The Department of Seniors, Disability Services and Aboriginal and Torres Strait Islander Partnerships (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 in the hands of the department also apply to that information when it is collected and handled by CSPs.

If a CSP which is bound to comply with the IP Act fails to comply with those obligations, it may be in breach of the contract *and* it may be liable under the IP Act for any privacy breaches.[[1]](#footnote-1) If a CSP is not contractually bound to comply with the IP Act, the department may be liable for the CSP’s privacy breaches.

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

The department cannot provide advice about how CSPs should respond to a privacy breach, but the department does need to be satisfied that the CSP has appropriate information privacy policies and procedures, and that it adequately responds to any privacy breaches that do occur.

This information sheet will assist you in identifying what you should look for to ensure that CSPs respond to privacy breaches appropriately and continue to meet their contractual obligations.

## What is personal information?

***Personal information*** is defined in section 12 of the IP Act. In summary, personal information is information or an opinion, including information or an opinion forming part of a database, whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Sometimes personal information 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.

## 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 access to, or collection, use or disclosure of, personal information in contravention of the IP Act. A privacy breach may be accidental or intentional. It may be a one-off occurrence or due to a breakdown in procedures. For example, a privacy breach may occur if:

* a CSP employee posts or emails personal information to the wrong person (e.g. posts a letter to the wrong address or sends an email to the wrong person or distribution list)
* CSP laptops, removable storage devices or physical files containing personal information are lost or stolen
* CSP employees access personal information outside of the requirements of their employment (e.g. out of curiosity)
* instead of shredding records containing personal information when they are no longer required, a CSP recycles them or leaves them in an insecure garbage bin
* a CSP disposes of computer hard drives and storage devices without erasing the contents
* a CSP’s databases containing personal information 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
* CSP collects more personal information than it needs to deliver its contracted services.

## Four key steps in responding to a privacy breach

## There are four key steps when responding to a breach or suspected 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 and seniority should be appointed to lead the investigation and response.

* 1. **Contain the breach**

The CSP should take immediate common-sense steps 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/Trash 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, they may 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.

* 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 about any breaches. Therefore, the responsible Contract Management team should be notified immediately and kept advised about the actions taken.

The Contract Management team should liaise with the Governance, Planning and Reporting team to ensure that the CSP’s response is appropriate and in accordance with the CSP’s contractual obligations. The Governance, Planning and Reporting team will liaise with Legal Affairs, Office of the Director-General and General Counsel, Legal Services as required in this regard. 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 and notify the Office of the Information Commissioner (OIC).

### *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 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 there is risk of it reoccurring** – does the breach expose a systemic issue making recurrence more likely?
* **Identify whether there is risk of harm to individuals** – this will normally depend on the nature of the information and the circumstances of the individuals concerned
* **Identify whether there is risk of harm to the department** – is there a risk of reputational damage/loss of trust, financial exposure, regulatory penalties?
* **Identify whether there is risk of harm to the CSP** – such as damage to its reputation, exposure to legal action and damages.

### *Step 3: Consider Notification*

**3.1 Notifying affected persons**

Consideration must also be given to whether to notify affected persons. Each incident should be considered on a case-by-case basis. However, it is expected that affected persons will be notified if there is a risk of harm or if there is any action they could take to minimise the risk of harm.

In some exceptional cases, notification may cause more harm than it would alleviate, and that impact of notification should also be considered.

**Generally, the CSP will be responsible for notifying affected individuals, but the department should consider whether it has a responsibility to notify affected individuals.**

* + 1. **Deciding whether to notify**

The following considerations are relevant when deciding whether to notify:

* What is the risk of harm, loss, or damage to the individual?
* Is there a risk of identity theft or fraud?
* Is there a risk of physical harm, stalking or harassment?
* Is there a risk of humiliation or damage to the individual’s reputation?
* What is the ability of the individual to avoid or mitigate possible harm?
* Is there a likelihood that being notified might cause the affected individual more distress than it would alleviate (particularly if there is little risk of harm)?

*Example of when notification* ***could*** *occur*

* A registration list, containing the names of staff who were to attend a training course, are left in a coffee shop by a CSP employee.

In this case the CSP could notify the affected individuals. The affected individuals are readily identifiable, but the potential for harm is significantly small.

*Example of when notification* ***should*** *occur*

* A document containing the names and addresses of clients who require wheelchairs and intimate domestic care provided by the CSP is left on a bus by a CSP employee.

In this case the CSP *should* notify the affected individuals. The affected individuals are readily identifiable, and the information is of a sensitive nature.

*Examples of when notification* ***need not*** *occur*

* A work laptop is stolen, but it is quickly recovered by the police, and a forensic examination of the laptop shows that the information has not been accessed.
* Documents containing sensitive personal information are accidentally put in the rubbish bin, but the error is identified, and the documents are retrieved by another employee before the rubbish is disposed.

In the above two examples it is not necessary to notify the individuals as there is no potential for harm, and notification could itself cause unnecessary distress.

* + 1. **Deciding when to notify**

If a decision is made to notify affected individuals, that should generally be done as soon as reasonably possible. If there is an ongoing investigation or law enforcement authorities are involved, you should check with them to determine whether notification should be delayed to avoid compromising their investigation.

**However, if the person is at risk of harm they should be notified as soon as possible.**

* + 1. **Deciding how to notify**

The preferred method of notification is **direct** (e.g. by phone, letter, email or in person) to affected individuals. Prompt contact of this type may result in the affected individuals being able to quickly take mitigating action to contain the harm.

**Indirect** notification (e.g. by way of a notice on the CSP’s website) should generally only occur where direct notification could cause further harm, is cost prohibitive, or the contact information for affected individuals is not known and cannot be reasonably obtained.

