Australia
Not-for-profit Law
Guide

Privacy Guide

A guide to compliance with privacy laws in Australia

July 2017

justice connect
Not-for-profit Law

Contents

Introduction

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

This guide describes obligations under the following legislation, collectively referred to as **Privacy Laws**:

- Commonwealth (**Cth**) law: *Privacy Act 1988* (Cth) (**Privacy Act**) which, from 12 March 2014, sets out the Australian Privacy Principles (**APPs**)
- Australian Capital Territory (**ACT**) law: *Information Privacy Act 2014* (ACT), *Health Records (Privacy and Access) Act 1997* (ACT)
- New South Wales (**NSW**) law: *Privacy and Personal Information Protection Act 1998* (NSW), *Health Records and Information Privacy Act 2002* (NSW)
- Northern Territory (**NT**) law: *Information Act 2003* (NT)
- Queensland (**Qld**) law: *Information Privacy Act 2009 (*Qld*)*
- Tasmanian (**Tas**) law: *Personal Information Protection Act 2004* (Tas)
- Victorian (**Vic**) law: *Privacy Data and Protection Act 2014* (Vic), *Health Records Act 2001* (Vic), and

South Australia and Western Australia currently have no legislative scheme for privacy law. However, South Australia has an administrative direction on handling personal information that binds the public service: PC012 – Information Privacy Principles (IPPs) Instruction.

If you work for a not-for-profit, you or your colleagues will likely collect, use, store and/or disclose information about individuals – for example, when you deliver services or gather information regarding new memberships. This information will often be classified 'personal information' under Privacy Laws, and may include 'sensitive information' and/or 'health information', which are subcategories of personal information requiring special treatment.

It is important to consider your responsibilities under Privacy Laws in all your dealings with personal information, whether engaging and managing employees and volunteers, advertising your products and services, fundraising and communicating with members and the public, or storing and managing records. 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.

This guide helps you understand your not-for-profit organisation's Privacy Law obligations by helping you to answer the following questions:

1. **what sorts of information do Privacy Laws cover?**
2. **is the information our organisation collects and holds covered by Privacy Laws?**
3. **which Privacy Laws apply to our organisation? and**

4. how do I apply the Privacy Law requirements to my not-for-profit organisation?

We also take a closer look at specific requirements for privacy policies and treatment of personal information in fundraising, and finish with some practical tips and extra resources.

CAUTION

The information contained in this privacy guide is of a generic nature and is not intended to replace legal advice but rather provide an overview of the Commonwealth and state laws on privacy. Privacy Laws are complex and are not always easy to apply in practice. If you have any doubts, seek advice from a privacy lawyer.

Part 1 – What information is covered by Privacy Laws?

What information is covered by Privacy Laws?

This section covers:

- what is 'personal information'?
- what is 'sensitive information'?
- what is 'health information'? and
- other special classes of information.

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

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

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

The Privacy Laws apply to these categories of information in different ways. The way the Privacy Laws apply to your organisation also depends on the size and type of your organisation, which is discussed further in Part 2 of this Guide.

1. Information covered by privacy laws

1.1 What is 'personal information'?

'Personal information' is information or an opinion about an identified individual, or an individual who is 'reasonably identifiable'.

Personal information can be:

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

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

WHEN WILL SOMEONE BE 'REASONABLY IDENTIFIABLE'?

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

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

Deceased persons **do not** have 'personal information' under federal Privacy Laws. Under some state and territoriy laws, the personal information of a deceased person may still require protection for a period of time. 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 does not include:

- anonymous information,
- aggregated information (eg. data that reflects trends without identifying the sample)
- de-identified information, or
- information about companies or other entities which does not identify individuals.

EXAMPLE

Consider a car licence plate. Most people would not be able to identify the owner of a car simply from the registration number. To most people, then, knowing a car's licence plate number would not make the owner of the car 'reasonably identifiable'.

But if you work for an agency responsible for car registration, you may have access to other information that enables you to you to identify the owner of the car. Holding information about the car registration would make the person 'reasonably identifiable' to you from the information you hold, so the registration number would be considered personal information.

1.1.1 When is unrecorded information covered by Privacy Laws?

It can be tricky to work out whether unrecorded information about an individual is subject to the Privacy Laws. It basically depends on why and how the recorded information was collected.

Personal information that is not collected for the purpose of being included in a 'record' (for example, a document, database or photographic image) is not subject to Privacy Laws. If a member tells you about what they did on the weekend, but no record is made of that information, then it will be outside the scope of Privacy Laws.

However, if the personal information was collected to be included in a record, and then you communicate that information verbally (for example over the phone), it may be subject to Privacy Laws in some jurisdictions (for example, under federal Privacy Laws).

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 to use on your website, or in brochures, newsletters or any other material, you should arrange notification forms for the people who appear in any images you collect. These forms should explain the purpose of the photographs and how you plan to use them, in addition to the other notification requirements discussed at section 2 of Part 3.
- While **information about companies will not be covered by the Privacy Laws**, it might be covered by confidentiality laws. Not-for-profit Law has produced information on confidentiality – see the IP topic on the Not-for-profit Law information hub at www.nfplaw.org.au/IP.

1.2 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 the Privacy Laws, information will be considered 'sensitive information' where it is 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.

! CAUTION

Your organisation needs to distinguish between different types of personal information to ensure you are applying the appropriate standard when dealing with that type of information

Health information (discussed further below) or genetic information or biometric information is also a form of 'sensitive information'.

