INDUSTRY NEWS

Mandatory Data Breach Reporting - The Privacy Amendment (Notifiable Data Breaches) Bill 2016

On 19 October 2016, a Bill to amend the *Privacy Act 1988* was presented to Federal Parliament which will bring Australia in line with other major economies in the area of mandatory data breach reporting.

Under the Bill, organisations will need to report to the Australian Information Commissioner incidents such as loss, interference or unauthorised disclosure of information which would be likely to result in serious harm to the individuals concerned.

Data Breaches Currently

The Australian Privacy Principles (APPs) in the Privacy Act apply to most Australian Government agencies and private sector organisations with an annual turnover of more than $3 million (subject to some exceptions).

APP 11 requires APP entities to take reasonable steps to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. However, at present, there is no general legal requirement that an entity notify anyone of a data breach.[1]

The Office of the Australian Information Commissioner (OAIC) administers a voluntary data breach notification scheme based on an Australian Law Reform Commission (ALRC) recommendation which includes a 'real risk of serious harm' notification threshold.

The OAIC's current 2014 Guide[2] was drafted to assist entities to manage data breaches, and provides guidance on how to assess the risk of harm to individuals following a data breach.

The 2014 Guide states that:

- Entities should have a data breach policy and response plan (that includes notifying affected individuals and the OAIC).
- Data breaches are not limited to malicious actions but can also occur due to internal errors or failure to follow information handling policies.
- If there is a **real risk of serious harm**[3] as a result of a data breach, the affected individuals and the OAIC **should** be notified.
- Notification can be an important mitigation strategy for individuals.
- Notification can promote transparency and trust in the organisation.

The Current Guide confirms that notification of a data breach is not required by the Privacy Act. However, the steps in the Guide are highly recommended by the OAIC, and will likely become mandatory should the Bill be passed.

There are four steps in responding to a data breach:

- Step 1 – Contain the breach and do a preliminary assessment
- Step 2 – Evaluate the risks associated with the breach
- Step 3 – Notification
- Step 4 – Prevent future breaches

The OAIC Guide refers to the ALRC's recommendations that the Privacy Act be amended to impose a mandatory obligation to notify the Privacy Commissioner and affected individuals in the event of a data breach that could give rise to a real risk of serious harm to affected individuals.

The Bill

If the Bill is passed, Australian legislation will reflect the position in similar jurisdictions, such as the UK, EU, USA, and Japan, where mandatory breach reporting has been a legislative requirement for many years.

The draft Bill's mandatory data breach notification scheme will commence 12 months after the Bill receives Royal Assent and will amend the Privacy Act to insert a new 'Part IIIC', which will define when a 'serious data breach' occurs and explain when and in what form notification of serious data breaches is required.

Notification to the Commissioner and affected individuals would only be required following a 'serious data breach'.

A serious data breach would occur if:

- personal information (which includes health information),
- credit reporting information,
- credit eligibility information, or
- tax file number information,

that an entity holds about individuals, is:

- subject to unauthorised access or unauthorised disclosure that, puts any of the individuals to whom the information relates at 'real risk of serious harm'.

There are also provisions in the Bill which note that if the organisation takes action before any serious harm is caused (such as retrieving or deleting the information before the unintended third party can access the information), then the "eligible data breach" is treated as never having occurred and therefore is not reportable, nor does it trigger the notification obligations to individuals.

Data breach notification allows individuals whose personal information has been compromised in a data breach to take remedial steps to avoid potential adverse consequences, such as financial loss or identity theft.

Examples might include cancelling a credit card, or changing an online password.

Implications

The Australian Red Cross recently suffered a large data breach of their DonateBlood website. The breach involved sensitive health information of many individuals.

This breach, and the manner in which it was handled, exemplified the importance of mandatory reporting, and demonstrates OAIC's priority for transparency on the part of the organisation when dealing with data breaches.

The penalties for not reporting "eligible data breaches" include fines of up to $1.8 million for organisations.

Organisations which have not already put in place a report policy which best reflects the steps in the 2014 OAIC Guide should familiarise themselves with the Guide and implement a policy which incorporates the Guide's 4 Steps when responding to a data breach noting, of course, that 'Step 3 Notification' for 'eligible data breaches' will soon be mandatory.

[1] Mandatory data breach notification is required only in the event of unauthorised access to eHealth information under the *My Health Records Act 2012*, and other provisions of the Privacy Act create equivalent obligations in relation to credit reporting information, credit eligibility information and tax file number information.

[2] "Data breach notification guide: A guide to handling personal information security breaches". The Guide can be found here.

[3] A 'real risk of serious harm' is not defined by the Act, however the Guidelines note that whether or not a breach poses a real risk of serious harm can be evaluated by assessing the type of information disclosed, the context, cause, and extent of the breach, and the risk to the individual – taking into consideration who the recipient was, and assessing the possible harm that could arise as a result of the breach (e.g. identity theft, threat to physical safety or emotional wellbeing, humiliation, damage to reputation etc).