SQUIRE PATTON BOGGS

The Notifiable Data Breaches Scheme Has Commenced – How Will It Impact Your Business?

New privacy legislation means that the vast majority of businesses in Australia are now required to report and publicise security breaches resulting in data loss.

Background

From 22 February 2018, any entity required to comply with the Privacy Act 1988 will be subject to additional obligations. The Privacy Amendment (Notifiable Breaches) Act 2017 (Data Breach Amendment) means that businesses are likely to be investigated and fined if they keep data breach or loss incidents secret, and brings Australia into line with a number of other jurisdictions, including the US and Europe.

Increased Exposure to Litigation

The experience in the US (which has had notification obligations in most states since 2002) suggests that increased visibility of data breaches will inevitably result in an increase in claims brought against entities, both from customers and shareholders.

To Whom Does the Data Breach Amendment Apply?

- Commonwealth government agencies and private sector organisations that are currently subject to the Australian Privacy Principles under the Privacy Act
- Private sector organisations (including non-for-profits) with annual turnover of more than AU$3 million
- Small businesses earning AU$3 million or less that are any of the following:
  - Health service providers
  - Involved in trading personal information
  - Contractors that provide services under a Commonwealth contract
  - Credit reporting bodies

Foreign organisations will also be subject to the Data Breach Amendment where they satisfy the "Australian link" test under the Privacy Act. This captures international corporations operating an online business targeting Australian individuals, collecting personal information from Australian residents or tracking them for marketing purposes.

The changes are particularly relevant to entities where the collection, storage, use and disclosure of personal information is an integral aspect of their business activities. For example providers of financial services, private sector healthcare providers or organisations which handle health information, and technology companies especially those in data-driven fields such as marketing, analytics and advertising. Government should also be included in this list, though typically the breach relates to a government contractor rather than the government entity itself[1].

What Is an "Eligible Data Breach"?

The legislation requires entities to take steps in response to an eligible data breach, in other words where both of the following criteria are met:

- There is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity
- A reasonable person would conclude that the access, disclosure or loss is likely to result in serious harm to any individual to whom that information relates

It is important to bear in mind that the notification obligations under the Data Breach Amendment apply to any loss or disclosure where serious harm is likely to result, not just loss or disclosure that results from malicious actions. A recent study by Ponemon Institute LLC found that 28% of data breaches in Australia were attributable to employee negligence[2], so it is important that employers review security measures to protect against unauthorised access, disclosure and loss in the handling of information by employees.

In the Event of a Reportable Data Breach

Entities are required to take a proactive approach to the monitoring of their information handling systems and processes. This means that on suspicion of breach or loss of data, entities must conduct an assessment within 30 days to confirm if breach or loss of data has in fact occurred. If so, the entity must:

- Prepare a statement which contains prescribed information, including the identity and contact details of the entity, a description of the eligible data breach and the kinds of information concerned, and recommendations about the steps that individuals should take in response to the data breach (**Statement**)

1 For example, the release of nearly 5,000 personal records of a total of nearly 50,000, which were released as a result of a contractor misconfiguring an Amazon S3 bucket or the November 2016 hack of a national security contractor which resulted in the disclosure of sensitive defence documents including information on the Joint Strike Fighter program.

2 2017 Cost of Data breach Study. Benchmark research sponsored by IBM Security

- Provide a copy of the Statement to the Office of the Australian Information Commissioner (**OAIC**)
- Notify those individuals who are at risk of serious harm from the eligible data breach, or all individuals to whom the information relates, depending on what is practicable

If it is not practicable to notify individuals directly, the entity must post the notification prominently on its website and take reasonable steps to publicise the notice.

Avoidance of Notification Requirement

There are exceptions to this notification requirement. One example is where the entity takes remedial action so that the breach would not be likely to result in serious harm to any individual. Other exemptions relate to healthcare providers with pre-existing obligations under the My Health Records Act 2012 (Cth), or where the obligations are inconsistent with law enforcement activities or specific legislation.

What You Need to Do

These changes have been widely publicised over the past 12 months and the expectation is that the OAIC will commence enforcement from day one. If you have not done so already, here are the key tasks to prepare your organisation for compliance:

- **Take a whole of entity approach**: Understand and approach data privacy as an enterprise-wide risk management issue – not just an IT issue. Discussions about the data privacy risk framework should appear regularly on board meeting agendas.
- **Identify at risk data**: Entities should perform an audit of the personal information they hold, consider whether that information is actually required to carry out the entity's business operations, and ensure that "at risk" information is held in a manner that complies with security obligations set out in the legislation.
- **Audit key contracts**: Entities should consider the extent to which they are exposed to supply chain risk through third-party suppliers or particular customers and ensure contractual provisions are in place to manage compliance with notification obligations. Generally, where a breach occurs in respect of jointly held information, only one entity will be required to comply with the notification obligations imposed under the Data Breach Amendment.
- **Develop a data breach response plan**: Responding to a data breach will typically require a collaborative approach which calls on the expertise of legal and communications firms, as well the entity itself. This is because there are a number of elements to a data breach response, including compliance with notification requirements at law, internal investigation of the breach, and publically communicating the breach in a manner which mitigates reputational damage to the extent possible. At a minimum, clear reporting lines to personnel with management and privacy compliance responsibilities should be in place.
- **Consider whether your organisation must also comply with foreign data breach laws**: Just as foreign entities engaging in business with Australian individuals must comply with our legislation, Australian entities holding information on certain foreign nationals may have reciprocal obligations under foreign laws.

Can We Help?

Our Data Privacy & Cybersecurity team includes legal and regulatory experts who focus on providing practical advice surrounding information collection, use, transfer, storage, sharing and security. Our advice balances legal requirements, best practice and business needs. With specialists based in the US, UK, Europe and Asia Pacific, we can assist you with your domestic and international compliance needs.

Contacts

Margie Tannock
Partner, Perth
T +61 8 9429 7456
E margie.tannock@squirepb.com

Richard Horton
Partner, Sydney
T +61 2 8248 7806
E richard.horton@squirepb.com

Michael Muratore
Senior Associate, Sydney
T +61 2 8248 7890
E michael.muratore@squirepb.com