Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – *Information Privacy Act 2009*

MNDB scheme – Assessing a Data Breach

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.

Table of contents

1. Introduction 2

2. MNDB Key concepts and definitions 3

3. Initial consideration of suspected eligible data breaches 9

4. Assessment of suspected eligible data breaches 9

4.1 Assessment timeframes, including extensions of time 10

4.2 Data breaches and other agencies 10

4.3 How to conduct the assessment 10

4.3.1 Gather information 11

4.3.2 Analysis 11

4.3.3 Assessing cyber related breaches 17

4.3.4 Make a decision 18

5. Further Information 18

Figure 1. Three step process to identify data breach eligibility 19

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 will impose the following obligations on agencies:[2]

- 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, and the agency only holds a reasonable suspicion that the data breach is eligible, it must rapidly **assess** (within 30 days),[3] whether there are reasonable grounds to believe the data breach is an eligible data breach of the agency.
- 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
    - **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 is intended to help agencies understand how to identify if a data breach of the agency meets the definition of eligible data breach under the MNDB scheme. It will also assist agencies to decide how sure they are that a breach is eligible, and consequently which of the MNDB obligations apply. It also explains the process for conducting an assessment to identify whether there are reasonable grounds to believe a data breach is eligible as required by section 48(2)(b).

[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. Noting the 12-month delay for local government. 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] Section 48.
[4] Section 51.
[5] Section 53.
[6] Section 73.
[7] Section 72.

1.2. Other MNDB resources

Information contained in this guideline should be read in conjunction with the ***MNDB Scheme***, ***MNDB Exemptions*** and ***MNDB Data breach registers and policies*** guidelines.

2. MNDB Key concepts and definitions

This section of the guideline discusses some of the key concepts and definitions which are central to the MNDB scheme, including:

- personal information
- when personal information is held by an agency
- data breach
- eligible data breach
- unauthorised access
- unauthorised disclosure
- loss
- serious harm
- determining the likelihood of serious harm, and
- the concept of reasonableness.

Understanding and recognising these concepts and definitions is critical to an agency taking the steps required to meet the obligations under the 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. When is 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.*

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, 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, 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*?

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

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.*[8]

Scenario:

An agency identifies that an unknown party has gained unauthorised access to the agency's financial information. Upon assessment, the agency identifies that no personal information was subject to the data breach incident. This scenario is a ***data breach*** only.

2.4. What is an *eligible data breach*?

For a data breach to be assessed as an '*eligible data breach*' triggering 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').[9]

[8] Schedule 5.
[9] Section 47.

Scenario: Eligible data breach example

Via a cyber attack, an unknown threat actor has gained unauthorised access to an agency ICT system. The threat actor has gained access to the agency's financial information. The agency is aware that the financial information includes personal banking information and details of approximately 125 agency employees. This personal information is the type of information that is often used by threat actors to commit identity theft and other related financial crimes.

Based on these circumstances, the agency identifies that serious harm in the form of financial loss is likely for at least some (if not all) of the individuals to whom the personal information relates.

2.5. Understanding unauthorised access, unauthorised disclosure, and loss

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

- Within an agency, where an employee browses agency records relating to a family member, a neighbour, or a celebrity without a legitimate purpose.
- Between agencies, where a team at one agency is provided with access to systems and data at another 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.

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 incidents. The last two dot point examples of 'unauthorised access' above would likely also comprise unauthorised disclosures. By way of further 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.

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 an eligible data breach only where such loss is likely to result in unauthorised access or disclosure of the information, and this is likely to result in serious harm to an individual to whom the personal information relates. If the personal information is inaccessible, or is known to have been destroyed, it will be unlikely that an eligible 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 at a cafe but is handed in and the agency can 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.

2.6. Serious Harm

Serious harm is a type of harm that can potentially eventuate from a data breach. This can 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:

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

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

The above definition is not exhaustive, and there are other kinds of harm that 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.

