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 – Data Breach Registers and Policies

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.

1.0 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 certain individuals of eligible data breaches. As part of the scheme, agencies are also:

- required to publish a data breach policy, which outlines an agency's overall strategy for managing data breaches.
- maintain an internal register of eligible data breaches.

This guideline is designed to assist Queensland government agencies to understand their data breach policy and eligible data breach register obligations under the MNDB scheme. It should be read in conjunction with the ***Mandatory Notification of Data Breach***, and ***MNDB Exemptions*** guidelines.

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

[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*.

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.

2.0 Key Definitions

Key definitions and concepts are discussed in detail in OIC's ***Mandatory Notification of Data Breach*** guideline. A summary of concepts relevant to agency data breach policy and register obligations as discussed in this guideline is set out below.

2.1 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.

2.2 'Data breach' and 'eligible data breach'

A 'data breach' of an agency means either of the following in relation to information held by the 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.[3]

The above definition encompasses *any* information held by an agency. Under section 47, for a data breach to be an '**eligible data breach**' triggering notification and 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 or disclosure of the information is likely to result in serious harm to an individual.

2.3 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

[3] Schedule 5.

- evaluating the likelihood of 'serious harm' for the purposes of assessing whether a data breach comprises an eligible data breach attracting notification obligations.

3. Data breach registers

Section 72 requires agencies to keep an internal register of eligible data breaches. The register must include the specific information required by section 72(2), as follows:

- a description of the eligible data breach, including the type of data breach under section 47
- the date the agency gave a statement to the Information Commissioner about the eligible data breach[4] and the date any additional information was provided to the Commissioner[5]
- if individuals were directly notified about the eligible data breach,[6] the register must include the individuals who were notified and the date and method by which they were notified
- if the agency relied on an exemption[7] exempting notification to either the Information Commissioner or individuals, details of the exemption
- details of the steps taken by the agency to contain the eligible data breach[8] and mitigate its harm;[9] and
- details of the actions taken by the agency to prevent future data breaches of a similar kind occurring.

Depending on the circumstances, agencies may find it useful to include additional information about a data breach in the register, for example:

- if an eligible data breach is also a breach of another Act, details of that Act; or
- if the agency was required by contract, another law, or circumstances to notify an external party, details of that party and the date of notification.

In addition to being a requirement under the MNDB scheme, maintaining an eligible data breach register will contribute to accurate record keeping and reporting processes. Data from the register may also assist with tracking and analysing data breach risk and reviewing the efficacy of response methods. This information will also assist agencies in responding to requests for information from the Information Commissioner.

Appendix A contains an example eligible data breach register to assist agencies to develop a register applicable to individual agency circumstances.

[4] Under section 51.
[5] Under section 52.
[6] Under section 53(1)(a) or (b).
[7] Under chapter 3A, part 3, division 3.
[8] Under section 48(2)(a) or (4)(a).
[9] Under section 48(4)(a).

4. Data Breach Policies

Section 73 requires agencies to prepare and publish a Data Breach Policy (**DBP**) outlining how it will respond to a data breach, including a suspected eligible data breach of the agency. It is important to note that the obligation publish a DBP includes data breaches generally. As noted above, the definition of data breach in schedule 5 of the IP Act refers to breaches involving any agency information, and not just those that meet the 'eligible data breach' threshold prescribed in section 47.

4.1. What is a DBP and what are the benefits?

A DBP is a documented policy or plan setting out the procedures to be followed in the event an agency experiences a data breach, including a breach that is a suspected eligible data breach. It should also establish the roles and responsibilities of agency staff in relation to responding to and managing a breach.

Data breaches can vary in size and complexity, and the consequences can be significant for individuals whose information is involved. The range of actual or potential harms they can cause includes financial fraud, identity theft, damage to reputation, violence, or psychological harms.

Agencies may also experience serious consequences as a result of a data breach. Depending on the data or information involved, breaches may have negative impacts on an agency's reputation, finances, interests, or operations. Data breaches can also result in a loss of confidence and trust in an agency, including in the service it provides.

Having a robust, documented and operationalised DBP can facilitate a timely and effective response to a data breach, in turn avoiding or mitigating potential harms to affected individuals, and reducing the risks to agencies.

4.2. Publication of the DBP

Agencies are required to publish their DBP on an accessible agency website.[10] This will generally be the agency's website, but if the agency does not have a website, it can be included on the website of another appropriate agency. For example, Ministerial DBPs could be published on the departmental website.

Agencies should link to their DBP policy from their Queensland Privacy Principles Policy (**QPP Policy**)[11] and intranet or other central staff repository, and ensure all staff know how to access the policy.

