Responding to privacy breaches – information for contract managers

The Department of Families, Seniors, Disability Services and Child Safety (**the department**) engages contracted service providers (**CSPs**) to perform some of its functions. While performing those functions, CSPs often handle personal information.

The *Information Privacy Act 2009* (**IP Act**) regulates how personal information should be collected, managed, used, and disclosed, to ensure that it is protected. The standard terms of government contracts require CSPs to comply with relevant parts of the IP Act in relation to personal information. This means that the protections which would apply to personal information handled by the department also apply to that information when it is collected and handled by CSPs.

If a CSP that is bound to comply with the IP Act fails to comply with those obligations, it may be in breach of the contract *and* may also be liable under the IP Act for any privacy breaches. If it is not contractually bound to comply with the IP Act, the department may be liable for their privacy breach.

The standard terms also require the CSP to notify the department if a breach occurs, so that the department can review the CSP's response to the breach and ensure that it is appropriate.

The department cannot provide advice to CSPs about how they should respond to a privacy breach, but the department does need to be satisfied that the CSP:

- has the ability to protect personal information (e.g. that it has appropriate information privacy policies and procedures, and staff training in place), and
- responds appropriately to any privacy breaches that do occur (including taking steps to prevent a recurrence).

This information sheet will assist you in identifying what you should look for to ensure that a CSP responds to privacy breaches appropriately and continues to meet its contractual obligations.

1. What is personal information?

Personal information is defined as information or 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 not, and whether it is recorded in a material form or not.

Sensitive information is personal information about an individual and includes:

- racial or ethnic origin
- religious beliefs or affiliations
- sexual orientation or practices
- criminal record
- political opinions
- membership of political, professional or trade association, or trade union
- health information
- genetic information
- some biometric information.

Information about a person can reveal a person's identity even if their name is not mentioned if there is sufficient information to enable their identity to be deduced.

2. What is a privacy breach?

A ***privacy breach*** occurs when personal information is not handled in accordance with the obligations in the IP Act. It will generally involve unauthorised access to, or disclosure of, personal information.

A privacy breach may be accidental or intentional. It may be a one-off occurrence or due to a systemic issue. For example, a privacy breach may occur if:

- a CSP employee posts or emails personal information to the wrong person
- a laptop, storage device or physical file containing personal information is lost or stolen
- CSP employee accesses personal information without a legitimate 'need to know' (e.g. out of curiosity)
- instead of securely disposing of records containing personal information, a CSP disposes of them in an insecure garbage bin where someone finds them
- a CSP disposes of computer hard drives and storage devices without erasing the contents
- a CSP's databases are 'hacked' or illegally accessed by external operators
- colleagues in a CSP workgroup discuss a client matter in a coffee shop where they are overheard by a third person who can identify the client
- a CSP collects more personal information than it needs to deliver its contracted services.

3. Four key steps in responding to a privacy breach

Step 1: Contain the breach
Step 2: Assess the risk
Step 3: Consider whether to notify affected persons
Step 4: Prevent a recurrence

Steps 1, 2 and 3 should be implemented as soon as possible and may happen simultaneously. Step 4 may occur after the immediate response and should include strategies to prevent a recurrence.

> ***Note:*** The decision on how to respond to a privacy breach should be made on a case-by-case basis: different types of breaches may require a different response.

Step 1: Breach containment and preliminary assessment

Someone with sufficient authority should be appointed to lead the investigation and response.

1.1 Contain the breach and mitigate risk

The CSP should take immediate common-sense steps to try to contain the breach, for example:

- recovering the records containing the personal information:
  - recalling emails sent to a wrong address
  - retrieving a device or hard copy records left at a client's home, or
  - remotely wiping a mobile device.
- asking email recipients to delete an email from their Inbox and Bin/Deleted items and confirm in writing when they have done so, and advising them not to disclose the information
- shutting down the system and changing/revoking computer access codes
- immediately ceasing a particular practice.
-

If a third party has the personal information and will not return it, it may be necessary for the CSP to seek legal advice to determine the appropriate action to recover the information. Depending on the sensitivity of the information, it may decide to ask the police to help retrieve the information.

The CSP must take all reasonable steps to ensure that no copies of the information have been made, or if they have, that all copies are recovered.

Step 2: Assess the risks associated with the breach

Assessing the risks will inform decisions about what immediate steps need to be taken.

