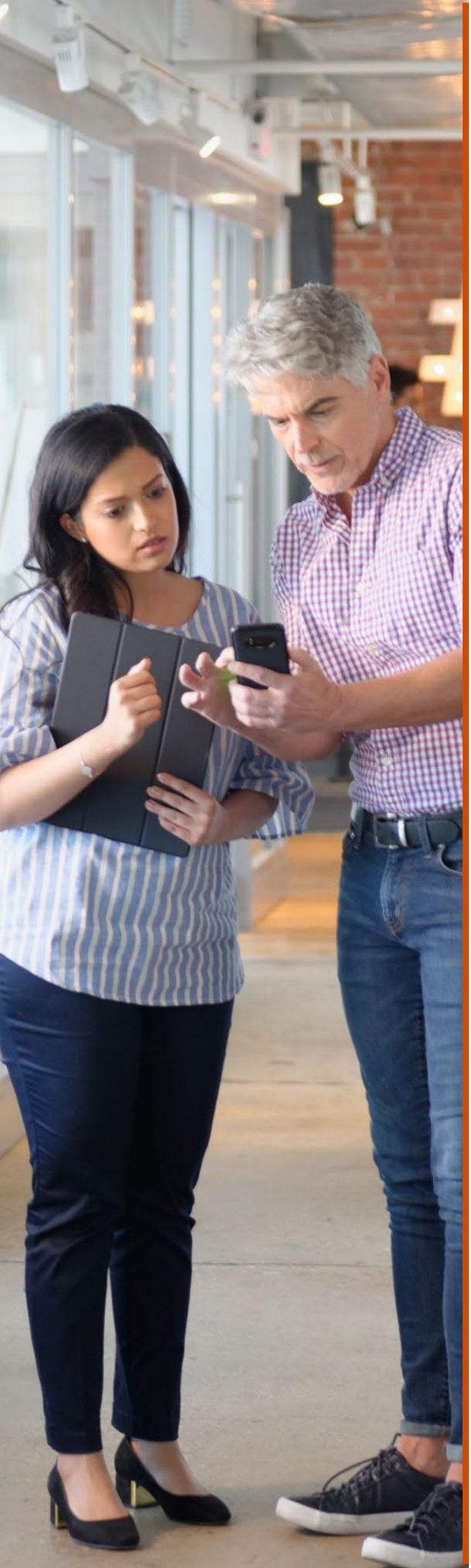
Privacy Guidelines for Not-For-Profits (NFPs)