4.3. What should a DBP include?

A DBP should set out an agency's plan for dealing with data breaches from start to finish. A clear and precise DBP will enable agencies to:

[10] Section 73(2).
[11] Under QPP 1.3, all agencies must have a clearly expressed and up-to-date 'QPP privacy policy'.

- prepare for, contain, assess, respond to and report on data breaches at the appropriate level and in a timely fashion
- identify who in the agency is responsible for taking what action in response to a data breach
- take action to mitigate potential harm to individuals and the agency; and
- meet obligations under the IP Act.

At a minimum, a DBP should include:

1. The agency's preparations for responding to a data breach.
2. A definition of what constitutes a breach, ensuring consistency with the statutory definitions of 'data breach' and 'eligible data breach' set out in schedule 5 and section 47 respectively.
3. The agency's strategy for containing, assessing, and managing eligible and suspected eligible data breaches.
4. How notification obligations will be met, in the event a data breach is assessed as an eligible data breach.
5. A description of the roles and responsibilities of staff members.
6. Record keeping requirements.
7. Post-breach review and evaluation procedures.

The checklist at Appendix B will help agencies ensure their DBP addresses all relevant issues.

4.4. The agency's preparations for responding to a data breach.

A DBP should provide a high-level outline of the actions the agency has taken to prepare for a data breach, including how these actions fit within the agency's broader systems, policies, and procedures, e.g., cyber response, general incident or emergency management processes, communications strategies, and risk management frameworks.

The DBP should also include the key controls, systems, and processes that the agency has established for expeditiously identifying suspected or actual data breaches and ensuring data breaches are effectively managed.

Training and awareness

Having well-trained and risk-aware staff contributes to a strong frontline defence against privacy risks, including from data breaches involving personal information. Data breach reporting by the Office of the Australian Information Commissioner indicates that breaches caused by human error are a significant component of all breaches involving government agencies.[12] Prompt identification by staff of

[12] Office of the Australian Information Commissioner, February 2024, "Notifiable data breaches report - July to December 2023", page 34, Notifiable data breaches report July to December 2023 (oaic.gov.au).

breaches and timely reporting is also an important factor in ensuring agencies can expeditiously respond to and manage breaches.

An agency's DBP should outline its approach to staff training and awareness in identifying, responding to, and managing data breaches, and any training or awareness activities about other aspects of privacy protection, e.g., enhancing staff awareness of privacy and cyber principles and current threat trends.

Processes for identifying and reporting breaches

Developing and documenting processes for promptly detecting data breaches will improve the chances of an agency being able to contain a breach and mitigate potential harms.

An agency's DBP should clearly explain how internal staff and external entities, e.g., the public or another agency, can report an actual or suspected data breach. The DBP should also outline the agency's processes for identifying data breaches, however this should not include details of specific controls which could place the agency at additional risk.

The appropriate processes for identifying and preventing data breaches will depend on the size and sophistication of an agency, its information holdings, and its security program and controls, but could include:

- technical controls (such as Data Loss Prevention tools)
- monitoring services (such as dark web monitoring, or social media monitoring)
- audits and reviews; and
- staff training and awareness.

Service providers and contract provisions

Agencies often outsource functions to external service providers or another agency (for example, payroll or IT services). These relationships are usually covered by legally binding contracts, memorandums of understanding or non-disclosure agreements.

Depending on the agreement and service, the service provider may be bound to comply with aspects of the IP Act,[13] although the application of the MNDB scheme is limited to agencies.[14] Regardless of whether the service provider is bound to the IP Act, agencies may wish to consider including data breach management and notification obligations in service provider contracts and agreements.

The DBP should include information about any contractual controls and how the agency monitors and manages service providers to ensure compliance.

[13] See sections 34 to 37.
[14] Section 46.

Testing and review schedule

Agencies should consider regular testing and review of the DBP to ensure it is operationally effective, up to date, and properly considers internal agency structure and function, and the changeability of the external threat environment.

Regular testing will also contribute to staff understanding their roles and responsibilities and becoming familiar with escalation procedures for more complex breach incidents. It will also allow for the checking of response processes, such as contact numbers, approval processes and reporting lines to ensure that they are current.

DBPs should be reviewed, tested, and updated at least annually, but agencies should consider developing a schedule for reviewing and updating their DBPs appropriate to their specific agency. The testing and review schedule should be set out in the DBP.

Alignment with other policies

A DBP should align with, and cross reference existing agency policies and procedures, such as cyber security response plans and QPP Policies. If an agency has existing incident or crisis management processes, the DBP should be integrated into those processes as well.

