Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – Information Privacy Act 2009

GUIDELINE *Information Privacy Act 2009*

Mandatory Notification of Data Breach 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. Mandatory Notification of Data Breach scheme

Agencies are required to deal with personal information in compliance with the *Information Privacy Act 2009* (Qld) (**IP Act**). Chapter 3A of the IP Act creates a mandatory notification of data breach (**MNDB**) scheme.

The MNDB scheme imposes the following obligations on agencies[1] (other than local government[2] which will be subject to the MNDB scheme from 1 July 2026):

- Where an agency knows or reasonably suspects that a data breach of the agency is an eligible data breach, the agency must:
    - immediately, and continue to take all reasonable steps to:
        - **contain** the data breach, and
        - **mitigate** the harm caused by the data breach, and
    - if there is uncertainty as to whether the data breach is eligible, **assess** whether there are reasonable grounds to believe the data breach is an eligible data breach of the agency within 30 days.[3]
- When an agency knows or reasonably believes that the data breach is an eligible data breach, the agency must as soon as practicable:
    - **notify** the Information Commissioner,[4] and

[1] In this guideline, agency includes a Minister but does not include a local government.
[2] Application of the MNDB scheme to local governments is delayed until 1 July 2026. Until that time, local government agencies should continue to refer to *Responding to a potential privacy breach*, and *Privacy breach management and notification*.
[3] Section 48.
[4] Section 51.

- **notify** particular individuals.[5]

- An agency must also:
  - prepare and publish a **data breach policy** about how it will respond to a data breach, including a suspected eligible data breach, of the agency,[6] and
  - keep a **register** of eligible data breaches of the agency.[7]

This guideline explains agency obligations under the MNDB scheme. It should be read in conjunction with the ***MNDB Exemptions*** *and* ***MNDB Data Breach Registers and Policies*** guidelines.

All references to legislation in this document refer to a section of the IP Act, unless otherwise stated.

The OIC will continue to develop this guideline and develop further resources to assist agencies to prepare for the commencement of the MNDB scheme. This guideline is based on and includes material from guidelines developed by the NSW Information and Privacy Commission.

2. Key Definitions

The following definitions and concepts are important when considering the MNDB scheme.

2.1. Personal Information

The MNDB scheme applies in relation to personal information, other than personal information in a document to which the privacy principle requirements do not apply, held by an agency.

Section 12 defines 'personal information' as follows:

> *Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion—*
>
> *(a) whether the information or opinion is true or not; and*
>
> *(b) whether the information or opinion is recorded in a material form or not.*

2.2. Personal information 'held' by an agency

Section 13 defines "held or holds" in relation to personal information as:

> *Personal information is held by a relevant entity, or the entity holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant entity.*

[5] Section 53.
[6] Section 73.
[7] Section 72.

The overall effect of this provision is to expand the ordinary meaning of the terms 'hold or held' to include situations where an agency may not be in physical possession of the relevant document containing personal information, but it still retains a legal power or a right to deal with the information.

Examples of physical possession include documents stored in an agency's records management or IT systems, and hard copy documents on a 'paper' file or in a physical storage repository.

Agencies will be in 'control' of a document where they have a present legal entitlement to physical possession,[8] or a power to handle the information, such as by way of a contractual or other legal right. This may include, for example, documents provided to a legal services provider by an agency for the purposes of seeking advice,[9] or documents an agency may require a service provider to provide to the agency under the terms of a service agreement.

2.3. What is a data breach?

Central to the MNDB scheme are the concepts of a 'data breach' and an 'eligible data breach'. Each is defined in the IP Act, and those definitions are discussed further below.

At the outset, it is important to note that the concept of a 'data breach' extends to *any* information held by an agency. An 'eligible data breach', however, *only* involves **personal information**.

A 'data breach' means either of the following in relation to information held by an agency:

> (a) unauthorised access to, or unauthorised disclosure of, the information.
>
> (b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur.[10]

2.3.1. Unauthorised access

As discussed above, the concept of a 'data breach' extends to any information held by an agency. As key obligations under the MDNB scheme only relate to personal information, the following discussion of key definitional concepts refers to personal information.

Unauthorised[11] access to personal information occurs when information held by an agency is accessed by someone who is not authorised to do so. For example:

---

[8] *Price and Nominal Defendant* (1999) 5 QAR 80, [18].

[9] For more information on this point, see OIC's guideline Documents held by third party legal providers. While this guideline concerns information access applications made under the RTI Act, the applicable statutory tests and legal principles are substantially similar.

[10] Schedule 5 of the IP Act.

[11] The term 'unauthorised' is not defined in the IP Act. The ordinary dictionary definition is '*without proper permission or licence*' (Macquarie Dictionary Online). The word is used in a similar context in section 476.2 of the *Criminal Code Act 1995* (Cth), which defines the phrase '*unauthorised access modification or impairment*' as encompassing circumstances where a '*person is not entitled to cause that access, modification or impairment*'.