Serious Harm - Likely to result

For a data breach involving personal information to be considered likely to result in serious harm, an objective analysis of the circumstances must indicate that serious harm is likely to occur to at least one of the individuals whose information has been accessed, disclosed or lost as a result of the breach. The term likely to result in the definition of an eligible data breach means that the risk of serious harm to an individual whose personal information is involved in the breach is more probable than not, as opposed to it being merely possible.[10]

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 one or some of those individuals.

2.7. Determining the likelihood of serious harm

When agencies experience a data breach involving personal information, they will be required to consider whether the breach is likely to result in serious harm to an individual to whom the personal information relates. When deciding on the likelihood of serious harm, agencies must have regard to the list of matters in section 47(2), and any other relevant matters as discussed in Part 4 of this guideline.

After considering all of these factors, agencies will need to decide if their analysis indicates that there is a likelihood of serious harm – or in other words – whether it is **more probable than not** that serious harm will occur. This is the threshold for a data breach to meet the definition of an eligible data breach – which then enlivens the obligations under the scheme. Parts 3 and 4 of this guideline provide information to assist agencies to conduct this analysis and decision making.

[10] See 'Data breach preparation and response', Office of Australian Information Commissioner website, https://www.oaic.gov.au/__data/assets/pdf_file/0023/214637/NDB-Team-Data-Breach-Preparation-and-Response-guide-June-2024.pdf, p.33.

2.8. Reasonable - Reasonably

The terms reasonable and reasonably are relevant to multiple components of the MNDB scheme. These terms are not defined in the Act, and thus will bear their ordinary meaning. Determining reasonableness requires a balanced and objective view to be brought to the question or situation. A fair, proper, and moderate approach must be taken, to ensure that all relevant factors are considered and properly balanced.

Whether or not there are reasonable grounds to suspect or believe a data breach is an eligible data breach will depend on the facts specific to each incident. When considering the existence of reasonable grounds to support an action, the High Court has observed that it ''requires the existence of facts which are sufficient to [persuade] a reasonable person', and that it 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'.[11] A 'reasonable person' is a hypothetical individual who is properly informed with sound judgement.

Reasonably Suspicion

The High Court has also noted that '[t]he facts which can reasonably ground a suspicion may be quite insufficient to reasonably ground a belief, yet some factual basis for the suspicion must be shown'.[12] This means that a reasonable suspicion requires some facts or evidence to support the suspicion, but this threshold falls short of requiring sufficient facts to support a belief. Although dealing with reasonable suspicion regarding police powers of stop and search, the NSW case of *R v Rondo* discusses reasonable suspicion as 'involv[ing] less than a reasonable belief but more than a possibility' and that it is not arbitrary and 'some factual basis for the suspicion must be shown.' [13]

Reasonable Belief

To reach the threshold of reasonable belief, the objective circumstances must be of sufficient weight that it results in an 'inclination of the mind towards assenting to, rather than rejecting, a proposition', but there is still some room for conjecture as it does not require proof that the issue being consider actually occurred or exists.[14] In other words, a reasonable belief will be founded when, after a thorough considerable of the available facts, a reasonable person would be more inclined to assent or agree on a proposition or occurrence of an event, as opposed to rejecting the proposition or disagreeing that the event occurred.

[11] *George v Rockett* (1990) 170 CLR 104 at 112 (Mason CJ, Brennan, Deane, Dawson, Toohey, Gaudron & McHugh JJ); McKinnon v Secretary, Department of Treasury (2006) 228 CLR 423 at 430 (Gleeson CJ & Kirby J).
[12] *George v Rockett* [1990] HCA 26; (1990) 170 CLR 104, 115 (Mason CJ, Brennan, Deane, Dawson Toohey, Gaudron and McHugh JJ).
[13] *R v Rondo* [2001] NSWCCA 540 (24 December 2001) at 53.
[14] *George v Rockett* [1990] HCA 26; (1990) 170 CLR 104, 115-116 (Mason CJ, Brennan, Deane, Dawson Toohey, Gaudron and McHugh JJ).