A DBP should also align to Queensland government information security reporting and incident response protocols.

4.5. Defining and identifying a data breach

A DBP should include a clear explanation of what a data breach is and how a data breach may occur. The explanation should be consistent with both the definition of data breach in schedule 5 of the IP Act, and the definition of eligible data breach in section 47. The DBP should also explain that identifying, assessing, and responding to data breaches must be conducted on a case-by-case basis to account for the different type of breaches that may occur.

To assist agency staff with understanding what constitutes a data breach, including an eligible data breach, it may be helpful to cover different types of data breach. This should include those that result from deliberate or accidental actions, and also explain that breaches can occur in a range of different ways, e.g., loss or theft of physical devices, misconfiguration or overprovisioning of access to systems, inadvertent disclosure, deliberate disclosure, social engineering or hacking.

Providing examples or scenarios which are relevant to the operating context of the agency will also improve staff understanding and increase the likelihood that data breaches will be identified promptly. Scenarios are also likely to help raise awareness of high-risk activities and processes which could lead to a breach. For example, an agency that handles a large amount of health information could provide examples or scenarios touching on the actual ways that health information is collected, used, stored, and disclosed in practice, reflecting any known risk factors for that agency. This will further help agency staff identify how

a breach might impact the agency, its functions, and the individuals whose information it handles.

4.6. The agency's strategy for containing, assessing, and mitigating eligible data breaches.

A DBP should outline the steps an agency will take to respond to a data breach, including a suspected eligible data breach.

Plan to contain, mitigate harm, assess, notify and prevent

To help ensure responses to data breaches are easily and quickly put into action, the DBP should clearly outline the agency's process for:

1. Initial identification and evaluation of suspected breaches and breach reports.
2. Containing a breach or suspected breach to minimise any harms.
3. Taking steps to mitigate any harms which may result from the breach. The plan should also make clear that the requirements to contain and mitigate are ongoing obligations which continue while the breach is being managed.
4. Assessing or evaluating the information involved in the breach and the risks associated with the breach, so as to determine next steps. This should also include steps to assess whether the breach is an eligible data breach as required under the MNDB scheme, including a list of factors which should be considered in this assessment process.
5. Notifying individuals and the Information Commissioner if the breach is assessed as an eligible data breach.
6. Post incident review and preventative efforts, based on the type and seriousness of the breach.

Where any of these processes require a decision to be made on how to proceed with managing the breach response, the DBP should identify who is responsible for making the decision.

Strategies for breaches involving more than one agency

The DBP should address strategies for managing, responding to, and providing notice of data breaches involving other agencies.[15]

This could include documenting key contacts and defining roles and responsibilities regarding assessment, remediation, information flow, and notification to affected individuals and the Information Commissioner.[16]

[15] Section 48(4) provides that where an agency becomes aware an eligible or suspected eligible data breach may affect another agency, the first agency must give that other agency written notice of the breach.
[16] This is particularly important, should an agency intend to rely on the exemption prescribed in section 56 permitting non-compliance with MNDB obligations where an eligible data breach involves more than one agency.

4.7. Notification strategy

The DBP should include a clear notification strategy that is consistent with sections 51 to 54 and enables quick and effective communication with affected individuals and the Information Commissioner.

The strategy should outline:

- responsibilities for implementing the notification strategy
- how to determine when affected individuals or organisations must be notified
- key contacts for communications
- responsibilities for notifying the Information Commissioner, consistently with the obligations imposed by sections 51 and 52
- how affected individuals will be contacted and notified in accordance with section 53, and communications with affected individuals managed – including how any inquiries will be made of disclosing agencies under section 54, and
- responsibilities for consulting with any other external stakeholders (such as other agencies who may be impacted by the data breach).

Additional obligations or reporting

Agencies may be required by contract, other laws, or the circumstances of the breach to take additional specific steps in response to a data breach. These could include taking specific containment or remediation actions or engaging with or notifying external stakeholders if a data breach occurs.

Depending on the circumstances of the data breach and the categories of data involved, agencies may need to report to or engage with:

- Queensland Police Service
- Crime and Corruption Commission Queensland
- Queensland Government Chief Information Officer
- The Office of the Australian Information Commissioner
- Australian Federal Police
- The Australian Taxation Office
- The Australian Digital Health Agency
- The Australian Cyber Security Centre
- Any third-party organisations or agencies whose data may be affected
- Financial services providers
- Professional associations, regulatory bodies, or insurers; or
- Foreign regulatory agencies.

Agencies may also wish to canvass media and general communications strategies in their DBP.

A DBP should outline the situations in which external reporting or engagement is necessary. If reporting is discretionary, it should include guidance on making the decision.