- Within an agency, if an employee browses agency records relating to a family member, a neighbour, or a celebrity without a legitimate purpose.
- Between agencies, if a team at one agency is provided with access to systems and data at a second agency as part of a joint project. Unauthorised access may occur if a member of the team uses that access beyond what is required for their role as part of the project.
- Outside an agency, if information is compromised during a cyberattack and intentionally accessed by a person external to the agency.

2.3.2. Unauthorised disclosure

Unauthorised disclosure occurs when an agency intentionally or unintentionally discloses personal information when the agency does not have permission or is not entitled to make that disclosure. For example:

- An agency software update, either conducted by the agency or a third-party service provider, results in the unintended publication of customer records containing personal information on the agency's website.
- An agency intends to provide de-identified information to a researcher and accidently sends the data with personal identifiers included.
- An agency discloses an individual's personal information to a third party who is not the intended recipient.
- A database hosted in a cloud environment or a web facing application containing personal information does not have appropriate access controls and personal information in the data set is visible and accessed by unauthorised individuals.

Unauthorised access and disclosure are not mutually exclusive and can occur as a result of the same breach or as part of a chain of events. For example, if an agency mistakenly discloses personal information via a webform on its internet site and a third party can view the information, this may amount to unauthorised disclosure of personal information by the agency and unauthorised access by the external party.

2.3.3. Loss

Loss of personal information involves an agency no longer having possession or control of the information. Loss may occur because of a deliberate or accidental act or omission of an agency, or due to the deliberate action of a third party. For example:

- An agency sells or disposes of a physical asset, such as a laptop or filing cabinet, that contains an individual's personal information.
- An agency employee accidentally leaves a device, such as a USB or external drive, containing personal information on public transport.
- A device containing personal information is stolen from an agency's premises or an employee's home.

The loss of personal information will result in a data breach only where such loss is likely to result in unauthorised access or disclosure of the information. If the personal information is inaccessible, or is known to have been destroyed, it will be unlikely that a data breach has occurred.

Examples of the above may include where:

- Agency documents containing personal information are destroyed in a natural disaster (e.g., bushfire or flood event).
- A password protected laptop containing client files is left on public transport but is handed in and the agency is able to establish there was no access to the stored information.
- A USB containing personal information is lost, but security measures are in place, such as the data being encrypted or protected by a strong password.
- A tablet device containing a client's records is stolen from an agency employee's home, but it is only accessible via multifactor authentication (noting that some of these considerations may also be relevant in assessing the question of 'serious harm', discussed below).

As the loss of personal information in the above examples did not or was unlikely to result in unauthorised access or disclosure, it will be unlikely that a data breach has occurred.

2.4. What is an eligible data breach?

For a data breach to be an 'eligible data breach' triggering notification and other obligations under the MNDB scheme, both of the following must apply:

1. There is unauthorised access to, or unauthorised disclosure of, personal information held by the agency, or there is a loss of personal information held by the agency in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and
2. The unauthorised access to, or disclosure of the information is likely to result in serious harm to an individual to whom the personal information relates (an 'affected individual').[12]

2.4.1. Serious harm

The harms which can potentially arise from a data breach will vary based on the nature of the personal information involved and the context of the breach.

Serious harm is defined in schedule 5 of the IP Act as including:

- serious physical, psychological, emotional, or financial harm to the individual because of the access or disclosure; or

[12] Section 47.

- serious harm to the individual's reputation because of the access or disclosure.

This is not an exhaustive definition, and other kinds of harm can meet the serious threshold. Serious harm occurs where the harm arising from the data breach has, or may, result in a real and substantial detrimental effect to an individual. The effect on an individual must be more than mere irritation, annoyance, or inconvenience. It is important to note that serious harm is not limited to physical harm to a person or their physical safety and can involve emotional or reputational harm arising from a data breach.

Section 47(2) contains a list of stated matters to which an agency must have regard to when considering if a breach is likely to result in serious harm.

The section 47(2) matters are:

- the kind of personal information accessed, disclosed or lost
- the sensitivity of the personal information
- whether the personal information is protected by one or more security measures
- if the personal information is protected by one or more security measures, the likelihood that any of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information
- the nature of the harm likely to result from the data breach, and
- any other relevant matter.

Other relevant matters to consider may include (but not be limited to):

- the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk
- the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm)
- the circumstances in which the breach occurred, and
- actions taken by the agency to reduce the risk of harm following the breach.

2.4.2. Likely to result

'Likely to result' requires that the risk of serious harm to an individual be more than merely possible; it must be more probable than not to occur.

Whether a data breach is likely to result in serious harm is an objective test to be determined on the facts of the specific breach, taking into account the section 47(2) matters, as set out above.

