Contents

Introduction

Part 1 – What information is covered by Privacy Laws?

1. Information covered by privacy laws

1.1 What is ‘personal information’?

1.1.1 When is unrecorded information covered by Privacy Laws?

1.2 What is ‘sensitive information’?

1.3 What is ‘health information’?

1.4 Other classes of protected information

Part 2 – Is your NFP subject to Privacy Laws?

2. Sources of privacy laws and exemptions

2.1 Australian Privacy Principles (APPs)

2.2 Exemptions to the APPs

2.2.1 Employee records

2.2.2 Generally available publications

2.2.3 Government contractors

2.2.4 Political exemption

2.2.5 Other exemptions

2.3 Information Privacy Principles (Victorian IPPs)

2.4 Exceptions to the Victorian IPPs

2.5 Health Privacy Principles (HPPs)

Part 3 – Obligations under Privacy Laws

3. When are you ‘collecting’ information

3.1 Sensitive information

3.2 Health information

3.2.1 Special requirements when collecting health information

4. Notification

5. Consent

6. Storing personal information

6.1 Special requirements for health information

7. Using or disclosing personal information
This guide is for not-for-profit (NFP) organisations in Victoria who want to understand more about their obligations under Victorian and Commonwealth privacy legislation.

This guide describes obligations under the following legislation:

- **Commonwealth law:** Privacy Act 1988 (Cth) (Privacy Act) which, from 12 March 2014, sets out the new Australian Privacy Principles (APPs), and
- **State law:** Privacy Data and Protection Act 2014 (Vic) (PDPA),¹ which sets out the Information Privacy Principles (Victorian IPPs); and Health Records Act 2001 (Vic) which sets out the Health Privacy Principles (Victorian HPPs),

(collectively referred to as Privacy Laws).

If you work for an NFP you, or your colleagues, will likely collect, use, store and/or disclose information about individuals. This information will often be classified ‘personal information’ under Privacy Laws, possibly because you either deliver services or gather information regarding new memberships. Sometimes, the personal information you collect and handle may include ‘sensitive information’ and/or ‘health information’, which are subcategories of personal information and have onerous requirements. It’s also important to remember that Privacy Law requirements need to be considered in how your organisation approaches its online (eg through social media) and employment practices.

Understanding your Privacy Law responsibilities is vital. Understanding how your NFP uses personal information and disclosing how that personal information is being handled is an important part of both building the trust of your clients, members, and employees, and in making sure you are complying with the legal obligations that may apply to your NFP.

This fact sheet helps you understand your NFP organisation’s Privacy Law obligations using a four question process:

1. **is the information I’m in possession of ‘personal information’?**
2. **what Privacy Laws apply to me and my organisation?**
3. **are there any exceptions or exemptions that apply to me?** and
4. **how do I apply the Privacy Law requirements to my NFP organisation?**

---

1 The PDPA repeals the Information Privacy Act 2000 and the Commissioner for Law Enforcement Security Data Security Act 2005, and establishes a Commissioner for Privacy and Data Protection (Commissioner), merging the previous roles of Privacy Commissioner and the Commissioner for Law Enforcement Data Security.
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 of the information your organisation gathers or deals with.

So, the first step in understanding your obligations under Privacy Laws is determining if the information you’re in possession of, or want to acquire, 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’ refers to 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, or
- recorded or unrecorded (except in relation to the Victorian IPPs where ‘personal information’ refers only to information that is recorded in some form).

What constitutes ‘personal information’ will vary depending on the particular circumstances. Typically, ‘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
- the circumstances of its receipt
- how the information was received, and
- whether it is possible for someone holding the information to identify the person from resources you hold (including other information available to you).

Deceased persons do not have ‘personal information’. However, 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 (e.g., data that reflects trends without identifying the sample)
- de-personalised 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 were an agency responsible for car registration (like VicRoads), you may be able to use other information available 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.

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 principles. 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 the privacy principles. 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 is subject to Privacy Laws.
1.2 What is ‘sensitive information’?

‘Sensitive information’ is a special category of personal information and has more strict Privacy Law obligations for collection, storage and use.

Under the Privacy Laws, information will generally be considered ‘sensitive information’ where it is personal information more specifically 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 records.

Health information (discussed further below) about a person 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 and sensitive information that is defined broadly to include information or opinion about matters such as:

- 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 identify 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
• 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 protected 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**

A new regime for credit reporting commenced in March 2014. If your group deals with credit information it should seek advice on complying with the new regime if it has not done this already.
Part 2 – Is your NFP subject to Privacy Laws?
This section covers:

- who the APPs apply to
- who the Victorian IPPs apply to, and
- who the HPPs apply to.