Identifying sensitive information is important as different requirements and thresholds apply to this kind of information under the Privacy Laws.

1.3 What is 'health information'?

'Health information' is a type of personal information that includes information or opinion 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 (eg. blood, organs), and
- genetics.

You need to establish when you are collecting, using, storing or disclosing information that is considered 'health information' as this type of information is generally afforded a higher level of protection under Privacy Laws.

EXAMPLE

Examples of 'health information' include:

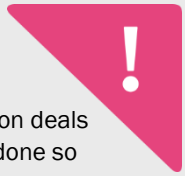
- notes of a person's symptoms or diagnosis and treatment
- specialist reports or test results
- appointment and billing details
- dental records
- a person's healthcare identifier when it is collected to provide a health service
- prescriptions and other pharmaceutical purchases, and
- any other personal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

1.4 Other classes of confidential information

The following types of information are also protected in particular ways. This guide does not cover these types of information. If you deal with this kind of information and are not aware of the particular requirements that apply to your organisation, you should seek advice from a privacy lawyer.

- 'spent convictions' (old, minor criminal convictions)
- tax file numbers
- electoral roll information
- surveillance information, and
- credit history.

CAUTION



Stricter legal requirements are applied to the handling of information about a person's credit worthiness. The current credit reporting regime commenced in March 2014. If your organisation deals with credit information it should seek advice on complying with these obligations if it has not done so already.

Part 2 – Is your organisation subject to Privacy Laws?

Is your organisation subject to Privacy Laws?

This section covers:

- who the Privacy Laws apply to.

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

Organisations will have to follow Privacy Law obligations when they meet the criteria set out below. It is possible that a not-for-profit organisation will be governed by more than one of the three laws which comprise the Privacy Laws.

The Privacy Laws comprise three separate laws:

1. **the Australian Privacy Principles (APPS) under federal Privacy Laws**
2. **the applicable state and territory Privacy Laws, if any, and**
3. **the applicable state and territory health privacy legislation (Health Privacy Laws), if any.**

CAUTION

Your organisation may be required 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 ensure that your practices are consistent with all the Privacy Laws that apply to your organisation. If you're not sure, you should seek legal advice.

1. Sources of privacy laws and exemptions

1.1 Australian Privacy Principles (APPs)

The APPs are legal obligations under federal Privacy Laws that apply to every organisation and government agency that meets the qualifying criteria (explained below) across Australia.

'Organisation' is defined in the Privacy Act to include individuals, bodies corporate, partnerships, trusts and other unincorporated associations. 'Bodies corporate' include many of the common legal structures within the not-for-profit sector, including incorporated associations, co-operatives, companies limited by guarantee and indigenous corporations. Not-for-profit organisations that are unincorporated associations and trusts also fit within the definition of 'organisation'.

Your organisation will need to comply with the APPs if it falls into any of the following categories:

- has an annual turnover of more than $3 million
- provides a health service to a person – even when providing that health service is not the organisation's primary activity – including:
  - private hospitals, day surgeries, medical practitioners, pharmacies and allied health professionals
  - naturopaths and chiropractors
  - gyms and weight loss clinics, and
  - child care centres, private schools and private tertiary educational institutions.
- discloses personal information about another individual to anyone else for a benefit, service or advantage
- provides a benefit, service or advantage to collect personal information about another individual from anyone else
- is a contracted service provider under a Commonwealth contract (e.g. an aged care provider or a disability services provider under a Commonwealth agreement)
- is a credit reporting body
- 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
- has opted in to the Privacy Act (choosing to comply despite not falling into one of the above categories).

FURTHER READING

Organisations that would not otherwise be covered by the APPs can choose to be treated as an 'organisation' for the purposes of the Privacy Act and therefore 'opt in' to be bound by the APPs.

For more information on how to opt in and opt out go to http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-registers/opt-in-register.

Do the APPs apply to us?

✔ You run a charity that recorded an annual income of $3.2 million in its most recent Annual Report. The APPs apply to you.

✔ You are a club with a turnover of less than $3 million. Your club has a program or facilities to assist members with injuries or improve fitness and health. It is probably providing a health service, especially if it hires a health professional. The APPs apply to you.

✔ You are a theatre company whose turnover is 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 benefit of sponsorship). The APPs apply to you.

✔ You are a not-for-profit organisation that provides childcare services or activities. While you have a turnover of less than $3 million per year, you collect, use and store information about

children's allergies, disabilities and medical needs (i.e. health information). The APPs apply to you.

✔ You are a subsidiary not-for-profit organisation that has a 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 over $3 million turnover. You provide information about your members, donors and/or volunteers to your parent not-for-profit organisation. The APPs apply to you.

✔ You are a not-for-profit organisation that has a turnover of less than $3 million. You obtain funding from the Commonwealth Government to run a specific program, and there is an associated funding contract you have entered into. The APPs apply to you.

✖ You are a sporting club that collects the names and addresses of team participants. You earn $120,000 in revenue. The APPs do not apply to you.

1.2 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 initial 'threshold' criteria, you need to consider if your not-for-profit organisation or particular information you are handling falls into one of the categories of exemptions. The main categories of exemptions relevant to not-for-profit organisations are addressed below.

1.2.1 Employee records

If an employer handles information that is part of an employee record 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 (e.g. subsidiaries).

It is important to consider that this exemption may not extend to records of an employee's (after-hours) behaviour on social media whilst employed by your organisation.

