steps to make sure you make the person aware of certain mandatory information (APP 5):

- your organisation's identity and contact details
- if you collected the information from a third party or the person is otherwise unaware of the collection of their personal information, the fact that your organisation has collected the personal information
- if the collection of personal information is required or authorised by law or a court or tribunal order, the fact that it's so required or authorised (including the name of the law or details about the court or tribunal order)
- the purposes for which the information is being collected
- the main consequences if the personal information is not collected
- any other person or entity to which you may disclose the personal information
- circumstances under which your organisation would disclose the information or be required to disclose the information

- that your privacy policy has information about how the person may access and correct the information you hold about them, or otherwise seek correction of the information
- that your privacy policy has information about how someone can make a complaint about a breach of the applicable APPs, and
- whether you are likely to disclose personal information to overseas recipients and, if so, the countries in which those recipients are located (if it's reasonably practical to specify the locations)

Note

The process for a user to remove their information from your service should be easy and accessible.

You should also make the potential consequences of the user withdrawing their consent clear – for instance:

- your organisation may not be able to rely on past consent in relation to its services, or
- the user may no longer have access to your services

You can make the person aware of this information in a number of ways.

Typically, organisations give the person a short privacy notice (sometimes called a 'collection notice') which addresses the matters listed above.

You could also provide, or refer the person to, your privacy policy. If you do this, make sure your privacy policy covers the matters listed above in relation to the particular collection of personal information.

Getting consent

Although it's not always practical to get a person's consent (nor necessary when collecting non-sensitive personal information), if you get consent, your organisation will generally be allowed to deal with that information under the Privacy Laws in any way that is consistent with the consent provided.

Note

Consent is required to collect sensitive information and health information, unless an exception applies (**APP 3**).

There are strict requirements about the type of consent that must be given. For instance, consent, whether express or implied, must involve the person:

- being adequately informed before giving consent
- giving consent voluntarily
- giving consent that is current and specific, and
- having the capacity to understand and communicate their consent

Consent doesn't have to be in writing, but it's a good idea to keep a record of a person's consent in case it's challenged later.

Consent can take a variety of forms. Where practical, a signature or check box is a good way to document evidence of consent. Voice recordings are also often used when consent is sought over the phone.

Consent can be express or implied, but privacy regulators:

- caution against inferring consent from a person's failure to opt out, and
- require that consent be fully informed and provided voluntarily

It's therefore important to give users the opportunity to opt out to communications (such as communications by email or text).

Tips

- Use a 'double opt-in' to give the user another opportunity to document evidence of consent. For example, if you request a person's name and email address, you can require them to confirm their opt-in to the mailing list by clicking on a link in a confirmation email (which can be auto-generated) you send to them.
- Make sure you provide existing users with details of updates to your privacy policy when you amend your policy.

Continuing consent

Evidence of continuing consent is important in many circumstances.

Just because you obtained consent for one or more matters doesn't mean the user has provided consent to process, store or handle their data in other ways.

Your services, the law or prevailing circumstances may change, and it may be important at different times to seek and affirm consent that is both current and specific.

Caution – consent and capacity

Always consider whether someone has capacity to give you their consent.

- Are they under 18?
- Do they appear to understand what they are consenting to?
- Could they be suffering from an illness (such as dementia) that prevents them from providing informed consent?
- Is the person temporarily incapacitated?
- Can the person sufficiently comprehend the language or technological methods through which you are trying to engage?

You may need to involve a guardian, or someone recognised as a 'responsible person' in the consent decision. In these and other circumstances, it may be prudent to offer the individual support services, such as an interpreter.

Make sure the person you are engaging, or their parent or guardian:

- understands what they are consenting to, and
- can and does communicate their decision on consent

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

Unsolicited information

Unsolicited information (**APP 4**) is personal, sensitive or health information that you have received that you took no active steps to collect. If you receive unsolicited personal information, you need to consider whether you could have lawfully collected the information. That is:

- was the information reasonably necessary for one or more or your organisation's functions or activities? and
- was it sensitive information requiring consent?

If you could have lawfully collected the information, you may keep the information, but you must handle it in accordance with Privacy Laws. This includes notifying the person concerned where reasonable.

If the information is not reasonably necessary for one or more of your organisation's functions or activities, then you must destroy or de-identify the information. However, before you destroy information, you must make sure you don't have a legal requirement to retain it. If you are not sure, get legal advice before destroying or de-identifying information.

Different rules apply to information in Commonwealth records. A Commonwealth record includes any record that is, or that has been deemed by law to be, a record that is the property of the Commonwealth. Commonwealth records must not be destroyed as they must be handled in accordance with the *Archives Act 1983* (Cth).

Example

A person sends their CV to your organisation, requesting a job (but not responding to an advertised vacancy). There are no positions currently available, but the person has a relevant skillset and could be a potential candidate for future positions. Your organisation can keep that information on file, as long as you give the person the required notification under APP 5 and handle the information in accordance with the Privacy Laws.

Storing personal information

Your organisation must take reasonable operational and technical measures to protect the personal, sensitive and health information it stores from misuse, interference and loss, and from unauthorised access, modification or disclosure (**APP 11**).

Operational measures are security practices applicable to your staff and to how your business is run, while technical measures relate to your organisation's use of technology, how the technology maintains the privacy of personal information collected, and the integrity of your systems generally.

Security measures

Depending on your organisation's circumstances, consider the following security operational and technical measures, ensuring that you employ both, to the greatest extent practicable:

Operational measures

- require staff to lock relevant documents away
- enforce a 'clean desk' policy to minimise the risk of inadvertent disclosure of personal information
- make sure employees, volunteers or others return information at the end of their employment or involvement with the organisation and that they have no method of retaining access to information
- place computer screens out of the view of others, particularly visitors to the organisation
- training employees on data protection
- developing standard operating procedures and policies for securing personal information

Technical measures

- limit the use of portable storage devices, such as disks and USB keys, or use encryption or other security measures
- record audit trails of access to documents
- encrypt documents containing personal information, particularly when those documents are being sent by email
- to the extent feasible, present data in a way that individuals can't be identified or linked to the data in the case of a breach
- include email addresses for group emails in the 'BCC' field rather than the 'to' field so recipients can't see other recipients' email addresses
- include confidentiality and privacy clauses in agreements with volunteers or others who have access to the personal information (and give specific examples of activities that would be considered a breach), and
- place access restrictions on relevant documents or systems, including electronic access restrictions (the more people who have access, the greater likelihood a breach may occur)

Caution – cloud-based storage

In addition to taking the security measures listed above, if you use internet (or 'cloud') based storage systems for your data, there are other important issues to consider.

Under the APPs, if you outsource data services to a third-party provider based overseas (such as a server provider in another country), you must take reasonable steps to make sure that the third-party provider does not breach the APPs.

Also, if that provider breaches the Privacy Act, you may be accountable for those breaches!

Cloud storage contract checklist

Steps you can take to limit the possibility of your third-party provider breaching the APPs include:	
• in any contract you sign with an overseas service provider, require the provider to comply with the APPs, your privacy policy and include indemnities against any breach of the applicable Privacy Law or Health Privacy Law	☐
• provide the service provider with a copy of your privacy policy	☐
• understand how the third-party provider handles, stores, and deals with data and personal information	☐
• ensure that by providing access to the data that your organisation's or the third-party provider's processes are not rendering the data more publicly accessible (this is how some of the most well-publicised data breaches have occurred)	☐
• maintain strong access, security controls and procedures over who has access to your data and what they can do with it	☐
• if you are unable to achieve equivalent protections to the Privacy Act with the overseas cloud service provider, you will need to get consent from each relevant individual for any transfer of personal information to the overseas provider. For this consent to be valid, the individual will need to be informed that they will not be able to rely on their rights under the Privacy Act, and that the overseas entity is in no way bound by the Privacy Act	☐

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.

Other recommended action

Your organisation must also take reasonable steps to ensure the personal information it collects, uses or discloses is accurate, up to date and complete. It must also be relevant to the purposes for which it's being used or disclosed (**APP 10**).

