Commercial and Corporate | February 2018

Mandatory data breach notification – Are you ready?

In a Nutshell

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) imposes significant changes to the *Privacy Act 1988* (Cth). The amendments oblige many organisations to notify individuals who are affected by an unauthorised disclosure of, or access to, their personal information. Failure to notify those individuals can result in compensation orders or civil penalties being imposed.

THESE CHANGES COME INTO FORCE ON 22 FEBRUARY 2018

Mandatory data breach notification scheme

The new Privacy Act 1988 (Cth) (***Privacy Act***) provisions will give individuals a statutory right to receive notification when a data breach occurs in relation to their personal information.

Australian Privacy Principle (***APP***) 11.1 already requires organisations to take reasonable steps to protect personal information from misuse, loss, or unauthorised access. However, it does not currently oblige organisations to notify affected individuals if the personal information is inadvertently accessed or disclosed.

The new Part IIIC of the *Privacy Act* obliges government agencies and medium-to-large private sector organisations (with an annual turnover of more than $3 million) to provide notice to the Office of the Australian Information Commissioner and, most notably, affected or aggrieved individuals, when organisations become aware of an "eligible data breach".

This should enable aggrieved individuals to take steps to mitigate the effect of the breach in a timely manner when notified of an information "leak".

Eligible data breaches

An eligible data breach will occur when either:

- there is unauthorised access to, or unauthorised disclosure of, an individual's personal information that a reasonable person would conclude as likely to result in serious harm to an individual to whom the personal information relates; or
- an individual's personal information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur and a reasonable person would conclude that any resulting access or disclosure would likely result in serious harm to an individual to whom the information relates.

In determining whether loss or unauthorised access is likely to cause serious harm, the legislation provides that an entity should have regard to the following (not limited):

- the "kind" of information concerned;
- the sensitivity of the information; and
- whether the information is protected by any security measures.

Therefore use of advanced security technologies (i.e. encryption) will be a relevant consideration.

Suspected eligible data breaches

In cases where harmful loss or disclosure is suspected to have taken place the entity must carry out, within 30 days of becoming aware of the grounds to suspect a breach, a "reasonable and expeditious assessment" in determining whether an eligible breach has occurred.

Notification requirements

An entity, "as soon as practicable" after becoming aware of an eligible data breach, must prepare a statement setting out:

- the identity and contact details of the data holding entity;
- a description of the eligible data breach that the entity has reasonable grounds to believe has happened;
- the kinds of information concerned; and
- recommendations about the steps that aggrieved individuals should take.

The entity must then distribute the statement's contents to the Information Commissioner, and if it is practicable to do so, the contents of the statement to individuals to whom the compromised personal information relates.

If it is not practicable to distribute to individuals, the entity must publish a copy of the statement on its website and take reasonable steps to publicise the contents of the statement.

For this reason, it will be extremely important that all complying entities, regardless of the likelihood of a data breach, ensure that they are capable of contacting each and every individual with respect to which they hold personal information.

If they fail to do so, the consequences of a breach will be considerably more public, and in turn potentially much more damaging. The reputational costs of a public statement could be critical in many industries.

Exceptions to compliance with notification

There are multiple exceptions and exemptions to the notifying provisions. The most notable of these is where an entity has made successful attempts to remedy unauthorised access, loss, or disclosure before any serious harm results.

This exception represents an important incentive for information holders to upgrade response procedures in preparation for a breaching event.

The Information Commissioner may also exempt entities in certain circumstances via a formal application.

Penalties for non–compliance

Non-compliant entities risk Information Commissioner orders to pay compensation to aggrieved individuals, along with the risk of paying very significant civil penalties, especially in the case of a corporation.

Serious or repeated "interferences with privacy" are considerably more likely to attract penalties.

Next steps

The upcoming amendments should significantly impact upon the attitudes and protocols of most businesses.

You should consider steps or policies that your business can take or develop to ensure compliance with the new privacy provisions. For further information on how the amendments could affect your business, please contact Lan Lam or Ralph Bönig on the details below.

Lan Lam *Partner*
lan.lam@finlaysons.com.au
+618 8235 7838

Ralph Bönig *Special Counsel*
ralph.bonig@finlaysons.com.au
+618 8235 7684