Employee records exempted from the APPs may be subject to special requirements under the *Fair Work Act 2009* (Cth). If you are uncertain about your obligations in handling employee records you should seek legal advice.

It is also important to note that state and territory Privacy Laws may still apply to certain employee information despite the employee records exemption under the federal Privacy Laws. 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 full time employee asking for personal information related to his employment record with your organisation. This information is subject to the employee records exemption.

However, during the course of the conversation, she asks if you noticed any unusual activity on the employee's social media accounts during the course of his employment. It is 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.

1.2.2 Generally available publications

A publication which is generally available to the public is exempt from the APPs. Magazines, books, articles, newspapers, or other publications available to the public fall into this category, irrespective of whether they are published physically or electronically, and irrespective of whether there is a payment of a fee associated with the information.

EXAMPLE

You have a copy of the White Pages that lists some of your clients' home phone numbers and contact addresses. This information is not covered by the APPs.

1.2.3 Government contractors

Where an organisation is required to follow the APPs only because it has a contract with government, the organisation will only be required to follow the APPs for personal information it is managing in relation to the 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 is exempt.

Where an organisation is required to do something under 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 the State Government to assist in rehabilitating juvenile offenders. You are required to disclose information regarding possible offences by the residents under the terms of your contract, despite it being in conflict with an APP. This information is subject to an exemption to the APPs and may be disclosed.

1.2.4 Political exemption

If you work on behalf of a registered political party or representative, and you do so with their authority, work you complete for them will be exempt from the APPs where 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.

1.2.5 Other exemptions

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

- journalism exemption – this only applies where 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 seek legal advice.

1.3 Health Privacy Laws

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

You may be required to comply with the Health Privacy Laws if you operate in New South Wales, Victoria and the Australian Capital Territory and:

- you are a health service provider, or
- you collect, hold or use health information (described in paragraph 1.3 in Part 1 of this guide).

1.3.1 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
- child care centres and private schools.

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

Do the Health Privacy Laws apply to my organisation?

- ✔ You are a contracted service provider of health services 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.
- ✖ You provide first aid at music festivals on an anonymous basis. You would not be required to comply with the Health Privacy Laws.

Part 3 – Obligations under Privacy Laws

Obligations under Privacy Laws

This section covers:

- collecting personal information
- notification of collection
- obtaining consent
- unsolicited information
- using and disclosing health information
- special rules for sensitive and health information
- storage of personal information
- fundraising and privacy, and
- cross-border disclosure and international cooperation.

If you are holding or want to collect information which is considered 'personal', 'sensitive' or 'health' information about an individual, you need to understand the rules that apply.

The Australian Privacy Principles (**APPs**) are 13 legally binding principles which set the basic standard for privacy protection regarding 'personal', 'sensitive' or 'health' information at the federal level. They set out requirements about how not-for-profit organisations bound by the federal Privacy Laws may collect, use, disclose, and store these types of information. The APPs are also 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. See the table under paragraph 8 of Part 6 for a comparison.

In summary, the APPs require an organisation to:

1. take reasonable steps to make individuals aware that it is collecting 'personal', 'sensitive' or 'health' information about them

2. notify those individuals about the purpose/s for which it is collecting the information and who it might share that information with (among other things)

3. if the personal information is sensitive information, ensure that consent for such collection, use or disclosure is obtained (expressly or impliedly)

4. comply with restrictions on how personal information can be used and to whom it can be disclosed, including at any offshore location where the information may be disclosed, and

5. give individuals the right to access the information you hold about them and to have that information corrected or modified.

Organisations must also have a publicly available privacy policy, discussed further at Part 4.

The APPs cover the following subjects, which are explained further below.

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

1. Collecting personal information

The following basic rules apply to all personal information collected by your organisation:

- you should only collect personal information reasonably necessary for one or more of your organisation's function or activities (**APP 3**)
- personal information can only be collected by 'lawful and fair means' – that is, not through criminal or illegal activity, trickery or deception (**APP 3**)

- personal information should only be collected directly from the person it belongs to, unless it's impossible or impracticable to do so (**APP 3**)
- individuals should be given the option of remaining anonymous or using a pseudonym, unless this is impracticable, or your organisation is required by law to deal with an identified individual (**APP 2**), and
- individuals must be notified about the purposes for which their personal information will be used, among other things (**APP 5**).

When collecting sensitive information and health information, the individual's consent is required, unless an exception applies. (Consent is discussed further at section 3 of this Part 3.)

TIP

If you use street based direct marketing, it's important to remember you are only permitted to 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 in regard to what information they are supposed to collect and how they are supposed to do it.

1.1 Sensitive and health information

You must not collect sensitive information (including health information) unless:

- the individual specifically consents to the information being collected, and
- the information is reasonably necessary for one or more of your functions or activities.

However, there are 'permitted situations' in which sensitive information can be collected, used, or disclosed without consent. These are listed in the 'Permitted Situations Quick Reference Table – Sensitive Information', at the end of this Guide.

There is also an exception for certain non-profit organisations, which are able to collect certain types of sensitive information without consent. 'Non-profit organisation' is defined in the federal Privacy Law as a non-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 are entitled to collect 'sensitive' information without consent where:

- the information relates to the activities of your organisation, and
- the information relates solely to the members of the organisation, or to individuals 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 the views of their members on religious or moral issues

- a trade union collecting information about the political views of a job applicant, or
- a community not-for-profit organisation aimed at assisting persons with disabilities, collecting information about their disability, as well as diagnosis and medical reports in order to provide counselling and support.