If your organisation is storing personal information it no longer needs, it must take reasonable steps to destroy or de-identify the information, unless:

- the information is contained in a Commonwealth record, or
- there is a legal requirement to retain the information

Health information

If your organisation 'holds' health information, you may have additional obligations under the APPs and state and territory Health Privacy Laws (which only apply in NSW, Vic, and the ACT) or other state and territory Privacy Laws applicable to your not-for-profit.

You will hold health information if you possess a document (paper or electronic), or if your organisation has control over a document, that contains health information.

If you participate in the My Health Record system, you must comply with the *My Health Records Act 2012* (Cth) (**MHR Act**) and the *Healthcare Identifiers Act 2010* (Cth) (**HI Act**). The MHR Act limits when and how health information included in a person's My Health Record can be collected, used and disclosed.

If you are storing health information, you have certain obligations to the person whose information you have.

You are required to ensure, at their request, that that person has:

- an understanding of:
  - why you are storing that information
  - how you collected that information
  - details of the health information you have
  - what rights they have to access that information, and
- an ability to update, correct, or amend that information (subject to a reasonable request)

Tip

Regardless whether a document is located in your organisation or your state or territory, or whether you have sole custody of the information, if the information has a connection to your organisation's state or territory operations, a state or service contract, or a client of your state or territory, the state or territory privacy requirements may apply.

Using or disclosing information

Using information for the primary purpose

Unless an exception applies, you must not use or disclose personal information you have collected for any other reason other than the **primary purpose** you collected it for (**APP 6**). The exceptions are listed below.

Tip

Remind staff regularly of your organisation's primary purpose for collecting personal information.

Consider including a 'mission statement' or 'primary objective' reminder on documents circulated to telemarketers or street side information collectors.

Using information for a secondary purpose (exceptions)

A secondary purpose is any purpose other than the primary purpose for which you collected the information.

These are:

- **Consent** – the person specifically consents to its use for another purpose.
- **Reasonable expectation** – this exception is a two-limb test. First, the person must reasonably expect that you would use or disclose their information for such a purpose. Second, the secondary purpose must be related to the primary purpose, that is, it must be connected or associated with the primary purpose. If the information is sensitive information, then the secondary purpose must be directly related to the primary purpose, that is, it must be closely associated with the primary purpose.
- **Law** – an exception in the law (either in Privacy Laws or in another law) expressly applies to permit the secondary use of the information. For an overview of some exceptions in law, see the Permitted Situations section in part 6 of this guide: Practical tips for compliance and 'permitted situations'.

Example

Your not-for-profit organisation collects personal information from people interested in receiving news about saving the rainforest, and you notify them you are collecting their personal information to provide email updates. You must not use that information to do anything other than this unless you get the person's specific consent (or an exception applies).

Additional requirements limit the adoption, use and disclosure of government identifiers (for example, Medicare number, drivers licence number, passport number).

Automated Decision Making

Under recent amendment to the Privacy Act (by the *Privacy and Other Legislation Amendment Act 2024 (Cth)*), from 10 December 2026, APP entities' privacy policies will be required to disclose information about the use of automated processes to make decisions based on personal information.

If your organisation satisfies the following requirements, you will need to update your privacy policy before 10 December 2026 when these Automated Decision Making (**ADM**) provisions come into force:

- your organisation has arranged for a computer program to make, or do a thing that is substantially 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 the individual is used in the operation of the computer program to make the decision or do the thing that is substantially and directly related to making the decision

What constitutes a 'decision'?

When considering these requirements, note that failing or refusing to make a decision is considered making a decision.

A decision will be considered to affect the rights of an individual, whether an individual is adversely or beneficially affected. Examples of decisions that affect the rights and interests of individuals include deciding an individual's entitlements under a contract, or whether the individual is eligible to access a significant support service.

What does the ADM provision require?

If your organisation satisfies the requirements for the ADM provisions to apply, you will have to disclose your ADM process in your privacy policy.

The details of what you need to disclose include:

- the personal information used in the operation of such computer programs (this includes information which was acquired and created before or after the start of the ADM system), and
- the decisions for which a thing, that is substantially and directly related to making the decision, is done by the operation of such computer programs

Tip

Although these provisions will not be enforceable until 10 December 2026, it is best practice to include them now, or at least be aware of how ADM's handle personal information in your organisation.

Direct marketing

Direct marketing (**APP 7**) is communicating with a person to promote goods and services and can include fundraising. Any contact information should be secured through an 'opt-in' system. If your organisation uses or discloses personal information for the purposes of direct marketing, you should consider the following issues.

You can only use or disclose sensitive information (including health information) for direct marketing if a person has consented to that use or disclosure. You can only use or disclose non-sensitive personal information for direct marketing if you meet all the following conditions:

- you collected that information **directly from the person**
- the person whose information is disclosed would **reasonably** expect you to use the information for direct marketing
- you provide an easy '**opt-out**' option for anyone who doesn't want to receive direct marketing, and
- the person has not chosen to opt out

You may also use or disclose non-sensitive personal information for the purpose of direct marketing in circumstances where you collected the personal information from a third party, or the person would not expect you to use or disclose their personal information for the purpose of direct marketing, if you meet all of the following conditions:

- you have the person's consent or it's not practical to obtain consent
- you provide a simple opt-out mechanism from direct marketing and, in each direct marketing communication, you include a prominent statement drawing attention to this mechanism, and
- the person has not chosen to opt out

Caution – the Spam Act

In addition to the Privacy Laws, the *Spam Act 2003* (Cth) (**Spam Act**) prohibits the sending of unsolicited commercial electronic messages (spam) with an Australian link. A message has an Australian link if it originates or was commissioned in Australia or originates overseas but was sent to an address accessed in Australia.

Where the Spam Act or the *Do Not Call Register Act* 2006 (Cth) apply, they prevail over the requirements of APP 7 in relation to the relevant act or practice.

Not-for-profit organisations, community service organisations and non-government organisations must comply with the Spam Act. However, in some circumstances under the Spam Act, charities registered with the Australian Charities and Not-for-profits Commission may be exempt from obtaining consent from recipients.

Access to and correcting personal information

Accessing personal information (APP 12)

If a person asks for access to their own personal information held by your organisation, you are generally required to give access in the way the person has requested. You should respond to the request in a reasonable period. Take care, when providing access to information, that you don't inadvertently disclose a third party's personal information.

Your organisation may refuse a request for access in limited circumstances (for example, where providing access would result in a serious threat to a person's safety or where the access would be unlawful). If your organisation refuses to give access, you must provide the person with a written notice setting out the reasons for the refusal and the mechanism for making a complaint about it.

Your organisation can't charge the individual for the making of the request. Your organisation can, however, charge the individual for giving access to the personal information but the charge must not be excessive.

Correcting personal information (APP 13)

If a person can show that personal information about them held by an organisation is inaccurate, incomplete, irrelevant, out-of-date or misleading, the organisation must:

- take reasonable steps to correct the information and notify third parties to which it has provided the information, or
- if the information is not correct, provide the person with written reasons for the organisation's refusal to correct the information, including information about how to make a complaint and a statement noting the person claims the information is incorrect, incomplete, irrelevant, out-of-date or misleading

Your organisation must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information.

Disclosing across borders

Because more organisations operate across national borders than ever before, privacy has become an international problem. Many not-for-profit organisations are not sure what privacy obligations apply to information they receive from overseas, as well as information they send or store overseas.

Under federal Privacy Laws, before an organisation discloses personal information to an overseas recipient, it must take reasonable steps to ensure the overseas recipient does not breach the APPs (**APP 8**). This requirement does not apply if the disclosing organisation reasonably believes that:

- the overseas recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is substantially similar to protection given under the APPs, and
- there are mechanisms available to enforce that protection

When disclosing to an overseas recipient you should take reasonable steps to ensure that the overseas recipient does not breach the APPs as an act done, or a practice engaged in by them is taken, to have been done, or engaged in, by you and may be a breach of the APPs.

