Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – *Information Privacy Act 2009*

Notification under the MNDB scheme

This guide does not reflect the current law.

It highlights important changes to the *Information Privacy Act 2009*.

This guide does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

1. Introduction

1.1. Background

Chapter 3A of the *Information Privacy Act 2009* establishes a mandatory notification of data breach (**MNDB**) scheme.[1] It is currently expected that the scheme will commence on 1 July 2025 (other than local government which will be subject to the MNDB scheme 12 months later).

The MNDB scheme imposes various obligations on agencies[2] regarding data breaches and suspected eligible data breaches. Two of the main obligations are to notify the Information Commissioner and to notify particular individuals when an agency knows or reasonably believes that there has been an eligible data breach of the agency.[3]

This guideline is intended to help agencies understand and comply with these obligations to notify.

1.2. Other MNDB resources

Information contained in this guideline should be read in conjunction with other OIC MNDB guidelines, available at **IPOLA Guidelines**.

[1] All references to legislation in this document refer to a section of the *Information Privacy Act 2009*, unless otherwise stated.
[2] As per section 18, in this guideline, an agency includes a Minister, or a Department, or a local government, or a public authority. Agencies should note that OIC will continue operation of our existing voluntary breach reporting scheme after commencement of the MNDB; agencies are encouraged to report non-eligible breaches by way of the voluntary scheme.
[3] Sections 51 & 53.

2. Notification obligations

If an agency reasonably believes that there has been an eligible data breach involving personal information held by the agency, it must:[4]

- prepare a statement which includes the information stated in section 51(2)
- give the statement to the Information Commissioner, and
- notify any individuals affected by the breach, including notifying the information stated in section 53(2).

2.1. Notifying the Information Commissioner

Unless an exemption applies, agencies must notify the Information Commissioner as soon as practicable after forming the belief that a data breach is an eligible data breach.

Under section 51, the agency must prepare and give the Information Commissioner a statement, which must include:

- the name of the agency and, if more than one agency was affected by the data breach, the name of any other agency
- whether the agency is reporting on behalf of other agencies affected by the same data breach and, if so, the details of the other agencies
- the contact details of the agency or a person nominated the agency for the individual to contact in relation to the data breach
- the date the data breach occurred (if known)
- a description of the data breach, including the type of eligible data breach under section 47
- a description of the kind of personal information involved in the data breach, without including any personal information in the description
- information about how the data breach occurred
- if the data breach involved unauthorised access to or disclosure of personal information, the period during which the access or disclosure was available or made
- the steps the agency has taken or will take to contain the data breach and mitigate the harm caused to individuals by the data breach
- the agency's recommendations about the steps individuals should take in response to the data breach
- the total number or, if it is not reasonably practicable to work out the total number, an estimate of the total number of individuals whose personal information was accessed, disclosed or lost and affected individuals for the data breach

[4] To the extent that an exemption may apply under Part 3, Division 3 of Chapter 3A of the IP Act.

- whether the notified individuals have been advised how to make a privacy complaint to the agency under section 166A, and
- the total number of individuals notified of the data breach or, if it is not reasonably practicable to work out the total number, an estimate of the total number, or
- if relying on section 57, the total number of individuals who would have been notified or, if it is not reasonably practicable to work out the total number, an estimate of the total number.

If it is not reasonably practicable to include some of the above information in the initial notification to the Information Commissioner (e.g. the agency may not yet know the total number of affected individuals), the agency must take all reasonable steps to provide the required information to the Information Commissioner as soon as practicable.[5]

2.2. Notifying the Information Commissioner via online portal

The OIC is developing an online reporting portal to facilitate agency notification of eligible data breaches. Expected to be completed before the commencement of the scheme, the portal will guide agencies through a number of steps to provide the required information. Agencies will be able to supply further information as it is obtained, and the portal will also allow for agencies to notify the Commissioner of extensions of time for assessment periods and any further reporting regarding notification exemptions.

2.3. Notifying particular individuals

Unless an exemption applies, as soon as practicable after forming a reasonable belief that a data breach is an eligible data breach, an agency must take the steps set out in section 53 to notify particular individuals and provide them with the information required in 53(2) (the required information).