Using multiple methods of notification may be appropriate in certain cases.

* + 1. **What should be included in the notification?**

The content of notifications will vary depending on the nature of the breach and the method of notification chosen. Notifications should include, as appropriate:

* general information about the nature of the incident and when it happened
* a description of the personal information involved
* a general account of the steps taken to control or reduce the harm
* what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves
* what the CSP and/or the department will do to assist individuals
* contact information of an individual within the CSP or the department who can answer questions or provide further information, or offer assistance
* information about complaint avenues, including how to make a privacy complaint.

**Care must be taken not to include unnecessary personal information in the notice, to avoid a possible further unauthorised disclosure.**

* 1. **Notifying the OIC**

Data breach notification is not mandatory in Queensland, but there may be situations in which it is appropriate. For example, if a large number of people are likely to be affected (e.g. computer hacking), it may be appropriate to notify the OIC so that they can provide advice and be prepared to respond to any queries or complaints which they receive.

* 1. **Notifying others**

Additional considerations include:

* ifthe breach involves theft or other criminal action, the police should be notified
* if the information is health information or tax file numbers, there may be specific obligations under relevant legislation.

### *Step 4: Prevent future breaches*

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

In assessing whether any additional action is necessary, consider:

* Has the CSP responded to the breach and has it been effectively contained?
* Have you notified everyone within the department who needs to be made aware of the breach (e.g. the Governance, Planning and Reporting team; Legal Affairs, Office of the Director-General; General Counsel, Legal Services; relevant managers and senior executives)?
* If the breach has created risk of harm to individuals, have they been notified? Alternatively, was it determined that notification would cause more harm than it would alleviate or due to an ongoing investigation?

**4.1 Preventing a recurrence of the breach**

In relation to the specific privacy breach that has occurred, review:

* 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 been taken to address the risk of a recurrence of the breach? For example:
	+ has the CSP undertaken an audit of physical and technical security controls
	+ has the CSP reviewed its information handling policies and procedures
	+ has the CSP reviewed its employee training practices generally, including induction and refresher training
	+ has the employee responsible been required to undertake further training?

### Next steps

## Once you are satisfied that the issue has been dealt with, you should 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 the CSP respond appropriately to the breach?
* Did the CSP take appropriate steps to prevent a recurrence?
* Did this incident raise any concerns about the ability of the CSP to provide services to departmental clients?
* Have you briefed senior departmental officers about any concerns that have been highlighted by this incident?

## Further assistance

For further information about responding to privacy breaches refer to **Appendix A of this information sheet ‘Checklist – Responding to Privacy Breaches: Contracted Service Providers’.**

Contact the Manager, Governance, Planning and Reporting at privacy@dsdsatsip.qld.gov.au for further information and guidance.

This information sheet and associated Responding to a Privacy Breach checklist (Appendix A) is based upon the *Privacy Breach Management and Notification* guideline published by the Office of the Information Commissioner (Queensland).

***Step 1: Containment***

What containment action has been taken? Has it contained the breach? *For example:*

* *email successfully recalled*
* *recipient confirmed email deleted from Inbox and Trash and not shared with anyone else*
* *hard copy records retrieved*
* *password protected device wiped remotely*
* *system access revoked; system access codes revoked*
* *legal advice or police assistance sought to retrieve information*

[Insert details]

***Step 2: Risk assessment***

A risk assessment should be conducted to inform the next steps. *For example:*

* *What personal information was involved and how sensitive is it? e.g. medical details or training list*
* *Who is affected by the breach and what are their circumstances? e.g. high-profile person*
* *What is the context? e.g. address of DFV victim given to former partner, or to brother*
* *What was the cause and extent of the breach? Do any protections or mitigations apply?*
* *Is there a risk of harm to the individual? e.g. physical, financial, reputational damage*
* *Is there a risk of harm to the department/CSP? e.g. reputational damage; regulatory penalties*

[Insert details]

***Step 3: Notification***

Consideration should be given to who should be notified. *For example:*

* *Have senior managers in the CSP been notified?*
* *Should police be notified? (e.g. if it involves theft)*
* *Should the Queensland OIC be notified? NB: data breach notification is not mandatory in Queensland.*
* *Should the OAIC be notified? NB: Privacy Act 1988 (Cth) does not apply to contracts with State Government agencies, but may apply to certain types of information e.g. TFNs*
* *Should affected persons be notified?*

**Notifying affected persons**

Each incident should be assessed on its facts, but it is expected that affected persons will be notified if there is a risk of harm, or if there is any action the person could take to minimise harm.

*Relevant considerations include:*

* *What is the risk of harm, loss, or damage to the individual?*
* *Is there a risk of identity theft or fraud?*
* *Is there a risk of physical harm, stalking or harassment?*
* *Is there a risk of humiliation or damage to the individual’s reputation?*
* *What is the ability of the individual to avoid or mitigate possible harm?*
* *Is there a likelihood that being notified might cause the affected individual more distress than it would alleviate (particularly if there is little risk of harm)?*

Generally, the CSP will be responsible for notifying affected individuals, but the department should consider whether the particular circumstances affect that assessment.

[Insert details]

***Step 4: Preventing future breaches***

Consider what caused the breach and how it could have been prevented. Has the CSP taken action to prevent a recurrence? *For example:*

* *improved physical or technical controls*
* *reviewed information handling policies and procedures*
* *reviewed staff training and completion rates*
* *considered whether disciplinary action is appropriate.*

[Insert details]

***Other information***

Is there any other information the department should be aware of?

[Insert details]

1. *Information Privacy Act 2009,* sections 34-37 [↑](#footnote-ref-1)