However, identifying these countries should become easier due to the recent amendment to the Privacy Act which gives ministerial powers to 'whitelist' countries that provide substantially similar privacy protections to the way in which the APPs protect personal information. While these powers have been effective since 11 December 2024, a list of 'whitelist' countries has not yet been published.

Tip

It's always good practice to identify the location of the countries in which the organisation is likely to disclose to if it is practicable to do so. This is important to ensure that adequate protections are in place for cross-border disclosure, and that the relevant country is named in the Privacy Policy.

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

Recent amendment to the Privacy Act introduced a framework for a Children's Online Privacy Code (**COP Code**) to be developed by the OAIC and registered by 10 December 2026.

The COP Code will impose additional privacy obligations on online service providers (such as apps, websites, messaging platforms) accessible by children.

The COP Code will apply to an organisation if all the following apply:

- the entity is a provider of a social media service, relevant electronic service or designated internet service (all 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 can also list a specified APP entity or class of entities in the COP Code.

Tip

The COP Code will likely be accompanied by OAIC guidelines to assist organisations to determine if a service is likely to be accessed by children.

Although the compliance requirements of the COP Code have not been finalised or released, it would be prudent to determine whether your organisation's activities fall within its ambit (as currently defined), and to actively monitor and prepare for any coming developments.

The COP Code is expected to mirror the APPs, but with additional protections. If your organisation is not currently required to the comply with the APPs, but your activities would be covered by the COP Code, you may want to consider preparing to 'opt in' soon.

Comparison of Commonwealth and State and Territory Privacy Principles

The table below provides a high-level comparison of some of the key privacy principles. It's intended as reference guide only and is not a substitute for legal advice or for reading the privacy principles.

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 VIC WA	TPP 3.1 IPP 8(1) IPP 1.1 QPP 3.1 - PIPP 1(1) 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 VIC WA	TPP 7 (s 23) - - QPP 6 - - - -
APP 8 – Cross-broader 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	TPP 9 - IPP 7.2 - -

	TAS VIC WA	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 114(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 SA TAS VIC WA	TPP 11.1 IPP 12 IPP 4.1 QPP 11.1 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 -

Part 5

Notifiable Data Breaches scheme

Notifiable Data Breaches scheme

This part covers:

- what is the Notifiable Data Breaches scheme?
- what organisations must comply with the scheme?
- what kind of data breaches require notification?
- the process for responding to data breaches
- notification when there is an eligible data breach
- declaration of an eligible data breach by the Minister
- declaration of an emergency by the M/minister
- penalties for not complying with the scheme

This part of the guide explains your organisation's obligations if there is a data breach and how to comply with the Notifiable Data Breaches scheme under the Privacy Act.

Note – state and territory mandatory notification of data breach schemes

New South Wales and Queensland have implemented mandatory data breach notification schemes for their public sector agencies. These schemes are specific to state-level entities and require public sector agencies to report certain data breaches to the relevant state privacy commission.

For more information about these states-based schemes, see:

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

This guide does not cover state and territory notification of data breach schemes.

Read this part of the guide in conjunction with our fact sheet on cybersecurity (a data breach response will often incorporate cyber security measures).

Data breaches are a significant part of the evolving privacy landscape in Australia

The Office of the Australian Information Commissioner's (**OAIC**) Australian Community Attitudes to Privacy Survey 2023 found that almost half of Australians reported their personal information had been involved in a data breach.

Australians value organisations who take proactive and quick reactive actions to protect customers from harm. If your organisation doesn't respond to data breaches in a way that is consistent with community and

regulatory expectations, this can cause significant damage to the organisation from a legal, financial, and reputational perspective.

The Notifiable Data Breach Scheme is a mature regime and OAIC expects organisations have strong practices to protect personal information as well as processes to ensure timely response to data breaches.

The OAIC publishes a biannual Notifiable Data Breaches Report. Refer to these reports for helpful insights on the evolving risks.

What is the Notifiable Data Breaches scheme?

Since the introduction of the Australian Privacy Principles (**APPs**) under the Privacy Act, organisations must take all reasonable steps to prevent the loss, unauthorised access, modification or disclosure of personal information it holds.

Under the Notifiable Data Breaches (**NDB**) scheme, any organisation or agency covered by the Privacy Act must notify the OAIC and affected individuals when a data breach is **likely** to result in serious harm to an individual whose personal information is involved.

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

What organisations must comply with the scheme?

The NDB scheme applies to organisations which have obligations under APP 11 (APP entities).

The NDB scheme also applies to organisations which hold credit reporting information, credit eligibility information and tax file numbers (**TFNs**), regardless of whether they are an APP entity.

Organisations subject to the NDB scheme include:

- **Organisations which are subject to the Privacy Act**

  This includes businesses and not-for profit organisations with a turnover of more than $3 million per financial year, Australian Government agencies, and certain organisations with a turnover of less than $3 million per financial year.

  Organisations with a turnover of less than $3 million per financial year that are subject to the NDB scheme include:

  - organisations who hold health information and provide a health service (which may include not-for-profit organisations)
  - employee associations registered under the *Fair Work (Registered Organisations) Act 2009* (Cth)
  - organisations reporting under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (Cth)
  - organisations that hold accreditation for the *Consumer Data Right system under the Competition and Consumer Act 2010* (Cth)
  - organisations that have voluntarily opted in for APP coverage
  - credit reporting bodies
  - credit providers
  - organisations contracted by the Commonwealth government to provide services, and organisations that trade in personal information

- **Organisations which hold TFNs**

  These organisations include organisations that are employers or hold TFNs of people they assist (such as organisations assisting people with finding employment). These are referred to as **TFN recipients**.

  To find out more about how to protect TFN information, see the Commissioner Office of the Australian Information (**OAIC**) webpage 'The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information'.

If your organisation is required to comply with privacy law, has a privacy policy, or both these things apply, refer to the OAIC website which has published guides to privacy obligations and dealing with data breaches.

The Australian Signals Directorate's Australian Cyber Security Centre website also contains resources to help your organisation manage cybersecurity.

Note – organisations without physical or electronic copies of personal information

Data breach notification obligations apply to an organisation that holds physical or electronic personal information.

An organisation holds personal information if the organisation has possession or control of a record that contains the personal information. This can include cloud service providers that possess records.

This applies where the organisation has the right or power to deal with the personal information, even if the organisation does not physically possess or own the physical or electronic records of the personal information.

If an organisation has outsourced the storage of personal information to a third party but retains the right to access or amend the information, that organisation still 'holds' the personal information and has a responsibility to assess prospective eligible data breaches and ensure notification and compliance following any eligible breach under the NDB scheme.

What kind of data breaches require notification?

Under the NDB scheme an organisation must notify affected individuals and the OAIC if it experiences (or has reasonable grounds to believe that it has experienced) an **eligible data breach**.

An eligible data breach occurs if:

- there is unauthorised access, unauthorised disclosure or loss of **personal information**
- the data breach is likely to result in serious harm to **one or more** individuals affected, and
- the organisation has not been able to prevent the likely risk of serious harm with remedial action

In addition, the Minister now has powers to make:

- a declaration that an eligible data breach has occurred (an eligible data breach declaration), and
- an emergency declaration

Both declarations authorise the collection, use and disclosure of personal information that would otherwise not be permitted under the APPs, to minimise harm and for any other purpose stated in the declaration. These declarations are discussed further below.

The NDB scheme applies to breaches that occurred on or after 22 February 2018.

For organisations who are not APP organisations but are TFN recipients (see above), an eligible data breach occurs to the extent that TFN information is involved in the breach.

For TFN recipients – if the unauthorised access, unauthorised disclosure, or loss of information does not include TFN information, this is unlikely to be an eligible data breach and further steps may not be necessary as part of the NDB scheme.

Note

TFN information is information that connects a TFN with the identity of a particular individual. An example of this might be a document or set of data that links someone's name and date of birth to their TFN, or allows someone to be able to make that link.

