HERBERT SMITH FREEHILLS

NEW MANDATORY DATA BREACH REPORTING LAW PASSED

13 February 2017 | Australia
Legal Briefings – By **Kaman Tsoi**, **Daniel Forrest** and **Nikki Dalla Valle**

The Federal Government has today passed the *Privacy Amendment (Notifiable Data Breaches) Act 2016* to amend the *Privacy Act 1988* to include mandatory notification of eligible data breaches.

This was the government's third attempt at legislating data breach notification as a result of recommendations from the Australian Law Reform Commission in 2008. The rules are aimed at directing entities to become proactive in protecting their data, implementing data breach response plans and taking steps to protect individuals whose information has been compromised.

Update: The key amendments will commence 22nd February 2018.

As with many other requirements under the Privacy Act, serious and repeated breaches will be subject to enforcement action including civil penalty orders of up to $1.8 million.

WHEN IS NOTIFICATION REQUIRED?

Those entities are now required to provide notification where the entity has reasonable grounds to believe that an 'eligible data breach' has occurred. An 'eligible data breach' happens where;

- there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
- the access, disclosure or loss is likely to result in serious harm to any of the individuals whom the information relates.

This new test for the requirement to notify a data breach is narrower than the 'real risk of serious harm' test which was found in the 2015 draft bill and in the Office of the Australian Information Commissioner's (**OAIC**) best practice guide.[1] The change is in response to feedback on the draft bill from stakeholders concerned about certainty and regulatory burden.

The amending Act does not define 'serious harm', but does list a number of relevant matters to assessing whether serious harm is likely, including the kind of information, sensitivity of the information, the security protections in place, the type of person or people who obtained the information and the nature of the harm. Applying these considerations, notification is more likely to be required in relation to a targeted hack to obtain consumer password data, rather than where an encrypted list of staff names and titles was accidentally emailed to a director of the company.

Notably, the amending Act does not mention the number of individuals affected by a data breach as being relevant to the assessment of whether serious harm is likely. In other words, harm to one individual can be enough.

In terms of the types of harm, the government has commented as follows:

It is expected that a likely risk of serious financial, economic or physical harm would be the most common likely forms of serious harm that may give rise to notification. Nonetheless, a reasonable person may conclude in some cases that a likely risk of serious psychological or emotional harm, serious harm to reputation or other serious harms … may exist. For example, this may be the case where an eligible data breach involves health information or other 'sensitive information'.[2]

RISK ASSESSMENT AND REMEDIAL ACTION

The new law creates a positive obligation for entities to carry out a reasonable and expeditious assessment where an eligible data breach is suspected. The entity must take reasonable steps to ensure this assessment is completed within 30 days. The government's Explanatory Memorandum for the amending Act notes that in some cases a reasonable and expeditious assessment should take less than 30 days, and in other cases will need to take more.

An eligible data breach is taken to not exist where unauthorised access, disclosure or loss has occurred but the entity takes remedial action with the effect that serious harm becomes unlikely. The Explanatory Memorandum indicates that actions such as freezing accounts, remote wiping of devices and having accidental recipients delete or return data may be relevant remedial actions here.

WHAT DOES NOTIFICATION INVOLVE?

Prior to this law being passed, notification was voluntary for most entities where a data breach had occurred. Going forward, where there is an eligible data breach or where the OAIC directs, entities must prepare and provide a statement to the OAIC and to the affected individuals as soon as practicable.

The statement should set out the identity and contact details of the entity and a description of the eligible data breach, the kind of information involved and recommendations about the steps that individuals should take in response to the breach.

THIRD PARTIES

In response to submissions on the previous draft bill, the new law provides an exception from the notification obligations where another entity has already notified the same data breach. This is intended to apply in cases where more than one entity holds the data record, for example in connection with outsourcing, joint venture and shared services arrangements.

The amending Act also provides that in certain circumstances an entity will remain accountable for an eligible data breaches involving an overseas third party to which the entity disclosed the relevant personal information.

PREPARING FOR COMPLIANCE

The new law is an amendment to the Privacy Act and will apply to all entities bound by that Act, namely Federal Government agencies, private sector organisations with an annual turnover above $3 million (and their related companies) and some others.

Entities should prepare by ensuring their data breach response plans are effective and up-to-date, and they have internal and external contacts ready to respond swiftly when a breach occurs. Entities should also review their service provider arrangements and other information sharing, to ensure that there is appropriate communication and assistance between the parties in relation to data breaches.

Entities may also take the opportunity to review their procedures and controls in respect of storage, retention and security of personal information, as this may help to reduce the risk of a notifiable data breach occurring in the first place.

ENDNOTES

1. Office of the Australian Information Commissioner, Data Breach Notification: A guide to handling personal information security breaches.

2. Privacy Amendment (Notifiable Data Breaches) Bill 2016 Explanatory Memorandum, available here.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

KAMAN TSOI
SPECIAL COUNSEL,
MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com

JULIAN LINCOLN
PARTNER,
MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

LEGAL NOTICE