3. Initial consideration of suspected eligible data breaches

When an agency first becomes aware of a data breach, an initial consideration will be required to identify if the breach involves personal information and whether it is likely to enliven obligations under the MNDB scheme. For data breaches involving personal information, an agency will need to objectively decide if the known circumstances support knowledge, reasonable belief or reasonable suspicion that the data breach is an eligible data breach of the agency. This is an important consideration, as it determines what MNDB obligations the agency will need to comply with.

The obligations under the scheme are enlivened when an agency knows or reasonably suspects that the data breach is an eligible data breach of the agency. When this occurs, 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.[15]

Section 48(2)(b) deals with the possibility that when a data breach is first identified, agencies may not have sufficient information to reach a level of certainty that the data breach is eligible. Where this occurs and an agency only has a reasonable suspicion of an eligible data breach, there is a requirement to rapidly assess whether there are reasonable grounds to believe the data breach is an eligible data breach of the agency.[16]

4. Assessment of suspected eligible data breaches

There will be a multitude of ways that an agency may be alerted to a data breach, including a suspected eligible data breach. Depending on the circumstances, an agency may initially only have enough information to reasonably suspect they have experienced an eligible data breach. When this occurs, agencies will need to conduct further enquiries and examinations to reach a higher level of confidence or certainty that a data breach is eligible under the scheme (or not, as the case may be). An agency's assessment and any decisions made should be recorded in writing and include the material facts of the specific breach.

The remainder of this part of the guideline discusses how an assessment should be done, including consideration of how the mandatory section 47(2) factors and other relevant matters may apply. Although this discussion is aimed at assessments being conducted pursuant to section 48(2)(b), most of the concepts also apply to the initial consideration of a data breach when it first comes to the attention of the agency as discussed at Part 3 of this guideline.

[15] Note: If the agency knows or reasonably believes there has been an eligible data breach of the agency, it must also comply with the obligations to notify the Information Commissioner and particular individuals.
[16] As discussed in Part 4 of this guideline, this assessment must be completed within 30 days, although this can be extended if reasonably required – see sections 48(3) and 49 of the IP Act.

4.1. Assessment timeframes, including extensions of time

Data breach assessments being conducted as a result of an agency having a reasonable suspicion that the breach is an eligible data breach must be completed within ***30 days*** after the suspicion was formed***.***

In the event an agency is satisfied the assessment cannot reasonably be completed within this 30 day period, the agency may extend the period within which the assessment must be completed. Any such extension must be no longer than the period reasonably required for the agency to complete the assessment. [17]

If the period is extended, within the initial 30-day period, the agency must start the assessment, and give written notice to the Information Commissioner stating;

- *that the assessment has started,*
- *the period within which the assessment must be completed has been extended under section 49, and*
- *The day this extended period ends.*

The Information Commissioner may ask the agency to provide further information or updates about the progress of the assessment during the extension period.

4.2. Data breaches and other agencies

If at any time, an agency becomes aware that the data breach affects another agency, the agency must give written notice to the other agency. The written notice needs to include;

- a description of the data breach; and
- a description of the kind of personal information the subject of the data breach, without including any personal information in the description.

Where all of the personal information involved in a data beach is also the subject of a data breach of one or more other agencies, and at least one of the other agencies has undertaken to conduct the assessment in relation to the data breach, the other involved agencies do not need to conduct an assessment under sections 48(2(b)and (3). However, the requirements to contain and mitigate will still apply. [18]

4.3. How to conduct the assessment

As each data breach will involve a different set of circumstances, there is no pre-determined procedure that must be adhered to for every incident. However, assessment should generally involve:

- gathering information and evidence about the breach
- analysing this information with regard to the factors which influence the likelihood of serious harm, and

[17] Section 49.
[18] Section 48 (5).

- making a decision on whether the gathered information and analysis supports knowledge, reasonable belief or reasonable suspicion that the data breach is eligible.

4.3.1. Gather information

This will involve collecting information relevant to the circumstances of the breach, including:

- identifying the cause of the breach
- identifying the types of personal information that has been accessed, disclosed or lost
- investigating IT systems through assessing audit logs or other records
- identifying the extent of the breach, and
- contacting relevant stakeholders.

4.3.2. Analysis

Analysis involves the review of the collected information to identify the context of the breach, including the type of information involved, and the amount of information and number of individuals who may be affected.

