Information privacy breach checklist – for contracted service providers

This checklist has been developed for use by Contracted Service Providers (**CSPs**) when notifying the Department of Families, Seniors, Disability Services and Child Safety (**the department**) about a privacy breach.

It should be read in conjunction with the Office of the Information Commissioner (**OIC**) guideline.

The department cannot provide advice about how a CSP should respond to a breach, so CSPs should consider whether to seek independent advice from the OIC or a legal advisor.

1. What happened?

Please provide a summary of what occurred, including what information was involved.

[Insert details]

2. Response

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 Deleted items 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*
- *What was the cause and extent of the breach? Do any protections or mitigations apply?*
- *Is there a risk of serious 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*

Does the use/disclosure of this information create a risk of serious harm to anyone? Yes/No

[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)*
- *Has the department been notified?*
- *Should the Office of the Australian Information Commissioner (OAIC) be notified?* ***Note:*** *this obligation may arise in relation to certain types of information e.g. TFNs*

[Insert details]

- **Is it an *eligible data breach*?**

Note: An *eligible data breach* is a data breach that involves unauthorised access to, or disclosure of, personal information which is likely to result in serious harm to an individual OR personal information is lost in circumstances where unauthorised access or disclosure is likely to occur and if it occurred, it would be likely to result in serious harm to an individual.

A Mandatory Data Breach Notification Scheme (**MDBNS**) applies in relation to eligible data breaches. The MDBNS does not apply to CSPs, but the department may be required to notify the OIC and affected persons about CSP breaches in some cases. We will need your assistance if this is necessary.

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 kind of information was affected? How sensitive is it?*
- *Is the information protected by security measures? What is the likelihood that they could be overcome?*
- *Who has obtained, or could obtain, the information? Does that affect the assessment of risk?*
- *What is the nature of harm likely to arise? For example:*
  - *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 likelihood of the harm occurring?*
- *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)?*

[Insert details]

Step 4: Preventing future breaches

Consider what caused the breach and how it could have been prevented. For example:

- *Human error due to lack of training or work pressure*
- *Staff misconduct (i.e. acting in breach of policies, procedures and training)*
- *Failure to update security settings leading to system vulnerabilities*

[Insert details]

Have you taken action to prevent a recurrence? For example:

- *Improved physical or technical controls*
- *Review information handling policies and procedures*
- *Review staff training and completion rates*
- *Is disciplinary action appropriate?*

[Insert details]

3. Other information

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

[Insert details]