Once you have established if the information you collect, store, use or disclose is information 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 NFP organisation will be governed by more than one of the three laws which comprise the Privacy Laws.

Remember, the Privacy Laws are comprised of 3 separate laws:

1. the Australian Privacy Principles (Federal law)
2. the Victorian Information Privacy Principles (Victorian law), and
3. the Health Privacy Principles (Victorian law).

CAUTION

Your organisation may be required to comply with more than one set of privacy obligations listed above (e.g., your organisation may need to comply with the APPs as they apply to all businesses and organisations, and may also need to comply with the Victorian IPPs through a contract with a Victorian government agency). You will need to ensure that your practices are consistent with each of 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 form the Federal privacy regime, and they apply to every business or organisation that meets the qualifying criteria (explained below) across Australia.

The Privacy Act does not specifically address whether the APPs apply to a NFP organisation. The Privacy Act, instead, applies to ‘organisations’, which is broadly expressed to include individuals, bodies corporate, partnerships and other unincorporated associations. ‘Bodies corporate’ include many of the common legal structures within the NFP sector, including incorporated associations, co-
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
- exchanges for any benefit, service or advantage in individuals' personal information by providing it to or collecting it from others
- is a contracted service provider under a Commonwealth contract (e.g. an aged care provider or a disability services provider under a Commonwealth agreement), or
- your NFP organisation is related to a body corporate (for example, a subsidiary) that meets any of the above criteria (even if your NFP alone does not).

**Do the APPs apply to me?**

- ✔ You run a charity that recorded an annual income of $3.2 million in its 2012/2013 Annual Report. The APPs apply to you.

- ✔ You are a club with 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 run a NFP organisation that has a turnover of $700,000. You collect information from homeless youths and provide their contact details to local health services and legal aid centres. The APPs apply to you.

- ✔ You are a theatre company whose turnover is less than $3 million, but enter into a sponsorship deal and, as part of that sponsorship deal; you pass your customer list to the sponsor corporation. The APPs apply to you.

- ✔ You are a NFP organisation that provides childcare services or activities. While you have turnover of less than $3 million per year, you collect, use and store information about children’s allergies, disabilities, medical needs (i.e. health information). The APPs apply to you.

- ✔ You are a subsidiary NFP organisation that has turnover of less than $3 million in Australia. Your NFP organisation is part of a larger global network of NFPs. 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 NFP organisation. The APPs apply to you.

- ✔ You are a NFP organisation that has 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 NFP organisation is required to comply with the APPs under the initial ‘threshold’ criteria, you need to consider if your NFP organisation or particular information you possess falls into one of the categories of exemptions. The main categories of exemptions relevant to NFP organisations are addressed below.

1.2.1 Employee records

If an employer handles information that is directly related to the employee records of a current or former employee, 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 firm.

It is also important to note that State Privacy Laws may still apply to certain employee information notwithstanding the application of the employee records exemption under the Federal Privacy Act. In particular, the Health Records Act applies to private sector organisations, including to NFPs 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 firm. 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 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 possess 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

Government (state or federal) contractors are generally exempt from the APPs where their conduct is in accordance with a government contract, and that contract is inconsistent with the relevant APP.

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 as it is inconsistent with your state government contract.

1.2.4 Political exemption

If you work on behalf of a registered political party, and you do so with their authority, any work you complete for them will be exempt from the APPs where it is in conjunction with:

- an election
- a referendum
- the 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:

- media exemption – this only applies where an organisation adopts other media privacy standards
- journalism exemption, and
- an exemption from some APPs for transfers of information between related organisations.

CAUTION

If your organisation is required to comply with the APPs, but some of the information you deal with might fall into one of the categories of exemptions discussed here, but you’re not sure, you should seek legal advice.

1.3 Information Privacy Principles (Victorian IPPs)

The Victorian IPPs apply to Victorian government agencies (including public sector agencies, local councils, courts, Victoria Police etc.), except where the Health Privacy Principles (HPPs) apply.

The Victorian IPPs may also be imposed on non-government as well as commercial organisations through a contract. This often occurs when an organisation provides services to a Victorian government agency in connection with that agency’s functions, or under a funding agreement with a Victorian government agency. Where the IPPs apply through a contract, your organisation will be responsible for any breaches of the Victorian IPPs.
Do the IPPs apply to my organisation?

