Notifiable Data Breaches and the Privacy Act: Is your Law Practice bound?

GRANT FEARY, DEPUTY DIRECTOR, LAW CLAIMS

The Notifiable Data Breach Scheme imposes additional obligations on entities subject to the Australian Privacy Principles. You should carefully check whether your Law Practice is subject to the scheme.

The *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)* commenced on 22 February, 2018. The Scheme contained in this Act (the NDB scheme) is an adjunct to the Australian Privacy Principles (APPs). One of the key APPs is APP 11 which requires entities subject to the APP to take such steps as are reasonable in the circumstances to protect personal information that they hold from misuse, interference, loss and unauthorised access, modification or disclosure.

The NDB Scheme requires entities which are subject to the scheme to notify the Australian Information Commissioner (AIC) and affected individuals if the entity has reasonable grounds to suspect that an "*eligible data breach*" has occurred. This is where there has been unauthorised access to or disclosure of information and a reasonable person would conclude that that access or disclosure would likely result in serious harm to any of the individuals to whom the information relates.

The relevant entity must itself make a judgement as to whether it is likely that the data breach will result in serious harm. According to the Explanatory Memorandum to the NDB Scheme *"serious harm"* is defined as including:

> *"serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach."*

If an entity suspects that an eligible data breach has occurred the entity must investigate the relevant circumstances within 30 days and if such a judgement as to serious harm is made then the data breach must be notified to the AIC and the affected individuals.

The notification must include:

- the identity and contact details of the notifying entity;
- a description of the data breach;
- the kind of information concerned; and
- recommendations about the steps that individuals should take.

A failure to comply with an obligation to notify will be deemed to be an interference with the privacy of an individual for the purposes of the *Privacy Act* and may result in orders for compensation or substantial penalties.

So, you are probably thinking, that's all very well but how is it relevant to my Law Practice? Obviously all law practices have duties of confidentiality with respect to their clients' personal information imposed as a result of the solicitor-client relationship but is your Law Practice subject to the additional requirements contained in the APP and the NDB scheme?

The APPs and, after 22 February, 2018 the NDB Scheme, apply to **all business including law practices with an annual turnover of more than $3 million** in any year since 2002. Businesses with a turnover of $3 million or less are known as *"small businesses"* in the *Privacy Act*. Whilst many such small businesses do not need to comply with the APPs, some small businesses that handle personal information do.

The AIC publishes a checklist on the AIC website **(Appendix A to Privacy Business Resource 10: Does my small business need to comply with the Privacy Act?).**

In summary though, if your Law Practice with a turnover of less than $3 million per annum:

- does not provide health services;
- is not related to a body corporate that is subject to the *Privacy Act;*
- does not provide contracted services to the Commonwealth;
- is not reporting entity or authorised agent of a report entity under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)* or its regulations or rules;
- does not carry on a credit reporting business;
- is not an employee association registered or recognised under the *Fair Work (Registered Organisations) Act 2009 (Cth)*;
- is not a protected action ballot agent for a protected action ballot conducted under Part 3-3 of the *Fair Work Act 2009 (Cth);*
- is not a service provider that is required to comply with the data retention provisions in Part 5-1A of the *Telecommunications (Interception and Access) Act 1979 (Cth)*; or
- has voluntarily opted into the *Privacy Act,*

then it will not be bound by the APPs or the NDB scheme.

It is unlikely that many Law Practices will be "caught" under these provisions.

There is, however, another provision which some commentators think means that all Law Practices will be caught. This provision (*Privacy Act* s.6D(4)(c)) applies the APPs/NDB Scheme to small businesses which disclose personal information about another individual for a benefit, service or advantage. This provision, read literally, could, of course apply to Law Practices. The AIC's check list and guidance documents, however, summarise this provision as applying to businesses that *"trade"* in personal information. Further, the AIC give an example of such a business as one where a small business "sells its customer list to a marketing company or gives its own list in return for another list". This would, in my view, not be an apt description of the use of personal information in a Law Practice.

In my view the situation is in fact made tolerably clear by s.6D(7) which provides that s.6D(4)(c) does not prevent an entity from being a small business only because it discloses personal information about another individual with the consent of that other individual.

Again, in my view, a Law Practice disclosing personal information relating to a client to, for example, an insurance company or an opposing Law Practice in the course of acting for that client does so with the consent of the client and would therefore not be bound by the APP's/NDB scheme. As noted above, some commentators disagree and assert that Law Practices that hold personal information (which of course will be all Law Practices) are bound. The Law Society is seeking further guidance from the AIC on this specific issue and further information will be provided to the profession as soon as possible.

If your Law Practice **does** have a turnover of more than $3 million then the NDB scheme will be applicable to your law practice from 22 February, 2018 (and the APPs will have, of course been applicable to your law practice for some time). If your Law Practice **does not** have a turnover of more than $3 million then you should nevertheless carefully examine the AIC checklist and satisfy yourself that the APPs and the NDB scheme do not apply.