CAUTION

- A not-for-profit organisation can rely on the exception if the purpose of collecting the sensitive information is related to the purposes in the definition of the not-for-profit organisation (e.g. related to the purpose or objects stated in the Constitution of the not-for-profit organisation). An organisation conducting activities for some other purpose can't rely on this exception.
- A not-for-profit organisation can rely on the exception if there is a clear relationship, assessed objectively, which exists between the information collected and that activity. For example, that information may relate to a fundraising activity undertaken by a not-for-profit organisation to support its cultural, recreational, political, religious, philosophical, professional, trade or trade union purpose.
- A not-for-profit organisation can rely on the exception if the sensitive information relates solely to a member of the organisation or to an individual who has regular contact with the not-for-profit organisation. 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.

Whether or not consent is required for the collection of sensitive information, the general rules for collecting personal information should be applied. That is:

- collect it by lawful and fair means
- try to collect it directly from the individual concerned, and
- inform the individual of the identity of your organisation and the purpose of collecting the information, as well as the other notification matters listed under section 0 of this Part 3.

Collecting health information from third parties

If you can't reasonably and practicably collect the 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.

The Privacy Laws require you to notify the individual that the information was collected – whether you collect the information directly from the individual or from a third party. In some instances, however, the Privacy Laws recognise it might not be reasonably practicable to notify the individual. For example, in an emergency situation, there may not be sufficient time to notify the individual concerned. See section 2 of this Part 3 for further information on notification.

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 are in the business of managing health information, make sure you pay close attention to the obligations that apply.

2. Notification

When you collect personal information, or as soon as you can after collection, you must take steps to ensure that 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/tribunal order, the fact that it is so required or authorised (including the name of the law or details about the court/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
- that your privacy policy contains information about how the person may access and correct the information you hold about them
- that your privacy policy contains 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 is reasonably practicable to specify the locations).

You can make the person aware of this information in a number of ways. Typically, organisations give 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 that particular collection of personal information.

3. Consent

Although obtaining individuals' consent isn't always practicable or necessary when collecting non-sensitive personal information, seeking consent from individuals will generally allow your organisation to deal with that information under the applicable Privacy Laws or Health Privacy Laws in any way that is consistent with the consent sought.

Consent is required for the collection of sensitive information and health information, unless an exception applies (**APP 3**).

There are strict requirements regarding the type of consent that must be given. For instance, consent, whether express or implied, must meet the following key elements:

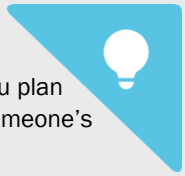
- the individual must be adequately informed before giving consent
- the individual must give consent voluntarily, and
- the individual must have the capacity to understand and communicate their consent.

Consent does not have to be in writing, but it is a good idea to keep a record of a person's consent in case it is challenged later. Consent can take a variety of forms, but a signature is always best. 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.

TIP



Consent is something you should always think about up-front when you're considering how you plan to use, disclose and store personal, sensitive and health information. It's a lot easier to get someone's permission before you use their information than it is afterwards.

This means that it's doubly important to think about how and why you will want to use someone's information before you ask them for it!

CAUTION

Always remember to consider whether someone has capacity to give you their consent.
Ask yourself: 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?

If you have any doubts about whether someone knows what they're signing, explain it to them carefully and ensure they understand your explanation.

4. Unsolicited information

Unsolicited information (**APP 4**) is personal, sensitive and/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 organisations functions or activities? and
- was it sensitive information requiring consent?

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

If the information is not reasonably necessary for one or more of your organisations functions or activities, then you will need to destroy or de-identify the information. However, before you destroy any information, you must make sure there is no other legal requirement to retain it. If you are not sure, seek legal advice before destroying or de-identifying information you have on file.

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

Somebody 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 provide the person with the required notification under APP 5 and handle the information in accordance with the Privacy Laws.

5. Storing personal information

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

Depending on your organisation's circumstances, you should consider the following security measures:

- requiring staff to keep relevant documents in locked drawers or cabinets
- placing access restrictions on relevant documents or systems, including electronic access restrictions
- enforcing a 'clean desk' policy to minimise the risk of inadvertent disclosure of personal information
- placing computer screens out of the view of others, particularly visitors to the organisation
- limiting the use of portable storage devices, including laptops, disks and USB keys, or using encryption or other security measures
- recording audit trails of access to documents
- encrypting documents containing personal information, particularly when those documents are being sent by email
- including email addresses for group emails in the 'BCC' field rather than the 'To' field so recipients cannot see other recipients' email addresses
- including confidentiality and privacy clauses in agreements with volunteers or others who have access to the personal information, and
- making sure employees, volunteers or others return information at the end of their employment or involvement with the organisation.

CAUTION – CLOUD-BASED STORAGE

If you use internet (or 'cloud') based storage systems for your data, as well as adhering to the tips above there are some 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 ensure 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

Consider the steps you can take to ensure you limit the possibility of the provider breaching the APPs, including:

- ☐ in any contract you sign with an overseas service provider, require the provider to comply with the APPs and include indemnities against any breach of the applicable Privacy Law or Health Privacy Law
- ☐ understand how a third party provider handles, stores, and deals with data and personal information, and
- ☐ maintain strong access, security controls and procedures over who has access to your data and what they can do with it
- ☐

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 is 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.

5.1 Special requirements for 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.

TIP

It doesn't matter if the document is situated in your organisation, or even in your state or territory, or if you have sole custody of the information. If the information has a connection to your state operations, a state service contract, or a client of your state, the state privacy requirements may apply.

