ipsec

Privacy Legislation Update

$1.7 Million Civil Penalty for a Privacy Act Breach from March 2014

The Privacy Amendment Act 2012 (No. 197, 2012), has passed through the Australian Parliament taking effect on 12 March 2014. The new legislation introduces significant obligations for the protection of personal information held by Australian organisations, and material financial penalties.

Organisations that collect and or hold personal information are required to comply with the Privacy Act 1988 and its Amendments. Privacy Amendment (Enhancing Privacy Protection) Act 2012 (No. 197, 2012) introduces the Australian Privacy Principles (APPs) which includes, "APP11 – Security of Personal Information".

APP11 requires that "If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information: (a) from misuse, interference and loss; and (b) from unauthorised access, modification or disclosure."

The Privacy Act 1988, under the heading "Serious and repeated interferences with privacy" states "An entity contravenes this subsection if: (a) the entity does an act, or engages in a practice, that is a serious interference with the privacy of an individual; or (b) the entity repeatedly does an act, or engages in a practice, that is an interference with the privacy of one or more individuals. Civil Penalty: 2,000 penalty units."

The Privacy Amendment Act 2012 (No. 192, 2012) states that "The pecuniary penalty must not be more than: (a) if the entity is a body corporate – 5 times the amount of the pecuniary penalty specified for the civil penalty provision;"

Each "penalty unit" is worth $170, allowing the Privacy Commissioner to request a court levy a civil penalty of up to $1.7 million for an organisation found to be in breach of the Privacy Act.

Key points:

1

New Privacy Act Requirements for all Australian Organisations with revenue greater than $3mil.

2

Enforced from 12 March 2014.

3

All organisations must "take such steps as are reasonable in the circumstances to protect" personal information.

4

Organisations retain responsibilty when outsourcing, this includes when using Cloud service providers.

5

Possible incoming compulsory breach notification requirements.

6

Up to $1.7mil civil penalty for organisations.

What is personal information?

The Privacy Act 1988 defines personal information as being "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or an opinion."

The amended Privacy Act defines personal information as including:

- The person's name and address; or
- Medical records & health information; or
- Bank account details; or
- Photos & videos; or
- Biometric & genetic information; or
- Likes & dislikes; or
- Opinions; or
- Places of work; or
- Racial or ethnic origin; or
- Memberships; or
- Beliefs; or
- Criminal record; or
- Sexual preference or practises.

What is "reasonable" security?

The concept of "reasonable" security is fairly subjective and is very much contextual to the circumstances of the organisation.

Broadly speaking, however, organisation's specific "reasonable security" level will be determined based on:

- The nature of the entity
- The nature & quantity of personal information held
- The risk to individuals of unsecured personal information
- The data handling practises of the organisation
- The ease with which a security measure can be implemented

Organisations looking to comply with the Privacy Act requirements for information security should look to achieve measures to prevent, detect and respond to a breach.

Preventing a Breach

Organisations should look to have explicit tools in place to prevent a breach of the personal information held by them. This should include, but is not limited to:

- Privacy by design
- Policies, Processes & Procedures
- Preventative Countermeasures:
  - Firewalls & Intrusion Prevention
  - Network Segmentation
  - Role Based Access Controls
  - Anti-Malware
  - Email & Web Security Controls
  - Encryption
  - Remote Access with Strong Authentication
  - Mobile Device Security & Control
  - Patching & Vulnerability Detection
  - Physical Security
  - Application Whitelisting
- Auditing (e.g. Penetration Testing)
- Training of Personnel

Detecting a Breach

Due to the rapidly evolving nature of the information security threat spectrum, it is important that organisations also include breach detection capabilities within their environment. This should include:

- Malware Detection
- Intrusion Detection
- Security Incident & Event Management (SIEM)
- Whistle blowing

Responding to a Breach

As and when a breach occurs the organisation must have policies, processes and tools in place to provide a suitable response. This includes, but is not limited to:

- Notification of impacted individuals & the Office of the Australian Information Commissioner
- Forensic Analysis Tools
- Business Continuity & Disaster Recovery tools.

About IPSec

IPSec are specialists in information asset security; technology experts who know how to mitigate risk to business by implementing end-to-end solutions that protect invaluable intelligence, data and information. Their capabilities extend from assessing vulnerabilities and threats, to designing and implementing customised security strategies, to managing execution and optimising results. IPSec are guardians of business confidence, providing high levels of protection and optimal assurance of an organisation's security posture.

IPSec is about mitigating risk, enabling confidence and agility by ensuring a reliable IT environment that allows business to get on with business.

Phone 1300 890 902
ipsec.com.au
enquiry@ipsec.com.au

Building 10, Omnico Business Centre
270 Ferntree Gully Rd, Notting Hill
VIC 3168, Australia