Section 53 provides three options for notifying individuals, depending on what is reasonably practicable in the circumstances. Whether an option is reasonably practicable will depend on a consideration of factors, including:

- the time, cost and the effort required to notify affected individuals, and
- the currency and accuracy of their contact details, which will affect the ability of the agency to notify the affected individuals (noting however, the mechanism for confirming the contact details and other information of affected individuals prescribed in section 54, discussed below).[6]

Option 1: Notify each individual

If it is reasonably practicable to notify each individual whose personal information was accessed, disclosed or lost, the agency must take reasonable steps to notify each individual of the required information.

[5] Section 52.
[6] In summary terms, section 54 will allow agencies to seek and receive contact details and other relevant personal information of affected individuals, from 'disclosing agencies' to be prescribed under regulation.

Option 2: Notify each affected individual

If Option 1 does not apply, agencies must take reasonable steps to notify each *affected individual* of the required information for the data breach, if doing so is reasonably practicable.

Under section 47(1)(a)(ii) and (b)(ii), an 'affected individual' is someone:

- to whom the personal information relates, and
- who is likely to suffer serious harm as a result of the data breach.

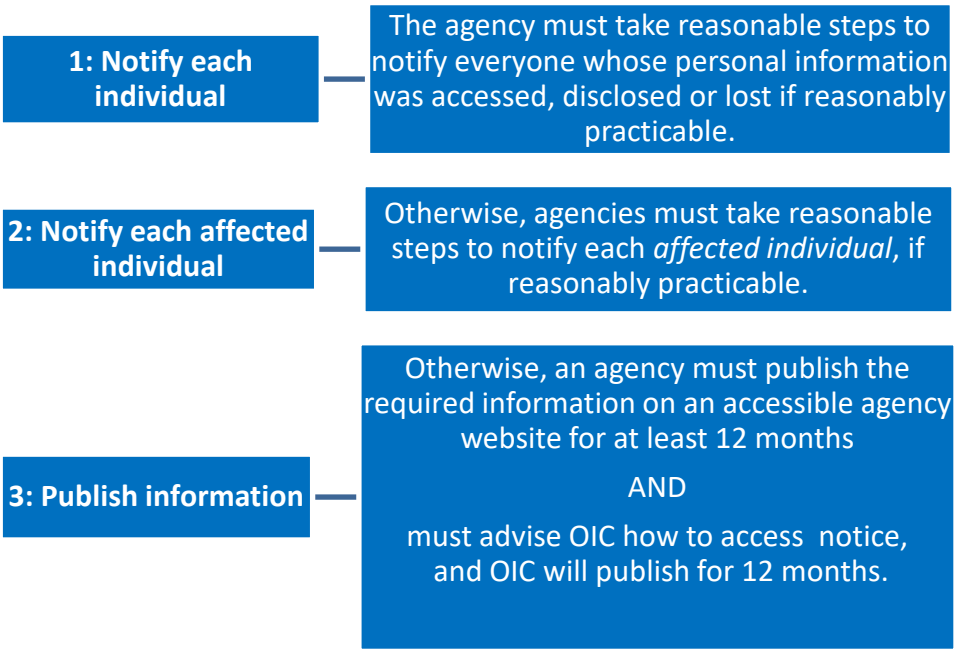
'To whom the information relates' is not defined in the IP Act. It should be given its ordinary meaning, which is the individual about whom the personal information concerns. An individual will be an affected individual if the information involved in an eligible data breach is about them, regardless of whether it was originally collected from that individual or a third party.

Option 3: Publish information

If options 1 and 2 do not apply, an agency must publish the required information on an accessible agency website for a period of at least 12 months. An agency is not required to include information in its notice if it would prejudice its functions.

An agency must advise the Information Commissioner how to access the notice and the Information Commissioner is required to publish the notice on the Commissioner's website for at least 12 months.