If you participate in the 'personally controlled electronic health record system' (**eHealth**), you must comply with the *Personally Controlled Electronic Health Records Act 2012* (Cth) (**PCEHR Act**) and the *Healthcare Identifiers Act 2010* (Cth) (**HI Act**). The PCEHR Act limits when and how health information included in an eHealth record can be collected, used and disclosed.

If you are storing health information, you are under certain obligations to the person whose information you possess. You are required to ensure, at their request, that that person has:

- an understanding of why you are storing their health information
- an understanding of how you collected that information
- an understanding of what the health information you possess entails
- an understanding of what rights they have to access that information, and
- an ability to update, correct, or amend that information subject to a reasonable request.

6. Using or disclosing personal information

The most important thing to be aware of when it comes to using personal information you have collected is that you must not use or disclose that information for any reason other than the **primary purpose** you collected it for (**APP 6**).

TIP

This means it's very important for all staff to be regularly reminded of the primary purpose of your not-for-profit's collection of personal information. Consider including a 'mission statement' or 'primary objective' reminder on documents circulated to telemarketers or street side information collectors.

There are only three situations where you can lawfully use personal information for a secondary purpose (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 individual 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, or
- **Law.** An exception within the law (either in the Privacy Laws or in another law) expressly applies to permit the secondary use of the information.

EXAMPLE

Your not-for-profit 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 them with email updates. You must not use that information to do anything other than this unless you gain the individual's specific consent (or an exception applies).

There are additional requirements that limit the adoption, use and disclosure of government identifiers (e.g. Medicare number, drivers licence number, passport number).

6.1 Using or disclosing personal information for direct marketing

Direct marketing (**APP 7**) is communicating with a person to promote goods and services, and can include fundraising. If your organisation uses or discloses personal information for the purposes of direct marketing, there are some important issues for you to consider.

Sensitive information (including health information) can only be used or disclosed for direct marketing if a person has consented to that use or disclosure. **Non-sensitive personal information** can be used or disclosed for direct marketing where:

- 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 does not wish 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 have the person's consent or it is impracticable to obtain that consent
- you provide a simple opt-out mechanism from direct marketing in a prominent statement in each direct marketing communication with the person, and
- the person has not chosen to opt out.

CAUTION – *SPAM ACT 2003* (CTH)

In addition to the Privacy Laws, it is also important to be aware that the *Spam Act 2003* (Cth) (**Spam Act**) prohibits the sending of unsolicited commercial electronic messages – known as 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.

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

6.2 Access to and correction of personal information

Accessing personal information (APP 12): If a person requests access to their own personal information held by your organisation, you are generally required to give access in the manner requested. A response to the request should be given within a reasonable period of time. You will need to take care when providing access to information that you do not 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 the safety of an individual 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 mechanisms for making a complaint about it.

Correcting personal information (APP 13): If an individual can show that personal information about him or her held by an organisation is inaccurate, incomplete, irrelevant or out-of-date, the organisation must:

- take reasonable steps to correct the information and notify third parties to which it has provided the information, or
- if there is disagreement about the accuracy, provide the person with written reasons for its refusal to correct the information and information about how to make a complaint and attach to the information a statement noting that the individual claims the information is incorrect, incomplete, irrelevant or out-of-date.

6.3 Consequences of breaching Privacy Laws

Failing to comply with your privacy obligations can carry serious consequences, both legally and for the reputation of your organisation. The federal Privacy Commissioner has the power to seek court enforced fines of up to $1.8 million against an organisation for serious or repeated interferences with an individual's privacy. The Privacy Commissioner also has a range of other powers including the power to make a determination that your organisation breached the Privacy Act. These determinations are publically available on the OAIC's website and can therefore create reputational harm. The Privacy Commissioner also has the power to undertake privacy assessments (previously called auidts). The findings of these assessments are also published on the OAIC's website.

The Privacy Commissioner recommends that all organisations have a plan in place to deal with privacy breaches. A Data Breach Notification Plan will assist you in minimising the harm of any breach and will

also require you to assess whether notification is required (to both the individual concerned and the Privacy Commisisoner).

On 22 Februaray 2018, mandatory notification requirements will come into operation for all entities subject to the federal Privacy Laws.

TIP

Consider having a plan in place to deal with privacy breaches. A Data Breach Notification Plan is considered best practice. It will also help you to adjust to the new mandatory notification requirements that will come into operation in February 2018.

Information to help you draft a Data Breach Notification Plan can be found here: OAIC's Guide to Developing a Data Breach Notification Plan.

The Office of the Australian Information Commissioner has also launched a web page to assist organisations to comply with the new notifiable data breach laws.

If you have any doubts about your organisation's obligations or whether you are doing enough to satisfy them, we recommend you contact a privacy lawyer as soon as possible.

7. Cross-border disclosure

With more companies and organisations operating across national borders than ever before, privacy has become an international problem. Many not-for-profits are unsure what privacy obligations apply to information they receive from overseas, and also information they may 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 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.

Part 4 – Privacy Policies

Privacy Policies

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

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

There are a number of matters that must be covered in your privacy policy.

Things your organisation must include in its 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, and/or disclose that personal information
- ☐ how an individual may access and correct the personal information you hold about them
- ☐ how an individual can complain about a suspected breach of privacy laws
- ☐ whether you are likely to disclose the information to overseas recipients, and
- ☐ if you are disclosing information to overseas recipients, what countries those recipients might be in (if it is practicable to specify).

