CYBER PRECEDENT

Strengthening the legal profession's defence against online threats

Content prepared by the Law Society of NSW for the Law Council of Australia's

CYBER PRECEDENT ON THE AUSTRALIAN PRIVACY PRINCIPLES AND CYBER SECURITY

Cyber threats and risks continue to grow in scale and complexity. These threats create legal and regulatory risk, as well as business risk to law firms. Law firms are not immune and are often targeted businesses. Accordingly, it is important for law firms take security measures to prevent breaches of their cyber security.

Cyber security incidents often occur due to the failure by an organisation to take active and effective measures to ensure the security of their networks, systems and data. Data leakage may result from internal or external factors. These include data theft by intruders or employees, unauthorised access, or accidental disclosures of information caused by systems failures of an organisation or its agents.

Where any data breach or cyber security incident involves personal information, the *Privacy Act 1988* (Cth) ("Privacy Act") will be relevant. The Privacy Act requires all private sector organisations with an annual turnover of more than $3 million (in addition to other specified small businesses) to comply with thirteen Australian Privacy Principles ("APPs") with regard to the handling, use and management of personal information. Even if a law firm is not regulated under the Privacy Act it is considered best practice to take steps to comply with the APPs.

Under the Privacy Act, an act or practice of an entity covered by the Privacy Act that occurs on or after 12 March 2014 and that breaches an APP in relation to personal information about an individual, is 'an interference with the privacy' of the individual. The Office of the Australian Information Commissioner ("OAIC") has powers to investigate possible interferences with privacy, either following a complaint by the individual concerned or on the Commissioner's own initiative. The Commissioner also has a range of enforcement powers and other remedies available. In cases where the Commissioner has determined that there has been a breach of an APP which has caused interference with the privacy of an individual, the remedies will often include a review of the organisation's procedures and processes, along with a written apology and an award of damages for non-economic loss. Past determinations of the Commissioner are available at www.oaic.gov.au/privacy-law/determinations.

A breach of an APP has significant reputational and legal consequences for an organisation. Law firms need to be alert to the risks and have risk management procedures in place. The key APP in relation to cyber security is APP 11. Law firms may also wish to consider the application of APP 6. Further information about these principles and their application is set out below.

Law Council OF AUSTRALIA

THE LAW SOCIETY OF NEW SOUTH WALES

APP 11

APP 11 relates to the security of personal information. APP 11.1 provides:

> 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.

Determining what are "reasonable steps" will depend on a number of factors relating to the type of personal information held and the size of the organisation. According to the OAIC, reasonable steps include implementing strategies in relation to:

- governance, culture and training;
- ICT security;
- access security;
- third party providers (including cloud computing);
- data breaches; and
- physical security.[1]

Failure to take reasonable steps to prevent a cyber security breach or incident that results in any loss or unauthorised access or disclosure of personal information could expose law firms to regulatory attention from the OAIC.

At a minimum every law firm should ensure that it has:

- a cyber security or information security system framework;
- up to date staff training on security breaches;
- up to date software and hardware, and is aware of new and emerging cyber risks (including ongoing monitoring);
- appropriate cyber security insurance is in place as either a standalone policy or as an extension to its professional indemnity insurance policy. It is also important to check whether the insurance covers first party and third party cyber risks; and
- the implementation of a data incident response plan.

Many organisations outsource a variety of operations, such as data storage and website management. Where this is the case, it is important to have contracts in place with partners or suppliers to ensure that their cyber security and data management practices are adequate. It is also important to have arrangements in place to ensure adequate supervision of the partners' compliance with privacy standards.

APP 6

APP 6 sets out when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (the "primary purpose") or for a secondary purpose if an exception applies.

The reference to disclosure in APP 6 does not extend to 'unauthorised access'. An APP entity is not taken to have disclosed personal information where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information.[2] There will be no disclosure where information held by an APP entity is accessed as a result of a sophisticated security cyber-attack.[3]

In some cases the question of whether there is intended access for a third party may be ambiguous – for example, it may not be clear whether there was any form of lock or barrier denying authorisation presented to the third party. APP entities should consider the possibility that sufficiently ineffective or non-existent security measures could be taken as an invitation and implicit authorisation to access the information, which may result in a breach of APP 6.

---

1 Office of the Australian Information Commissioner, *APP Guidelines*, "Chapter 11: APP 11 – Security of Personal Information", 11.8, dated March 2015, available at www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information.

2 Office of the Australian Information Commissioner, *APP Guidelines*, "Chapter 6: A PP 6 – Use or disclosure of personal information", 6.11, dated February 2014, available at www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information.

3 Office of the Australian Information Commissioner "Own Motion Investigation Report — Sony Playstation Network/ Qriocity", September 2011, available at www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/sony-playstation-network-qriocity.

While generally not a 'disclosure' for the purpose of APP 6, personal data which is accessed or distributed without authorisation through a cyber security breach may be treated as a notifiable data breach under the new mandatory scheme, triggering an urgent obligation to evaluate and possibly notify those affected so as to assist their capacity to consider a prompt mitigating response of their own. For further information, please see separate guidance on obligations under the new mandatory Notifiable Data Breaches scheme.

Content prepared by the Law Society of NSW for the Law Council of Australia's Cyber Precedent on obligations under the new mandatory Notifiable Data Breaches scheme and the costs of those obligations

From 22 February 2018 the *Privacy Amendment (Notifiable Data Breaches) Act 2017* will establish a Notifiable Data Breaches scheme in Australia. All private sector organisations with an annual turnover of more than $3 million (in addition to other specified small businesses under the *Privacy Act 1988* (Cth)) must notify both individuals likely to be at risk of serious harm and the Office of the Australian Information Commissioner ("OAIC") if the organisation suspects an eligible data breach has occurred.

The Notifiable Data Breaches scheme will therefore apply to the majority of law firms in Australia. All law firms are encouraged to review their policies, procedures and systems for ensuring data security and responsiveness to cyber security threats and incidences. Law firms should have a data breach response plan to ensure they are able to respond quickly to any actual or suspected data breach. A data breach response plan will also be important as the Notifiable Data Breaches scheme is likely to lead to an increase in the number of claims consequent upon a cyber breach including not only claims potentially to be made by clients but claims made by other parties to litigation.

The OAIC has published a guide to developing a data breach response plan as well as guidelines relating to which data breaches are notifiable, how to notify individuals about an eligible data breach and the role of the OAIC. Further helpful resources to prepare for the Notifiable Data Breaches scheme can be found at www.oaic.gov.au. Where such notifications are required, consideration should also be given to the law firm's insurance coverage and broader applicable disclosure obligations (e.g. under the *Corporations Act 2001* (Cth)).

If a law firm fails to notify an eligible data breach it may be:

(a) directed by the OAIC to notify an eligible data breach and to notify the individuals involved or take such steps as are reasonable in the circumstances to notify the content to each of the individuals or publish a statement advising of the breach on the law firm's website; and

(b) subject to penalties which include the existing powers of the OAIC under the Privacy Act 1988 (Cth) including written undertakings and civil penalties of up to $420,000 for individuals and $ 2.1 million for companies.

It is important that law firms protect themselves from potential cyber risks by taking active measures to ensure the security of personal information.

Except in incidents where the number of affected individuals is high, the overall cost of complying with the notification requirements should be low and absorbed within the overall steps to respond to the incident.