IS YOUR FIRM **PRIVACY COMPLIANT?**

Simone Herbert-Lowe is a senior claims solicitor at Lawcover.

By Simone Herbert-Lowe

Solicitors have always been custodians of confidential information. Our obligations to maintain the confidentiality of information received during the solicitor/client relationship arise through the common law, contract and equity. More recently, privacy legislation has put additional obligations upon many organisations that hold sensitive personal information.

These obligations are not limited to clients and may extend to personal information held about any individuals.

While there has always been a need for solicitors to keep information confidential, there is now increased awareness of the need to prevent or respond to data breaches in a world where digital communications are the norm and where technology amplifies the risk of information being illegally accessed or unwittingly disclosed to a wider audience.

Law practices that fall within the ambit of the *Privacy Act 1988 (Cth)* ('***Privacy Act***') are required to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure (Australian Privacy Principle 11).

How do data breaches occur?

Data breaches can occur in many different ways. Examples provided by the Office of the Australian Information Commissioner ('**OAIC**') include lost or stolen laptops, removable storage devices, hard disk drives and other digital storage media being disposed of or returned without the contents being first erased, the hacking of databases containing personal information, paper records being stolen from insecure recycling bins – and the list goes on.

Snapshot

- New privacy legislation due to commence in early 2018 will require the mandatory reporting of certain data breaches for organisations which are required to comply with the *Privacy Act*.
- Be aware that the new legislation could apply to your firm and to your clients.
- Consider a 'privacy audit' involving a review of employees' access to information, the quality of your cyber security measures and the adequacy of training programs.

New privacy compliance obligations

The Privacy Amendment (Notifiable Data Breaches) Bill 2016 passed through the senate on 13 February 2017. The scheme is expected to commence operation in early 2018.

The impact of these changes was discussed by Nick Abrahams and Jamie Griffin in their article 'The End of a Long Road: Mandatory Data Breach Notification Becomes Law' (32 *LSJ*, April 2017, 76). Of particular significance is the new legislative requirement that the Privacy Commissioner and any affected individuals be notified when an 'eligible data breach' has occurred.

An eligible data breach occurs where:

- there is unauthorised access to, or unauthorised disclosure of, personal information held by the agency or organisation, or personal information is lost in circumstances where access to, or unauthorised disclosure of, information is likely to occur; and
- a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates (s 26WE(2)).

The legislation grants the Privacy Commissioner the power to seek civil penalty orders of up to $360,000 for individuals and $1.8 million for corporations in cases where the failure to make an eligible data breach notification amounts to a serious or repeated interference with privacy.

Organisations required to comply with the legislation

Relevant entities include:

- Australian Government agencies;
- all businesses and not-for-profit organisations with an annual turnover of more than $3 million;
- health service providers and holders of health records;
- credit reporting agencies; and
- organisations holding personal tax file numbers ('**TFNs**').

Risk for solicitors

Direct risks for law practices

Regardless of size, all law practices should be aware of the new privacy legislation because:

- larger practices with annual turnover in excess of $3 million will be subject to the legislation;
- many practices hold TFNs and are subject to the legislation for the purposes of those records; and
- many solicitors hold health records (for example lawyers who act in personal injury litigation or those who hold medical certificates in relation to individuals' legal capacity for the purposes of powers of attorney).

If your law practice falls into any of these categories it will be required to comply with the new privacy regime and you should prepare for its introduction in early 2018.

Risks in failing to advise clients

If you advise clients who fall into the above categories and your retainer includes general corporate or commercial advice, consider whether your retainer includes an obligation to advise about the need to prepare for the privacy legislation.

Assessing whether your firm's privacy protections are adequate

Breaches of privacy occur through both failures in technology and negligent (or sometimes malicious) actions by individuals. Workplace culture is an important predictor of an organisation's vulnerability to data breaches (*Daily Willis ReView*, Willis Towers Watson, 16 March 2017). When assessing the likelihood of privacy breaches, consider the potential consequences of privacy breaches and whether it is appropriate for all employees to have access to sensitive personal information. Implement appropriate training to emphasise the importance of protecting private information, particularly for new employees.

In terms of technology, ensure that software is up to date, and consider engaging a cyber security expert to assist you if required.

The OAIC has recommended that organisations consider implementing privacy enhancing technologies to secure personal information through encryption, access control, copy protection and intrusion detection (Please refer to the OAIC's guide for additional recommended measures – see 'Data breach notification — A guide to handling personal information security breaches', available at www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches). **LSJ**

While there has always been a need for solicitors to keep information confidential, there is now increased awareness of the need to prevent or respond to data breaches in a world where digital communications are the norm and where technology amplifies the risk of information being illegally accessed or unwittingly disclosed to a wider audience.