TIPS FOR PRIVACY POLICIES

- **Don't copy slabs of text from another organisation's policies, because the text might:**
  - not be relevant to the handling practices of your organisation
  - be drafted according to laws from different states or countries to those that apply to you
  - not cover all of the requirements you're obliged to meet, and/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 yourself can make it difficult to avoid breaking that commitment.
- **Keep it easy to read**. Drafting your Privacy Policy in plain, easy-to-understand language will help your clients and staff understand the policy, and can help to avoid any potential legal ambiguity caused by overly complex language.
- **Keep it updated.** The ways your organisation collects and uses personal information can change, and so do technology and laws. Regularly review your privacy policy 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.

FURTHER READING

Norton Rose Fulbright has published a template privacy policy for use by charities and not-for-profits as part of its Privacy Compliance Manual, which you can access on the Not-for-profit Law information Hub at www.nfplaw.org.au/privacy.

Part 5 – Fundraising and Privacy

Fundraising and Privacy

This section covers:

- privacy issues when fundraising, and
- special considerations for private ancillary funds.

1. Fundraising and privacy

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 activities comply with the Privacy Laws. You are required to ensure:

- when collecting personal information from donors, volunteers, clients and others, and intend to use that information for fundraising purposes, you notify them about that from the start
- if you have not notified a person that their personal information might be used for fundraising purposes, you do not use it for those purposes unless:
  - you first obtain consent, or
  - an exception applies (for example, for non-sensitive personal information, that the fundraising purpose is related to the primary purpose and the person would reasonably expect you to use the information in that way)
- 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 at the start, and
- provide an opt out option in all fundraising communications.

It's a good idea to only allow staff access to client information on a 'need to know' basis. For example, ensure that those involved in soliciting donor memberships do not have routine access to personal information that may be kept on client databases, and have checks and balances in place to protect the security of personal information.

It is also important to familiarise yourself with the fundraising laws applicable in each state and territory where your not-for-profit organisation is conducting fundraising activities.

2. Private ancillary funds

The Australian Charities and Not-for-profits Commission (**ACNC**) has the power to register charities on the ACNC Register which can be viewed by any member of the public. Registration by the ACNC is a prerequisite for a charity to access certain Commonwealth tax benefits. As such, although charity registration is voluntary, most not-for-profits that are charitable organisations will need to register.

Charities that are private ancillary funds may reveal the personal information of individual donors on the ACNC Register. As such, if you are a private ancillary fund concerned that the publication of the name, ABN, contact details, governing rules, financial reports or annual information statement is likely to result in the identification of an individual donor, you can apply to have identifying information withheld under the *Australian Charities and Not-for-profits Commission Regulations 2013* (Cth) prior to registration.

If your not-for-profit is a private ancillary fund and a charity which was endorsed by the Australian Tax Office (**ATO**) for charity tax concessions prior to December 2012, then it will be automatically registered with the ACNC.

Part 6 – Practical tips for Privacy Law compliance and extra resources

Practical Privacy Law compliance tips for organisations

This section covers:

- privacy compliance tips
- ongoing obligations
- sensitive information 'Permitted Situation' Quick Reference, and
- Health Information 'Permitted Situation' Quick Reference.

Practical tips

A not-for-profit organisation may take a number of practical steps to assist them to comply with Privacy Laws. These include:

1. **Privacy Audit** – A not-for-profit organisation may consider conducting a privacy audit to determine what sort of personal information it collects, uses, stores and discloses. An audit may further reveal how the not-for-profit organisation implements safeguards to protect personal information, and how it manages personal information, including how it manages privacy queries and complaints and how personal information that needs to be updated, destroyed or deidentified is managed.

2. **Privacy Officer** – A not-for-profit organisation may consider appointing a person ('privacy officer') responsible for developing, implementing and updating its privacy policies, and to be the first point of contact for privacy issues or complaints.

3. **Privacy Policy** – If your not-for-profit falls under the Privacy Laws, you will need to ensure you 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 co-ordinating and implementing the privacy policy for the not-for-profit organisation, involving administrative and operational staff and volunteers in this process is a good idea to make sure the privacy policy reflects current organisational practices as well as complying with current Privacy Laws. Once your privacy policy is developed, it should be regularly reviewed (e.g. annually) for relevance and updated for any changes in law or organisational practice.

4. **Review Contracts for Privacy Law Impact** – A not-for-profit organisation should consider reviewing its contracts for Privacy Law impact and/or obligations. In some situations (e.g. 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 situations, a not-for-profit organisation may outsource or contract with a third party to provide services (e.g. fundraising, sponsorship or general services

contracts) and the third party may come into contact with or otherwise use, collect, store or disclose personal information of the not-for-profit organisation's staff, clients, donors or volunteers. Consider what privacy compliance measures are required in those contracts to ensure obligations 'flow through' to contractors and third parties.

5. **Privacy Checklists, Guidelines and Manuals –** A not-for-profit organisation should consider developing privacy checklists, guidelines and/or manuals to assist staff (and/or donors, volunteers, clients) understand how the organisation uses, stores, discloses and safeguards personal information. These documents may also outline how the organisation implements its privacy complaint handling procedure or procedure for handling personal information breaches discovered by the organisation, and steps that staff should follow.

6. **Data breach response plan** – Consider having a written internal policy setting out how your organisation will respond in the case of a breach or susptected breach of privacy.

