Proposed new mandatory data breach reporting: major implications for managing your privacy law compliance risk[1]

The Australian Government has just announced a proposal to introduce a new mandatory data breach reporting requirement to notify impacted individuals and the Commissioner of a serious data breach. The proposed new changes further highlight the need for private sector organisations and Commonwealth Government agencies to take the necessary action to ensure they are complying with their privacy law obligations to minimise their exposure to potentially significant new civil penalties set to take effect in March next year.

As mentioned in our December 2012 article ' Privacy law reform - put it on your 2013 to-do list!' the Privacy Act 1988 (Cth) (**Act**) has been amended to make provision for the imposition of a civil penalty of up to $1.7m on entities (such as corporations with a turnover of more than $3 million and Commonwealth Government agencies) for a serious breach of privacy or for repeated interferences with the privacy of an individual.[1]

The Federal Government now proposes to take these reforms a step further. The proposed new mandatory notification requirements (which were announced by the Attorney General on 29 May 2013) would mean that if a data breach notification (**privacy alert**) is not issued to a significantly affected individual or the Commissioner in respect of a serious data breach, the Privacy Amendment (Privacy Alerts) Bill 2013 (**Bill**) would deem such non-compliance to be an interference with the privacy of an individual under the Privacy Law to which civil penalties may apply.

Practically what does this mean?

If personal information held by an entity is lost, subjected to unauthorised access, use, disclosure or other misuse (e.g. internal errors) the significantly affected individuals concerned would have to be notified.

For example, a privacy alert may be required where:

- devices such as laptops, USB sticks or paper records containing personal information are lost or stolen;
- leased computer equipment is returned to the lessor without personal information being erased (e.g. from the hard drive of a PC);
- an employee accesses or discloses personal information and such access or disclosure was not within their role description; or
- personal information is mistakenly sent to the wrong recipient or inadvertently lost when scheduled for destruction.

An entity should therefore consider whether it has adequate privacy systems, practices and procedures in place to comply if this mandatory privacy alert requirement is implemented.

The consequences of reporting a serious or repeated breach of privacy, or failing to report a serious data breach, therefore have the potential to be much more severe from 14 March 2013 when the proposed changes to the Act are scheduled to take effect. These may include the imposition of a significant civil penalty, compensation orders and enforceable undertakings – just to name a few. Therefore, when getting your 'privacy house in order', entities should also consider the action needed to comply with the Bill.

[1] Holding Redlich, Article by Michael Grosser and Christie Green, 6 June 2013

Background

If the Bill is passed, entities regulated by the *Privacy Act 1988* (Cth) (**Act**) and the *Privacy (Enhancing Privacy Protection) Act 2012* (Cth) (**Privacy Amendment Act**) would need to notify significantly affected individuals if a 'serious data breach' occurs in relation to personal information held by them.

This requirement was one of 98 recommendations identified by the Australian Law Reform Commission (**ALRC**) in its 2008 Report which proposed a number of changes to the Act. Despite this recommendation, the Federal Government initially stated that mandatory data breach reporting would not be included as part of the first stage of reforms to the privacy law under the Privacy Amendment Act.

However, the Federal Government has now changed its approach and brought forward the implementation of mandatory data loss reporting. The Federal Government has said that this is due to:

- recent 'spectacular' privacy breaches by high profile Australian businesses[2];
- the outcomes generated from targeted consultations and submissions in response to discussion papers and guides; and
- the adoption of some similar reforms in certain international jurisdictions.

If the Bill is passed before the September election, mandatory data loss reporting requirements may even apply immediately after commencement of the Privacy Amendment Act on 12 March 2014.

What is the effect of the Bill?

If passed in its current form, the Bill generally provides:

- For the imposition of a mandatory obligation on an entity to notify individuals who are significantly affected by a 'serious data breach' that the entity reasonably believes a serious data breach has happened as soon as reasonably practicable after forming that belief. No more precise time period for reporting a serious data loss is currently included in the Bill;
- The privacy alert must contain particular information about the relevant loss of data;
- Apart from being issued to the significantly affected individual, the privacy alert must also be given to the Commissioner. In other words, an entity must 'dob itself in';
- The manner in which the privacy alert can be communicated to the significantly affected individual;
- The circumstances in which a privacy alert is not required to be issued;
- When an entity must issue a privacy alert to the affected individual and the Commissioner if personal information has been disclosed to foreign recipients; and
- The Commissioner may direct an entity to notify the significantly affected individual of the entity's serious data breach (if the entity has not already done so).

Most importantly, if an entity fails to comply with an obligation included in the Bill, the Commissioner may use his or her existing powers with respect to that failure (and also those prescribed under the Privacy Amendment Act from 12 March 2014). Accordingly, significant penalties (both severe in the form of $1.7m civil penalty and less severe in the form of a public or personal apology) may be imposed on an entity for non-compliance in future.

Meaning of 'serious data breach' and 'significantly affected individual'

These terms are defined in the Bill. Generally a '*serious data breach*' will arise if:

- there is unauthorised access to, or unauthorised disclosure of, personal information held by an entity, or where personal information is lost in circumstances that could give rise to authorised loss or disclosure; and

- the unauthorised access or disclosure will result in a real risk of serious harm to an individual to whom the personal information relates. Further:
    -
    - 'real risk' is defined to mean a risk that is not a remote risk;
    - 'harm' is defined to mean harm to reputation, economic harm and financial harm;
    - 'serious' harm includes physical and psychological harm, as well as injury to feelings, and humiliation.

The Bill provides for regulations to be made to:

- specify particular situations which may also constitute a serious data breach, where the 'serious harm' threshold may not otherwise be reached. An example cited is the unauthorised disclosure of health records; and
- describe the circumstances in which it may be impossible or impractical for an entity to contact a significantly affected individual.

Generally, an '*individual is significantly affected*' by a data breach if:

- the individual is an individual to whom the risk (eg, unauthorised access to or unauthorised disclosure of) relates;
- the individual is an individual to whom the personal information (being the subject of serious data breach) relates; and
- an individual who, under the regulations, is taken to be affected by the serious data breach.

Next Steps

If the Bill is passed in its current form, this leaves entities with only nine months to ensure their privacy compliance system is ready for mandatory data loss notification.

To prepare, an affected entity should add to their '2013 privacy to-do list' the following considerations:

- Are existing privacy compliance systems adequate? For example:
    -
    - Have all reasonable steps been taken to prevent unauthorised access to or loss of data?
    - Are existing defences against computer hacking sufficient?
    - Are information handling practices appropriate and are relevant policies actually being followed?
    - Are existing privacy practices and information technology systems able to detect and/or prevent a serious data breach?
- What needs to be implemented (eg training and new practices, policies and procedures) to be ready for 14 March 2014?
- How will we practically determine if a privacy alert needs to be issued in a timely way?

Footnotes

[1]Since publication of this article on 11 December 2012, the maximum civil penalty amount for a body corporate has increased from $1.1m to $1.7m due to an increase of the penalty unit amount as a result of the commencement of the *Crimes Legislation Amendment (Serious Drugs, Identity Crime and Other Measures) Act 2012* (Cth) on 28 December 2012 (as stated in our article http://www.holdingredlich.com/information-technology/penalty-unit-hike-cost-of-offending-soars).

[2]The Attorney General cited the examples of Sony Playstation, Australia Post, Vodafone and Telstra – http://news.ninemsn.com.au/national/2013/05/28/18/20/govt-to-introduce-privacy-alert-laws