PiperAlderman

Article Information

Service: Corporate & Commercial, Privacy & Data Protection

Counting down to the introduction of the mandatory data breach notification obligations

The incoming mandatory breach obligations that are soon taking effect, and outline the steps that you can take to prepare for these changes now.

Snapshot of new obligations

A mandatory data breach notification regime under the new *Privacy Amendment (Notifiable Data Breaches) Act 2017* will come into force from 22 February 2018, under which various entities will be required to assess data breaches and notify individuals and the Commissioner of any such breaches in certain circumstances.

Who will be affected?

Any entity which is currently, or will be, subject to the *Privacy Act 1998* will be required to comply with these notification obligations. This broadly includes entities which:

- operate a business with an annual turnover of more than $3,000,000;
- provide a health service and hold health information other than in an employee record;
- disclose personal information about another individual for a benefit, service or advantage, or provide a benefit, service or advantage to collect personal information about another individual from anyone else, except in certain circumstances;
- are contracted service providers for a Commonwealth contract;
- are credit reporting bodies which hold credit reporting information;
- are credit providers which hold credit eligibility information; or
- are file number recipients which hold tax file number information.

What do the new obligations relate to?

The new obligations focus on the steps that a relevant entity is required to take in respect of an 'eligible data breach'.

Broadly, there is an 'eligible data breach' where there is unauthorised access to, unauthorised disclosure of, or loss of, information held, where such access, disclosure or loss is likely to result in 'serious harm' to any of the individuals to whom the information relates.

'Serious harm' may include serious physical, psychological, or emotional harm, in addition to economic, reputational and financial harm.

When assessing whether a data breach is likely to result in 'serious harm', consideration should be given to:

- the kinds of information kept and the sensitivity of such information;
- whether the information is protected by one or more security measures and, if so, the likelihood that any of those security measures could be overcome (for example, is the information encrypted or otherwise protected?);
- the likelihood that the persons who could obtain this information would have the intention of causing harm to any of the individuals affected (for example, is the person a cyber criminal who has hacked the system or an employee who has accessed the information by accident?);
- the likelihood that malicious users who obtain the information would have the technology or methodology to circumvent the security mechanisms and the nature of the harm (for example, the encryption key for the encrypted information).

What to do if you suspect a breach

If you suspect that there is an eligible data breach but do not have reasonable grounds to believe there has in fact been a breach, the first step to take is to assess the suspected breach. This involves carrying out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that there has in fact been an eligible data breach, and taking all reasonable steps to complete the assessment within 30 days of suspecting a breach.

What to do if you become aware of a breach

Notify the Commissioner

If there are reasonable grounds to believe that there has been an eligible data breach, then you must, as soon as practicable, provide a statement to the Commissioner setting out:

- the entity's identity and contact details; and
- a description of the eligible data breach; and
- the kinds of information concerned in the eligible data breach; and
- recommendations about the steps that individuals should take in response to the eligible data breach (**Notification Statement**).

If there are reasonable grounds to believe that the eligible data breach was also an eligible data breach of another entity, the Notification Statement may also set out the identity and contact details of the other entity.

If the Commissioner is aware that there are reasonable grounds to believe that there has been an eligible data breach, then the Commissioner has the power to direct that a Notification Statement be prepared.

Notify individuals

After providing a Notification Statement to the Commissioner, you must also notify the individuals or the public in one of three ways, as soon as practicable:

- if practicable, take reasonable steps to notify the contents of the Notification Statement to each individual to whom the relevant information relates;
- if practicable, take reasonable steps to notify the contents of the Notification Statement to each of the individuals who are at risk from the eligible data breach; or
- if neither of the above two options are practicable, publish a copy of the Notification Statement on your website, and take reasonable steps to publicise the contents of the Notification Statement.

You may notify individuals in the first two options by using the normal method of communication for those individuals, including by email. If there is no normal method of communication, then notification can be made by post.

What are the exceptions to notification?

There are a number of exceptions to the notification obligations which apply in certain circumstances. Broadly, these include:

- where remedial action is taken in relation to the access, disclosure or loss of information and before any serious harm has resulted, and as a result of such action, a reasonable person would conclude that the access, disclosure or loss would not be likely to result in serious harm to any of the individuals;
- where an eligible data breach is an eligible data breach of a number of other entities and one entity has complied with the notification obligations;
- where the eligible data breach has been, or is required to be, notified under the *My Health Records Act 2012*;
- where the Commissioner makes a declaration in the public interest; and
- where notification may prejudice enforcement related activities or is inconsistent with various secrecy provisions.

What you should do to prepare for these notification obligations

Given the impending commencement of these notification obligations, consideration should be given to taking steps now to review your internal systems and prepare for these changes. The steps that you should be taking now include:

- preparing, reviewing, and implementing your cyber security action plan and breach response plan;
- reviewing and updating your contracts to deal with these notification obligations;
- updating your corporate governance plan and internal policies;
- understanding your obligations and the steps to take to comply with these notification obligations;

- preparing draft notification statements in preparation for any potential breaches to control the message provided to the public; and
- educating and training employees, management and board members to understand what steps to take in the event of a data breach.

Seek assistance from the experts

Most entities do not have the specific skills, knowledge, experience or expertise to put in place appropriate cyber security measures and protections on their own. It is therefore crucial to engage cyber security experts who are skilled and experienced to assist in managing and reducing the impact of cyber security risks, both from a legal and an IT security perspective.

Legal experts who specialise in cyber security can assist by working with IT security experts to raise awareness and educate the board, assist organisations to understand their legal, regulatory and contractual obligations, prepare a cyber security action plan, establish good corporate governance procedures, prepare appropriate policies, provide training, and review contracts and insurance policies to ensure you are ready for these new changes.