The analysis should also consider the potential impact on affected individuals, including:

- actual or potential harms to individuals whose personal information is involved in the breach
- the seriousness of that harm, and
- the likelihood that the harm will occur.

When reviewing and analysing the collected information, agencies must have regard to the stated matters listed in Section 47(2) of the IP Act, which 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.

The term “any other relevant matter” indicates that the list above is not exhaustive, and the analysis must consider the specific circumstances of the breach. Other relevant matters to consider may include (but not be limited to):

- 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.

These matters are considered below. The examples are provided to assist with understanding and should be read with the stipulation that data breaches must be assessed after an assessment of all the factors relevant to the specific incident.

The kind of personal information accessed, disclosed or lost

Regard must be had to the kind of personal information involved in the breach, with the understanding that the compromise of some types of personal information may pose a higher risk of harm. For example, where a data breach involves identity credentials or documents, such as passports, driver licences or Medicare cards, agencies should be alert to a heightened risk of harm. This type of information can be used by those with criminal intent to commit offences such as identity theft and fraud, which can obviously cause significant harm to an individual through financial loss, impact on credit ratings, and potentially mental health complications from being the victim of such offending. As a result of this heightened risk, a breach involving this type of information may be more likely to result in serious harm when compared with a breach involving other types of information such as an email address or mobile phone number. Financial information, such as credit card numbers or banking account details are another category of information which may be more likely to result in serious harm through the individual becoming a victim of crimes such as fraud or other types of financial crime.

The sensitivity of the personal information

The IP Act contains specific rules for the collection, use and disclosure of sensitive information, such as racial or ethnic origin, political opinions or associations, religious beliefs or affiliations, and sexual orientation or practices. These rules recognise that there may be specific risks to individuals that may arise from unauthorised use or disclosure, or loss of these types of information. Data breaches involving these types of personal information may be more likely to result in serious harm.

Additionally, there are other types of information that may not meet the IP Act definition of sensitive information, but depending on the circumstances may lead to more significant risks of harm. As discussed above, identity information which can be misused in fraud related activities would fit within this category. Another example could be personal information related to a certain vulnerability which could result in an individual suffering some form of prejudice it was made public.

It is also true that information which is considered in the same class may present different levels of risk depending on the circumstances. This is apparent when considering health information which encompasses a very broad range of different types of information, and the "sensitivity" or risk of harm will vary depending on the type of information and the circumstances of the breach. For example, historical health information related to treatment for a minor injury a number of years ago may not necessarily indicate a significant risk of harm, but if this type of information is relevant to a person's employment and could negatively affect their career if misused, this may change the assessment of risk.

Whether the personal information is protected by one or more security measures

This factor concerns the different types of security measures which may be involved in the assessment of data breaches. Generally, robust encryption will decrease the risk of serious harm, but other measures, such as controls restricting access and a capability to remotely remove or wipe data, can also affect the risks of harm. When considering the effect of security measures, agencies should take into account both the strength or effectiveness of the measure, and the potential ability of the person in possession of the information to circumvent the measure. For example, if encrypted data is lost or accidentally disclosed to the wrong recipient, the perceived capability or motive of this person to circumvent the encryption will lead to a different assessment of risk when compared to a situation involving a hacker gaining access to information which is protected by a weak security measure.

The likelihood that any security measures could be overcome

As discussed above, agencies need to be aware that not all security measures will remove or significantly decrease the risk of harm. Agencies will need to assess the perceived strength of the encryption, and the anticipated abilities of any unauthorized recipient of the information to negate or circumvent the security measures. As an example, the presence of a protection due to a weak password will create a higher level of risk, when compared with protection afforded by a highly regarded industry recognised security or encryption measure.

The persons, or kinds of persons, who have obtained, or who could obtain, the personal information

If an agency has information about the identity or motives of peoples who have, or may have had, access to the personal information, this may enable a more thorough assessment of the likelihood of serious harm. For instance, personal information obtained through a targeted cyber-attack is more likely to result in serious harm to an individual, when compared to a breach which involves the same type of information being incorrectly emailed to a trusted recipient such as a law firm or another agency.

