Notifiable Data Breaches scheme

Legal information for not-for-profit community organisations

This fact sheet covers:

- what is the notifiable data breaches scheme?
- whether the notifiable data breaches scheme applies to your organisation
- how to identify which data breaches should be notified
- what to do if your organisation suspects a data breach
- how to notify when there is an eligible data breach
- what are the penalties of not complying with the scheme, and
- how the scheme works when more than one organisation shares personal information

This fact sheet is a supplement to our privacy guide and is for not-for-profit organisations in Australia who want to understand more about their obligations under the notifiable data breaches scheme.

Note

This fact sheet provides information on the notifiable data breaches scheme and how it might apply to not-for profits. This information is intended as a guide only and is not legal advice. If you or your organisation has a specific legal issue or are unsure if the scheme applies to you, you should seek legal advice before making a decision about what to do.

Please refer to the full disclaimer that applies to this fact sheet.

As described in our privacy guide, many not-for-profit organisations collect, use and store disclosure information about people they interact with including employees. This information is often classified as 'personal information' under privacy laws.

If there has been unauthorised access, disclosure or loss of that personal information, the organisation which holds it is required, in certain circumstances, to notify both the Office of the Australian Information Commissioner (**OAIC**) and affected people.

This fact sheet explains your organisation's obligations if there is a data breach and how to comply with the notifiable data breaches scheme.

© 2021 Justice Connect. This information was last updated in December 2021 and is not legal advice; full disclaimer and copyright notice at www.nfplaw.org.au/disclaimer.

What is the notifiable data breaches scheme?

Since the introduction of the Australian Privacy Principles under the *Privacy Act 1988* (Cth) (**Privacy Act**), organisations must take all reasonable steps to prevent the loss, unauthorised access, modification or disclosure of personal information it holds.

The introduction of the notifiable data breaches scheme under the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) (**NDB scheme**), creates a requirement for organisations who discover a data breach that is likely to cause serious harm, to notify the OAIC and affected people.

Only certain organisations are subject to the NDB scheme and only certain data breaches require notification. We discuss these concepts further in this fact sheet.

Organisations that must notify eligible breaches

The NDB scheme applies to agencies and organisations which have existing obligations under APP 11 of the Privacy Act. These organisations are known as 'APP entities' and will be referred to as APP organisations in this fact sheet.

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

We set out below how to determine whether your organisation is covered by the Privacy Act, however you can find more detailed information to help you consider this in our privacy guide.

As a general rule, organisations subject to the NDB scheme include:

1. **Organisations which are subject to the Privacy Act**

   Organisations which are subject to the Privacy Act generally include:

   - businesses and not-for profit organisations with a turnover of more than $3 million per financial year
   - Australian Government agencies, and
   - certain organisations with a turnover of less than $3 million per financial year, including:
     - private sector health services
     - credit reporting bodies
     - credit providers
     - organisations contracted by the Commonwealth government to provide services
     - organisations that trade in personal information

2. **Organisations which hold TFNs**

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

Caution

Determining whether the Privacy Act (and therefore the NDB scheme) applies to your organisation can be difficult. A number of the relevant considerations and exceptions are not contained in this factsheet. Please refer to our privacy guide for further guidance to determine whether your organisation is an 'APP organisation'.

What kind of data breaches require notification?

An organisation must notify under the NDB scheme if it experiences (or has reasonable grounds to believe that it has experienced) a data breach in which:

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

Note

Personal information has a special meaning in the Privacy Act. For more information on what may be considered personal information and therefore subject to the NDB scheme, please see our privacy guide.

This is described as an **eligible data breach**. An eligible data breach is one where unauthorised access, disclosure or loss of personal information occurred on or after 22 February 2018.

These points are discussed in more detail below.

For organisations who are not subject to the Privacy Act but are TFN recipients (see above), an eligible data breach occurs to the extent that TFN information is involved in the breach. For such organisations, if the unauthorised access, unauthorised disclosure or loss of information does not include TFN information then this is unlikely to be an eligible data breach and further steps may not be necessary as part of the NDB scheme. You may still want to consider further steps and seeking legal advice if your organisation discovers that TFN information, further data or other information it held has been compromised.

Note

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

What is unauthorised access, disclosure or loss

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

Example

Sandra is a volunteer at a not-for-profit which provides support to LGBTI people and is an APP organisation. The organisation retains basic information about people who have used its services such as names, addresses and telephone numbers. It restricts access to this database to certain employees only. Sandra is curious as to whether one of her friends might be LGBTI and searches the organisation's private records and finds her friend. **This is unauthorised access.**

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

Example 1

Michael works for a large not-for-profit which provides financial assistance to Australian military veterans' families during times of crisis. Michael fields a call from a journalist asking for information in regards to a tip-off about a celebrity who has been scamming the organisation. Michael confirms the celebrity is one of his clients but refuses to provide any information about the file. Instead, Michael provides the journalist with the celebrity's contact details contained on the system. **This is unauthorised disclosure.**

Example 2

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

Example 3

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

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

Example

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

Exceptions may apply if the personal information which has been lost is unlikely to be able to be accessed or disclosed (more on this below).