Figure 1: Option for individual notification (must be attempted in sequence)



2.4. Required information when notifying individuals

The information that must be given to an affected individual or included in the agency's public notice under section 53(2), must, to the extent it is reasonably practicable, include:

- the name of the agency and, if more than one agency was affected by the data breach, the name of any other agency
- the contact details of the agency or a person nominated by the agency for an affected individual to contact in relation to the data breach
- the date the data breach occurred (if known)
- a description of the data breach, including the type of eligible data breach under section 47
- information about how the data breach occurred
- the agency's recommendations about the steps an affected individual should take in response to the data breach
- if the data breach involved unauthorised access to or disclosure of personal information, the period during which the access or disclosure was available or made
- the steps the agency has taken or will take to contain the data breach and mitigate the harm caused to affected individuals due to the data breach, and
- information about how an individual can make a privacy complaint to the agency under section 166A.

If an individual is notified directly, the notice to the individual must also include a description of their personal information involved in the data breach, and the agency's recommendations about any steps they should take in response to the eligible data breach. Appendix 1 provides a template for individual notification.

For public notification via an agency's website, the notification must include a description of the kind of personal information involved in the data breach, ***without*** including any personal information in the description.

Notifying children

Where a data breach involves the personal information of a child, notification should generally be made to the child's parent or legal guardian.

For minors aged 16 years or older, it may be appropriate to make the notification directly to the child.

2.5. Notifying other individuals

There is no requirement to notify individuals whose personal information is not involved in a data breach. However, if an agency identifies an individual who is likely to suffer harm for reasons other than their personal information being involved, agencies may wish to consider notifying these individuals if it is possible to do so without the risk of further breaches - as this may assist in mitigating any risk of harm.

3. Exemptions from notification obligations

Chapter 3A, part 3, division 3 of the IP Act sets out the circumstances in which an agency is not required to comply with the notification obligations, including where:

- complying with the obligation would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or tribunal
- the eligible data breach involves more than one agency, and another agency is undertaking the notification obligations
- the agency has taken specified remedial action under section 57
- compliance would be inconsistent with a provision of an Act of the Commonwealth or a State that prohibits or regulates the use or disclosure of the information
- compliance would create a serious risk of harm to an individual's health or safety, and
- compliance is likely to compromise or worsen the agency's cybersecurity or lead to further data breaches of the agency.

A number of these exemptions have limitations or impose additional obligations. Refer to the ***MNDB Exemptions*** *guideline* for more information.[7]

3.1. Notifying other entities

While not required by the IP Act, in some circumstances it may be appropriate – or agencies may be required – to notify other entities of a data breach, for example:

- If the breach involves 'corrupt conduct' within the meaning of the *Crime and Corruption Act 2001* (Qld), the Crime and Corruption Commission Queensland must be notified.
- Requirements to report cyber and information security incidents to Queensland Government Information Security Virtual Response Team, according to the Business Impact Level.
- If the breach involves a cyber security incident that results in a loss and the entity is an agency covered by the Queensland Government Insurance Fund (**QGIF**), QGIF should be notified.

[7] For example, some of the exemptions apply only to the obligation to notify individuals, meaning that the Information Commissioner must still be notified.

- If the breach appears to involve theft or other criminal activity, the Queensland Police Service (**QPS**) should be notified as a matter of course. The QPS website has links and assistance to report cybercrime and other offences.
- If the breach involves the loss or unauthorised destruction of a public record, an entity subject to the *Public Records Act 2023* (Qld) must notify the State Archivist.
- Entities with obligations under the *Privacy Act 1988* (Cth) National Data Breach (**NDB**) scheme (e.g. Tax File Number recipients) may be obliged under the NDB scheme to report the breach to the Office of the Australian Information Commissioner.

Depending on the circumstances of the data breach and the information involved, other notifications may be appropriate. For example, the agency's portfolio Minister, financial institutions, or credit card companies, or professional or other regulatory bodies.

Agencies should note that the above reporting obligations and considerations may apply to *any* breach or compromise of *any* type of information, and not only to those assessed as eligible data breaches under the MNDB scheme.

4. Non-eligible data breaches and voluntary reporting to OIC

Prior to the commencement of the MNDB scheme, OIC administered a voluntary data breach reporting scheme, which we continue to operate.

