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 – Exemptions

**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

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 requires agencies[1] (other than local government[2] which will be subject to the MNDB scheme from 1 July 2026) to notify the Information Commissioner and affected individuals of eligible data breaches. However, there are some exemptions to these notification obligations.

This guideline outlines those exemptions under the MNDB scheme. It should be read in conjunction with the ***Mandatory Notification of Data Breach***, and ***MNDB Data Breach Registers and Policies*** guidelines.

All references to legislation in this document refer to a section of the *Information Privacy Act 2009*, 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.

[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. Local government should refer to *Responding to a potential privacy breach, and Privacy breach management and notification*.

## 2. Background and Definitions

Key definitions and concepts are discussed in detail in OIC's ***Mandatory Notification of Data Breach*** guideline. A summary of concepts relevant to MNDB exemptions as discussed in this guideline is set out below.

### *Personal Information*

Section 12 provides that personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion, whether the information or opinion is true or recorded in a material form.

### *'Eligible data breach'*

Obligations to notify of the Information Commissioner and individuals under the MNDB scheme arise where a data breach is assessed by an agency as an 'eligible data breach'.

The concept of an 'eligible data breach' is defined in section 47. Both of the following requirements must be satisfied:

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 or disclosure of the information is likely to result in serious harm to an individual.

### *More information on eligible data breaches*

For more guidance on eligible data breaches refer to the ***Mandatory Notification of Data Breach*** guideline. This guideline includes discussion of key concepts such as:

- when personal information is 'held' by an agency
- unauthorised access, disclosure and loss; and
- evaluating the likelihood of 'serious harm' for the purposes of assessing whether a data breach comprises an eligible data breach attracting notification obligations.

## 2.1. Notification of eligible data breaches

As soon as practicable after forming a reasonable belief that there has been an eligible data breach, agencies must notify both the Information Commissioner and individuals whose information was involved in an eligible data breach about the eligible data breach.[3]

[3] Sections 51 and 53.

Refer to the ***Mandatory Notification of Data Breach*** guideline for more information on notification obligations and determining if a data breach is an eligible data breach.

## 3. Exemption from notifications

Under section 50(2), an agency is not required to comply with the MNDB notification obligations to the extent that an exemption applies. Sections 55 to 60 outline the exemptions from notification which are available under the scheme. Three of these exemptions only exempt agencies from the requirement to notify individuals – under these exemptions, agencies must still notify the Information Commissioner. The remaining three exemptions exempt agencies from the requirement to notify both the Information Commissioner and individuals.

The policy intent of the MNDB scheme is to empower individuals, enhance transparency, and build trust in agency management of personal information. In most cases, notification of individuals affected by an eligible data breach can be presumed to be beneficial, as it empowers those individuals to take steps to protect themselves. Notification delays can have significant impacts on affected individuals. Exemptions to notification are intended to apply only in exceptional circumstances.

Additionally, reliance on an exemption is discretionary. Accordingly, an agency may still choose to undertake notification in appropriate circumstances, even where the requirements for an exemption are satisfied.

Agencies should keep appropriate records of the assessment and decision-making process when deciding to rely on an exemption, including accurate records of information and evidence used to support that decision.

### 3.1. Exemption from notification to individuals

#### 3.1.1. Agency has taken remedial action

Section 57 provides that an agency is not required to notify individuals if the agency has taken remedial action to mitigate the breach, so that the breach is no longer likely to result in serious harm to any individual.

If the data breach involves ***unauthorised access*** to, or ***disclosure*** of, personal information, the agency can rely on section 57 if:

- it takes action to mitigate the harm caused by the data breach before the access or disclosure results in serious harm to any individual; and
- as a result of the action taken, the data breach is no longer likely to result in serious harm to any individual.

If the data breach involves ***loss*** of personal information, the agency can rely on section 57 in two circumstances.

Firstly, where the agency takes action to mitigate the loss ***before*** there is unauthorised access to or disclosure of the personal information and as a result there is no unauthorised access to, or disclosure of, the personal information.