7. **Train personnel –** A not-for-profit organisation should train staff, contractors and volunteers on implementing privacy procedures and your organisation's privacy policies.

Ongoing obligations

Not-for-profit organisations have an ongoing obligation to ensure that they continue to comply with Privacy Laws. The OAIC has published a privacy management framework (**Framework**) that outlines four steps that not-for-profits and other organisations are expected to take to ensure compliance.

> FURTHER READING
>
> The Framework, along with ways of implementing the steps can be found on the OAIC website.

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. In summary, the four steps are:

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

Sensitive information 'permitted situation' quick reference

Applies to	Permitted Situation
Collection, use or disclosure of sensitive information	(a) It is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure, and (b) you reasonably believe that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
(a) Personal information, or (b) a government related identifier.	(a) The entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in, and (b) the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.
Personal information	(a) You reasonably believe 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 (b) the collection, use or disclosure complies with the applicable Privacy Law.
Personal information	The collection, use or disclosure is reasonably necessary: (a) for the establishment, exercise or defence of a legal or equitable claim, and (b) for the purposes of a confidential alternative dispute resolution process.

CAUTION – SENSITIVE INFORMATION IN PERMITTED SITUATIONS

If you're unsure whether your collection, use or disclosure of sensitive information falls under any of the above permitted situations, you should seek legal advice.

Health information 'permitted situation' quick reference

Applies to	Permitted Situation
Collection of health information	The information is necessary to provide a health service to the individual and either: (a) the collection is required or authorised under an Australian law (other than the Privacy Act), or (b) the information is collected in accordance with binding professional confidentiality rules set by competent health or medical bodies.
Collection of health information	The collection is necessary for research related to public health or safety, compilation or analysis of statistics relating to public health or safety, or management, funding or monitoring of a health service, and: (a) the purpose cannot be achieved by collecting de-identified information, (b) it is impracticable to obtain consent, and (c) the collection is required under an Australian law (other than the Privacy Act), in accordance with binding professional confidentiality rules set by competent health or medical bodies or otherwise in accordance with approved guidelines.
Use or disclosure of health information	The use / disclosure is necessary for research, or the compilation or analysis of statistics relevant to public health or safety and: (a) it is impracticable to obtain consent, (b) the use / disclosure is conducted in accordance with approved guidelines, and (c) for disclosure, you reasonably believe the recipient will not disclose the information or personal information derived from that information.
Use of disclosure of genetic information	(a) you have obtained the information in the course of providing a health service to the individual, (b) you reasonably believe the use / disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the individual, (c) the use / disclosure is conducted in accordance with approved guidelines, and (d) for disclosure, the recipient is a genetic relative of the individual.
Disclosure of health information	(a) You provide a health service to the individual,

	(b) the recipient is a responsible person for the individual, (c) the individual is physically or legally incapable of giving or communicating consent to disclosure, (d) another individual providing the health service for your organisation (**the carer**) is satisfied that the disclosure is necessary to provide appropriate care or treatment or made for compassionate reasons, (e) the disclosure is not contrary to any prior wish communicated by the individual of which the care is aware or should reasonably be expected to be aware of, and (f) the disclosure is limited to the extent reasonable and necessary to provide appropriate care or treatment or fulfil the purpose of making a disclosure for compassionate purposes.

CAUTION

If you're unsure whether your collection, use or disclosure of health information falls under any of the above permitted situations, you should seek legal advice.

8. State and territory Privacy Principles (IPPs)

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 Principles (**HPPs**) apply. The state and territory IPPs may also apply to organisations that contract with state government. The laws and directions containing the various state and territory IPPs are:

- ACT: *Information Privacy Act 2014* (ACT) sets out 12 Territory Privacy Principles 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 2003* (NT) sets out 10 Information Privacy Principles in Schedule 2
- Qld: *Information Privacy Act 2009 (*QLD*)* sets out 11 Information Privacy Principles in Schedule 3
- SA: Part II of the administrative instruction, PC012 – Information Privacy Principles (IPPs) 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 Data and Protection Act 2014* (Vic) (**PDPA**) sets out 10 Information Privacy Principles in Schedule 1

- WA There is currently no legislative privacy scheme however some privacy principles (dealing with access to information and correction of information) are provided for in the *Freedom of Information Act 2001* (WA)

8.1 State and territory index comparison of IPPs

Despite slight differences in terminology, the fundamental principles regulating the collection and handling of personal information are dealt with in state and territory privacy principles and can be compared in the following index:

Principles	Cth	ACT	NSW	NT	QLD	SA	TAS	VIC
Collection of personal information	APP 3, 5	TPP 3, 5	IPP 1-4, 12	IPP 1, 3, 10	IPP 1-3	IPP 1-3	PIPP 1, 10, 3	IPP 1, 10, 3
Must only collect via lawful and fair means	✓	✓	✓	✓	✓	✓	✓	✓
Information must be reasonably necessary for or directly related to your organisation's functions or activities	✓	✓	✓	✓	✓	✓	✓	✓

