**IPOLA RESOURCE**

**Applying the legislation –**

**Information Privacy Act 2009**

**MNDB notification template – Individuals**

**This resource does not reflect the current law.**

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

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

**Who should use this template?**

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

**Why should I utilise this template?**

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

**How to use this template**

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

***[Date]***

Dear ***[name of affected individual],***

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

**Incident Information**

Date***: ‘on or ‘between dates’***

Time: ***‘at’ or ‘between times’***

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

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

**Affected personal information**

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

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

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

**What has our agency done to contain the breach?**

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

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

**Next steps**

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

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

**Risk of harm is identity fraud including contact information**

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

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

**Risk of harm involves financial information**

* **The below are suggestions** *only* **– agencies will need to determine appropriate advice:*Contact your financial institution as soon as possible, to enable additional monitoring and security actions to your account.***
* ***Enable multi-factor authentication (if able), change your online banking password (if applicable), cancel affected debit or credit card, change your personal identification number (PIN).***
* ***Continue to review your bank statements and online banking transactions for unauthorised purchases. Report any discrepancies to your bank as soon as possible.***
* ***You may consider contacting Australia’s three credit reporting agencies (Equifax, Illion and Experian) to understand if your identity has been used to obtain credit without your knowledge. You may consider making a request for a credit ban to be put in place.***
* ***If the affected personal information relates to your tax file number of superannuation, contact the Australian Tax Office on 1800 467 033 and your superannuation fund to discuss if additional monitoring needs to be placed on your account.***

**Risk of harm involves Health Information**

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

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

Further information is also available at the Office of the Information Commissioner website [What to do if you’re affected by a privacy breach | Office of the Information Commissioner Queensland](https://www.oic.qld.gov.au/information-for/general-public/what-if-youre-affected-by-a-privacy-breach)

**Seeking more information and making a complaint**

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

***[individual or department’s name within your organisation]***

***[phone number] or [email].***

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

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

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

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

Please find website link for further information below. [Make a privacy complaint | Office of the Information Commissioner Queensland](https://www.oic.qld.gov.au/about/privacy/make-a-privacy-complaint)

Yours sincerely,

***[Name]***

***[Position/Title]***

***[Organisation name]***

**For additional IPOLA assistance, please contact the IPOLA team by email** [**IPOLA.Project@oic.qld.gov.au**](mailto: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**](mailto:enquiries@oic.qld.gov.au)

Published February 2025 and Last Updated February 2025