22 February 2018: Mandatory Data Breach Notification Laws Take Effect –

November 2017

As of 22 February 2018, entities which are required to comply with the *Privacy Act 1988* (Cth) will be required to promptly notify the Office of Australian Information Commission (OAIC) and any potentially affected individuals of an "eligible data breach".

An "eligible data breach" is where personal information held by the entity in relation to a person is lost, subject to unauthorised access or disclosure.

The entity will need to notify the OAIC and the affected individuals when there is a data breach that is likely to result in "serious harm" to an individual to whom the information relates.

"Serious harm" includes serious physical, psychological, emotional, economic and financial harm as well as harm to reputation.

Where the entity is uncertain if data breach is likely to result in serious harm, there is an obligation to conduct an assessment of the breach. The matters to be considered include the sensitivity of the information, any security measures taken (eg encryption) and how easily those security measures could be overcome.

The notification must set out:

- the entity's identity and contact details;
- a description of the data breach;
- the kinds of information concerned; and
- recommendations about the steps the affected individuals should take in response to the data breach.

There are some exceptions from the requirements including where the entity takes action in relation to the access or disclosure of personal information before the access or disclosure results in any serious harm.

The purpose of the mandatory reporting requirement is to ensure that affected individuals can take remedial steps in the event their personal information is compromised.

Up until 22 February 2018, any reporting is voluntary. Post that date there are a range of penalties for non-compliance ranging from public and personal apologies to civil penalties for serious and repeated contraventions.

Good corporate governance steps

Entities need to put themselves in the position so that they have a strong understanding of:

- when the breach occurred
- when it was discovered
- what was the cause of the breach
- what type of records were compromised
- whether other entities are affected
- who was affected and how many
- how they will manage an incident and consider the need to engage an independent expert
- whether they are able to undertake an expeditious assessment to determine if the data breach is likely to result in serious harm
- what their data response plan is and its ability to respond quickly to data breaches
- the policies and systems they have in place to make the mandatory notifications