When are data breaches likely to result in serious harm?

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

There is no special definition given to the phrase 'likely to result in serious harm' and it simply means that the risk of serious harm to a person is more probable than not. Whether or not the data breach is likely to result in serious harm is assessed from the perspective of a reasonable person in the organisation's position, who has been properly informed based on either the information immediately available or information that could be obtained following reasonable inquiries.

Serious harm could include:

- physical harm
- psychological harm
- emotional harm
- financial harm
- reputational harm

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

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

Organisations should assess the risk holistically, having regard to the consequences for the people whose personal information were part of the data breach and the likelihood of harm occurring.

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

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

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

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

- **How many people are involved?**

  The more people affected by a breach, the greater the likelihood that one or more of them will experience serious harm. If the breach involves a very large number of people, organisations should assume the serious harm threshold is met unless the specific circumstances do not support that conclusion.

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

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

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

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

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

  The length of time between a data breach and an organisation's discovery of the data breach is another consideration. The longer this period of time is, the greater the likelihood that the information has been misused or accessed in a way that will cause serious harm.

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

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

  Organisations should consider who is or may be the recipient of the personal information. If, for example, the data breach appears to target specific information about a person, there is a greater potential the information is going to be used for malicious purposes and therefore a higher likelihood that serious harms will result.

Exception – remedial action

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

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

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

Example 1

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

Example 2

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

Assessing suspected data breaches

When should an assessment take place?

If an organisation is aware that there are reasonable grounds to suspect there may have been a data breach, the organisation must quickly assess the situation to determine whether or not the breach is an eligible breach.

How long can an assessment take?

The assessment of the suspected data breach must be prompt and occur no later than 30 calendar days from the date of suspicion. The organisation should not unreasonably delay its investigations, for instance, by waiting for board approval or executive discussion. The 30 days should be treated as a maximum period of time and organisations should aim for as short a time frame as possible.

An organisation should ensure that it can explain that it has taken reasonable steps to conduct an assessment within the timeframe expected by the OAIC. In the event that an organisation can't complete an assessment within 30 calendar days, it's prudent to document the reasons why.

How is an assessment done?

There are no specific legal requirements of the steps an organisation must take in relation to an assessment. However, the guidance from the OAIC suggests a 3 stage process:

1. • **Initiate** – identify the person or group responsible for completing the assessment
2. • **Investigate** – gather all the relevant information about the data breach. For example, ask 'Can we employ any remedial action?', 'What personal information has been affected?', 'Who may have had access to it?', 'What are the likely impacts?'
3. • **Evaluate** – the person or group needs to make a decision as to whether it is a notifiable data breach. This decision should be well documented, including the reasons why that decision was reached.

Data breach response plan

The OAIC expects organisations to have practices, procedures, and systems in place to comply with their information security obligations under APP 11, enabling suspected breaches to be promptly identified, reported to relevant personnel, and assessed if necessary. A data breach response plan is a document that clearly sets out the steps to take and the people responsible for responding to a suspected or actual data breach.

Related resource

The OAIC has published a guide 'Data breach preparation and response' — this is a guide to managing data breaches in accordance with the Privacy Act 1988.

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

Notification

Who, what and how does notification occur?

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

1. **Contain** the breach in so far as it is possible.
2. **Prepare a notification statement** that contains: the identity and contact details of the organisation, a description of the data breach, the kinds of information affected, and recommendations for affected people.
3. **File the notification statement** with the OAIC via the online form or contact the OAIC (enquiries line on 1300 363 992) to make alternative arrangements.
4. Quickly **notify people** at likely risk of serious harm.

A notification statement is published on the OAIC website.

Preparing the notification statement

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

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

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

☐ **A description of the data breach**

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

This type of information may include:

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

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

☐ **The kind of information compromised**

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

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

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

Recommendations should reflect the circumstances of the breach and the kind of information compromised. For example, if credit card details have been compromised, recommending that people contact their financial institutions to cancel those cards and be issued with new ones. If an organisation is unaware of what advice to provide, it should seek assistance from specialists when preparing this section. In limited circumstances and only after following consultation with a specialist, the advice may be that no steps are required.

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

Related resource

You can notify the OAIC of an eligible data breach using their online form.

Notifying people

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

When the organisation is deciding which method or combination of methods to undertake it can consider the cost, time and effort it will have to spend, in light of the particular circumstances and capacities of the organisation. The OAIC has an expectation that notification occurs expeditiously in all circumstances unless cost, time and effort are excessively prohibitive.

The NDB scheme provides **3 options** for notifying individuals at risk of serious harm set out below.

Option 1 – notify all individuals

If an organisation considers that the data breach will result in serious harm to one or more people but can't assess which people are at risk, it should notify all affected people.