Secondly, where the agency takes action to mitigate the loss *after* there is unauthorised access or disclosure but *before* it results in serious harm to any individual and as a result the data breach is no longer likely to result in serious harm to any individual.

The remedial action exemption *only* exempts agencies from the obligation to notify individuals. Agencies must still notify the Information Commissioner under section 52 and include information about the mitigation actions taken.

### 3.1.2. Serious risk of harm to health or safety

Under section 59, an agency is not required to notify individuals of an eligible data breach – as would otherwise be required under section 53 – to the extent that compliance with section 53 would create a serious risk of harm to an individual's health or safety. The agency must, however, still notify the Information Commissioner,[4] and provide the Information Commissioner with written notice of its reliance on this exemption.

When determining whether this exemption applies, the agency must have regard to whether the harm caused by complying with notification obligations is greater than the harm of not complying, the currency of the information the agency is relying on to make its decision, and any other relevant matters.

Health refers to a person's mental and physical wellbeing. Safety refers to freedom from danger, risk, or injury. Whether notification would create a serious risk of harm to an individual's health or safety should be assessed objectively, based on best available information and a careful evaluation of all relevant circumstances.

It is important to note that this exemption encompasses serious risk of harm to any individual – not just a person affected by the eligible data breach. The test is also whether there exists a 'serious risk of harm', rather than 'serious harm', which is the threshold for an eligible data breach under section 47.

Determining whether notification would result in a serious risk of harm to an individual requires consideration of both the likelihood and consequence of harm to an individual. A high likelihood of detrimental impact on the health or safety of an individual would constitute a serious risk of harm.

However, a lower likelihood could still amount to a serious risk of harm if the potential consequences would be extremely detrimental to an individual's health or safety. For example, the threshold for application of the exemption may be met where the agency makes an assessment that there is a serious risk:

- that notification will exacerbate the mental health condition of an affected individual

[4] Under section 52.

- of harm to the physical safety of agency staff members – for example where an affected individual has a documented history of actual or threatened violence against staff
- of an individual disengaging from treatment for a significant or life-threatening medical condition; or
- of at-risk individuals disengaging with domestic violence or child protection services in circumstances where the agency is aware that is a real risk of serious physical harm or death to the individual and/or their family if service provision is discontinued.

A serious risk of harm to the health or safety of an individual ***other*** than the person to whom the information relates may be a relevant risk for the purpose of section 59. For example, circumstances may exist where notification would cause a serious risk of harm to the affected individual's spouse or another family member.

Individuals for whom notification would create a serious risk of harm may be a sub-group of those affected by the breach. If the broader group can be notified without creating a serious risk of harm to the at-risk subgroup, the exemption will not apply in relation to notification to the broader group.

Systematic risks such as harm to the individual's confidence in a service or system will not usually meet the threshold for this exemption. However, in exceptional and limited circumstances where notification is likely to damage an individual's trust in an agency to such an extent that they would completely disengage from a medical or other essential services, the exemption may apply.

### *Balancing impacts*

When deciding whether to rely on section 59, the agency must consider whether the harm of notification outweighs the harm of not notifying. It must be satisfied that the harm that could result from notifying is real, substantial and, in practice, not unlikely to result.

Taking into account the policy intent of the MNDB scheme and the starting point that notification to affected individuals is usually beneficial, agencies should only rely on section 59 in circumstances where the harm posed by notification is substantively greater than the potential harm from failing to notify.

### *Actions to mitigate risk*

When making a decision on whether to rely on this exemption, agencies should consider whether there are additional steps or actions available that could lessen or manage the anticipated harms. If there is a practical means of delivering the notification in a way that will mitigate the risks to an individual's health or safety, the exemption will not apply.

Actions to mitigate risk of harm could include:

- In person notification and/or provision of support – if an agency is concerned that receiving a notification might cause significant distress to

an affected individual, this may be mitigated by providing notice in person with a support person and clinical staff in attendance.