July 2021

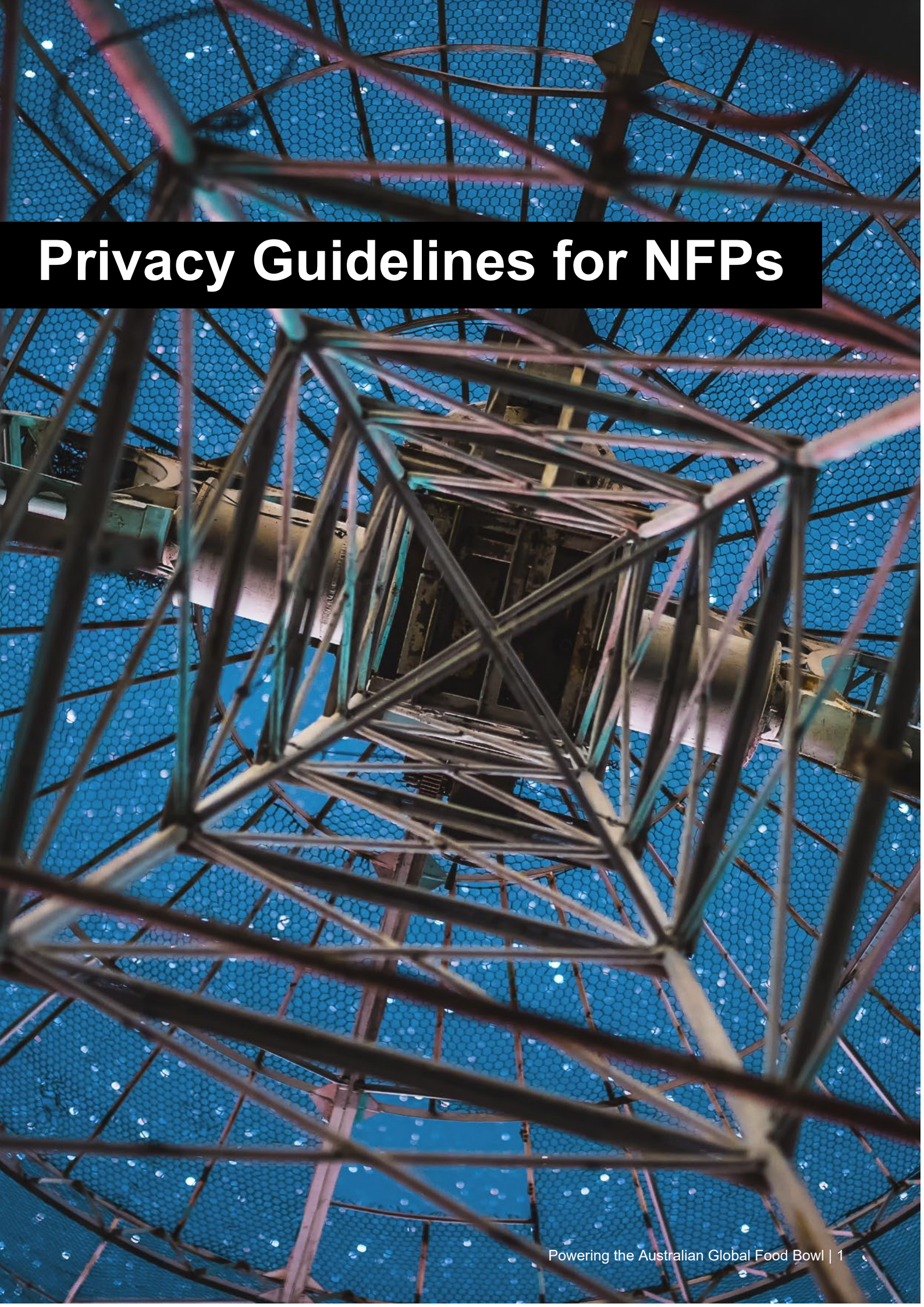
www.pwc.com.au

pwc



Contents

Privacy Guidelines for NFPs



Privacy Guidelines for NFPs

What is personal information?

"Personal information" is any information or an opinion about an identified individual (or an individual who is reasonably identifiable). It can be true or false, recorded or unrecorded. It can be verbal, written or photographic. Typical examples include name, contact and address details, date of birth, health information, financial information, donation records, authentication credentials, identity documents, membership or affiliation with professional, trade, religious or political organisations, device identifiers, or cookie data.

Applicability

A not-for-profit organisation may be governed by the *Privacy Act* and Australian Privacy Principles (APPs). The *Privacy Act* applies to many different types of entities which are applicable to the not-for-profit sector, such as trusts, cooperatives, body corporate and unincorporated associations.

Generally, your organisation must comply with the *Privacy Act* and APPs, if it falls into any of the following categories:

- It has an annual turnover of more than $3 million (e.g. your charity recorded an annual income of more than $3 million in your Annual Report), or
- It provides a health service to a person (even if the service is not an organisation's primary activity; for example, your club has a program to assist members with injuries or improve fitness, especially if you engage a health professional), or
- It trades in personal information (for example, you sell customer lists in exchange for sponsorship benefits or you purchase customer lists), or
- It is a contracted service provider under a Commonwealth contract (e.g. administering Commonwealth-funded community programs, or providing aged care or disability services under a Commonwealth agreement) or
- It has voluntarily opted into the Privacy Act.

