Data Breach Notification Decision Tool

Australia

Use this tool to determine if a data breach incident must be notified under the Privacy Act 1988 (Cth) (**Privacy Act**), as part of a comprehensive incident response. **This diagram is a summary of relevant considerations and is not legal advice.**

Incident occurs or is suspected

An incident can include unauthorised access to, disclosure of, or loss of data. For example:

- Data is removed from systems without authorisation (external intruder, staff member misusing access)
- Data is mishandled by supplier
- Hard copy documents are lost or stolen.

Does the incident involve personal information collected or held in Australia?

Personal information and personal data mean information or an opinion about an individual who is identified, or is reasonably identifiable: Privacy Act s6.

- The incident doesn't involve personal information
- The incident does involve personal information

Is there a risk of harm to individuals?

If you have taken remedial action that eliminated or reduced the risk to all affected individuals, then there is no risk of harm: Privacy Act s26WF.

If the remedial action did not reduce the risk to all individuals, then there is still a risk of harm.

- There is a risk of harm to individuals
- There is no risk of harm to individuals

Is the risk likely to occur?

A risk is likely if there is a greater than 50% chance of it occurring.*

- >50% The risk is likely to occur
- <50% The risk is not likely to occur

Are the potential harms serious?

Serious harm to an individual may include serious **physical**, **psychological**, **emotional**, **financial**, or **reputational** harm.* Risk of serious harm should be assessed holistically, taking into account:

- The kind of information and its sensitivity
- The kind of person who has obtained (or could obtain) the information
- Whether the information is protected by security measures (such as encryption)
- The likelihood that security measures could be defeated by a person who intends to cause harm
- The nature of the harm: Privacy Act s26WG.

- Potential harms are not serious
- Potential harms are serious

Notification not required

Consider whether voluntary notification to the OAIC and/or individuals is appropriate, particularly if:

- the incident is likely to be brought to the OAIC's attention
- user action is necessary to secure customer accounts, or
- the incident may otherwise come to the attention of the public or receive media attention.

Notify OAIC and affected individuals

See oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify for details on notifying the OAIC and affected individuals.

* See the OAIC's Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth), available at oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

elevenm.com.au

elevenM

September 2018 DBNDT-AU-1.0