If your organisation discovers that TFN information, further data or other information it held has been compromised, consider further steps and seek legal advice.

Even where a TFN recipient's data breach does not include TFN information, given community expectations around the handling of personal information, the organisation may want to consider notifying affected individuals where a breach is likely to result in serious harm.

What is unauthorised access, disclosure or loss?

Unauthorised access of personal information occurs when a person accesses this information and was not permitted to do so. This can include unauthorised access by an employee, an independent contractor or an external hacker.

Example – unauthorised access

Sandra is a volunteer at an APP organisation which provides support to LGBTI people. The organisation retains basic information about people who have used its services such as names, addresses and telephone numbers. It restricts access to this database to certain employees only. Sandra is curious about whether one of her friends might be LGBTI and searches the organisation's private records and finds her friend.

This is unauthorised access.

Unauthorised disclosure of personal information occurs when an organisation makes personal information accessible or visible to others outside the organisation, whether intentionally or unintentionally.

Examples – unauthorised disclosure

Example 1 – Michael works for a large not-for-profit organisation which provides financial assistance to Australian military veterans' families. Michael fields a call from a journalist asking for information in response to a tip-off that a celebrity has been scamming the organisation. Michael confirms the celebrity is a client of the organisation and provides the journalist with the celebrity's contact details from the organisation's records. This is unauthorised disclosure.

Example 2 – Sandeep, who works for the same organisation, emails a client. She accidentally uses the wrong email address and sends the email, containing personal information about her client, to someone else. This is unauthorised disclosure.

Example 3 – Carrie-Anne is working on a private database of client's contact details and includes a link to the database on a report in a webpage which renders the data publicly accessible. This is unauthorised disclosure.

Loss refers to the accidental or inadvertent loss of personal information held by an organisation in circumstances where is it is likely to result in unauthorised access or disclosure.

Example – loss

Anthea is working over the weekend. She downloads documents which contain payroll information, including employee tax file numbers and names, onto an unencrypted USB. She catches the train home, but can no longer find the USB. Anthea thinks she may have lost it on the train. This is a loss of personal and TFN information.

Exceptions may apply if the personal information which has been lost is unlikely to be able to be accessed or disclosed.

The process for responding to data breaches

The OAIC expects organisations to have practices, procedures, and systems in place to comply with their information security obligations under APP 11, enabling suspected breaches to be promptly identified, reported to relevant personnel, and assessed if necessary.

A data breach response plan is a document that clearly sets out the steps to take and the people responsible for responding to a suspected or actual data breach.

See the OAIC's guide to managing data breaches in accordance with the Privacy Act – 'Data breach preparation and response'.

The guide includes information about preparing a data breach response plan, assessing a suspected notifiable data breach and responding to a data breach.

The OAIC states that effective data breach responses generally follow a four step process:

Step 1 Contain	• Take action to stop the breach happening further • Take care not to destroy evidence that could help you work out how the breach happened
Step 2 Assess	• Work out what happened and assess risks to people • If possible, take action to stop or mitigate any risks • Assess whether there has been a notifiable data breach or an eligible data breach declaration (see below) • This assessment should be made within 30 days following the breach
Step 3 Notify	• If required, following the assessment, notify the people affected and the regulator (OAIC) of the breach • If the breach is an 'eligible data breach' under the Notifiable Data Breach scheme, it may be mandatory for the entity to notify.
Step 4 Review	• Review the breach circumstances • Identify action to take to prevent breaches in future and take this action

Every data breach is different and the four steps may not necessarily happen in order

For example, in some data breaches, it may be more important to notify affected individuals while the assessment is ongoing.

Containing a data breach

Once an organisation discovers or suspects that there has been unauthorised loss, access or disclosure of its personal information, it should immediately take action to limit and contain the data breach.

Note

How a data breach is contained depends on the kind of breach, but some common containment methods include:

- stopping the unauthorised practice
- shutting down the relevant systems, or
- revoking computer access privileges

During the containment stage, take care to not destroy any evidence

At this stage, an APP organisation may either:

- **suspect** an eligible data breach has occurred which triggers **assessing** (step 2):
  - whether the data breach would be likely to result in serious harm to one or more individuals, and
  - the serious harm has not been able to be prevented with remedial action, or
- **believe** the data breach is an eligible data breach which triggers **notification** obligations (step 3)

Assessing suspected data breaches

If an organisation is aware there are reasonable grounds to suspect there may have been a data breach, the organisation must quickly assess the situation to determine whether the breach is an eligible breach.

The assessment of the suspected data breach must occur no later than 30 calendar days after the day the organisation becomes aware of the grounds (or information) that caused it to suspect an eligible data breach had occurred.

The organisation should not unreasonably delay its investigations, for instance, by waiting for board approval or executive discussion.

Organisations are required to undertake reasonable and expeditious assessments by being flexible and adaptive. The OAIC expects that the amount of time and effort organisations expend on assessment is proportionate to the likelihood that an eligible data breach has occurred and its apparent severity.

If an organisation can't complete an assessment within 30 calendar days, it's prudent to document the reasons why.

How is an assessment done?

There are no specific legal requirements of the steps an organisation must take in relation to an assessment. However, guidance from the OAIC suggests a **three stage assessment process**:

Initiate the assessment process – identify the person or group responsible for completing the assessment

Investigate the matter – gather all the relevant information about the data breach.

For example, ask 'Can we employ any remedial action?', 'What personal information has been affected?', 'Who may have had access to it?', 'What are the likely impacts?'.

Evaluate the breach – the person or group needs to decide whether it is a notifiable data breach. This decision should be well documented, including the reasons why that decision was reached

Data breaches are often complex and, at times, APP organisations may not have sufficient or evidence when making an assessment under the NDB scheme. In these circumstances, the OAIC encourages entities to:

- **take a cautious approach** – if an APP organisation can't conclude that unauthorised access, disclosure or loss has occurred, it should consider proceeding on the presumption that there has been a data breach
- **consider all relevant factors and risk of harms** – APP organisations should assess a range of factors (see below), and
- **focus on unauthorised access** – do not over emphasise data exfiltration in your assessment period, eligible data breaches can occur on unauthorised access alone and data can be exfiltrated by less traceable means (ie. screenshots)

When are data breaches likely to result in serious harm?

The next step in determining whether a data breach requires notification is deciding whether it is likely to result in serious harm to one or more of the impacted individuals.

The phrase 'likely to result in serious harm' has no special definition – it simply means that the risk of serious harm to a person is more probable than not.

Whether the data breach is likely to result in serious harm is assessed from the perspective of a reasonable person in the organisation's position, who has been properly informed based on the information immediately available or information that could be obtained following reasonable inquiries.

Serious harm could include physical harm, psychological harm, emotional harm, financial harm, and reputational harm.

OAIC guidance states that APP organisations should assess the risk holistically, having regard to the consequences for the people whose personal information were part of the data breach and the likelihood of harm occurring.

The NDB Scheme provides the following non-exhaustive list of factors which should be considered when deciding whether a data breach is likely to result in serious harm:

Factors	Example of less serious breach	Example of more serious breach
The kinds of information involved and the sensitivity of the information	Name (without other linking information)	HIV status
Whether the information is protected by one or more security measures and the likelihood those measures could be overcome	Reputable encryption by software Multi-factor authentication required and is difficult to bypass	No encryption Standard windows password Encrypted or secured information that may be overcome due to knowledge or resources of actors (such as hackers)
The persons, or the kinds of persons, who have obtained, or who could obtain, the information	Internal employee trained in safe treatment of personal information receives a confidential client file in error	Disclosure to public Access by hackers
The nature of the harm	Information previously available publicly	Identity theft Financial loss Physical safety Reputational damage Humiliation

An organisation is not expected to contact individuals who have been affected by a data breach to find out their personal circumstances before deciding whether there has been or likely will be ‘serious harm’.

Things to consider when deciding whether the breach will ‘likely result in serious harm’

- **Which people have had their personal data affected?**

  The severity of harm can differ between two people with the same personal information released.