- Redaction of some information – an agency should consider whether identified risks could be mitigated by redacting specific information or providing a high-level summary. For example, if a law enforcement officer
- investigating serious organised crime inappropriately accessed information held about individuals in an organised crime group, it may be open to the relevant agency to form the reasonable belief that notification would create a real risk of harm to the relevant officer's health or safety. When balancing the relevant impacts, the agency should consider whether notification of the data breach can be provided without identifying the individual officer.
- Notification to an authorised representative – in circumstances where an affected individual lacks decision making capacity, the agency may make the notification to the individual's authorised representative. The notification should include information about the health or safety risks to the affected individual and the services available to support the authorised representative to inform the affected person of the breach after they regain capacity.

It is expected that an agency would take all reasonable steps to identify any actions it could reasonably take to mitigate the identified harms, to enable notification to occur.

**Children's information**

If 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.

If an agency decides that notifying a child aged 16 years or over would result in a serious risk of harm to their health or safety, the agency should consider whether it is appropriate to make notification to the child's parent or guardian rather than exercising the exemption.

In these circumstances the notification should be accompanied by information on counselling or support services for the child and their family and factors for the parent or legal guardian to consider before informing their child.

### *Currency of information*

Before relying on section 59, the agency must consider the currency of the information it is relying on to assess whether notification could create a serious risk of harm. This is because individuals' vulnerability to harm is dynamic and relative rather than being a fixed trait, and agency records may be old and reflect a particular moment in time.

If agency records indicate that a situational factor or a particular characteristic of the individual gives rise to a risk of harm, consideration should be given to the

age of those records and the likelihood that the individual's circumstances may have changed in the intervening time.

Determining the duration of the exemption

The agency can decide to rely on section 59 permanently or temporarily. In keeping with the policy intent of the MNDB scheme, the exemption should be applied for the minimum amount of time required to avoid or mitigate the anticipated harm.

Where notification would create a serious risk of harm to an individual's health or safety and the risk cannot be mitigated or removed over time, it may be appropriate to apply the exemption permanently.

A permanent exemption should only be granted in exceptional circumstances and where the agency has a high degree of confidence that harm mitigation measures, alternative methods of notification and/or the passage of time will not substantially lessen the risk. For example, a permanent exemption may be appropriate where an affected individual has a persistent, serious mental health condition and a documented history of violence or self-harm.

Where the risk of harm arises from a particular factual scenario or a temporary vulnerability, agencies should consider applying section 59 only until notification can be safely made. For example, if an individual is suffering a mental illness that puts them at risk of causing harm to themselves or others if notified of a breach, consideration should be given to whether that mental illness is episodic or likely to resolve, and whether notification obligations could be deferred until the individual is well enough to safely receive notification.

### *Notifying the Information Commissioner*

If an agency relies on the serious risk of harm exemption in section 59, the agency must, in addition to its notification obligations under section 51, give written notice to the Information Commissioner setting out:

- that the agency is relying on the exemption and the extent to which it is relying on it, e.g., to not notify only a sub-class of affected individuals
- whether the exemption is temporary or permanent; and
- if temporary, the expected duration of the exemption.

OIC recommends that agencies also include the following information in their notice, where practicable to do so:

- the number of people to whom the exemption is applied
- the total number of people affected by the breach
- the nature of the serious risk of harm to health or safety expected to arise from notification
- an explanation of why the risk arising from notifying affected individuals outweighs the risk of not notifying

- the nature and age of information the agency relied on to form its reasonable belief; and
- whether agency records were searched to assess the impact of notification and the grounds on which the search was authorised.

This can be a high-level summary and must not include any personal information. The Information Commissioner may seek further information from an agency in relation to a suspected eligible data breach if required.

### 3.1.3. Compromise to cybersecurity

Section 60 exempts an agency from the obligation to notify an individual under section 53, to the extent that complying with that notification obligation is likely to:

- compromise or worsen the agency's cybersecurity; or
- lead to further data breaches.

Exemption under section 60 is temporary. It only applies for the period that notification to individuals is likely to result in either of the above outcomes.