An organisation can use any method or combination of methods to notify a person (see the tip below), as long as it has taken all reasonable steps. The organisation should assess the likelihood that the affected people to be notified will become aware of and understand the notification and weigh this against the resources involved in undertaking the notification.

Tip

Some examples for possible methods of notification include telephone call, SMS, post, in-person meeting, social media post, newspaper advertisement, or email.

Organisations can also notify people through their usual method of communication, which may be an intermediary if applicable.

Option 2 – only notify people at risk of serious harm

An organisation must take all reasonable steps in the circumstances to notify affected people. If the organisation can identify which specific people are at risk of serious harm, it has the option of only notifying those people.

Notifying only people at risk of serious harm has the additional benefit of reduced costs and decreased notification fatigue among members of the public. The organisation should be confident however that it is able to identify all affected people.

Example

A website compromised for two days allowed a hacker to obtain all information, including credit card information, entered into the website during the two days. Following a comprehensive risk assessment, the organisation considers that only customers which logged into their account within those two days are at serious risk and no other personal information has been accessed. The organisation is only required to notify those people that logged in during the time the website was compromised, being the people it considers to be at likely risk of serious harm.

Option 3 – publish notification

This option is only available if it's not practicable for the organisation to complete the notifications described above. In that scenario, the organisation must publish a copy of the statement provided to the OAIC (discussed earlier in this fact sheet) on its website (if it has one), other or further digital outlets as appropriate and take reasonable steps to publicise the contents of the statement.

The notification should be clearly displayed in a prominent location on the organisation's website with the ability to be caught by search engines. An alternative to this method suggested by the OAIC is to take out a print or online advertisement in a publication or on a website the organisation considers reasonably likely to reach people at risk of serious harm. The purpose of the notification is to relay the information to as many affected people as possible.

Note

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

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

Penalties for not complying

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

Power	Example
Applying to a court for a civil penalty order for a breach of a civil provision	Court can order a civil penalty of up to **$2.1 million** if the failure to notify is a serious or repeated interference with the privacy of individuals
Accept an enforceable undertaking and bring proceedings to enforce a determination	Organisation agrees to apologise and to implement a compliance program in lieu of other civil action. OAIC can go to Court to enforce that undertaking.
Direct an organisation prepare a notification statement and notify as soon as practicable	If the OAIC finds out about a data breach externally it can direct an organisation to comply with the NDB Scheme

Seek an injunction to prevent ongoing activity or a recurrence	Apply to the Court for an order preventing an organisation from running a website whilst it is compromised or until adequate security measures are in place

Caution

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

Note

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

Example

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

Data breaches involving more than one organisation

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

Common examples where two or more organisations may share the same person information include: IT vendor agreements, outsourcing agreements, commonwealth contracts, and joint ventures or shared service agreement.

Responding to data breaches of jointly held information

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

If one entity has assessed the suspected breach, the other entities are not also required to do so, but this doesn't mean the other organisations can't make their own assessments. Even if organisations determine that another entity is or will appropriately execute the reporting requirements to the OAIC and individuals affected, they should secure a written statement from the reporting organisation regarding the eligible data breach.

Only one organisation is required to prepare a statement for the OAIC and notify individuals. That organisation may, if it decides to do so, include details as to the identity, contact details and information regarding the relationship with the other organisations in the statement and information provided to the OAIC and affected individuals. This will depend on the circumstances, the relationships between the entities

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

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

In general, compliance by one entity will also be taken as compliance by each of the relevant entities. As a general principle the OAIC suggests that the entity with the most direct relationship with the individuals affected should action the notification.

Who has responsibility for compliance (and costs)

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

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

Note – organisations without physical or electronic copies of personal information

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

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

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

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

Resources

Not-for-profit Law resources

- Privacy Guide

  This guide looks at privacy laws more generally and includes detailed information about the Privacy Act and state privacy laws in Australia and explains the obligations an organisation has under these laws.
- The People Involved

  This page includes specific matters to address before setting up a not-for-profit organisation.

Related resources

- OAIC Data breach preparation and response- A Guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)

  This guide aims to assist you in developing and implementing an effective data breach response.
- OAIC Guide to securing personal information

  Provides guidance on the reasonable steps entities are required to take under the Privacy Act to protect the personal information they hold. It also includes guidance on the reasonable steps entities are required to take to destroy or de-identify personal information that they hold once it is no longer needed (unless an exception applies).
- OAIC What to do after a data breach notification

  This information is targeted at individuals who receive a data breach notification and what they should do to protect themselves. It includes links to support services available.
- OAIC Business resources

  The OAIC has developed a range of resources for organisations including guidelines and top tips to guide you in complying with the Privacy Act.
- OAIC Quarterly Reports on the Notifiable Data Breach Scheme

  For information on trends in the scheme and common pitfalls.

Legislation

- *Privacy Act 1988*
- *Privacy Amendment (Notifiable Data Breaches) Act 2017*