An organisation must also comply with the Privacy Act if it is related to a body corporate (for example, a subsidiary or parent organisation) that meets any of the above criteria (for example, even if your not-for-profit organisation itself does not meet any of these criteria, but your parent organisation does and you provide personal information about your members to the parent organisation).

Note: This brochure only covers obligations under the *Privacy Act*. A not-for-profit organisation may also be subject to

- Other state and territory laws covering privacy and health records;
- Contractual information security obligations as part of a funding agreement; or
- Other international regulations for those operating or marketing to other countries and holding personal information of non-Australian residents, e.g., EU General Data Protection Regulation.

Applicability

Once you have determined that your not-for-profit organisation is required to comply with the APPs under the criteria set out above, you should consider whether any exemptions may apply for some of your organisation's activities and data holdings. Some of the key exemption categories that are relevant to not-for-profit organisations are:

- Employee records that are directly related to your employee's current or former employment relationship (note: this exemption does not apply to contractors, volunteers or unsuccessful job applicants)[1];
- If your non-for-profit needs to comply with APPs only because you are a contract with government - you are only required to follow the APPs for personal information that you manage in relation to activities under that contract; or
- If you work on behalf of a registered political party or representative - the part of your work that relates to an election, a referendum, facilitating their participation in the political process will be exempted.

Australian Privacy Principles (APPs) Overview

The APPs are 13 legally binding principles which set out the basic requirements governing how an organisation may collect, use, disclose and store personal information. The APPs require organisations to:

- Have a clearly expressed and up-to-date privacy policy that explains how the organisation collects, uses, handles and discloses personal information, and which explains how individuals may raise a complaint or request access or amendment of their information (**APP 1**).
- When collecting personal information:
  - Only collect personal information reasonably necessary for your organisation's functions or activities (**APP 3**);
  - Only collect personal information by "lawful and fair means" - for example, if your organisation's representatives approach people directly on the street, make sure your street representatives don't trick someone into revealing their personal information; if you collect personal information indirectly, such as through web browsing analytics, ensure individuals are informed of the collection activities and have an opportunity to opt-out (**APP 3**);
  - Collect personal information directly from the person it belongs to wherever possible, unless it's impossible or not practical to do this (**APP 3**);
  - Ensure that express consent is obtained from individuals whenever sensitive categories of personal information are collected (**APP 3**). Sensitive categories of personal information are defined as information about an individual's racial or ethnic origin, political opinions, membership of political associations, religious beliefs and affiliations, philosophical beliefs, membership of professional and trade associations, membership of trade unions, sexual orientation or practices, criminal records, health information, genetic information or biometric information;

[1] State or territory privacy laws may still apply to certain employee information notwithstanding this exemption. In particular, some health privacy laws may apply to not-for-profits that handle health information, including employee's health information.

Australian Privacy Principles (APPs) Overview

  - Give individuals the option of remaining anonymous or using a pseudonym, unless this is not practical, or your organisation has to deal with an identified person (**APP 2**);
  - Tell individuals what purposes your organisation will use their personal information for (**APP 5**); and
  - Deal with unsolicited information in a way that complies with **APP 4**.
- When 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**).
- Using or disclosing personal information:
  - Unless an exception applies, you must not use or disclose personal information you have collected for any other reason other than the primary purpose you collected it for (**APP 6**). Exceptions permitted under APP 6 include where you use the information for a related secondary purpose and i) you have obtained consent, or ii) the individual reasonably expects you to use or disclose their information for such secondary purpose, iii) or you are required to disclose such information by law.
- Your organisation must take reasonable steps to ensure the personal information it collects, uses or discloses is accurate, up to date and complete. It must also be relevant to the purposes for which it's being used or disclosed (**APP 10**).
- Direct marketing (**APP 7**) is communicating with a person to promote goods and services, including fundraising. If your organisation uses or discloses personal information for the purposes of direct marketing, make sure it complies with the criteria outline in APP 7, including managing withdrawal of consent to receive communications. Your organisation should also ensure it can meet marketing communication obligations under the *Spam Act* and *Do Not Call Register Act*.
- If a person asks for access to or correction of their own personal information held by your organisation, you are generally required to give access in the way the person has requested. You should respond to the request in a reasonable period, generally interpreted as within 30 days (**APP 12** and **APP 13**).
- Before you disclose personal information to an overseas recipient, you must take reasonable steps to ensure the overseas recipient does not breach the APPs **(APP 8)**.