'Cybersecurity' is not defined in the IP Act. The Queensland Government's Cyber Security Hazard Plan uses the relevant International Standard definition 'actions required to preclude unauthorised use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets'.[5]

The cybersecurity exemption in section 60 requires that notification would likely have a detrimental impact on these measures. There is no specific threshold or degree to which an agency's cybersecurity must be negatively affected to trigger section 60, however the effect must be non-trivial.

Before relying on section 60, the agency should be satisfied that there is a real risk that notification would compromise or worsen the agency's cybersecurity or lead to a further data breach. A mere possibility will not be sufficient. It must be more likely than not to occur. Exemptions under this section should be tightly framed and exercised for the least amount of time necessary to avoid cybersecurity detriment, or further data breaches. Another important point is that the likelihood of notification leading to further data breaches is not specific to further eligible data breaches.

The Information Commissioner recommends that departments, Ministers, statutory bodies and other State government agencies should consider seeking advice from the Queensland Government Cybersecurity Unit when contemplating use of this exemption. Local government, universities, and other non-State agencies should consult with their internal or external cybersecurity specialists.

[5] International Standard: IECT/TS 62443-1-1 ed. 1.0, as quoted in the Queensland Government Cyber Security Hazard Plan, page 6.

Circumstances where notification would likely compromise or worsen an agency's cybersecurity or lead to further data breaches could include:

- Where notification could lead to further unauthorised access to, or disclosure of information. For example, where a system upgrade reconfigures access restrictions, making personal information available online to users who should not be able to access it, and the access restrictions have not yet been rectified, notification could alert people to the issue and result in further unauthorised access. In this example, it is likely the exemption would only apply for a short period while containment and mitigation activities were undertaken by the agency.
- Where the notification could allow the breach, or a similar breach, to be replicated. For example, if the breach was caused by a cyber-attack which took advantage of a system vulnerability or a new or emerging cyber method, and steps to protect the system from similar attacks have not been finalised, notification could result in compromising the agency's cyber security, and also lead to further data breaches.

### *When agencies could choose not to rely on the exemption*

When deciding whether to rely on section 60, agencies should consider whether there are options available to notify affected individuals without increasing risk to the agency. It may be possible to comply with the notification obligations without revealing specific details of how the breach occurred, or the actions the agency is conducting to contain or mitigate the impact of the breach. For example, a notification could include a high-level statement that the breach occurred due to a cyberattack on agency systems, without providing detailed information on the methods used or the vulnerabilities exploited.

If an agency takes this approach, it may be appropriate to advise individuals that further information will be provided as investigation and remedial action is undertaken by the agency.

### *Resolving any cybersecurity flaws or weaknesses giving rise to the exemption*

Exemption from notification to individuals under section 60 is only temporary. Agencies should address any cybersecurity or information security weaknesses as promptly as possible, so as to mitigate any risks giving rise to reliance on the cybersecurity exemption and permit notification as soon as is possible.

### *Notifying the Information Commissioner*

An agency relying on the cybersecurity exemption must, in addition to its notification obligations under section 51, also give written notice to the Information Commissioner stating:

- the agency is exempt from complying with notification obligations under the scheme; and
- when it expects the exemption will no longer apply; and
- how the application of the exemption will be reviewed.

The agency must also review the application of the exemption for each month during the period it is relying on the exemption and provide the Information Commissioner with a summary of the monthly review as soon as practicable.

To assist the Information Commissioner with assessing the notification, OIC recommends that agencies should also include the following information in their notice, if practicable to do so:

- the number of individuals to whom the exemption has been applied
- an explanation of why notification is likely to compromise or worsen the agency's cybersecurity or lead to further breaches
- confirm whether the agency has consulted with the Queensland Government Cybersecurity Unit or, for non-State government agencies, its cybersecurity adviser; and
- an explanation of the timelines and work planned to remedy the issue and enable notification.

The Information Commissioner may seek further information from an agency in relation to a suspected eligible data breach if required.

