# 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 the Privacy Guide. It is for not-for-profit organisations in Australia who want to understand more about their obligations under the notifiable data breaches scheme.**

As described in our Privacy Guide, many not-for-profit organisations will collect, use and/or store disclosure information about individuals they interact with. 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 now required, in certain circumstances, to notify both the Office of the Australian Information Commissioner (**OAIC**) and affected individuals.

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

## 1. What is the notifiable data breaches scheme?

Since the introduction of the Australian Privacy Principles under the *Privacy Act 1988* (Cth), 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* (**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 individuals. 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.

# 2. 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 organisations'. 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 available at www.nfplaw.org.au/privacy.

As a general rule, organisations subject to the Privacy Act include:

a) businesses and not-for profit organisations with a turnover of *more* than $3 million per financial year

b) Australian Government agencies, and

c) certain organisations with a turnover of *l*ess 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, and
- organisations which hold tax file numbers.

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 fact sheet. Please refer to our Privacy Guide at www.nfplaw.org.au/privacy for further guidance to determine whether your organisaition is an 'APP organisation'.

# 3. 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, and
- the data breach is *likely to result in serious harm* to one or more individuals affected.

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.

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.

## 3.1 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 individuals and is an APP organisation. The organisation retains basic information about individuals which 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.

EXAMPLE

Michael works for a 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 regard 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.**

**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 decides she wants to do some work on files over the weekend. She downloads a number of documents which contain personal information of clients 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 loss of personal 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).

## 3.2 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 an individual 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.

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<br>Driver licence<br>Credit card information<br>Multiple types of personal information |
| Whether the information is protected by one or more security measures & the likelihood those measures could be overcome | Reputable encryption by software | No encryption<br>Standard windows password |
| 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<br>Access by hackers |
| The nature of the harm | Information previously available publically | Identity theft<br>Financial loss<br>Physical safety<br>Reputational damage<br>Humiliation |

Organisations should assess the risk holisitically, having regard to the consequences for the individuals 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'.

**More things to consider when deciding whether the breach will 'likely result in serious harm':**

- **Which individuals 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 persons. 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 individuals 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 individuals affected:** organisations should consider what kind of information can be determined by the data breach. If it links an individual with a sensitive product or service, such as for example HIV treatment, it will increase the risk that serious harm has occurred.
- **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 is unlikely there is an eligible data breach.
- **How long ago the breach occurred:** 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.
- **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 an individual, 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.

## 3.3 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 individuals within a larger group of individuals whose personal information has been compromised, the organisation still needs to notify the affected individuals who will likely experience serious harm.

EXAMPLE

Whilst 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.

# 4. Assessing suspected data breaches

## 4.1 Assessing whether there has been a reportable data breach

### 4.1.1 When should an assessment take place

If an organisation only ***suspects*** that it has experienced an eligible data breach (as opposed to having reasonable grounds to *believe* it has experienced an eligible data breach, in which case it skips to the notification stage), the organisation must quickly assess the situation to determine whether or not the breach is reportable.

### 4.1.2 How long can an assessment take

The assessment of the suspected data breach must be prompt, but 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 cannot complete an assessment within 30 calendar days, it is prudent to document the reasons why.

### 4.1.3 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:
    - 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.

## 4.2 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 data breach.

The OAIC has produced a guide called *Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth).* The guide includes information about preparing a data breach response plan, assessing a suspected notifiable data breach and responding to a data breach. It is available at http://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response.

# 5. Notification

## 5.1 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 it is possible
2. prepare a notification statement that contains:
   a) the identity and contact details of the organisation
   b) a description of the data breach
   c) the kinds of information affected, and
   d) recommendations for affected individuals.
3. provide a copy of the notification statement to the OAIC via the online portal (www.oaic.gov.au/NDBform) or contact the OAIC enquiries line on 1300 363 992 to make alternative arrangements, and
4. quickly notify individuals at likely risk of serious harm.

**RELATED RESOURCES**

The OAIC has produced a flowchart on what organisations need to do if they suspect or know a data breach has occurred.

### 5.1.1 Preparing the notification statement

An organisation is free to customise its notification statement so 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 (e.g. a trading name), the organisation should use the name most recognisable to

the individuals 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 individuals 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 date(s) 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" unless the organisation may have some relevance to the individual, for example, their current employer), and
- relevant information the organisation has taken to contain or remediate the breach.