X You are a clinic that provides doctors to conduct STI testing at Victorian prisons through a funding agreement with the Department of Health. You are not required to comply with the IPPs as the HPPs apply to your organisation.

✓ You are a legal aid provider that has a funding agreement with the Victorian Government’s Department of Justice which expressly requires you to comply with the IPPs. You are required to comply with the IPPs.

1.4 Exceptions to the Victorian IPPs

The PDPA contains some limited exceptions to the Victorian IPPs. For example, the Commissioner may:

- issue a public interest determination which permits an organisation to depart from a Victorian IPP; or
- certify that a specific act or practice is consistent with a Victorian IPP.

You should seek legal advice to assess whether your organisation qualifies under any of the exceptions before relying on the exceptions or making any applications to the Commissioner.

1.5 Health Privacy Principles (HPPs)

The HPPs apply to Victorian health service providers and to others who handle health information (described in paragraph 1.3 in Part 1 of this Guide). Usually, if the HPPs apply, then the IPPs do not (because the HPPs set a high standard of protection of information).
Do the HPPs 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 HPPs.

✔ You run a safe injection house in St Kilda that takes the names of drop-in patients. You are required to comply with the HPPs.

❌ You provide first aid at music festivals on an anonymous basis. You would not be required to comply with the HPPs.
Part 3 – Obligations under Privacy Laws
Obligations under Privacy Laws

This section covers:

- privacy policies
- obtaining consent
- when you are ‘collecting’ information
- notification of collection
- unsolicited information
- special rules for health information
- storage rules, and
- fundraising and privacy.

If you are in possession of (or want to obtain) information which is considered ‘personal’, ‘sensitive’ or ‘health’ information about an individual, you need to understand the rules that apply.

The APPs are legally binding principles which set the basic standard for privacy protection regarding ‘personal’, ‘sensitive’ or ‘health’ information. They set out requirements about how NFP organisations may collect, use, disclose, and store these types of information.

In summary, the APPs require an organisation to (without limitation):

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 may 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 the offshore location to which 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.
1. When are you ‘collecting’ information

It’s important to remember you must not collect personal information unless that information is reasonably necessary for your organisation’s function or activities. Also, an organisation must not collect ‘sensitive’ or ‘health’ information without the individual’s consent, unless an exception applies. Consent is discussed further at section 3 of this Part 1.

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

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

Many NFP organisations established for cultural, political or religious purposes may collect information from their members that would be considered ‘sensitive’ information (e.g. their race and ethnic background).

1.1 Sensitive information

You must not collect sensitive 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. As a NFP organisation you are entitled to collect sensitive information 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 (i.e. to the activity that is being conducted for a specified purpose).

EXAMPLES OF COLLECTION OF SENSITIVE INFORMATION

- a religious NFP 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
- a community NFP 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 NFP organisation can rely on the exception if the purpose of collecting the ‘sensitive’ information is related to the purposes in the definition of the NFP organisation (e.g. related to the purpose or objects stated in the Constitution of the NFP organisation). An organisation conducting activities for some other purpose can’t rely on this exception.
- A NFP 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 NFP organisation to support its cultural, recreational, political, religious, philosophical, professional, trade or trade union purpose.
- A NFP 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 NFP organisation. Collection of sensitive information about a relative of the member would not be covered unless that person also had regular contact with the NFP organisation.

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’re supposed to collect and how they’re supposed to do it.

1.2 Health information

Generally, you must not collect sensitive (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.

There are some ‘permitted situations’ in which health information can be collected, used, or disclosed without consent. These are listed in our ‘Permitted Situations Quick Reference Table – Health Information’ at the end of this Guide.

TIP

Health information has a number of special protocols that must be followed. If you are in the business of collecting and processing health information, make sure you pay close attention to the lists below!

1.2.1 Special requirements when collecting health information

If you can collect health information via either consent or in one of the Permitted Situations, you must make sure to:

- collect it by lawful and fair means, in an unobtrusive way
- try to collect it only from the individual concerned, and
- inform the individual of the identity of your organisation, as well as the other notification matters listed under section 2 of this Part 1.
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. If this is the case, you must:

- inform the individual that the information was collected; unless
  - it would imperil the individual’s health, or
  - breach confidence.

If the information was given in confidence, you must ensure it:

- will remain confidential
- is recorded only if relevant
- is accurate and not misleading, and
- is marked as confidential.