#### *Monthly review*

Issues that may be considered during the mandatory monthly review of the use of the cybersecurity exemption could include considering whether:

- the risks identified during the initial assessment continue to apply
- mitigation action removed the risk to agency cybersecurity
- notification to affected individuals is still likely to compromise or worsen the agency's cybersecurity, or lead to further data breaches
- mitigation activities can be completed within the estimated timeframe; and
- the timeframe of the exemption should be amended.

The agency must give the Information Commissioner a summary of every review as soon as practicable after the review is completed.

## 3.2. Exemptions from notification to both the Information Commissioner and individuals

### 3.2.1. Investigations and proceedings

Section 55 exempts an agency from notifying both individuals and the Information Commissioner to the extent that providing notifications otherwise required would likely prejudice:

- an investigation that could lead to the prosecution of an offence; or
- proceedings before a court or tribunal.

There must be more than a mere possibility of the prejudice occurring; it must be more likely than not to occur.

The agency the subject of the data breach does not need to be itself conducting the investigation to rely on this exemption. It is sufficient that notifying would prejudice an investigation being conducted by another agency or entity.

This exemption is not confined to criminal investigations by law enforcement agencies such as the Queensland Police Service. It can apply to any investigation which may result in a prosecution, for example, investigations:

- by agency compliance officers into breaches of environmental regulations or permit conditions
- by local government officers into breaches of local or other laws
- investigations into breaches of liquor licensing laws; and
- into official misconduct or police misconduct which could result in prosecution.

The exemption can apply to any proceedings before any court or tribunal, regardless of jurisdiction. It does not need to be a court or tribunal of Queensland and the agency the subject of the data breach does not need have to have instigated or be involved in the proceedings.

The investigation or proceedings can be at any stage of the process. Finalised investigation or proceedings, however, would not enliven this exemption.

Before relying on this exemption, agencies should carefully whether it is possible to undertake notification under section 52 or 53 in a manner that would avoid likely prejudice to relevant investigation or proceedings. If an agency can provide some of the information required under sections 52 and 53, without causing the anticipated prejudice, the exemption will not apply to that information.

### 3.2.2. Multiple agency breach

If a data breach involves more than one agency, an agency may be able to rely on section 56 to not notify individuals and the Commissioner. Section 56 will apply where:

- all of the personal information the subject of the breach is also the subject of a data breach of one or more other agencies;[6] and
- at least one of the other agencies is undertaking assessment[7] and is required to notify individuals and the Commissioner[8] in relation to the data breach.

Section 56 does not apply where the other entity or entities involved in the breach are not agencies as defined in the IP Act. In those circumstances, the agency must comply with its notification obligations, even if another entity, including an

[6] Under section 48(5) .
[7] Under section 48(2)(b) and (3).
[8] Section 56(1)(b).

agency of the Commonwealth or another state or territory, was also required to notify affected individuals under Commonwealth or other law.

Where a breach involves multiple agencies, the agencies should consult with each other to determine which agency will be responsible for assessment and notification of the data breach. Agencies should work together during the assessment process to ensure all affected individuals are identified.

The notification should identify all agencies involved in the breach and include a central contact for further enquiries.

Agencies relying on section 56 should ensure they assess the data breach in terms of mitigating future or current risks, preventing future data breaches, and identifying if the data breach is also a breach of another law, or if they may have non-IP Act obligations to notify or mitigate.

Section 56 does not remove the agency's obligation to update its data breach register with details of the breach.

### 3.2.3. Inconsistency with confidentiality and secrecy provisions

Most agencies are subject to confidentiality or secrecy provisions in addition to their obligations under the IP Act. These may be contained in agency-specific legislation or in laws that apply to certain kinds of information, regardless of who holds it, or certain actions or functions, regardless of who undertakes them.

Under section 58, if notifying individuals or the Commissioner would be inconsistent with a provision of a Commonwealth or State Act that prohibits or regulates the use or disclosure of the information, agencies are not required to notify in relation to that information.

Careful consideration must be given to the relevant provision and its specifics to determine if and how much of the information required by section 52 or 53 would breach the relevant provisions if it was provided to individuals or the Commissioner. If an agency can provide some of the required information without breaching the relevant provisions, the exemption will not apply to that information.

**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*