The Information Commissioner encourages agencies to advise the OIC of data breaches that do not meet the threshold of an 'eligible data breach'. Information gathered from voluntary reports will allow the OIC to provide agencies with assistance and advice in relation to a data breach and to assist the Information Commissioner in fulfilling the broader performance and monitoring statutory functions under section 135, including:

- promoting understanding of and compliance with the privacy principles
- providing best practice leadership and advice, including by providing advice and assistance to relevant entities on the interpretation and administration of this Act
- conducting compliance audits to assess relevant entities' compliance with the privacy principles
- initiating privacy education and training, including education and training programs targeted at particular aspects of privacy administration, and education and training programs to promote greater awareness of the operation of this Act in the community and within the public sector environment
- commenting on any issues relating to the administration of privacy in the public sector environment
- issuing guidelines about any matter relating to the Information Commissioner's functions, including guidelines on how the IP Act should be applied and on privacy best practice generally, and

- supporting applicants of any type under the IP Act, and all relevant entities to the extent they are subject to the operation of the IP Act.

5. Regulation to collect, use and disclose relevant personal information

Under section 54, a regulation may provide for the collection, use, and disclosure of 'relevant personal information' between agencies where the receiving agency is involved in an eligible data breach, and the information is needed to confirm the name and contact details of a notifiable individual or whether a notifiable individual is deceased.

Neither the disclosing agency or receiving agency are required to comply with a QPP in relation to this disclosure, collection, or use.

'Notifiable individual' and 'relevant personal information' are defined in section 54. Currently, no regulation exists in relation to section 54.

For additional IPOLA assistance, please contact the IPOLA team by email IPOLA.Project@oic.qld.gov.au

For information and assistance on current legislation, please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or by email enquiries@oic.qld.gov.au

Published February 2025 and Last Updated February 2025

Office of the Information Commissioner
Queensland

IPOLA

Appendix 1: Notification template for individuals

IPOLA RESOURCE

Applying the legislation – Information Privacy Act 2009

MNDB notification template – Individuals

This resource does not reflect the current law.

It highlights important changes to the *Information Privacy Act 2009*.

This resource does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

Who should use this template?

This template will assist Queensland government agencies to complete a notification to affected individuals under the mandatory notification of data breach scheme.

Why should I utilise this template?

The template is provided as a guide for agencies when they are required to notify affected individuals about an eligible data breach. Under the MNDB scheme an agency has an obligation to notify affected individuals, the template provides a framework and overview of information that may be relevant when an agency is required to notify an affected individual. The agency should also refer to the Information Privacy Act 2009 s 53(2) to ensure relevant information regarding the data breach is included in the notification letter.

How to use this template

Text in ***bold and italics*** are provided as a guide and should be reviewed to **update or delete.** Your letter should reflect information specific of the data breach and consider the affected individual you are notifying to ensure the reader can understand what has occurred. Keep the language plain and free from jargon.

[Date]

Dear *[name of affected individual],*

We are writing to notify you of a recent data breach that involves ***a/an access, disclosure, loss*** of your personal information. Our agency, ***add name of your agency,*** is making contact to provide you information regarding the breach, including information about the actions taken by our agency to contain the breach and options you may want to consider, or further actions you can take.

Incident Information

Date***: 'on or 'between dates'***

Time: ***'at' or 'between times'***

****The summary of the incident is to be provided here.***

- ***Include a description of the data breach, including the type of eligible data breach (s 47) so the affected person understands why the incident is considered a data breach.***
- ***Advise how the data breach occurred.***

Affected personal information

Whilst responding to the breach our agency identified the personal information that has been affected due to the incident. The personal information involved includes:

- ***Provide a full list and description of the personal information subject of the data breach.***

  This aim of providing the full information subject of the breach is to enable the affected person to take proactive steps and make their decisions regarding other actions steps they may need to take to protect themselves.

What has our agency done to contain the breach?

****List the steps your agency has taken to contain and mitigate - s 48 (2) E.g. restricted access to affected system, isolated affected device, reset passwords etc.***

You can also provide information on the actions taken to reduce the likelihood of a future breach occurring. E.g. introduction of multi-factor authentication, encryption of sensitive data.

