# 2018: A year of significant changes to privacy law, affecting legal practices and clients

## Snapshot

- Two significant reforms to privacy law commence in 2018. Legal practitioners will need to consider the impact on clients, as well as on the operation of their own legal practices.
- The changes will affect all medium-large Australian businesses; some smaller businesses depending on the nature of their business; all Australian government agencies; and to a lesser extent state and territory agencies and small businesses in their capacity as employers.
- The changes include mandatory notification of data breaches, and the extension of European data protection law to Australia.

## February – Notifiable data breaches

### Who is affected

Commencing 22 February, amendments to Part IIIC of the *Privacy Act 1988* (Cth) will affect almost every organisation in Australia in some way:

- All entities already required to comply with the 13 Australian Privacy Principles (APPs), which includes all Australian government agencies, almost all businesses and non-profits with a turnover of more than $3m pa, plus some smaller businesses such as health service providers and contracted service providers to the Commonwealth;
- All organisations which receive Tax File Numbers (TFNs) – which will include bodies not regulated by the APPs, such as state and territory agencies and most small businesses, in their capacity as employers; and
- Credit providers and credit reporting bodies.

### The key requirements

The amendments require notification of certain types of data breaches. Notifiable data breaches are incidents which involve the loss of, or unauthorised access to or disclosure of, 'personal information' (or a TFN, or credit eligibility/reporting information) and which are likely to result in serious harm to one or more individuals. When a data breach meets this threshold test, notification is required, as soon as practicable, to both the Australian Privacy Commissioner and the affected individuals. The Privacy Commissioner is part of the Office of the Australian Information Commissioner (OAIC).

The legislation sets out the factors which impact on whether or not a data breach is 'likely to result in serious harm'; the timeframes in which an assessment must be carried out on a suspected breach; what a notification must contain; and how a notification must be made.

A failure to comply with the new notification requirements attracts a civil penalty of up to $2.1m.

### The takeaway

There are two objectives driving the move towards mandatory notification of data breaches. The first is to fulfil a duty of care to the affected individuals, by letting them know that their personal information has been put at risk. The second is to create a sufficient financial disincentive, such as to prompt organisations into investing

**Anna Johnston**
Director of Salinger Privacy

more in their privacy and security programs, to avoid data breaches in the first place.

### What to focus on

To prepare for a data breach, every organisation should prepare a Data Breach Response Plan. Having a plan in place can clarify what needs to be done when and by whom, in the first few hours and days after a data breach is discovered.

To avoid data breaches in the first place, the privacy team or legal advisor should be working hand-in-hand with the information security team. Staff need privacy training and constant reminders of privacy messaging; and third-party contractors, vendors and suppliers need to be bound by appropriate terms and subject to additional controls to avoid becoming the weakest link in the security chain.

### Further resources

The OAIC has guidance material available at www.oaic.gov.au. Salinger Privacy has Privacy Tools including a template Data Breach Response Plan available at www.salingerprivacy.com.au.

## May – The GDPR

### Who is affected

Commencing 25 May, the General Data Protection Regulation (GDPR) will regulate not only businesses based in the European Union (EU), but any organisation anywhere in the world which provides goods or services (including free services) to, or monitors the behaviour of, people in the EU.

The GDPR will replace the current set of differing national privacy statutes with one piece of legislation, and will offer a one-stop-shop approach when dealing with privacy regulators across all 28-member states of the EU – including the UK post-Brexit.

### The key requirements

In addition to harmonising the privacy rules across the EU, the GDPR introduces some new privacy obligations (although using the European term 'data protection' rather than 'privacy'). One is the Accountability principle, which requires organisations to be proactive. This means that if an organisation doesn't have an effective privacy compliance program, it can be found in breach of its data protection obligations even if it doesn't suffer a data breach. Although by no means a European invention – APP 1 in the *Australian Privacy Act* has the same objective – the financial penalties attached to the GDPR are intended to kick-start proper privacy governance in even the most recalcitrant organisations.

To help achieve this, the GDPR embeds a proactive requirement to do 'data protection by design', or as we tend to know it in Australia, 'privacy by design'. The technique used to ensure privacy is built-in to project design is known in the GDPR as Data Protection Impact Assessment, or here as Privacy Impact Assessment (PIA).

The GDPR also has a strong focus on getting reactive strategies right. It sets a default timeframe for notifying data breaches of only 72 hours, which adds further complexity for Australian organisations already adjusting to the new Australian notification scheme (above).

The GDPR also updates the scope of privacy law to cover such things as data portability and the 'right to erasure', and aims to ensure that algorithmic decision-making is subject to human review.

# 2018: A year of significant changes to privacy law, affecting legal practices and clients

### The takeaway

The objectives of the GDPR are to harmonise privacy law across the EU and streamline its application, and dramatically increase the penalties for non-compliance. Fines for failing to comply with the GDPR will reach up to €20m, or 4 per cent of a company's annual global turnover, whichever is the greater.

### What to focus on

Organisations of any size and sector in Australia will need to determine whether they fall within the scope of the GDPR, and then prepare accordingly. A comprehensive privacy management program and a culture of conducting PIAs on new projects will be needed to ensure compliance with both European and Australian privacy law.

## Further resources

Salinger Privacy has a free Privacy Officer's Handbook, to explain what should be included in a comprehensive privacy management program; and a range of commercial Privacy Tools to assist compliance, including PIA tools, training modules, template policies and procedures; see *www.salingerprivacy.com.au*.

The OAIC has guidance material about the GDPR and Australian businesses available at www.oaic.gov.au.

A different version of this article first appeared in the Law Society of NSW Journal, issue 41, February 2018.