  Organisations should consider whether any of the personal information that is part of the breach belongs to vulnerable people. For example, a simple list of names and addresses might not in itself result in serious harm, however if there are names of people who may be targeted or are otherwise vulnerable, the risk of serious harm is increased.

- **How many people are involved?**

  The more people affected by a breach, the greater the likelihood that one or more of them will experience serious harm.

  The OAIC Guidance states that where a data breach involves many people, it may be prudent to assume that serious harm is likely to result in respect of at least one of those individuals and the serious harm threshold is likely met unless the specific circumstances do not support that conclusion.

- **What kind of information can be determined about the people affected?**

  Organisations should consider what kind of information can be determined by the data breach.

  If the information links a person with a sensitive product or service, such as HIV treatment, it will increase the risk that serious harm has occurred. Organisations should also consider the breadth of information that has been made available – the more pieces of identifiable personal information that have been disclosed, the more likely it is that there has been an eligible data breach.

- **Is the personal information adequately encrypted, anonymised, or otherwise not easily accessible?**

  If the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, it's unlikely there is an eligible data breach.

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

  The length of time between a data breach and an organisation's discovery of the data breach is another consideration.

  The longer this period is, the greater the likelihood that the information has been misused or accessed in a way that will cause serious harm. For example, if a malicious third party has had unauthorised access to a mailbox for a long period, they may have had more opportunity to understand how to commit financial harm and issue fraudulent invoices to customers.

  Also consider how readily the information was discernible – if it was disclosed through a webpage, was it linked to from other pages for periods of time, or did the page rank prominently in search engines?

- **Who has or may gain access to the personal information?**

  Organisations should consider who is or may be the recipient of the personal information.

  If, for example, the data breach appears to target specific information about a person, there is a greater potential the information is going to be used for malicious purposes and therefore a higher likelihood that serious harms will result.

Exceptions to the requirement to notify

Organisations may not need to notify if they take positive steps to address a data breach in a timely manner.

To avoid the need to notify, the remedial actions need to be effective enough so that the organisation believes that the data breach will no longer likely result in serious harm.

If the remedial action only prevents the likelihood of serious harm to some people in a larger group of people whose personal information has been compromised, the organisation still needs to notify the affected people who are likely to experience serious harm.

Example 1

While cycling to work, Fernando's smartphone falls out of his pocket. The smartphone is pin protected. On arrival at work, Fernando requests his company's IT staff to remotely delete the information on the smartphone. The IT staff are confident that the contents are deleted and the phone could not have been accessed during the short period.

Example 2

While updating the company website, Madeleine unintentionally makes a resource with people's personal information public. As soon as she realises what has happened she makes the webpage private, ensures that the information isn't displayed publicly elsewhere on the website and clears the website cache so the updated webpage is displayed to online visitors. Madeleine believes that serious harm is not likely to occur and discloses the situation to her supervisor for assessment.

Notification

If an organisation reasonably believes an **eligible data breach** has occurred, the organisation must:

Contain the breach as far as it is possible

Prepare a notification statement that contains the identity and contact details of the organisation, a description of the data breach, the kinds of information affected, and recommendations for affected people

File the notification statement with OAIC through the online form or contact OAIC (enquiries line on 1300 363 992) to make alternative arrangements

Notify people at likely risk of serious harm

To notify OAIC of a data breach, use the online Notifiable Data Breach form.

Preparing the notification statement for OAIC

An organisation is free to customise its notification statement as long as it contains the following information:

- **The identity and contact details of the organisation** ☐

  If an organisation is known by a name other than its company name (for example, a trading name), the organisation should use the name most recognisable to the people impacted by the data breach. Depending on the circumstances of the data breach, contact details could include a specialised email address or dedicated phone line.

- **A description of the data breach** ☐

  The description should be sufficient to allow affected people to properly assess the possible consequences of the data breach for them, and therefore allow them to take steps to mitigate the harm.

  This type of information may include:

  – the dates when the personal information was compromised, accessed or disclosed
  – the date when the organisation detected the data breach
  – the circumstances of the data breach (such as whether there is a known cause for the breach)
  – who has likely obtained the personal information (this can be general such as 'an external third party' or 'former employee.'), and
  – relevant information the organisation has taken to contain or remediate the breach

  The OAIC doesn't expect entities to identify specific individuals who have accessed the personal information unless this has particular relevance to the steps the reporting organisation recommends affected individuals take in response (for instance, in regard to the accidental disclosure of information in a domestic violence situation)

- **The kind of information compromised** ☐

  The statement should include the type of personal information which likely has been accessed, for example, peoples' names, addresses and telephone numbers. The organisation should clearly state if sensitive information, government related identifiers or financial information are involved in the breach, for example, health information, passport numbers or credit card details.

- **Steps the organisation recommends that affected people take** ☐

  The organisation must make practical recommendations as to what the people should do in response to the breach to mitigate the harm.

  Recommendations should reflect the circumstances of the breach and the kind of information compromised. For example, if credit card details have been compromised, recommending that people contact their financial institutions to cancel those cards and be issued with new ones.

  If an organisation is unaware of what advice to provide, it should seek assistance from specialists when preparing this section. In limited circumstances and only after following consultation with a specialist, the advice may be that no steps are required.

Organisations must ensure they don't disclose personal information about any affected person in the process of notification.

Notifying people

The NDB scheme requires organisations to notify people as soon as practicable after completing the statement prepared for notifying the OAIC. As appropriate and expeditious, it can notify the people before or at the same time as the OAIC, as long as it contains all the required information. **Reporting organisations are required to notify both individuals affected and the OAIC.**

As noted above, it's also possible for notification to affected individuals to take place in some cases before containment or assessment of the breach occurs (for example, where serious harm is imminent).

When the organisation is deciding which method or combination of methods to undertake it can consider the cost, time and effort it will have to spend, in light of the particular circumstances and capacities of the organisation.

The OAIC has an expectation that notification occurs expeditiously in all circumstances unless cost, time and effort are excessively prohibitive.

The NDB scheme provides three options for notifying individuals at risk of serious harm:	
Option 1 **Notify all individuals**	If an organisation considers that the data breach will result in serious harm to one or more people but can't assess which people are at risk, it should notify all affected people. An organisation can use any method or combination of methods to notify a person (see the tip below), as long as it has taken all reasonable steps. The organisation should assess the likelihood that the affected people to be notified will become aware of and understand the notification and weigh this against the resources involved in undertaking the notification. Some examples for possible methods of notification include email, telephone call, SMS, post, in-person meeting, social media post, or newspaper advertisement. Organisations can also notify people through their usual method of communication, which may be an intermediary if applicable.
Option 2 **Only notify people at risk of serious harm**	An organisation must take all reasonable steps in the circumstances to notify affected people. If the organisation can identify which specific people are at risk of serious harm, it has the option of only notifying those people. Notifying only people at risk of serious harm has the additional benefit of reduced costs and decreased notification fatigue among members of the public. The organisation should be confident however that it is able to identify all affected people.

Example

While a website was compromised for two days, a hacker obtained all information (including credit card information) that was entered into the website during the two days.

Following a comprehensive risk assessment, the organisation considers that only customers who logged into their account during those two days are at serious risk and no other personal information has been accessed. The organisation is only required to notify the people that logged in during the time the website was compromised, being the people it considers to be at likely risk of serious harm.

When notifying people, the organisation can use any method (for example, a telephone call, SMS, physical mail, social media post, so long as the method is reasonable.

Option 3 **Publish notification**	This option is only available if it's not practicable for the organisation to complete the notifications described above. In this scenario, the organisation must publish a copy of the statement provided to the OAIC on its website (if it has one), other digital outlets as appropriate and take reasonable steps to publicise the contents of the statement. The notification should be clearly displayed in a prominent location on the organisation's website with the ability to be caught by search engines. An alternative to this method suggested by the OAIC is to take out a print or online advertisement in a publication or on a website the organisation considers reasonably likely to reach people at risk of serious harm. The purpose of the notification is to relay the information to as many affected people as possible.