4.8. Roles and responsibilities

Clearly establishing required roles and responsibilities is important to ensure prompt responses to a data breach.

A DBP should include clear guidance for agency heads, executive officers, privacy officers, staff generally and any other relevant internal party that explains their roles and functions in identifying, reporting, and responding to a breach or suspected breach.

The DBP should also identify the breach response team including:

- roles and functions within the team
- subject matter expertise required in the team—this could include incident response specialists, legal, communications, cybersecurity, physical security, human resources, key agency operations staff and key outsourcing/relationship managers; and
- who in the team is responsible for dealing with the relevant elements of the breach.

The DBP should contain escalation procedures for staff, including how to immediately report a suspected breach, when line managers can handle a breach, and the circumstances in which a breach should be escalated to the response team, generally based on severity or the level of response required.

It should also identify who is responsible for:

- making escalation decisions at each level
- assessing and identifying the agency's reporting obligations, including notification to the Information Commissioner, individuals, external stakeholders, or other bodies
- maintaining, testing, and updating the DBP
- data breach recordkeeping; and
- post-breach review and evaluation.

Capability, expertise, and resourcing

Prompt action is critical when responding to a data breach. Response strategies will only be effective if they can be quickly and effectively implemented and actioned. This depends on staff, or other people such as external contractors, having the relevant skillsets and being available to deal with the breach.

A DBP should outline the agency's strategy for ensuring:

- That it has resourcing and personnel with the necessary expertise to respond effectively. To be properly prepared for complex incidents, this may involve engaging (in advance) an outsourced cyber incident response service provider.
- That agency staff who are likely to be required to assess a data breach or make an escalation decision, are trained and capable of adequately assessing the breach and its impact. Where possible, these staff should be involved in policy testing and review processes.

4.9. Recordkeeping

The agency's processes for documenting breach and suspected breach management and response should be included in the DBP. Keeping appropriate records of data breach response and management will provide evidence of how the agency actually responds to breaches or suspected breaches, including those breaches that do not get escalated to the breach response team, or those that do not meet the eligible data breach threshold under the MNDB scheme.

Accurate records will also assist in tracking and analysing data breaches, including the effectiveness of the response methods. This may enable agencies to identify and remedy weaknesses in security or processes that present a higher risk of error.

Recordkeeping responsibility should be clarified in the DBP. This should include:

- Assigning responsibility for keeping the register of eligible data breaches required under section 72 (discussed above); and
- Publishing, monitoring and reviewing the currency of public notifications of data breaches published to the agency website under section 53(1)(c).

4.10. Post-breach review and evaluation

Understanding what processes worked well, how issues were handled, and areas for improvement in the management of a data breach is an important component of the data breach administration process. This is particularly relevant to mitigating future risks, preventing reoccurrence or similar breaches, and improving personal information handling processes in line with expectations of the community and regulators.

DBPs should include:

- A strategy to identify and remediate any processes or weaknesses in data handing that may have contributed to the breach.
- A post-response assessment of how the agency responded to the breach and the effectiveness of the DBP.

Post-breach review and evaluation will identify any changes needed to process or procedures and is a key part of ensuring agencies can proactively and effectively manage data breaches.

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 16 August 2024

Appendix A – Eligible Data Breach Register example

Register of Eligible Data Breaches (**EDB**) (as required by section 72 *Information Privacy Act 2009*)							
Date of Breach	Description of EDB / type of data breach	Date statement provided to OIC	Date additional information supplied to OIC or N/A	Individuals notified, including date and method	Details of any exemption(s) relied on, or N/A	Steps taken to contain and mitigate	Actions taken to prevent similar breaches

Appendix B – Checklist for Data Breach Policy (DBP)

Information to be included	Yes/No	Comments
Steps the agency has taken to prepare for a data breach		
What a data breach is and how staff can identify one		
The agency's plan for containing, assessing, and managing data breaches		
Processes that outline when and how individuals are notified		
Processes for responding to incidents that involve another entity		
Circumstances in which external engagement, including with law enforcement, regulators (such as the Information Commissioner), or other third parties may be necessary		
Requirements under agreements with third parties such as insurance policies or service agreements		
A clear communication strategy		
Clear escalation procedures and reporting lines for suspected data breaches		
Members of the data breach response team, including roles, reporting lines and responsibilities		
Details of any relevant external expertise or resources and when they should be engaged		
A record-keeping policy to ensure that breaches are documented		
A schedule for regular review and testing of the DBP		
A review process for identifying and addressing any root causes that contributed to the breach		
A system for a post-breach review and assessment of the data breach response and the effectiveness of the data breach policy		