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:

- your organisation’s identity and contact details
- the fact that your organisation has collected the personal information if you collected the information from a third party or the person is otherwise unaware of the collection of their personal information
- whether the collection of personal information is required or authorised by law or a court/tribunal order (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 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, asking for consent from individuals to use, collect, store or disclose their ‘personal’, ‘sensitive’ or ‘health’ information will generally allow your organisation to deal with that information under the Privacy Laws in any way that is consistent with the consent sought.

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 relying on ‘opt-out’ consents, 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 anything to do with ‘personal’, ‘sensitive’ or ‘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 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. Storing personal information

Your organisation must take reasonable steps to protect the security of the personal, sensitive and health information that it stores.

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 relevant involvement with the organisation.

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 will be accountable for those breaches!

CAUTION – CLOUD BASED STORAGE

CLOUD STORAGE CONTRACT CHECKLIST

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

☐ ensuring any contract you sign with an overseas service provider requires them to comply with the APPs and contains indemnities against Privacy Law breaches

☐ ensuring you understand how a third party provider handles, stores, and deals with data and personal information

☐ ensuring you maintain strong access, security controls and procedures over who has access to your data and what they can do with it, and

☐ ensuring the third party provider understands your obligations under Privacy Laws.
4.1 Special requirements for health information

If your organisation ‘holds’ health information, you have obligations under Victorian Privacy Laws as well as the APPs. You will hold health information if you possess a document (paper or electronic) with that information in it, or if your organisation has control over a document with that information in it.

TIP

It doesn’t matter if the document is situated in Victoria or not, or if you have sole custody of the information. If the information has a connection to your Victorian operations, a Victorian service contract, or a Victorian client, the Victorian Privacy Law requirements may apply.

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.

5. 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.

TIP

This means it’s very important for all staff to be regularly reminded of the primary purpose of your NFP’s collection of personal information. Consider including a ‘mission statement’ or ‘primary objective’ reminder on documents circulated to telemarketers or street side information collectors.

This limitation on use and disclosure remains unless the person specifically consents to its use for another purpose (or a secondary purpose use or disclosure exception applies).

EXAMPLES

- You are a NFP who collects personal information from people interested in receiving news about saving the rainforest in order to include them in your email database. You must not use that information to do anything other than this unless you gain the individual’s specific consent (or an exception applies).
- This often comes up in organisations when personal information is collected to provide a service, and that same information is then later used for fundraising activities.
5.1 Using or disclosing personal information for direct marketing

If your organisation does intend to disclose personal information to other parties – e.g. through a membership sharing agreement with another NFP – for the purposes of direct marketing, there are some important issues for you to consider.

This is allowed where:
- you collected that information from the individual
- the person whose information is disclosed would reasonably expect you to do so
- you provide an easy ‘opt-out’ option for anyone who no longer / does not wish to receive direct marketing, and
- the opt-out option has not been utilised by that person.

You may also use or disclose personal information (other than sensitive or health information) for the purpose of direct marketing if:
- you collected the personal information from a third party, or the individual would not expect you to use or disclose their personal information for the purpose of direct marketing
- either you have the individual’s consent or it is impracticable to obtain that consent
- you provide the individual with a simple opt-out mechanism from direct marketing
- you include a prominent statement in each direct marketing communication that the individual may opt-out if they choose, and
- the individual has not already made such a request.

6. Special requirements for health information

Special rules apply to the use and disclosure of health information.

Health information may only be used or disclosed where the individual in question:
- consents to that use, or
- where the proposed use is for a purpose directly related to the purpose for which the health information was collected and someone would expect the organisation to use the information for that secondary purpose,

or where
- it is reasonably believed by the organisation to be necessary to prevent or lessen a serious and imminent threat to the life, health or safety of an individual or to public health or safety (for example where someone’s address and medical condition details are provided to an ambulance service where there are serious concerns for that person’s wellbeing).
6.1 Extra requirements

- **Data quality:** Your organisation must take reasonable steps to ensure that the personal information your organisation collects, uses, discloses and stores is accurate, complete, relevant and up-to-date.

- **Government identifiers:** There are requirements to limit the use and disclosure of government identifiers (e.g. Medicare number, drivers licence numbers).

- **Correcting personal information:** If an individual can show that the information about him or her that an organisation holds is inaccurate, incomplete, irrelevant or out-of-date, the organisation must:
  - take reasonable steps to correct the information, or
  - if there is disagreement about the accuracy, attach a statement noting that the individual claims the information is incorrect, incomplete, irrelevant or out-of-date.