Notifiable Data Breach Scheme

The Notifiable Data Breaches (NDB) scheme requires an organisation subject to the Privacy Act to report certain types of data breach to the OAIC (Office of the Australian Information Commissioner) and to provide notification to individuals impacted by the breach.

A data breach will be covered by the mandatory notification process if:

1. There is unauthorised access to or disclosure of personal information (or loss of that data in circumstances where unauthorised access or disclosure are likely), and
2. Which is likely to result in serious harm to one or more individuals, and
3. The organisation has not been able to prevent the likelihood of serious harm occurring.

OAIC recommends that organisations follow a four-step process in response to a data breach — contain, assess, notify, and review.

- **Contain** – Take action to limit the breach and preserve forensic evidence where possible.
- **Assess** – Capture key facts of the breach and assess the likelihood of serious harm to individuals and reporting requirements.
- **Notify** – Provide notification to affected individuals and prepare a statement to the OAIC.
- **Review** – Complete a post incident review and decide if additional protections are required.

Refer to the OAIC's *Data Breach Preparation and Response Guide* online for detailed guidance.

Australian Not-for-profit Organisation Breaches

The OAIC received just over 1,000 data breach notifications in 2020 (see OAIC's *Notifiable Data Breaches Report* for periods Jan-June 2020 and Jul-Dec 2020). The sector reporting the highest number of breaches was the health services sector, accounting for just over a fifth of all reported breaches. Although the OAIC does not report statistics directly addressing the not for profit sector, a number of high profile breach examples have emerged in recent years.

Large health focused non-profit, 2017	Large international non-profit, 2021	State-based health and community sector non-profit, 2018
In October 2017, the personal details of over half a million individuals were leaked from a large health-focused organisation. A service provider's oversight led to the sensitive files of individuals being placed on an unsecured web server which was then accessed by an unauthorised person. Lost data included highly sensitive medical screening data including sexual practices and sexually transmitted disease history.	In addition to human errors, not-for-profits are also a target for malicious acts. In February 2021, a large charity focused on supporting international poverty-stricken communities suffered a cyber-attack which resulted in unauthorised access to the details of 1.8 million individuals. The data leak was posted for sale on a hacker forum on the dark web.	In 2018, a cyber-attack on a state-based non-profit exposed the personal information of up to 8000 clients, including those seeking help about highly sensitive health services.

Good practices to manage privacy in your organisation

Not-For-Profit organisations should consider adopting the following good practices to improve their management of privacy risks and help them to meet compliance obligations.

Privacy impact assessments

- A privacy impact assessment helps identify the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. It facilitates a privacy-by-design approach.

01

Privacy management plan

- A privacy management plan sets out specific, measurable goals and targets that identify how you will implement a privacy management framework. It provides an operational guideline for embedding and establishing privacy processes in your organisation. It will help you evaluate your privacy process and enhance your response to privacy issues.

02

Appoint a privacy officer

- A not-for-profit organisation may appoint a person as their privacy officer to be responsible for developing, implementing and updating its privacy policy, and to be the first point of contact for privacy issues or complaints.

03

Data management

- Having a defined process of storing, organising and maintaining data, including replying to an individual's request to access and correct data, mapping the source and destination of data, will help mitigate privacy risks.

04

Controls Assurance

- You may also consider conducting controls assurance (through internal audits or reviews) to understand what kind of personal information you possess, what kind of risks exist with respect to this information and the efficacy of the measures you have in place to protect that information.

05

Data breach response plan

- Have a written, tested and rehearsed plan and supporting playbooks that sets out how your organisation responds to a suspected breach will help you comply with laws and mitigate damage.

06