Note

As the organisation is required to take reasonable, active steps to publicise the copy of the statement, it may be in breach of the NDB scheme if it merely uploads it to its website without anything more.

Sometimes more than one step will be required to try to reach those who may be impacted by the breach, such as in the case where contact details for individuals are outdated or more than likely outdated. The Privacy Act does not specify a time for which the statement must remain publicly available, although the OAIC has provided some guidance that it expects the publication to exist for at least six months.

Data breaches involving more than one organisation

Organisations may hold personal information jointly with other organisations. If there is unauthorised access or disclosure of that personal information, both organisations will have an eligible data breach.

Common examples where two or more organisations may share the same person information include:

- IT vendor agreements
- outsourcing agreements
- commonwealth contracts, and
- joint ventures or shared service agreements

Responding to data breaches of jointly held information

If the data breach solely relates to personal information jointly held between two or more organisations, the suspected breach needs to be assessed and, if it is an eligible data breach, only one organisation needs to comply with the notification requirements of the NDB scheme on behalf of the group.

While only one organisation is required to assess the suspected breach, this doesn't mean the other organisations can't make their own assessments. If the group determines that one of the organisations will appropriately execute the reporting requirements to the OAIC and individuals affected, the group should secure a written statement from the reporting organisation regarding the eligible data breach.

The organisation that will prepare a statement for the OAIC and notify individuals may, if it decides to do so, include details as to the identity, contact details and information regarding the relationship with the other organisations in the statement and notification. Whether the organisation includes this information depends on the circumstances, the relationships between the organisations and extent to which it is useful to provide this information.

In certain circumstances, where it is not necessary to disclose the identity of the other organisations, it may still be useful and relevant to describe the nature of the relationships between the organisations in the description of the data breach, including potentially in circumstances where the individuals affected don't have a relationship with the other organisations.

The organisations are responsible for deciding who is responsible for notification. If none of the organisations notify, each organisation may be found to have breached the requirements of the NDB scheme.

The NDB scheme doesn't provide any specification as to which organisation is required to conduct the assessment or notify individuals and the OAIC about an eligible breach. It's therefore up to the organisations to quickly reach an agreement based on their arrangement and potentially, which organisation is more at fault for the breach.

In general, compliance by one entity will also be taken as compliance by each of the relevant organisations.

Organisations may wish to agree on who is responsible for compliance with the NDB scheme, including assessment and notification requirements together with related procedures, **before** entering into arrangements in which personal information is jointly held. While not a legal requirement, the OAIC has suggested that the organisation with the most direct relationship with the people at risk of serious harm may be best placed to notify.

Reporting data breaches to other authorities

In addition to notifying eligible data breaches to affected individuals and the OAIC, organisations may also need to consider whether:

- the data breach triggers other notification requirements, and
- other authorities should be contacted to provide specific actions and protections

For example, in cases where TFNs are involved, it may be appropriate to seek advice from the Australian Tax Office (**ATO**). And where health information stored in the My Health Record system is involved, it may be appropriate to seek guidance from the Australian Digital Health Agency.

Organisations may also be required to notify other industry-specific regulators or other organisations under contractual arrangements.

If other regulatory authorities have been notified, it is useful to state this on the OAIC notification form.

Reviewing the incident

The OAIC recommends that organisations review and learn from eligible data breach incidents once the containment, assessment and notification steps have taken place.

An eligible data breach incident is an opportunity to:

- use lessons learned to strengthen the organisation's own personal information security and handling practices, and
- prevent, or reduce the likelihood of, a similar breach

Reviewing the data breach may include measures such as:

- a security review and understanding the root cause of the data breach
- education and training
- implementing a prevention plan to prevent a reoccurrence, and
- a review of policies and procedures

Managing risks that arise from changing work environments

Work environments have evolved over the last three years, including a shift towards remote and hybrid work. As a result, organisations may have increased vulnerabilities.

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

Organisations are strongly encouraged to conduct a privacy impact assessment and address identified risks.

Declaration of an eligible data breach by the Minister

The Minister has the power to make an eligible data breach declaration. This is to prevent and reduce the risk of harm arising from misuse of personal information following unauthorised access to or disclosure of personal information. The declaration allows the collection, uses and disclosure of personal information that would otherwise not be permitted under the APPs, for organisations addressed by the declaration.

Example

An organisation's network experiences a cyber security incident when malicious actors have unauthorised access to their client's personal information such as their names, date of birth and credit card information. The hackers use this personal information to conduct fraud and identity crime. An eligible data breach declaration will permit the organisation to disclose the personal information to relevant services, such as a bank, so the bank can identify the affected customers, ensure enhanced monitoring of their accounts and impede financial loss.

When would an eligible data breach be declared?

The Minister can only make the declaration for certain permitted purposes which are related to preventing or reducing a risk of harm from the misuse of personal information about one or more individuals following unauthorised access to, or unauthorised disclosure of, that personal information.

Permitted purposes include:

- preventing a cyber security incident, fraud, scam activity or identity theft
- responding to a cyber security incident, fraud, scam activity or identity theft
- responding to the consequences of a cyber security incident, fraud, scam activity, identity crime and misuse, financial loss, emotional and psychological harm, family violence and physical harm or intimidation
- addressing malicious cyber activity

When would an eligible data breach declaration apply to you?

The declaration will outline what type of personal information and organisations are impacted including the following **information**:

- the kinds of personal information which applies
- the entity or class of entities that may collect, use or disclose the personal information
- the entity or class of entities (for example, banks) that the personal information may be disclosed to, and
- one or more permitted purposes of the collection, use or disclosure

At any time when an eligible data breach declaration is in force **you may collect, use or disclose personal information** about an individual if:

- you reasonably believe that the individual may be at risk from the eligible data breach
- the collection, use or disclosure is for a permitted purpose specified in the declaration
- the information is information of a kind or kinds specified in the declaration, and
- the information is disclosed by an entity specified in the declaration, or an entity included in a class of entities specified in the declaration

Declaration of an emergency by the Minister

The Minister may also make emergency declarations to respond to an emergency or disaster. The aim of the declaration is to allow for a more flexible approach with information sharing.

The declaration will, like the eligible data breach declaration, specify:

- kinds of personal information which apply
- the entity or class of entities that may collect, use or disclose the personal information
- the entity or class of entities (for example, banks, police, hospitals) that the personal information may be disclosed to, and
- one or more permitted purposes of the collection, use or disclosure

Circumstances in which an emergency declaration could be made include:

- identifying individuals who:
  - are or may be injured, missing or dead because of the emergency or disaster
  - are or may be at risk of injury, going missing or death because of the emergency or disaster
  - are or may be otherwise involved in or affected by the emergency or disaster, or
  - are or may be at risk of otherwise being involved in or affected by the emergency or disaster
- assisting individuals involved in or affected by the emergency or disaster to obtain services such as repatriation services, medical or other treatment, health services and financial or other humanitarian assistance
- assisting individuals who are or may be at risk of being involved in or affected by the emergency or disaster to obtain services such as repatriation services, medical or other treatment, health services and financial or other humanitarian assistance
- assisting with law enforcement in relation to the emergency or disaster coordination or management of the response to the emergency or disaster
- ensuring that responsible persons for individuals who are, or may be, involved in the emergency or disaster are appropriately informed of matters that are relevant to:
  - the involvement of those individuals in the emergency or disaster, or
  - the response to the emergency or disaster in relation to those individuals
- ensuring that responsible persons for individuals who are or may be at risk of being involved in or affected by the emergency or disaster are appropriately informed of matters that are relevant to:
  - the involvement of or effect on those individuals in the emergency or disaster, or
  - the response to the emergency or disaster in relation to those individuals

Penalties for not complying with the scheme

If an organisation fails to comply with the NDB scheme, the OAIC has a range of powers to seek damages (financial penalties) to be awarded or require action to be taken.

