becklegal
Solicitors

Notifiable Data Breaches (NDB)

- The commonwealth government amended the Privacy Act (Cth) 1988 (Privacy Act) which came into effective as at 22 February 2018 to introduce the NDB scheme.
- The NDB scheme requires entities to notify individuals and the Office of the Australian Information Commissioner (OAIC) about eligible data breaches.
- A data breach is eligible as a notifiable data breach if it is likely to result in serious harm to any of the individuals to whom the information relates.
- Whether a data breach is likely to result in serious harm is an objective test based upon a reasonable person's point of view in the position of the entity.
- An entity is exempt from reporting a data breach if an entity acts quickly to remediate the breach and because of this action the data breach is not likely to result in serious harm.

HOW TO PREPARE

- Seek advice as to your obligations under the Privacy Act and discuss the steps to protect the information from misuse, interference or loss.
- Undertake a threshold assessment to determine your organisation's compliance with the Privacy Act.
- Ensure you have an appointed privacy officer who is aware of all the obligations and your staff are adequately trained in both legal and technological matters.
- Consultation with you legal advisors and technology and communications personnel to prepare a data breach response plan.
- Undertake training in cyber security awareness and procedures.

Visit the website for the Office of the Australian Information Commissioner on the notifiable data breaches scheme which can be found by visiting www.oaic.gov.au

177 View St Bendigo Vic 3550
PO Box 628 Bendigo Vic 3552
DX 55011 Bendigo

Phone 03 5445 3333
Fax 03 5445 3355

Email info@becklegal.com.au
www.becklegal.com.au

Eligible Business

The Privacy Act applies to the following:

- Australian government agencies.
- All businesses and not for profits with annual turnover of more than three million dollars.
- All private sector health service providers, i.e. dentists and GPs.
- Traders in personal information, i.e. reporting agencies.
- Tax File Number (TFN) recipients, that is any entity that maintains TFN data which may be breached irrespective of that business' turnover.
- Related organisations to a qualifying entity.
- Personal information holders who undertake certain activities, i.e. such as government contracts.

Holds Personal Information

- "Personal information" under the Privacy Act is defined as information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.
- Common examples of Personal Information include (without limitation) an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.

Suspected Breach

An eligible data breach arises when the following three criteria are all satisfied:

a) There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds;

b) This is likely to result in serious harm to one or more individuals; and

c) The entity has not been able to prevent the likely risk of serious harm with remedial action.

Was personal data affected?

The OAIC defines an eligible data breach as when personal information held by an agency or organisation is lost or subjected to unauthorised access, use, modification, disclosure or misuse.

Is serious harm likely?

- The explanatory memorandum to the Privacy Act specifies that serious harm could include physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.
- The assessment of what constitutes serious harm is assessed from a reasonable person's perspective having regard to the circumstances.
- Whether access or disclosure would be likely, or would not be likely, to result in serious harm is to be considered taking into account the following relevant matters:
  - Type of information.
  - Sensitivity of the information.
  - If information is protected by security measures.
  - The likelihood that security measures could be overcome.
  - Intention of the person obtaining information to cause harm to any of the individuals to whom that information relates.
  - The nature of the harm.

Can remedial action be taken?

- The NDB scheme provides entities with the opportunity to take positive steps to address data breach in a timely manner and avoid the need to notify the affected individuals and the OAIC.
- If the remedial action prevents the likelihood of serious harm occurring, then the breach is not an eligible data breach for that entity or for any other entities.
- Ways to take remedial action can include recovering the information, destroying the information or making the information unusable through methods such as encryption.

Assessment of breach

- Carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that there has been a data breach.
- Take all reasonable steps to have the assessment completed within thirty days after the entity becomes aware of the suspected data breach.

Notification

- **The entity must prepare a statement about the breach and provide a copy of the statement to the Commissioner.**
- **The entity must also inform the relevant individuals.**
- **Form of notification is either:**
  - **Informs all individuals whose Personal Information is involved;**
  - **Inform only those individuals who are likely to be at risk of serious harm; or**
  - **Publish and publicise your notification to bring it to the attention of all individuals at likely risk of serious harm.**
- **When should an entity give notice?**
  - **If the entity has reasonable grounds to believe that an eligible data breach has happened; *or***
  - **It is directed to do so by the Commissioner.**