Gillis Delaney Lawyers

GD NEWS / FEBRUARY 2018

IN THIS EDITION

Privacy – the new Data Breach Notification Scheme begins

The Privacy Amendment (Notifiable Data Breaches) Act 2017 which commences on 22 February 2018 establishes a Notifiable Data Breach scheme that applies to all organisations with existing personal information security obligations under the Australian Privacy Act 1988 (Privacy Act). The scheme will apply to Australian Government agencies, businesses and not-for profit organisations that have an annual turnover of more than $3 million, private sector health service providers, credit reporting bodies, credit providers, entities that trade in personal information and tax file number (TFN) recipients.

Organisations will be obliged to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. The notification must be given to the individual and include recommendations about the steps individuals should take in response to the breach. The Office of the Australian Information Commissioner ("OAIC") must be notified as well and has an online form to facilitate notifications.

A breach is notifiable only 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 requires an objective assessment. The question is whether a reasonable person in the organisation's position would determine the breach is likely to result in serious harm. That is, is it is more probable than not that there will be serious harm.

'Serious harm' is not defined in the Privacy Act. However serious harm to an individual is likely to include serious physical, psychological, emotional, financial, or reputational harm.

There will be a notifiable data breach where:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information by an organisation;

Editors:


David Newey


Amanda Bond

GILLIS DELANEY LAWYERS
LEVEL 40, ANZ TOWER
161 CASTLEREAGH STREET
SYDNEY NSW 2000
AUSTRALIA
T: + 61 2 9394 1144
F: + 61 2 9394 1100
www.gdlaw.com.au

- there is likely to be serious harm to one or more individuals;
- the organisation has not been able to prevent the likely risk of serious harm with remedial action.

Information that if disclosed, which is likely to cause serious harm, includes:

- sensitive information such as information about an individual's health;
- documents commonly used for identity verification (including Medicare card, driver licence, and passport details);
- financial information;
- a combination of personal information (rather than a single piece of personal information).

The Privacy Act prescribes matters that should be considered when determining whether a data breach is likely to cause serious harm. The matters include:

- the kind or kinds of information lost or disclosed;
- the sensitivity of the information;
- whether the information is protected by one or more security measures;
- the likelihood that any of those security measures could be overcome;
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information;
- if a security technology or methodology was used in relation to the information, and was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information;
- the likelihood that the persons, or the kinds of persons, who have obtained, or who could obtain, the information, and have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology;
- the nature of the harm.

The potential harm that will be an issue where there is a data breach includes:

- identity theft
- significant financial loss by the individual;
- threats to an individual's physical safety;
- loss of business or employment opportunities;
- damage to reputation or relationships;
- humiliation;
- workplace or social bullying or marginalisation.

Early detection of a data breach and prompt remedial action by an organisation is vital as organisations will be exempted from notifying a data breach where action is taken that prevents serious harm.

Investigation into suspected data breaches will need to become the norm. An organisation is not obliged to notify potential data breaches where it has reasonable grounds to suspect that an eligible data breach has occurred but the organisation must complete a "reasonable and expeditious" assessment into the relevant circumstances within 30 days and if the data breach is confirmed the organisation will need to implement remedial action and if serious harm cannot be prevented the breach will need to be notified.

So there we have it. The new data breach notification scheme will drive organisations to introduce additional compliance procedures around data collection, data security and investigation of suspected data breaches. Businesses need to be aware of their obligations under the National Privacy Principles and the steps that must be taken where there is a suspected data breach or a data breach that is likely to cause serious harm.

Failure to comply with the notification requirements is subject to the standard penalty regime under the Privacy Act, which allows for monetary penalties of up to $1.8 million for companies and $360,000 for individuals for serious or repeated breaches.

However that's not the only change when it comes to privacy for Australian businesses dealing with the EU as additional issues will need to be considered as consequence of the European Union General Data Protection Regulation (the GDPR) that contains new data protection requirements that will apply from 25 May 2018.

Australian businesses with an establishment in the EU, or that offer goods and services in the EU, or that monitor the behaviour of individuals in the EU may need to comply with the GDPR.

The GDPR and the Australia Privacy Act 1988 have many common requirements and Australian businesses may already have some of the measures in place that will be required under the GDPR. Even so, businesses dealing with the EU should begin taking steps to evaluate their information handling practices and governance structures, and seek legal advice where necessary, to implement the necessary changes well before commencement of the GDPR.

There are interesting times ahead for businesses that collect and store personal and sensitive information about individuals and insurance coverage for the civil penalties that can result from breaches of the Privacy Act will be at the forefront of the thoughts of the prudent risk manager involved in those businesses.

David Newey
dtn@gdlaw.com.au