Notifiable Data Breaches scheme

Legal information for not-for-profit community organisations

This fact sheet covers:

- what is the Notifiable Data Breaches scheme?
- what organisations must comply with the scheme?
- what kind of data breaches require notification?
- the process for responding to data breaches
- notification when there is an eligible data breach
- penalties for not complying with the scheme

This fact sheet supplements our privacy guide and is for not-for-profit organisations in Australia who want to understand their obligations under the Notifiable Data Breaches scheme.

Disclaimer

This fact sheet provides information on the Notifiable Data Breaches scheme and how it might apply to not-for profit organisations. 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 deciding what to do.

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

Regardless of the industry your organisation operates in, your organisation probably collects and stores a significant amount of information and uses many kinds of technology in its daily operations. **It is extremely important to ensure that your organisation is taking steps to protect and secure that personal information.**

In certain circumstances, where serious harm is likely to occur – if there has been unauthorised access, disclosure or loss of personal information, the organisation which holds the information is required to notify both the Office of the Australian Information Commissioner (**OAIC**) and people affected.

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

Read this fact sheet in conjunction with our privacy guide, which outlines the sources of privacy laws and obligations under privacy laws, and our fact sheet on cybersecurity (a data breach response will often incorporate cybersecurity measures)

Note – data breaches are a significant part of the evolving privacy landscape in Australia

The Office of the Australian Information Commissioner's (**OAIC**) Australian Community Attitudes to Privacy Survey 2023 found that almost half of Australians reported their personal information had been involved in a data breach. Australians value organisations who take proactive and quick reactive actions to protect customers from harm. If your organisation doesn't respond to data breaches in a way that is consistent with community and regulatory expectations, this can cause significant damage to the organisation from a legal, financial, and reputational perspective.

The Notifiable Data Breach Scheme is a mature regime and OAIC expects organisations have strong practices to protect personal information as well as processes to ensure timely response to data breaches.

The OAIC publishes a biannual Notifiable Data Breaches Report. Refer to these reports for helpful insights on the evolving risks.

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.

Under the Notifiable Data Breaches (**NDB**) scheme, any organisation or agency covered by the Privacy Act must notify the OAIC and affected individuals when a data breach is likely to result in serious harm to an individual whose personal information is involved.

Only certain organisations are subject to the NDB scheme and only certain data breaches require notification.

What organisations must comply with the scheme?

The NDB scheme applies to organisations which have obligations under Australian Privacy Principle (**APP**) 11 of the Privacy Act. These organisations are known as 'APP entities' and we refer to them 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.

Organisations subject to the NDB scheme include:

- **Organisations which are subject to the Privacy Act**

  This includes 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.

  Organisations with a turnover of less than $3 million per financial year that are subject to the NDB scheme include:

- organisations who hold health information and provide a health service (which may include not-for-profit organisations)
- employee associations registered under the *Fair Work (Registered Organisations) Act 2009* (Cth)
- organisations reporting under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (Cth)
- organisations that hold accreditation for the *Consumer Data Right system under the Competition and Consumer Act 2010* (Cth)
- organisations that have voluntarily opted in for APP coverage
- credit reporting bodies
- credit providers
- organisations contracted by the Commonwealth government to provide services, and organisations that trade in personal information

- **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. Some of the relevant considerations and exceptions are not included in this fact sheet. Refer to our privacy guide for further guidance on whether your organisation is an 'APP organisation'.

If your organisation is required to comply with privacy law, has a privacy policy, or both these things apply, refer to the Office of the Australian Information Commissioner (**OAIC**) website which has published guides to privacy obligations and dealing with data breaches.

The Australian Signals Directorate's Australian Cyber Security Centre website also contains resources to help your organisation manage cybersecurity.

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.

What kind of data breaches require notification?

Under the NDB scheme an organisation must notify affected individuals and the OAIC if it experiences (or has reasonable grounds to believe that it has experienced) an **eligible data breach**.

An eligible data breach occurs if:

- 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 broad definition which includes information or an opinion about an identified individual, or an individual who is reasonably identifiable.

For more information on what may be considered personal information and therefore subject to the NDB scheme, see our privacy guide.

The NDB scheme applies to breaches that occurred on or after 22 February 2018.

For organisations who are not APP organisations but are TFN recipients (see above), an eligible data breach occurs to the extent that TFN information is involved in the breach.

For TFN recipients – if the unauthorised access, unauthorised disclosure, or loss of information does not include TFN information, this is unlikely to be an eligible data breach and further steps may not be necessary as part of the NDB scheme.

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.