OAIC's power	Example
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 an amount not more than the greater of: • $50 million • three times the value of benefits obtained or attributable to the breach (if quantifiable), or • if the court can't determine the value, 30% of the organisation's adjusted turnover' during the relevant period

	The court may order the maximum penalty if the failure to notify is a serious or repeated interference with the privacy of individuals.
Accept an enforceable undertaking and bring proceedings to enforce a determination	The organisation agrees to apologise and to implement a compliance program in lieu of other civil action. OAIC can go to court to enforce that undertaking.
Direct an organisation prepare a notification statement and notify as soon as practicable	If the OAIC finds out about a data breach externally it can direct an organisation to comply with the NDB Scheme
Apply to court for an injunction to prevent ongoing activity or a recurrence	Apply to the Court for an order preventing an organisation from running a website whilst it is compromised or until adequate security measures are in place

Caution

Even if an organisation completely complies with the NDB scheme, it may still be liable for civil penalties if it is found that the organisation has breached other provisions of the Privacy Act. Refer to our privacy guide for more details.

Note

Before directing an organisation to notify affected individuals, the OAIC must invite the organisation to make a submission within a specified period in which the organisation can raise information and put forward recommendations as to next steps.

Example

In 2017 there was an unintentional data breach involving an Australian Blood Service. The organisation engaged in an enforceable undertaking and promised to review newly implemented measures. The OAIC did not impose penalties, concluding that the Blood Service responded quickly, effectively and worked swiftly to implement steps to mitigate against future data breaches. Following the investigation the OAIC further concluded that the community can have confidence in the Blood Services' commitment to the security of personal information.

Part 6

Practical tips for compliance and ‘permitted situations’

Practical tips for compliance and 'permitted situations'

This part covers:

- practical compliance tips, and
- exceptions for 'Permitted Situations'

Practical compliance tips

Practical steps that a not-for-profit organisation can take to help them comply with Privacy Laws include:		
1.	**Privacy audit**	An organisation should conduct a privacy audit to work out what kind of personal information it collects, uses, stores and discloses. An audit may also show how the not-for-profit organisation manages and safeguards personal information, including how it manages privacy queries and complaints and how it updates, destroys or de-identifies personal information.
2.	**Privacy officer**	An organisation should appoint a person ('privacy officer') to be responsible for developing, implementing and updating its privacy policy, and to be the first point of contact for privacy issues or complaints. Ensure a privacy officer has a dedicated email address (such as *privacy@[organisation].com.au*) to avoid emails relating to privacy issues being missed.
3.	**Privacy policy**	If your organisation falls under the Privacy Laws, you must ensure someone is responsible for preparing, reviewing and updating your organisation's privacy policy. While a not-for-profit organisation's privacy officer should primarily be responsible for the privacy policy, involving administrative and operational staff and volunteers in this process is a good way to make sure the policy reflects current organisational practice and complies with Privacy Laws. A privacy policy should be reviewed regularly (for example, annually) for relevance and updated (for any changes in law or organisational practice).
4.	**Review contracts for impact on privacy law**	A not-for-profit organisation should review its contracts for Privacy Law impact and obligations. In some cases (for example, under Government funding contracts), a not-for-profit organisation may be required to comply with Privacy Laws even if it would otherwise be considered exempt. In other cases, a not-for-profit organisation may outsource services to a third party (for example, fundraising, sponsorship or general services contracts), who may come into contact with or use, collect, store or disclose personal information of the organisation's staff, clients, donors or volunteers. Consider what privacy compliance measures are required in those contracts to make sure obligations flow through to contractors and third parties.

5.	**Privacy checklists, guidelines and manuals**	A not-for-profit organisation should develop privacy checklists, guidelines and manuals to help staff, donors, volunteers and clients understand how the organisation uses, stores, discloses and safeguards personal information. These documents may also outline the organisation's privacy complaint handling procedure and its procedure for handling personal information breaches.
6.	**Data breach response plan**	Have a written internal policy that sets out how your organisation will respond in the case of a breach or suspected breach of privacy.
7.	**Train personnel**	A not-for-profit organisation should train staff, contractors and volunteers on your organisation's privacy policies and carrying out its privacy procedures.
8.	**Transparency**	Ensure your privacy policy, (including details about how users can address privacy issues) is available and accessible.

Exceptions for 'permitted situations'

The Privacy Act sets out certain 'permitted situations' that allow for the collection, use or disclosure of personal information (including sensitive and health information) in special circumstances, (referred to in part 4 of this guide: What are your organisation's obligations under Privacy Laws?).

An overview of 'permitted situations' most likely to apply to not-for-profit organisations is set out below.

Situation	Applies to	Conditions
Permitted general situations		
Serious threat to life, health or safety	Collection, use or disclosure of: • personal information, or • a government related identifier	• It's unreasonable or impractical to get the person's consent to the collection, use or disclosure, and • your organisation reasonably believes that 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 misconduct of a serious nature	Collection, use or disclosure of: • personal information, or • a government related identifier	• Your organisation has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to your organisation's functions or activities has been, is being or may be engaged in, and • your organisation reasonably believes that the collection, use or disclosure is necessary for it to take appropriate action in relation to the matter
Locating a missing person	Collection, use or disclosure of personal information	• Your organisation reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and • the collection, use or disclosure complies with special rules made by the OAIC under section 16A(2) of the Privacy Act

Situation	Applies to	Conditions
Disputes and claims	Collection, use or disclosure of personal information	• The collection, use or disclosure is reasonably necessary for: • the establishment, exercise or defence of a legal or equitable claim, or • the purposes of a confidential alternative dispute resolution process
Permitted health situations		
Provision of a health service	Collection of health information about a person who receives a health service	The information is necessary to provide a health service to the person and either: • the collection is required or authorised under an Australian law (other than the Privacy Act), or • the information is collected in accordance with binding professional confidentiality rules set by competent health or medical bodies
	Collection of health information about a third party	• The health information about the third party is part of the family, social or medical history of the health service recipient • It's necessary for your organisation to collect the health information in order to provide the health service, and • the health information is collected by your organisation from the health service recipient or, if the recipient is physically or legally incapable of giving the information, a responsible person for the recipient
	Disclosure of health information to a person responsible for the health service recipient	• Your organisation provides a health service to the person who the information is about • the recipient of the information is a responsible person for the person who the information is about • the person who the information is about is physically or legally incapable of giving consent to disclosure of the information, or physically can't communicate consent to disclosure • a person providing the heath service for your organisation is satisfied that either: – the disclosure is necessary to provide appropriate care or treatment of the person who the information is about, or – the disclosure is made for compassionate reasons and the disclosure is limited to the extent reasonable and necessary for this purpose, and • the disclosure is not contrary to any wish expressed by the person who the information is about before they became unable to give or communicate consent, of which the person

Situation	Applies to	Conditions
		providing the health service for your organisation is aware or could reasonably be expected to be aware
Use or disclosure of genetic information for the benefit of a family member	Use or disclosure of genetic information	• Your organisation has obtained the genetic information in the course of providing a health service to a person • your organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another person who is a genetic relative of the person who you collected the information from in the course of providing a health service • the use or disclosure is conducted in accordance with approved guidelines as published by the National Health and Medical Research Council **(NHMRC**), and • in the case of disclosure – the recipient of the genetic information is a genetic relative of the person who you collected the information from in the course of providing a health service
Research	Collection of health information	• The collection is necessary for research relevant to public health or safety, the compilation or analysis of statistics relevant to public health or safety, or the management, funding or monitoring of a health service • the purpose cannot be served by collecting de-identified information • it's not practical to get consent from the person who the information is about, and • any of the following apply: – the collection is required under an Australian law (other than the Privacy Act) – the information is collected in accordance with binding professional confidentiality rules set by competent health or medical bodies, or – the information is collected in accordance with approved guidelines as published by the NHMRC. A key requirement of the guidelines is approval by a human research ethics committee (**HREC**)

Situation	Applies to	Conditions
	Use or disclosure of health information	• The use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, • It's not practical to get consent from the person who the information is about • the use or disclosure is conducted in accordance with approved guidelines as published by the NHMRC. A key requirement of the guidelines is approval by a HREC, and • in the case of disclosure – your organisation reasonably believes that the recipient of the information will not disclose the health information, or any personal information derived from the health information

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

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

Caution – permitted situations

If you're not sure whether your collection, use or disclosure of sensitive information falls under any of the permitted situations, you should get legal advice.

