BULLETIN
Industrial Relations

Reference No: Privacy Act **Date issued:** 20/02/2018

Important change to the Privacy Act 1988
Mandatory reporting of eligible data breaches
Commencing on 23 February 2018

In February 2017, the Federal Parliament passed the Privacy Amendment (Notifiable Data Breaches) Act 2017. The amending legislation will come into operation on 23 February 2018. The legislation strengthens the law regarding the distribution of personal information provided by clients and consumers. The legislation also covers personal information provided as online information including personal, credit card or other financial details.

Organisations affected by the Privacy Amendment (Notifiable Data Breaches) Act 2017

The amending legislation will apply to organisations with existing obligations under the Privacy Act, namely:

- all Commonwealth Public Sector Agencies
- all companies and not for profit organisations with an annual turnover of $3 million or more, and
- private health service providers, child care centres, private schools, businesses that sell personal information, credit reporting bodies and others who trade in personal information (regardless of annual turnover).

Exempt organisations

Exempt organizations include:

- small businesses with less than 3 million turnover, and
- law enforcement bodies where notification is likely to prejudice law enforcement activities.

What is an Eligible Data Breach?

An eligible data breach is one 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 individuals to whom the information relates.

One example of unauthorised access which has had significant media coverage is unauthorised access by an external third party (i.e. hackers).

When is there a Data Breach?

A data breach will arise where there has been unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals, or where such information is lost in circumstances that are likely to give rise to unauthorised access or unauthorised disclosure (for example, leaving the information on the bus).

What is Personal Information?

Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable;

- whether the information is true or not, and
- whether the information or opinion is recorded in a material form or not.

If the Privacy Act applies to your business, then in the event of an Eligible Data Breach, the Office of the Australian Information Commissioner and the individual(s) affected must be notified where a reasonable person would conclude there is a likely risk of serious harm.

Definition of serious harm

Serious harm could include, physical, psychological, emotional, financial or reputational harm.

When making an assessment of seriousness of harm, the following factors are relevant:

- the kind of information compromised
- whether a security measure is in place
- the likelihood the security could be breached and/or
- any other relevant matter.

Penalties

A failure to comply with the notification obligations will fall under the Privacy Act's existing enforcement and civil penalty framework. Accordingly, organisations may be subject to anything from an investigation, written directions to issue a data breach notification or in the case of serious or repeated non-compliance, to substantial civil penalties of up to $1.8 million for companies and $360,000 for individuals.

Office of the Australian Information Commissioner

The Privacy Amendment (Notifiable Data Breaches) will require government agencies and businesses covered by the *Privacy Act* to notify any individuals affected by a data breach that is likely to result in serious harm. The Office of the Australian Information Commissioner must also be advised of these breaches, and can determine if further action is required.

The Office of the Australian Information Commissioner has introduced guidance material to assist businesses covered by the amending legislation to comply with the changes and reporting procedure details, including the *Guide to securing personal information* which can be found on their website at www.oaic.gov.au.

WJ Chesterman
Industrial Relations Manager