Applying the legislation

GUIDELINE *Information Privacy Act 2009*

Privacy Breach Management and Notification

A privacy breach occurs when there is a failure to comply with one or more of the privacy principles set out in the *Information Privacy Act 2009* (Qld) (IP Act).

Privacy breaches can occur because of a technical problem, human error, inadequate policies and training, a misunderstanding of the law, or a deliberate act. Some of the more common privacy breaches happen when personal information is lost, stolen or mistakenly disclosed (for example, a USB flash drive is lost or an email is sent to unintended recipients).

This guideline will assist agencies in managing a privacy breach, including the considerations around notifying persons whose privacy may be affected by the breach. A Privacy Breach Report Template is also available to guide you through the key steps in responding to a privacy breach and assist in your agency maintaining a record of the breach and the decisions made.

The IP Act does not impose a mandatory obligation on Queensland Government agencies to notify the Office of the Information Commissioner (OIC) or affected individuals in the event of a privacy breach. However, agencies are strongly encouraged to notify OIC of a breach. Not only can we provide advice on responding to the breach, notification also assists us to respond to any community enquiries about the breach.

OIC also strongly encourages notification to the affected individuals in appropriate circumstances as part of good privacy practice and in the interest of promoting openness and transparency.

Other obligations

Agencies may also be subject to additional mandatory data breach notification obligations through other legislative requirements, such as the information security incident reporting requirements under the Queensland Government Enterprise Architecture (QGEA), the Commonwealth Notifiable Data Breaches (NDB) scheme and the *My Health Records Act 2012* (Cth).

Agencies may need to seek legal advice about applicable laws or schemes, and/or their requirements.

Responding to a privacy breach

There are four key steps in responding to a privacy breach:

1. Contain the breach.
2. Evaluate the associated risks.

3. Consider notifying affected individuals.
4. Prevent a repeat.

Each step is set out in further detail below. The first three steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

Step one: Contain the breach

Take whatever steps possible to contain the breach and minimise any resulting damage. For example, recover the personal information, shut down the system that has been breached, suspend the activity that lead to the privacy breach, revoke or change access codes or passwords.

If a third party is in possession of the personal information and declines to return it, it may be necessary to seek legal advice on what action can be taken to recover the information. When recovering information, make sure that copies have not been made or, if they have, that all copies are recovered.

Be careful when taking steps to contain the breach not to destroy information that may be needed to investigate the cause of the breach.

Escalate the matter internally as appropriate. Senior management with responsibility for the area where the breach occurred should be immediately informed of the breach. Depending on the circumstances of the breach, it may also be appropriate to inform the media relations unit, the legal services area, the information security manager, the business unit responsible for managing matters of employee misconduct (such as internal audit, ethical standards or Crime and Corruption Commission liaison officer), Director-General and/or Ministerial liaison unit.

Hint

The agency's privacy contact officer should be informed of all breaches. This officer can provide advice on the application and interpretation of the IP Act and may assist in responding to inquiries made by the public, and managing any complaints that may be received as a result of the breach.

Reporting all privacy breaches to a designated position will also support an agency to maintain a central log of breaches that could then be used to identify training opportunities or improvements to information handling practices.

In some circumstances, it may be appropriate or necessary to notify a third party of the breach, for example:

- If the breach appears to involve theft or other criminal activity, the Queensland Police Service would be notified as a matter of course.

- Entities that have obligations under the *Privacy Act 1988* (Cth), or are a credit reporting body, credit provider or Tax File Number (TFN) recipient, may be obliged under the NDB scheme[1] to report the breach to the Office of the Australian Information Commissioner.

- Entities subject to the QGEA may be required to report information security incidents to the Queensland Government Chief Information Office, as per the QGEA Information security incident reporting standard[2].

- Certain entities (such as registered healthcare provider organisations) are required to report data breaches that meet the criterion set out under section 75(1) of the *My Health Records Act 2012*[3].

Step two: Evaluate the associated risks

To determine what other steps are needed, you should assess the type of personal information involved in the breach and the risks associated with the breach. Factors to consider include:

- **What type of personal information is involved?** Some types of personal information are more likely to cause an individual harm if it is compromised. For example, government-issued identifiers such as Medicare or driver's licence numbers, health information, and financial information such as credit or debit card numbers, will be more significant than a names and email addresses on a newsletter subscription list. A combination of personal information will typically create a greater potential for harm than a single piece of personal information (for example, an address, date of birth and driver licence number if combined could be used for identity theft).

- **Who is affected by the breach?** What individuals have been affected by the breach, how many individuals have been affected and do any of the individuals have personal circumstances which may put them at particular risk of harm?[3]

- **What was the cause of the breach?** Did the breach occur as part of a targeted attack or through inadvertent oversight? Was it a one-off incident or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the personal information been

[1] In certain circumstances, entities that are not otherwise covered by the *Privacy Act 1988*, such as state government bodies, are authorised to receive TFN information and will be considered TFN recipients. A TFN recipient is any entity who is in possession or control of a record that contains TFN information. The NDB scheme applies to TFN recipients in relation to their handling of TFN information (section 26WE(1)(d) of the *Privacy Act 1988* (Cth)). See https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme
[2] See https://www.qgcio.qld.gov.au/documents/information-security-incident-reporting-standard
[3] See https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-mandatory-data-breach-notification-in-the-my-health-record-system

recovered? Is the personal information encrypted or otherwise not readily accessible?