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 $1.7 million against an organisation for serious or repeated interferences with an individual’s privacy.

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.
If the APPs apply to your organisation, under the Privacy Laws 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 (eg on your website), and, if anyone asks you for it, to give them with a copy (for example by posting it to them).

**Things to include in your 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:**
  - be not 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.** Specific website security technologies can be used to protect personal information and these technologies update regularly.
- **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 NFPs, which you can access on the NFP Law information hub, here.
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 using, collecting or disclosing personal information as part of or in connection with its fundraising activities, you should be aware of the following privacy tips which were developed by the Australian Information Commissioner:

- when collecting personal information from donors, volunteers and clients, provide notice on how their personal information will be handled and used
- if your organisation has information about people and wishes to use it for a new purpose, give them the option of deciding whether or not they wish their information to be used for that purpose
- if you share your donor lists with other organisations, make sure that you provide people with information about who their information will be passed to from the start
- don’t disclose personal information about an individual for a purpose other than the primary purpose that it was collected for
- don’t consider clients as fundraising targets unless they have explicitly opted in to receive such communications
- always offer donors who support fundraising campaigns a choice about receiving information on non-fundraising activities or new campaigns, and
- 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 privacy of client’s personal information.

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 your charity accessing certain Commonwealth tax benefits. As such, although voluntary, most NFPs that are charitable organisations will need to register.
A key concern for private ancillary funds (a subset of NFP) is that individual donors may be identifiable after the registration of your entity on the ACNC Register. This could lead to donors who require anonymity to cease donating or wind up their private ancillary funds. 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 NFP 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 NFP organisations

This section covers:

- privacy compliance tips
- sensitive information ‘Permitted Situation’ Quick Reference, and
- Health Information ‘Permitted Situation’ Quick Reference.

Practical Tips

A NFP organisation may take a number of practical steps to assist them to comply with Privacy Laws. These include:

1. **Privacy Audit** – A NFP 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 NFP organisation implements safeguards to protect personal information, how it manages personal information, including how it manages privacy queries and complaints and how personal information that needs to be updated, destroyed or erased is managed.

2. **Privacy Policy** – Preparing, reviewing and updating the NFP organisation’s privacy policy. While a NFP organisation’s privacy officer should primarily be responsible for co-ordinating and implementing the privacy policy for the NFP organisation, consideration needs to be given to properly develop this policy (or if it has been developed, to have such policy reviewed and updated) to reflect current organisational practices and compliance with current Privacy Laws. Once such privacy policy is developed, it should be regularly reviewed (e.g. annually) for relevance and updated for any changes in law or organisational practice.

3. **Privacy Officer** – A NFP 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.

4. **Review Contracts for Privacy Law Impact** – A NFP organisation may consider reviewing its material contracts for Privacy Law impact and/or obligations. In some situations (e.g. under Government funding contracts), a NFP organisation may be obligated to comply with Privacy Laws even if it would otherwise be considered exempt. In other situations, a NFP 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 or otherwise use, collect, store or disclose personal information of the NFP 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 NFP 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 / data breaches discovered by the organisation and steps that staff should follow.

6. Train staff – A NFP organisation should consider training staff on implementing privacy procedures and your organisation’s privacy policies.

Sensitive information ‘permitted situation’ quick reference

<table>
<thead>
<tr>
<th>Applies to</th>
<th>Permitted Situation</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) Personal information, or (b) a government related identifier.</td>
<td>(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.</td>
</tr>
<tr>
<td>Personal information</td>
<td>(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.</td>
</tr>
<tr>
<td>Personal information</td>
<td>(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 Privacy Law.</td>
</tr>
<tr>
<td>Personal information</td>
<td>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.</td>
</tr>
</tbody>
</table>
**CAUTION – SENSITIVE INFORMATION 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

<table>
<thead>
<tr>
<th>Applies to</th>
<th>Permitted Situation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection of health information</td>
<td>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.</td>
</tr>
<tr>
<td>Collection of health information</td>
<td>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.</td>
</tr>
<tr>
<td>Use or disclosure of health information</td>
<td>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.</td>
</tr>
<tr>
<td>Use of disclosure of genetic information</td>
<td>(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</td>
</tr>
</tbody>
</table>
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 – HEALTH INFORMATION PERMITTED SITUATIONS**

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.
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 information can be obtained from the following sources:

- Commissioner of Privacy and Data Protection: www.dataprotection.vic.gov.au
- The Information and Privacy Commission NSW: www.ipc.nsw.gov.au