If there is a relationship between the individual to whom the personal information relates and the recipient of the information, this may increase the risk of serious harm. For example, information about a person's medical information could result in serious harm through distress or embarrassment if disclosed to a family member or work colleague. Another example could be disclosure of an address,

which may seem innocuous if disclosed to a person unrelated to the individual but may well pose a significant risk of harm if the recipient is the person's former partner and there has been a significant history of family violence.

For data breaches involving a cyber element, agencies should be alert to a higher risk of harm when compared to breaches caused by human error or a system issue. The level of complexity of a cyber breach may also be an indicator of higher degrees of criminal intent. If exfiltrated personal information is posted online following a breach, it is also dangerous to assume that the posted information is the only information that has been accessed, and consideration should be given to all the personal information which is held in the breached system. The Office of the Australian Information Commissioner (**OAIC**) has noted that trusting any assurances given by a cyber threat actor, or relying on assumptions when facts regarding a person's intent cannot be established, can result in agency's inaccurately assigning a lower risk of harm.[19] This can result in misclassifying a breach as non-eligible, and this could lead to results which do not align with the intent of the scheme.

The nature of the harm likely to result from the data breach

The types of harm that may occur as a result of a data breach will vary depending on the circumstances of the breach, including its cause, the personal information involved, and the people affected by the breach.

The different types of harm that may arise include:

Financial loss: Financial loss can occur through being a victim of identity theft or some other type of fraud. Examples include loss of money or other assets as a result of a scam, fraud or theft. It can also occur when an affected person incurs costs when responding to a data breach. This includes the costs involved in having identity documents being reissued, legal fees and services employed to cope with any psychological or medical issues arising from the incident. In cases involving physical or safety related harms, it could also include costs incurred as a result of increasing personal security, or even the costs of relocating.

Identity theft: Identity theft can result in an individual being victim to more than just financial loss, as the stress and time associated with restoring an individual back to the state before the breach can cause significant harms. Another outcome of a stolen identity can be an inability to access government services if the identify theft involves a threat actor using and taking over an individual's login details for government systems. Some examples of the range of activities that involves identity theft include:

- creation of fake government identity documents
- gaining access to a person's banking and other financial accounts
- taking over social media profiles and accounts
- opening bank accounts in the victim's name
- obtaining credit or loans in the victim's name, and

[19] OAIC, 'Notifiable data breaches report – January to June 2024', p. 18, https://www.oaic.gov.au/__data/assets/pdf_file/0013/242050/Notifiable-data-breaches-report-January-to-June-2024.pdf.

- using these above examples to conduct further criminal activity which is all linked to the victim's identity.

Emotional harm: Depending on the type of information and the specific circumstances, data breaches involving the publication of personal information may lead to different types of emotional harm. Disclosure of sensitive information, such as information relating to a person's health or a person's sexual orientation or practices, may be more likely to result in these types of harm. Harms stemming from the release of these types of information can include serious emotional distress and embarrassment, which can also result in serious detrimental impacts on mental and physical wellbeing. Another example could be information related to learning difficulties being released to members of a school community which could then result in distress and embarrassment to the involved students.

Reputational damage: Closely related to emotional harms, disclosure and misuse of personal information could result in individuals experiencing reputational damage, particularly for information which may cause embarrassment or be damaging if widely known. An example could be the misuse of personal information by an employer resulting in an individual missing out on employment or career development opportunities. Another example could be the release of information negatively affecting a person's professional or business reputation.

Physical and personal safety harms: Some data breaches may lead to risks of serious harm to an affected individual's safety or even the risk of physical harm occurring. These harms could occur where the disclosure of personal information identifies a person's home or work address, and due to the person's occupation or association with certain people, this makes them more susceptible to the risk of physical harm or being the victim of offences, such as stalking or harassment.

Domestic and family violence related harms: Data breaches also have the potential to increase the risk of harms related to domestic and family violence. An example of how this might occur is when a breach involves the inadvertent release of a domestic violence victim's new address to the perpetrator of that violence. This type of situation could result in serious harms caused through further domestic violence, including the possibility of personal injury.