**The kind of information compromised**. The statement should include the type of personal information which likely has been accessed, for example, individuals' 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 individuals take**. The organisation must make recommendations as to what the individuals 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 individuals 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.

**RELATED RESOURCES**

The OAIC has published a guide on *What to include in an eligible data breach statement*. You can notify the OAIC of an eligible data breach using their online form.

**Organisations must ensure that they do not disclose personal information about any affected individual in the process of notification.**

### 5.1.2 Notifying individuals

The NDB scheme requires organisations to notify individuals as soon as practicable after completing the statement prepared for notifying the OAIC. If the organisation wishes, it can notify the individuals before or at the same time as the OAIC, so long as it contains all the required information.

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. 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.

1. **Notify all individuals**

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

An organisation can use any method or combination of methods to notify an individual (see Tip below), so long as it has taken all reasonable steps. The organisation should assess the likelihood that the affected individuals 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 individuals through their usual method of communication, which may be an intermediary if applicable.

### 2. Notify only individuals at risk of serious harm

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

Notifying only individuals 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 individuals.

EXAMPLE

A website compromised for 2 days allowed a hacker to obtain all information, including credit card information, entered into the website during the 2 days. Following a comprehensive risk assessment, the organisation considers that only customers which logged into their account within those 2 days are at serious risk and no other personal information has been accessed. The organisation is only required to notify those individuals that logged in during the time the website was compromised, being the individuals it considers to be at likely risk of serious harm.

### 3. Publish notification

This option is only available if it is not practicable for the organisation to complete the notifications described above. In that scenario, the organisation must publish a copy of the statement to the OAIC (discussed earlier in this factsheet), on its website (if it has one) and take reasonable steps to publicise the contents of the statement.

The notification should be clearly displayed in a prominent location the organisation's website with the ability to be caught be 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 individuals at risk of serious harm.The purpose of the notification is to relay the information to as many affected individuals as possible.

NOTE

As the organisation is required to take 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.

The Privacy Act does not specify a time for which the statement must remain publically available though the OAIC has provided some guidance that it expects the publication to exist for at least 6 months.

# 6. 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.

# 7. 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.

## 7.1 Responding to data breaches of jointly held information

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

Similarly, only one organisation is required to notify the OAIC. The organisation is responsible for deciding who is responsible for notification is up to the organisations to decide. If none of the organisations notify, then each organisation may be found to have breached the requirements of the NDB scheme.

## 7.2 Who has responsibility for compliance (and costs)

The NDB scheme does not provide any specification as to which organisation is required to conduct the assessment or notify individuals and the OAIC about an eligible breach. It is 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 before entering into arrangements in which personal information is jointly held. Whilst not a legal requirement, the OAIC has suggested that the organisation with the most *direct* relationship with the individuals at risk of serious harm may be best placed to notify.

**Organisations without physical or electronic copies of personal information**

Data breach notification obligations apply to an organisation that ***holds*** the personal information.

An organisation ***holds*** personal information if the organisation has ***possession or control of a record*** that contains the personal information.

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 to notify any eligible breach under the NDB scheme.

# Resources

## Related Not-for-profit Law Resources

- Privacy Guide – www.nfplaw.org.au/privacy

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.

- People Involved - www.nfplaw.org.au/people

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

## Related Resources

- OAIC Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) - www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

This guide aims to assist you in developing and implementing an effective data breach response.

- OAIC Guide to securing personal information - www.oaic.gov.au/agencies-and-organisations/guides/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 - www.oaic.gov.au/individuals/data-breach-guidance/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 FAQs for agencies & organisations - www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/all/

Answers to common questions faced by businesses and organisations, start-ups, and health service providers.

- OAIC Business resources - www.oaic.gov.au/agencies-and-organisations/business-resources/

The OAIC has developed a range of resources for organisations including checklists, guidelines, flowcharts and top tips to guide you in complying with the Privacy Act.

## Legislation

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

A Not-for-profit Law Information Hub resource. Access more resources at www.nfplaw.org.au. Justice Connect Not-for-profit Law acknowledges the generous support of our funders and supporters. Find out more at www.nfplaw.org.au