A data breach will be an eligible data breach if serious harm is more likely than not to affect an individual, or a subset of individuals affected by a breach. Serious harm does not need to be likely for all individuals to whom a data breach relates.

An agency does not need to identify the specific individuals who may be harmed in order to determine that serious harm is likely to result for one or more individuals. A data breach affecting a large number of individuals may therefore be an eligible data breach even if the personal information involved is not highly sensitive – provided the agency concludes that serious harm is likely to result for some of those individuals.

OIC recommends that agencies should carefully consider the factors for assessing the risk of serious harm to an individual. If doubt or ambiguity exists as to whether a data breach is likely to result in serious harm, agencies should err on the side of caution, and treat the data breach as an eligible data breach.

3. MNDB Scheme Breach Obligations

Agencies have the following obligations regarding data breaches under the MNDB scheme.

3.1. Contain and mitigate

If an agency knows or reasonably suspects that a data breach is an eligible data breach involving personal information held by the agency, it must immediately take, and continue to take, all reasonable steps to contain the data breach and mitigate the harm caused by the data breach.[13] Steps may include:

- making efforts to recover the personal information
- securing, restricting access, or shutting down to breached systems
- suspending the activity that led to the data breach, or
- revoking or changing access codes or passwords.

If a third party is in possession of the personal information and declines to return it, it may be necessary to seek legal advice on what action can be taken to recover the information. When recovering information, agencies should also take steps to ascertain whether the information has been shared or disseminated and ensure copies have not been made or that all copies are recovered.

[13] Sections 48(1) and (2).

Agencies should be careful to ensure that while containing an eligible or suspected eligible data breach, they do not destroy information that may be required as part of an internal or external investigation into the breach.

An agency's data breach policy[14] should clearly identify the steps to be followed in responding to, containing, and mitigating an eligible or suspected eligible data breach, including appropriate escalation pathways. Depending on the circumstances of the data breach and an agency's data breach policy, this may include informing:

- the agency's privacy officer and/or senior management responsible for the area in which the breach occurred being informed immediately about the breach
- the head of the agency, and senior personnel responsible for information security, communications, legal services, human resources, and employee misconduct (such as internal audit, ethical standards or Crime and Corruption Commission liaison officer), as appropriate.

3.2. Assess

If an agency does not know, but reasonably suspects that a data breach is an eligible data breach, it must assess whether there are reasonable grounds to believe it is an eligible data breach.[15] This assessment must be completed within 30 days unless the assessment time is extended under section 49.

An agency's assessment and reasons for its decision as to whether a data breach is an eligible data breach should be recorded in writing and include the material facts of the specific breach. The assessment should address the section 47(2) matters set out above, and any other relevant factors.

3.2.1. Extension of time to assess a breach

If an agency is satisfied that it will not be able to complete the assessment in 30 days, it can extend that time under section 49.

An agency can only extend the assessment period by a further period that is reasonably required to complete the assessment.

Before the initial 30 day assessment period expires, the agency must:

- start the assessment, and
- give the Information Commissioner written notice that the agency has extended the time. This initial period can only be extended by a further period that is reasonably required to complete the assessment.

The notice to the Information Commissioner must state:

- that the assessment has started

[14] Required under section 73.
[15] Section 48(3).

- the period within which the assessment must be completed has been extended, and
- the day the extended period ends.

The Information Commissioner can ask the agency to provide information or progress updates about the assessment.

3.3. Data breaches affecting another agency

If the agency becomes aware that an eligible or suspected eligible data breach may affect another agency, it must give the other agency a written notice of the data breach that includes:

- a description of the data breach, and
- a description of the kind of personal information involved in the data breach, without including any personal information in the description.[16]

3.4. Notification obligations

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

- 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 the information stated in section 53(2).

3.4.1. 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.

Agencies are welcome to seek advice from the OIC about a data breach, but notification of an eligible data breach must be made in writing.

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)

[16] Section 48(4).

- 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
- 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 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 required information to the Information Commissioner as soon as practicable.

3.4.2. 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).[17]

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.

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 the 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.

Required information

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)

[17] 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.

- 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.

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, the OIC recommends that agencies 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.

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.

3.5. 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.[18]

3.6. 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.
- 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

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

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. Data breach registers and policies

An agency must keep an internal register of eligible data breaches[19] and publish a data breach policy on its website.[20]

Refer to ***MNDB Data Breach Registers and Policies*** for more information.

5. Information Commissioner's role

Eligible data breaches

Chapter 3A, part 4 of the IP Act sets out the Information Commissioner's role in relation to eligible data breaches, including:

- giving directions and recommendations to agencies when certain criteria are satisfied, and
- monitoring and investigating agency compliance with the MNDB scheme.

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 OIC to provide agencies with assistance and advice in relation to a data breach and to assist the Information Commissioner in fulfilling their 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

[19] Section 72.
[20] Section 73.

- 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.

6. 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 August 2024 and Last Updated 8 August 2024