NOTIFIABLE DATA BREACHES ACT QUICK GUIDE

In February 2017, the Privacy Amendment (Notifiable Data Breaches) Act 2017 was passed by the Australian senate with the intention of establishing a Notifiable Data Breaches (NDB) scheme within Australia. With the act in force as of 22 February 2018, organisations should be aware of what is required of them should they experience a data breach.

WHAT IT IS

As of 22 February 2018, all organisations with pre-existing obligations under the Privacy Act 1988 relating to the security of personal information will have to comply with the new NDB scheme. The NDB scheme introduces an obligation to notify certain individuals and the Australian Information Commissioner about incidents that are deemed to be "eligible data breaches."

WHO IT WILL APPLY TO

The NDB scheme will apply to any organisations that the Privacy Act 1988 requires to safeguard certain types of personal information. This means that it will apply to any private sector business or not for profit with an annual turnover of more than $3 million. Some entities in certain sectors will be affected regardless of their turnover, including health service providers, credit reporting bodies and entities that trade in personal information.

WHAT IT WILL REQUIRE ORGANISATIONS TO DO

The NDB scheme will require applicable organisations to notify affected individuals and the Australian Information Commissioner if an "eligible data breach" occurs. An eligible data breach is deemed to have occurred when the following points are satisfied:

- There is unauthorised access to, unauthorised disclosure of, or loss of personal information that an entity holds;
- The access to, disclosure of, or loss of this personal information is likely to result in serious harm to the affected individuals; and
- The entity in question has been unable to prevent the risk of serious harm to individuals through remedial action.

If an entity has reasonable cause to believe that an eligible data breach has taken place, then they must notify affected individuals and the Australian Information Commissioner as promptly as possible. The notification must contain the following information: the identity of the organisation in question with contact details provided alongside this; an explanation of the data breach; the types of information that have been accessed, disclosed or lost in the breach; and suggestions about what actions affected individuals should take in response to the breach.

With the act now in force, entities should take action to ensure that they understand the NDB scheme and what their responsibilities are in the event of a data breach. Failure to comply with the NDB scheme can attract fines of up to $2.1 million.

USEFUL LINKS

- NBD scheme overview on the Office of the Australian Information Commissioner (OAIC) website: https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme
- OAIC press release about the scheme's launch: https://www.oaic.gov.au/media-and-speeches/media-releases/mandatory-data-breach-notification-comes-into-force-this-thursday