The CSP should:

- **Identify what personal information was involved** – how sensitive is it and does the type of information create a greater risk of harm? e.g. the risk from disclosure of medical details may be greater than disclosure of a newsletter distribution list.
- **Identify who is affected by the breach** and their circumstances e.g. the disclosure of the address of a high-profile person may create a safety risk
- **Determine the context** – e.g. the risk is greater if the address of a victim of domestic violence was accidentally disclosed to a violent former partner instead of to her brother
- **Establish the cause and extent of the breach** – for example, identify the source, ongoing risk, protections inherent in the information, steps to mitigate, whether the breach is systemic or isolated and the number of individuals affected
- **Establish whether there is an ongoing breach or a risk of it reoccurring** – does the breach expose a systemic issue making recurrence more likely?
- **Identify whether there is risk of harm to individuals and the likelihood of the harm occurring** – this will normally depend on the nature of the information and the circumstances of the individuals
- **Identify whether there is risk of harm to the department and the likelihood of the harm occurring** – is there a risk of reputational damage/loss of trust, financial exposure, regulatory penalties?
- **Identify whether there is risk of harm to the CSP and the likelihood of the harm occurring** – such as damage to its reputation, exposure to legal action and damages.
-

Step 3: Consider Notification

3.1 Who should be notified?

The CSP should consider who needs to be informed about the breach. Generally, the contract will require them to notify the department, so the Contract Management team should be notified immediately and kept advised about the actions taken.

The Contract Management team should liaise with the Information Privacy team to ensure that the CSP's response is appropriate and in accordance with the CSP's contractual obligations. However, as noted above, the department cannot provide advice to the CSP. Depending on the seriousness of the matter, it may be prudent for the CSP to seek independent legal advice.

Note: Chapter 3A of the IP Act creates a mandatory data breach notification (**MDBN**) scheme, which requires agencies to notify the OIC and certain individuals of **eligible data breaches**. An eligible data breach is one which is likely to result in serious harm to an individual to whom the information relates.

Generally, the obligations under the MNDB scheme do not apply to CSPs. However, the obligations under the MNDB scheme apply to personal information **held by an agency.** This includes information which is **in the department's control.** Where data breaches involve personal information in the possession of a CSP but the department retains a legal entitlement to possession or a right to deal with the information, it may be a data breach of the agency and may trigger the department's MNDB notification obligations.

If it appears that the department retains a legal entitlement to the personal information which was affected by the breach, the contract manager should contact the Information Privacy team to discuss.

3.2 Other notification obligations

It may also be appropriate to notify other entities, for example:

- if the breach involves theft or criminal action, consider whether police should be notified
- if the breach involves Tax File Numbers, the Office of the Australian Information Commissioner must be notified
- if the information includes information which is subject to the *My Health Records Act 2012,* the MHR System Operator must be notified in certain circumstances.

Step 4: Prevent future breaches

It is important to document the actions taken by the CSP and the outcomes. This information can be used to reflect on what has happened and how to prevent a recurrence of the breach.

4.1 Preventing a recurrence

The CSP should consider:

- What happened? What personal information was compromised?
- Why did it happen?
  - Was it due to human/technological error?
  - Was it an isolated incident?
  - Was it a systemic issue?
  - Is there a risk of ongoing and/or recurrent breaches or further disclosure?
- What action has the CSP taken to address the risk of a recurrence? For example, has it:
  - undertaken an audit of physical and technical security controls, and updated them as necessary?
  - reviewed its information handling policies and procedures, and amended them as necessary?
  - reviewed its employee training, including induction and refresher training?
  - assessed whether the employee responsible should undertake further training?

4. Next steps

Once you are satisfied that there has been an appropriate privacy breach response, consider whether there are any additional contract management steps that should be taken. For example:

- Did the CSP notify the department promptly about the breach?
- Did the CSP appear to have an appropriate level of understanding about their privacy obligations and the ability to meet them? Did they seek external advice, if appropriate?
- Did the CSP respond appropriately to the breach?
- Did the CSP take appropriate steps to prevent a recurrence?
- Did this incident raise concerns about the CSP's ability to protect client information while providing services to departmental clients?
- Have you briefed your supervisor about any concerns highlighted by this incident?

5. Further assistance

Contract managers can contact the Information Privacy and Governance team on privacy@families.qld.gov.au or (07) 3097 5609 for further information.