Article Information

Authors: Craig Subocz, Tim Clark, Charlotte Coburn
Service: Cyber Security, Intellectual Property & Technology, Privacy & Data Protection
Sector: IT & Telecommunications

Overhaul of Privacy Act strengthens penalties and gives Information Commissioner greater powers to gather and share information on data breaches

Following high profile data breaches, the *Privacy Act 1988* (Cth) (Privacy Act) has been amended to increase the monetary penalties for serious or repeated privacy breaches. Additionally, the Information Commissioner now has greater powers to gather and to share information to resolve data breaches.

Up to an estimated 10 million Australians have been affected by at least one of the high profile data breaches affecting high profile Australian companies in 2022. In October 2022, the Attorney General, the Hon Mark Dreyfus KC MP, promised to toughen Australia's privacy laws. In December 2022, the Privacy Act was amended to increase penalties for serious or repeated breaches of privacy and to improve the capacity of the Information Commissioner to gather and share information about data breaches.

Tougher penalties

The headline grabber is the increase to penalties for serious or repeated breaches of privacy. The table below sets out how the amended Privacy Act provides for significantly greater civil penalties for serious or repeated interferences of privacy when compared to the penalties under the Act before the amendments received royal assent.

	Previous penalty amounts	New penalty amounts
Bodies corporate	$2.22 million	An amount not exceeding the greater of: • $50 million; • three times the value of the benefit directly or indirectly obtained by the body corporate, and any related body corporate, from the conduct constituting the serious or repeated interference with privacy and that is reasonably attributable to the conduct constituting the contravention; or • if the court cannot determine the value of the benefit obtained by the body corporate, and any related body corporate, 30% of the body corporate's adjusted turnover in the relevant period.
Other entities	$444,000	$2.5 million

The Government's intention for these changes is to ensure that tougher penalties meet community expectations for serious data breaches and deter organisations from continuing to engage in "problematic data practices".

Whilst the impetus for the amendments may have been large consumer-oriented businesses with high profile data breaches, the increased penalties apply to all public and private sector organisations governed by the Privacy Act.

Accordingly, all organisations governed by the Privacy Act should ensure that they give the necessary oversight, management and resources to privacy compliance and information security, having regard to the context of those organisations and their activities.

Greater information gathering and sharing powers

Under the Privacy Act's notifiable data breach (**NDB**) scheme, organisations governed by the Privacy Act have obligations to notify the Information Commissioner and affected individuals of an "eligible data breach". Although the concept of an "eligible data breach" has not changed, the Information Commissioner is now granted greater information gathering and information sharing powers.

The Information Commissioner now has the power to compel an organisation to provide information and/or documents relevant to an actual or suspected "eligible data breach" of the organisation, and/or the organisation's compliance with the Privacy Act in relation to an "eligible data breach".

Additionally, the Information Commissioner is provided with greater information-sharing powers to share information regarding a notified data breach with other regulators, both domestically and internationally. The Commissioner has the power to publish a determination or information relating to an assessment on the Commissioner's website, and disclose all other information acquired in the course of performing functions or duties if it is in the public interest.

Key Takeaways

- The amended Privacy Act has significantly increased the maximum penalties for serious and repeated privacy breaches and expanded the powers of the Information Commissioner to gather and share information about notifiable data breaches.
- Organisations governed by the Privacy Act should review their governance and management frameworks for privacy compliance (including privacy compliance manuals, internal privacy induction training and data breach response plans).
- Organisations should review their governance and management frameworks relating to information security to ensure that their organisation has strong information security frameworks and safeguards.
- Piper Alderman regularly works with clients from a wide range of industries to manage and minimise the risks of privacy compliance, data breaches and information security risks.