Other relevant matters

As discussed above, the list of matters in section 47(2) is non-exhaustive. Some possible examples of "any other relevant matter[s]" are discussed below.

Whether a combination of different types of personal information may lead to an increased risk

Agencies should be aware that combinations of personal information may create a higher risk of serious harm when compared to the risk of harm from the release of one of the component pieces of information. An example of this could be a breach involving contact details may not result in a risk of serious harm, but if the breach also involved health related information of the same individuals, this could result in a risk of serious harm through embarrassment, prejudice or those individuals being more susceptible to being targeted in scams which use this

information to gain access to further personal information. Another example could be combinations of personal information may be used for impersonation activity, such as using a combination of name, date of birth and other contact information to circumvent identity or user verification processes to gain access to customer systems of both government agencies and private entities such as banks.

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 amount of time that has elapsed between the data breach and the agency discovering it may be relevant to the consideration of the likelihood of serious harm. For example, if the breach involves personal information being publicly available, the likelihood of serious harm to an individual will generally increase the longer the period that the information was available. One reason for this is the longer the period, the more likely the information will have been accessed or used in ways that will cause harm.

The circumstances of the individuals affected and their vulnerability or susceptibility to harm

Another factor which may be relevant to determining the likelihood of serious harm is whether the involved individuals have any vulnerabilities or personal issues which make them more susceptible to harm, and/or less likely or able to take actions to protect themselves. Traits or conditions which may make a person more susceptible or less able to take protective steps in the event of a data breach includes age, poor physical or mental health, disability or issues with literacy and comprehension. Specific vulnerabilities which may be relevant includes issues with homelessness, financial position, and also a higher susceptibility to being a target due to a person's profession. Whilst these types of consideration may happen in smaller breaches where agencies will be in a position to individually consider each individual, breaches involving larger numbers of people may require an agency to consider the possibility of some people in the affected group of individuals being more susceptible.

The circumstances in which the breach occurred

Each breach will have its own specific set of circumstances. This includes consideration of the section 47(2) factors, but also other issues, such as the actual individuals impacted, the scale or size of the breach, whether the type of breach affects the sensitivity of the information, and how the relevant factors interact and overlap to influence the level of risk. Examples of how these issues may impact risks of harm are discussed below.

The actual individuals impacted: Similar to consideration of an individual's vulnerabilities or ability to cope with the effects of a data breach, agencies should also consider whether a data breach is more likely to result in harm due to the actual individuals involved. An example could be a breach involving a person's email address, which on the face of things would generally seem innocuous, being likely to result in serious harm due to the information being disclosed to another individual with whom the involved person has a long running dispute.

The scale or size of the breach: The size of the breach, or the amount of people involved, may impact the level of risk. For breaches involving larger number of people and/or large amounts of personal information, it may be appropriate to consider that due to the large amount of people involved it is realistic to consider at least one of the involved individuals would be likely to be at risk of serious harm, unless there are other circumstances or facts that would not support this conclusion.

Whether the type of breach affects the sensitivity of the information: Another relevant factor that may occur is where the circumstances of the breach change the level of risk or sensitivity that would normally be associated with certain types of information. This could occur when an individual's name is released in association with a particular group or association. Another example could occur when a person's information is linked to treatment they have received for a physical or mental health issue.

Interaction between factors: The way relevant factors, including the section 47(2) matters, overlap and interact will also be something agencies should consider. It is possible that one factor alone may not result in a breach being assessed as likely to result in serious harm. However, when combined with other factors, particularly if certain factors increase the likelihood of risk for other factors, this interaction will be a key part of the overall consideration of risk. How this will occur practically will depend on the circumstances. As an example, consider a person's name and address being disclosed publicly. On its own this may not present a high risk of harm, but if that person has recently relocated to a new address to escape a violent family relationship, the combination and interaction of factors starts to change the assessment of risk. If that person also has medical vulnerabilities and their circumstances mean they have a diminished capacity to take their own protective steps, it is evident that the interaction between the factors can change a risk level quite dramatically.

