Privacy Law Update August 2017

AUSTRALIAN BUSINESS
Lawyers & Advisors

1. AUSTRALIAN PRIVACY PRINCIPLES

The Australian Privacy Law changed significantly in March 2014 with the introduction of the Australian Privacy Principles (**APPs**). The APPs replaced the National Privacy Principles (**NPPs**). The changes reinforce and increase the security and record-keeping obligations of personal and sensitive information of persons whose data the business receives.

The changes include the following:

1. Use and disclosure of personal information related to health is now governed more strictly than personal information generally. This reflect the thinking that the release of certain health information can be extremely detrimental to a person's wellbeing and quality of life, and a privacy breach involving personal information related to health is accordingly held to be very serious by the regulator.
2. The APPs now require privacy policies to state the kinds of personal information collected by an entity, and how complaints may be made about a privacy breach, among other new requirements. The NPPs allowed privacy policies to be drafted in far more general terms APPs now allow.
3. APP entities (entities to whom the Privacy Act applies) must now set out any overseas disclosure of personal information that may occur. On our experience, many (if not all) APP entities run the risk of overseas disclosure of personal information due to the online servers that are used in most correspondence by and with APP entities. Normally, online services commonly used by APP entities are not generally capable of locking personal information to domestic servers. It is common for APP entities not to realise that they are running the risk of overseas disclosure, and privacy policies are frequently deficient with respect to how they deal with this aspect of the APPs.
4. Individuals must now be given the option to deal with APP entities anonymously or pseudonymously if that option is practicable for the APP entity.
5. APP entities must disclose any use of personal information for direct marketing purposes.
6. APP entities must respond to access requests within a reasonable period of time. This was not a requirement under the NPPs.
7. APP entities must take reasonable steps to correct personal information they hold, and must ensure (so far as is reasonable in the circumstances) that it is accurate, up to date, complete, relevant and not misleading. Previously, it was the responsibility of the individual to correct personal information.

Repeated interferences with the privacy of one or more individuals can attract civil penalties of up to **$420,000** for an individual, or **$2,100,000** for a body corporate.

2. RECENT LEGISLATIVE CHANGES

Following the assent of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* on 22 February 2017, new notification requirements under the *Privacy Act 1988* (Cth) (**Privacy Act**) will take effect by 22 February 2018. The new legislation will have the following effects:

1. APP entities must notify individuals who may be affected by a data breach or the potential exposure of their data. Penalties apply for not doing so.
2. Where there is a suspected data breach, an APP entity must carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an 'eligible data breach' of the entity. The APP entity must take all reasonable steps to ensure that the assessment is completed within 30 days after the entity becomes aware that there are reasonable grounds to believe that there has been a data breach.
3. An APP entity can avoid a suspected data breach from becoming an eligible data by taking remedial action before the any serious harms or loss of information occurs.
4. If there is an eligible data breach, the entity must prepare a statement that sets out the identity and contact details of the entity, describes the data breach that there are reasonable grounds to believe happened, sets out the kind of information concerned, and recommends steps that individuals should take in response.

Repeated interferences with the privacy of one or more individuals can attract civil penalties of up to **$420,000** for an individual, or **$2,100,000** for a body corporate.

3. EU DATA PROTECTION LEGISLATION

New data protection legislation in the EU changes the way that 'personal data' must be managed by businesses operating in the EU. If you have customers in the EU, or are conducting business in the EU, call us now to ensure that your data management is compliant with the new environment.

If you have any queries about your privacy policy or your data protection obligations, contact our privacy lawyer **Luke Topfer** on **(02) 9458 7239**, or email him at **luke.topfer@ablawyers.com.au**.