Part 7

Rights of action and penalties under Privacy Laws

Rights of action and penalties under Privacy Laws

This part covers:

- what happens if your organisation doesn't comply with Privacy Laws?
- tort of serious invasion of privacy
- doxxing offences
- is your organisation still liable if it's not an APP entity?

What happens if your organisation doesn't comply with Privacy Laws?

Failing to comply with your organisation's privacy obligations can have serious consequences.

The most severe offences under the Privacy Act are subject to civil penalties.

Interference with the privacy of an individual

Your organisation will have contravened the Privacy Act if it engages in an act or practice that is an interference with the privacy of an individual and the interference with privacy is serious.

Under recent amendments to the Privacy Act, the OAIC has extended civil powers to issue infringement notices and compliance notices, and to impose civil penalty orders for non-compliance for three levels of interference with the privacy of an individual.

An 'interference with the privacy of an individual' by an APP entity can be:

- the act or practice that breaches an APP in relation to personal information about the individual, or
- the act or practice that breaches a registered APP code that binds the entity in relation to personal information about the individual

In determining whether an interference with privacy is serious, a court will consider :

- the particular kinds of information involved
- the sensitivity of the personal information of the individual
- the consequences, or potential consequences, of the interference with privacy for the individual
- the number of individuals affected by the interference with privacy
- whether the individual is a child or person experiencing vulnerability
- whether the act was done, or the practice engaged in, repeatedly or continuously
- whether the offender failed to take steps to implement practices, procedures and systems to comply with their obligations in relation to privacy in a way that contributed to the interference with privacy, or
- any other matter the court deems relevant

Civil penalties for ‘serious interferences’

The maximum penalty for serious and repeated interferences of privacy is AUD 2.5 million for an individual and for a body corporate – the greater of:

- AUD 50 million
- three times the value of the benefit (if a court can determine the value of the benefit obtained from the contravention), or
- 30% of the body corporate's adjusted turnover during the breach turnover period (if a court cannot determine the value of the benefit obtained from the contravention)

The Privacy Commissioner also has a range of other powers, including powers to:

- make a determination that your organisation contravened the Privacy Act, and
- conduct privacy assessments (previously called audits)

Civil penalties for ‘interferences’

If the interference with the privacy of an individual is not ‘serious’, the maximum penalty for the interference is AUD 660,000 for an individual and AUD 3.3 million for a body corporate.

Civil penalties for ‘specific interferences’

Your organisation can also be liable for administrative breaches under the Privacy Act, including a breach of any enacted APP. An important measure to avoid a fine is to ensure your organisation’s privacy policy is compliant and remains up to date with your activities. Submissions of a non-compliant eligible data breach statement can also attract the same penalty.

The maximum penalty for specific interferences in breach of the Privacy Act is AUD 66,000 for an individual and $330,000 for a body corporate.

Tort of serious invasion of privacy

From 10 June 2025, an individual has a cause of action for serious invasions of their privacy in circumstances where either there has been:

- an intrusion on their seclusion, or
- misuse of their information where they had a reasonable expectation of privacy

For a claim to succeed, an individual will need to demonstrate the invasion of privacy was serious, intentional or reckless, and that the public interest in protecting their privacy outweighs any competing public interest. Note that proof of damage is not required by the individual to make a claim.

To be successful in a claim of serious invasion of privacy, the individual must establish:

1. an invasion of privacy: intrusion upon seclusion or misuse of information
2. a reasonable expectation of privacy in all the circumstances
3. fault: intentional or reckless
4. seriousness of invasion, and
5. public interest considerations (the public interest in privacy outweighs any countervailing public interests)

Invasion of privacy

The individual must first establish there was a serious invasion of privacy either by:

- an intrusion of their seclusion, or
- misuse of their information where they had a reasonable expectation of privacy

An intrusion of an individual’s seclusion could be the physical intrusion into a person’s private space or watching, listening to, or recording the person’s private activities or private affairs. Misuse of information refers to the unauthorised collection, use or disclosure of personal information about the individual.

Note – the information does not need to be true

If invasion of the individual's privacy was by misusing information that relates to them, it does not matter whether the information was true or not.

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 the purposes for which the information is being collected (for example the use of any device or technology)
- 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

Fault: intentional or reckless

The individual must prove that the defendant (the other party) intentionally or recklessly invaded their privacy. A person has intention with respect to a result if they mean to bring it about or is aware that it will occur in the ordinary course of things.

Recklessness is where the person is aware of a substantial risk that a result will occur, and considering the circumstances known to them, they take an unjustifiable risk in respect of that result occurring.

Seriousness of invasion

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

When assessing whether the invasion was serious the court may consider:

- **the degree** of any offence, distress or harm to dignity that the invasion of privacy was likely to cause to a person of ordinary sensibilities in the position of the individual
- whether the defendant **knew or ought to have known** that the invasion of privacy was likely to offend, distress or harm the dignity of the individual
- if the invasion of privacy was **intentional** (ie. whether the defendant was motivated by malice)

Public interest balancing

The individual would need to prove that the public interest in their privacy outweighs any countervailing public interest. This balancing exercise recognises competing interests in society and highlights that an individual's right to privacy is not an absolute.

A guidance as to what different countervailing public interest could be include:

- 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, or
- the prevention and detection of crime and fraud

Note – 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.

Example – a serious invasion of privacy

A not-for -profit organisation helps people experiencing homelessness. As part of its donation process and record keeping obligations, the organisation collects personal information about donors including their full names, phone numbers, and addresses.

In an effort to encourage larger donations, an employee of the organisation collects personal information about donors who have donated less than $10. The employee intentionally discloses the personal information publicly including a list of these donors with their names and contact details. The employee then writes a malicious post that shames the donors for making small donations knowing it would offend them.

This causes distress and harm to those donors who believed their information would be kept confidential.

Is your organisation exempt from this tort?

Exemptions apply in relation to intelligence agencies, law enforcement bodies, and persons under 18 years of age. Journalists and certain other persons are also exempt in certain 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 organisation reasonably believed that the invasion of privacy was necessary to prevent or lessen a serious threat to the life, health, or safety of a person, or
- the invasion of privacy was necessary to defend people or property

Doxxing offences

Doxxing relates to the intentional online exposure of one or more individuals' personal data using a carriage service. Doxxing is deemed a criminal offence under section 474.17 B of the *Criminal Code Act (Cth)* 1995.

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:

- the person uses a carriage service to make available, publish or otherwise distribute information
- the information is personal data of one or more individuals, and
- the person engages in the conduct in a way that reasonable persons would regard as being, in all the circumstances, menacing or harassing towards those individuals

Carriage service is a means of service for carrying communications by means of guided or unguided electromagnetic energy. This may include text messages, phone calls, email, and social media.

Doxxing against an individual has a maximum penalty of six years imprisonment. Doxxing against a person or targeted group because of their race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality or national or ethnic origin can attract a more serious penalty of seven years imprisonment.

Doxxing examples

Deanonymizing 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'.

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

Ongoing obligations

Not-for-profit organisations have an ongoing obligation to make sure they continue to comply with Privacy Laws.

The OAIC has published a privacy management framework with four steps that not-for-profits and other organisations should take to ensure compliance.

Four steps to ensure compliance:

Step 1.	Embed a culture of privacy that enables compliance
Step 2.	Establish a robust and effective privacy process
Step 3.	Evaluate your privacy processes to ensure continued effectiveness
Step 4.	Enhance your response to privacy issues

How your organisation implements these steps will depend on a number of factors, including the size of your organisation, your system of governance, and the information that you are dealing with.

justice connect