Next steps

Please take the time to review the information in this letter and the type of

personal information affected by the data breach. You should consider if the personal information involved in the data breach is likely to cause harm. This may include, financial loss, concern for physical safety or damage to reputation or relationships. Depending on the circumstances, some of the actions you may wish to consider to protect yourself include:

- ***Remember to delete text that is not applicable to the data breach incident. You can add further recommendations that are relevant to the data breach scenario to advise the affected individual what they should consider in response to the data breach***

Risk of harm is identity fraud including contact information

The below are suggestions *only* – agencies will need to determine appropriate advice:

- ***Change your related account password as soon as possible.***
- ***You may wish to contact IDCare on 1300 432 273 or visit www.idcare.org . IDCare can provide specific guidance on the steps you can take to protect yourself from identity fraud.***
- ***Keep an eye out for emails and telephone calls where they are requesting your personal details. This may include a request for information for your home address, an email address, your date of birth, account usernames, passwords or personal identification numbers.***
- ***Should you start to receive unwanted telemarketing calls, consider registering your number with the Australian Communications and Media Authority's 'Do Not Call register' by visiting www.donotcall.gov.au/consumers/register-your-numbers. You can also contact your service provider and request to change your number.***

Risk of harm involves financial information

- **The below are suggestions *only* – agencies will need to determine appropriate advice:*Contact your financial institution as soon as possible, to enable additional monitoring and security actions to your account.***
- ***Enable multi-factor authentication (if able), change your online banking password (if applicable), cancel affected debit or credit card, change your personal identification number (PIN).***
- ***Continue to review your bank statements and online banking transactions for unauthorised purchases. Report any discrepancies to your bank as soon as possible.***
- ***You may consider contacting Australia's three credit reporting agencies (Equifax, Illion and Experian) to understand if your***

identity has been used to obtain credit without your knowledge. You may consider making a request for a credit ban to be put in place.

- ***If the affected personal information relates to your tax file number of superannuation, contact the Australian Tax Office on 1800 467 033 and your superannuation fund to discuss if additional monitoring needs to be placed on your account.***

Risk of harm involves Health Information

- **The below are suggestions *only* – agencies will need to determine appropriate advice: *Contact your health service provider using their contact details, either located on their website or via hard copy information you may hold.***

It is also important to consider your physical safety. If you are at risk of domestic violence and in immediate danger, contact police on triple zero (000) immediately, or if you are not in immediate danger you may wish to contact DVConnect on 1800 737 732, Womensline on 1800 811 811 or Mens Helpline on 1800 600 636. If you are feeling distressed due to this incident, you may want to consider contacting your doctor, a support service or family or friends.

Further information is also available at the Office of the Information Commissioner website What to do if you're affected by a privacy breach | Office of the Information Commissioner Queensland

Seeking more information and making a complaint

If you have any questions or concerns about what has happened or would like further information, you can contact:

[individual or department's name within your organisation]

[phone number] or [email].

If you would like to make a privacy complaint because you are not satisfied with how our agency has managed this incident, or you have suffered harm as a result, you can do so by contacting us at this email address: ***@XXXXXX***

Our agency is committed to resolving your complaint and we would value an opportunity to understand how you were affected by the incident, and what you would like done to resolve the complaint.

Whilst we will endeavour to resolve your complaint, you are able to make a complaint to the Office of the Information Commissioner when:

- you do not consider our response to your complaint to be adequate, or
- we have not responded to you by the end of the response period, which is 45 days unless you have agreed to an extension of this time.

Office of the Information Commissioner
Queensland

IPOLA

Please find website link for further information below. [Make a privacy complaint | Office of the Information Commissioner Queensland]

Yours sincerely,

[Name]

[Position/Title]

[Organisation name]

For additional IPOLA assistance, please contact the IPOLA team by email IPOLA.Project@oic.qld.gov.au

For information and assistance on current legislation, please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or by email enquiries@oic.qld.gov.au

Published February 2025 and Last Updated February 2025