- **What is the foreseeable harm to the affected individuals?** Who is the recipient of the information? Is there evidence that suggests theft, and was the information the target? Evidence of theft could suggest a greater intention to do harm and heighten the need to provide notification to the individual, as well as law enforcement. What possible use is there for the personal information? For example, could it be used for identity theft, threats to physical safety, financial loss, workplace bullying, loss of employment opportunities, and humiliation or damage to reputation? What is the risk of further access, use or disclosure, including via media or online?

Step three: Consider notifying affected individuals

The IP Act does not specifically require an agency to notify individuals who have been affected by a privacy breach. However, a failure to notify may compound the damage for the individuals affected by the breach and reflect negatively on an agency's reputation. Notification can also demonstrate a commitment to open and transparent governance.

In general, if a data breach creates a risk of harm to an individual, the affected individuals should be notified. Prompt notification to individuals in these cases can help to avoid or lessen the damage by enabling the individual to take steps to protect themselves.

There are occasions where notification can be counter-productive. For example, notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors to consider when deciding whether notification is appropriate include:

- What is the risk of harm to the individual (as determined in the previous step)?
- What steps has your agency taken to date to avoid or remedy any actual or potential harm?
- What is the ability of the individual to take further steps to avoid or remedy harm? For example, can the individual have a new credit card number issued to avoid potential financial harm?[4]
- Even if the individual would not be able to take steps to fix the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?

[4] For example, in 2016, the Australian Red Cross Blood Service (ARCBS) inadvertently placed donor information where it was accessible to unauthorised users. ARCBS arranged access to IDCARE (www.idcare.org), which provided counselling support from specialist counsellors and information on additional responses that may be unique to the affected individual's own situation.

- Are there any applicable legislative provisions or contractual obligations that requires your agency to notify affected individuals?

Where notification may not be warranted

A staff member transfers agency information onto a memory stick so that they can work on some files at home. At some point between leaving work and arriving home, the staff member loses the memory stick. They report it missing the next day.

The agency checks with the lost property section of the bus company but the memory stick was not handed in. The staff member advises that the memory stick contains the names, phone numbers and email addresses of about 100 members of the public who are participating in a community consultation project lead by the agency, and includes email correspondence from these individuals.

The data on the memory stick is protected by encryption software. The agency confirms with its IT service area that even if the memory stick were to be found, the data on the memory stick is inaccessible without the proper key to decrypt the information. The agency decides that notifying the individuals whose personal information was held on the memory stick is not warranted.

Where notification may be warranted

A paper file containing the records of 50 employees is left in a café. The information included the names, home addresses, phone numbers, birth dates, salary information and bank account numbers. Enquiries with the café fail to locate the whereabouts of the file.

The agency decides to notify employees of the breach due to the potential risk of identity theft.

A senior manager emails the affected staff members to notify them of the breach. In the notification, the manager offers an apology, explains personal information was involved, and directs the employees to resources that set out the key signs of identity theft and what steps to take if affected. The manager also outlines what measures have been put in place to prevent any recurrences of the breach. Staff are informed of their right to make a privacy complaint to the agency, including information on the option of bringing their complaint to the OIC should they be dissatisfied with the subsequent response to their complaint.

The logistics of notifying affected individuals will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals. Considerations include the following.

When to notify

In general, individuals affected by the breach should be notified as soon as practicable. Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach or reveal a software vulnerability.[4]

How to notify

It is recommended that affected individuals be notified directly - by telephone, letter, email[5] or in person. Indirect notification – such as information posted on the agency's website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals is not known, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information on it).

What to say

Tailor the content of the notification advice to the circumstances of the particular breach.
Content of a notification could include:

- information about the breach, including when it happened6
- a description of what personal information has been disclosed
- assurances (as appropriate) about what personal information has not been disclosed
- what the agency is doing to control or reduce the harm
- what steps the person can take to further protect themselves and what the agency will do to assist people with this
- contact details within the agency where questions or requests for information can be directed
- the right to lodge a privacy complaint with the agency and the option to bring their complaint to the OIC if they then are dissatisfied with the subsequent response from the agency.

Step four: Prevent a repeat

Once the breach has been contained, you should further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Preventative actions could include a:

- security audit of both physical and technical security controls
- review of policies and procedures
- review of employee training practices; or
- review of contractual obligations with contracted service providers.

Tip

Following any breach, you should assess and evaluate how well the matter was handled. In some circumstances, preparing a documented breach response plan can assist an agency to respond to a breach in a timely manner and help mitigate potential harm to affected individuals.

The plan could set out contact details for appropriate staff to be notified in the event of a breach, clarify roles and responsibilities, and document processes which will assist your agency to contain the breach, coordinate an investigation and assess the need for breach notifications.

For additional information and assistance please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or email enquiries@oic.qld.gov.au.

This guide is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to feedback@oic.qld.gov.au.

Published 1 December 2009 and Last Updated 1 February 2018