If your organisation discovers that TFN information, further data or other information it held has been compromised, consider further steps and seek legal advice.

Even where a TFN recipient's data breach does not include TFN information, given community expectations around the handling of personal information, the organisation may want to consider notifying affected individuals where a breach is likely to result in serious harm.

What is unauthorised access, disclosure or loss?

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

Example – unauthorised access

Sandra is a volunteer at an APP organisation which provides support to LGBTI people. 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 about 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.

Examples – unauthorised disclosure

Example 1 – Michael works for a large not-for-profit organisation which provides financial assistance to Australian military veterans' families. Michael fields a call from a journalist asking for information in response to a tip-off that a celebrity has been scamming the organisation. Michael confirms the celebrity is a client of the organisation and provides the journalist with the celebrity's contact details from the organisation's records. 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 – loss

Anthea is working over the weekend. She downloads 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.

The process for responding to data breaches

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.

See the OAIC's guide to managing data breaches in accordance with the Privacy Act – 'Data breach preparation and response'.

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

The OAIC states that effective data breach responses generally follow a four step process:

step 1	• **Contain** the breach to prevent any further compromise of personal information
step 2	• **Assess** the risk of serious harms associated with the breach, and where possible, take action to remediate any risk of harm
step 3	• **Notify** affected individuals and the OAIC if required
step 4	• **Review** the incident, take action to prevent further breaches

Every data breach is different and the four steps may not necessarily happen in order

For example, in some data breaches, it may be more important to notify affected individuals while the assessment is ongoing.

Containing a data breach

Once an organisation discovers or suspects that there has been unauthorised loss, access or disclosure of its personal information, it should immediately take action to limit and contain the data breach.

Note

How a data breach is contained depends on the kind of breach, but some common containment methods include:

- stopping the unauthorised practice
- shutting down the relevant systems, or
- revoking computer access privileges

During the containment stage, take care to not destroy any evidence

At this stage, an APP organisation may either:

- **suspect** an eligible data breach has occurred which triggers **assessing** (step 2):
  - whether the data breach would be likely to result in serious harm to one or more individuals, and
  - the serious harm has not been able to be prevented with remedial action, or
- **believe** the data breach is an eligible data breach which triggers **notification** obligations (step 3)

Assessing suspected data breaches

If an organisation is aware there are reasonable grounds to suspect there may have been a data breach, the organisation must quickly assess the situation to determine whether the breach is an eligible breach.

The assessment of the suspected data breach must be prompt and occur no later than 30 calendar days after the day the organisation becomes aware of the grounds (or information) that caused it to suspect an eligible data breach.

The organisation should not unreasonably delay its investigations, for instance, by waiting for board approval or executive discussion. The OAIC expects that the 30 days should be treated as a maximum period and organisations should aim for as short a time frame as possible.

Organisations are required to undertake reasonable and expeditious assessments by being flexible and adaptive. The OAIC expects that the amount of time and effort organisations expend on assessment is proportionate to the likelihood that an eligible data breach has occurred and its apparent severity.

Generally, the four steps in response to a data breach should be taken simultaneously or in quick succession. Sometimes it may not be appropriate for the four steps to occur in succession. For example, OAIC guidance states that in some cases it may be appropriate to notify individuals before containment or assessment of the breach occurs.

If 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, guidance from the OAIC suggests a **three stage assessment process**:

Initiate the assessment process – identify the person or group responsible for completing the assessment

Investigate the matter – 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?'.

Evaluate the breach – the person or group needs to decide whether it is a notifiable data breach. This decision should be well documented, including the reasons why that decision was reached

Data breaches are often complex and, at times, APP organisations may not have sufficient or evidence when making an assessment under the NDB scheme. In these circumstances, the OAIC encourages entities to:

- **take a cautious approach** – if an APP organisation can't conclude that unauthorised access, disclosure or loss has occurred, it should consider proceeding on the presumption that there has been a data breach
- **consider all relevant factors and risk of harms** – APP organisations should assess a range of factors (see below), and

- **focus on unauthorised access** – do not over emphasise data exfiltration in your assessment period, eligible data breaches can occur on unauthorised access alone and data can be exfiltrated by less traceable means (ie. screenshots)

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.

The phrase 'likely to result in serious harm' has no special definition – it simply means that the risk of serious harm to a person is more probable than not.

Whether 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 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, and reputational harm.

OAIC guidance states that APP 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.

The NDB Scheme provides the following non-exhaustive list of factors which should be considered 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
Whether the information is protected by one or more security measures and the likelihood those measures could be overcome	Reputable encryption by software Multi-factor authentication required and is difficult to bypass	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 publicly	Identity theft Financial loss Physical safety Reputational damage Humiliation

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.