Actions taken by the agency to reduce the risk of harm following the breach

Agencies are required to take action to reduce risks of harm from data breaches involving information held by the agency. The efficacy of these actions will be a factor to consider when assessing likelihood of serious harm. If an agency has been able to take actions which greatly reduce or remove risks of harm before any has occurred, this will be a key consideration. It is also possible that agency action removes risks for some of the involved individuals. When this occurs a data breach may still enliven obligations under the MNDB scheme, but the pool of affected individuals will be smaller.

4.3.3. Assessing cyber related breaches

Assessing data breaches caused by a cyber-attack will generally rely on agencies being able to gather and analyse digital forensic evidence. Where required, agencies should consider consulting with forensic experts for assistance in assessment. Agencies should also ensure that requirements to report breaches

and incidents to the Queensland Cyber Security Unit are met as required by the Queensland Government Enterprise Architecture.[20]

If ICT systems do not allow for forensic examination, such as audit logging or retrospective analysis of internet gateway traffic, it may be difficult to confirm whether a breach has resulted in access to systems and exfiltration of personal information. A lack of evidence should not be the sole reason for deciding that access to ICT systems has not occurred. Where agencies face this type of situation, it is recommended that assessments are conducted with the presumption that unauthorised access, and subsequent exfiltration of information has occurred. It is also recommended that, if possible, agencies consider improving their personal information security processes through investment in improving ICT systems, including enhanced incident response functionality.

4.3.4. Make a decision

After analysing the data breach as discussed above, the agency must reach a position on the likelihood of serious harm to an individual to whom the personal information relates as a result of the breach, and decide whether there are reasonable grounds to believe the data breach is an eligible data breach of the agency. If the agency is satisfied that their analysis supports a reasonable belief that there has been an eligible data breach of the agency, the obligations to notify the Information Commissioner and particular individuals may apply subject to Part 3 of chapter 3A of the IP Act.

5. Further Information

For more detailed information regarding notification to the Information Commissioner and particular individuals, see guidelines ***Mandatory Notification of Data Breach scheme*** and guideline ***MNDB – Notification under the MNDB scheme*** (in development).

Figure 1 on the next page summarises the initial consideration and assessment of suspected eligible data breaches, with a workflow that will assist agencies to identify data breach eligibility and which MNDB scheme obligations apply.

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 January 2025 and Last Updated December 2024

[20] See Queensland Government Enterprise Architecture (QGEA) | For government | Queensland Government. Specifically, the Information Security Incident Reporting Standard.

Figure 1: 3 step process to identify data breach eligibility and which MNDB scheme obligations apply

Process for identifying Mandatory Notification of Data Breach (MNDB) scheme obligations (For initial consideration and s.48 assessments)

A data breach has occurred, does it involve personal information?

Yes → MNDB scheme obligations may apply

No → MNDB scheme obligations do not apply

Gather information and determine the likelihood of serious harm, having regard to:

- The kind of personal information
- The sensitivity of the information
- Is information protected by one or more security measures?
- The likelihood measures could be overcome
- Persons (or kinds), who have obtained, or who could obtain, the personal information
- The nature of the harm likely to result from the data breach
- Depending on the circumstances, any other relevant matters, like how long information was exposed, circumstances of affected individual, how it occurred, combinations of personal information and actions taken by agency to reduce the risk of harm.

Determine knowledge, suspicion or belief of EDB and relevant obligations

Does the information indicate and/or support an Eligible Data Breach (EDB)?	Eligibility	Scheme obligations		
		Contain and mitigate	Assess	Notify
Evidence indicates only a **possibility**, (**note**: you may need to seek more information and consider containment)	Possibility			
Some evidence supporting notion of EDB. Not enough for belief, but **more than a possibility**	Reasonable suspicion	✓	✓	
Sufficient evidence to accept the notion that the breach is eligible, as opposed to rejecting it	Reasonable belief	✓		✓
Knowledge that an EBD has occurred	Knowledge	✓		✓

For more detailed information see assessment guideline and tool. Agencies should also consider non-scheme obligations.