Sensitive information can only be collected with consent, where authorised by law, or where expressly permitted by the relevant privacy laws	✓	✓	Collection should not unreasonably intrude into the personal affairs of the individual.	✓	N/A	Should not collect information that is considered excessively personal (having regard to the circumstance)	✓	✓
Information must be collected directly from the individual – third party collection only authorised in limited circumstances	✓	✓	✓	✓	N/A	N/A	✓	✓
Privacy Notice required at time of collection or as soon as reasonably practicable	✓	✓	✓	✓	✓	✓	✓	✓
Must only collect information that is relevant, accurate and up to date	✓	✓	✓	✓	✓	✓	✓	✓
Use and disclosure of personal information	**APP 1, 6, 10**	**TPP 6, 10**	**IPP 6, 9,10, 11, 12**	**IPP 2, 3, 5**	**IPP 5-11**	**IPP 7,9, 10**	**PIPP 2, 3, 4, 5**	**IPP 2, 3, 5**
Can only use and/or disclose information for the primary purpose for which it was collected, unless: • the individual	✓	✓ If a public sector agency uses or discloses personal	✓	✓	✓	✓	✓ If a public sector agency uses or discloses personal	✓ If a public sector agency uses or discloses personal

has consented • the secondary purpose is reasonably expected and related to the primary purpose, or • a law applies (including an exception contained in the relevant privacy laws) permitting or requiring the use or disclosure		information, it must make a written note of the use or disclosure					information, it must make a written note of the use or disclosure	information, it must make a written note of the use or disclosure
Must only use and disclose information that is relevant, accurate and up to date	✓	✓	✓	✓	✓	✓	✓	✓
Organisation must be open and transparent in its management of personal information	✓	✓	✓	✓	✓	✓	✓	✓
The right to anonymity	**APP 2**	**TPP 2**		**IPP 8**			**PIPP 8**	**IPP 8**
Individuals must have the option of not identifying themselves, or of using a pseudonym (where lawful and practicable)	✓	✓	N/A	✓	N/A	N/A	✓	✓

Storage of and access to personal information	APP 11, 12, 13	TPP 11, 12, 13	IPP 5, 7-8	IPP 4, 6	IPP 4-7	IPP 4-6	PIPP 4, 6	IPP 4, 6
An organisation must protect any information it holds from loss, misuse or unauthorised access	✓	✓	✓	✓	✓	✓	✓	✓
The individual has the right to access personal information held by the organisation	✓	✓	✓	✓	✓	✓	✓	✓
The individual has the right to request that information be corrected where it is incorrect, inaccurate or out of date	✓	✓	✓	✓	✓	✓ Implied in IPP 6	✓	✓
Destruction of personal information	**APP 11**	**TPP 11**	**IPP 5**	**IPP 4**			**PIPP 4**	**IPP 4**
If an organisation no longer requires personal information, it must de-identify or destroy the information (subject to any document retention laws)	✓	✓	✓	✓	N/A	N/A	✓	✓
Cross-border data flows	**APP 8**	**TPP 8**		**IPP 9**			**PIPP 9**	**IPP 9**

Before an organisation discloses personal information to an overseas recipient, it must take steps to ensure that the overseas recipient is subject to similar privacy laws	✓	✓	N/A	✓	N/A	N/A	✓	✓

8.2 State and Territory Health Privacy

Federal Privacy Laws apply to health service providers in the private sector and to others who handle health information (described in paragraph 1.3 in Part 1 of this Guide). Federal Privacy Laws apply to health service providers not just for activities relating to providing a health service but more generally to management of all personal information.

New South Wales, Victoria and the Australian Capital Territory have specific health privacy legislation that applies to both public and private sector organisations which handle health information. When handling health information, organisations and agencies in those jurisdictions must comply with both federal and state/territory Health Privacy Laws. When handling personal information that is not health information, the relevant Federal and state/territory privacy laws will apply.

The state and territory Health Privacy Laws can be found 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)
- NT: *Information Act 2003* (NT)
- Qld: *Information Privacy Act 2009* (Qld)
- Tas: *Personal Information and Protection Act 2004* (Tas)
- SA: Currently has no legislative scheme; however, South Australian government agencies are required to comply with Information Privacy Principles in the PC012 Information Privacy Principles Instruction, and
- WA: Currently has no legislative scheme.

Resources

Related Not-for-profit Law Resources

The following Information Hub topics have related information, at www.nfplaw.org.au:

- Norton Rose Fulbright Privacy Manual

This Manual contains an overview of new federal privacy laws and a template privacy policy.

- Fundraising

The Fundraising page features a Guide to Fundraising and further information on gifts, wills and bequests, raffles and minor gaming, and trade promotions.

- Social Media

This page helps community organisations understand the risks to reputation and legal risks involved with social media use.

- People Involved

The People Involved section offers legal information on an organisation's relationships with its clients, employees, members and volunteers.

Other Resources

Further information on privacy can be obtained from the following sources:

- Office of the Australian Information Commissioner (**OAIC**): www.oaic.gov.au
- Office of the Information Commissioner, Queensland: www.oic.qld.gov.au
- Commissioner of Privacy and Data Protection, Victoria: www.dataprotection.vic.gov.au
- The Information and Privacy Commission, New South Wales: www.ipc.nsw.gov.au
- Office of the Information Commissioner, Northern Territory: www.infocomm.nt.gov.au

Contact us:
nfplaw@justiceconnect.org.au

Not-for-profit Law home:
justiceconnect.org.au/nfplaw

Not-for-profit Law legal information:
nfplaw.org.au

Melbourne Office
PO Box 16013
Melbourne VIC 8007
DX 128 Melbourne

Tel +61 3 8636 4400
Fax +61 3 8636 4455

Sydney Office
GPO Box 863
Sydney NSW 2001
DX 78 Sydney

Tel +61 2 9114 1793
Fax +61 2 9114 1792

ABN: 54 206 789 276 | ACN: 164 567 917