  The OAIC Guidance states that where a data breach involves many people, it may be prudent to assume that serious harm is likely to result in respect of at least one of those individuals and the serious harm threshold is likely 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 the information links a person with a sensitive product or service, such as 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, 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 is, the greater the likelihood that the information has been misused or accessed in a way that will cause serious harm. For example, if a malicious third party has had unauthorised access to a mailbox for a long period, they may have had more opportunity to understand how to commit financial harm and issue fraudulent invoices to customers.

  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.

Exceptions to the requirement to notify

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.

Notification

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

Contain the breach as far as it is possible

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

File the notification statement with OAIC through the online form or contact OAIC (enquiries line on 1300 363 992) to make alternative arrangements

Notify people at likely risk of serious harm

To notify OAIC of a data breach, use the online Notifiable Data Breach form.

Preparing the notification statement for OAIC

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 regard 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 they don’t disclose personal information about any affected person in the process of notification.

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.**

As noted above, it's also possible for notification to affected individuals to take place in some cases before containment or assessment of the breach occurs (for example, where serious harm is imminent).

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 three options for notifying individuals at risk of serious harm:	
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. Some examples for possible methods of notification include email, telephone call, SMS, post, in-person meeting, social media post, or newspaper advertisement. 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

While a website was compromised for two days, a hacker obtained all information (including credit card information) that was entered into the website during the two days.

Following a comprehensive risk assessment, the organisation considers that only customers who logged into their account during those two days are at serious risk and no other personal information has been accessed. The organisation is only required to notify the 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 this scenario, the organisation must publish a copy of the statement provided to the OAIC on its website (if it has one), other 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 publicly available, although the OAIC has provided some guidance that it expects the publication to exist for at least six months.

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 agreements

Responding to data breaches of jointly held information

If the data breach solely relates to personal information jointly held 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.

While only one organisation is required to assess the suspected breach, this doesn't mean the other organisations can't make their own assessments. If the group determines that one of the organisations will appropriately execute the reporting requirements to the OAIC and individuals affected, the group should secure a written statement from the reporting organisation regarding the eligible data breach.

The organisation that will prepare a statement for the OAIC and notify individuals 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 notification. Whether the organisation includes this information depends on the circumstances, the relationships between the organisations and extent to which it is useful to provide this information.

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

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

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 arrangement and potentially, which organisation is more at fault for the breach.

In general, compliance by one entity will also be taken as compliance by each of the relevant organisations.

As a general principle the OAIC suggests that the organisation with the most direct relationship with the individuals affected should action the notification.

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.

Reporting data breaches to other authorities

In addition to notifying eligible data breaches to affected individuals and the OAIC, organisations may also need to consider whether:

- the data breach triggers other notification requirements, and
- other authorities should be contacted to provide specific actions and protections

For example, in cases where TFNs are involved, it may be appropriate to seek advice from the Australian Tax Office (**ATO**). And where health information stored in the My Health Record system is involved, it may be appropriate to seek guidance from the Australian Digital Health Agency.

Organisations may also be required to notify other industry-specific regulators or other organisations under contractual arrangements.

If other regulatory authorities have been notified, it is useful to state this on the OAIC notification form.

Reviewing the incident

The OAIC recommends that organisations review and learn from eligible data breach incidents once the containment, assessment and notification steps have taken place.

An eligible data breach incident is an opportunity to:

- use lessons learned to strengthen the organisation's own personal information security and handling practices, and
- prevent, or reduce the likelihood of, a similar breach

Reviewing the data breach may include measures such as:

- a security review and understanding the root cause of the data breach
- education and training
- implementing a prevention plan to prevent a reoccurrence, and
- a review of policies and procedures

Managing risks that arise from changing work environments

With the impact of COVID-19, work environments have evolved over the last three years, including a shift towards remote and hybrid work. As a result, organisations may have increased vulnerabilities.

The OAIC has published guidance 'Assessing privacy risks in changed working environments: privacy impact assessments' to assist organisations.

Organisations are strongly encouraged to conduct a privacy impact assessment and address identified risks.

Penalties for not complying with the NDB scheme

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.

OAIC's power	Example
Apply to a court for a civil penalty order for a breach of a civil provision	The maximum penalty for serious or repeated interferences with privacy is an amount not more than the greater of: • $50 million • three times the value of benefits obtained or attributable to the breach (if quantifiable), or • if the court can't determine the value, 30% of the organisation's adjusted turnover' during the relevant period The court may order the maximum penalty 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	The 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
Apply to court for 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. 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.