



Law Council
OF AUSTRALIA

Office of the President

11 July 2017

Mr Andrew Solomon
Assistant Commissioner
Dispute Resolution Branch
Office of the Australian Information Commissioner

By email: consultation@oaic.gov.au

Dear Mr Solomon

Feedback on Notifiable Data Breaches Scheme Draft Resources

1. The Law Council of Australia thanks the Office of the Australian Information Commissioner (**OAIC**) for the opportunity to provide feedback on the Notifiable Data Breaches (**NDB**) scheme draft resources.
2. The Law Council acknowledges the assistance of its Privacy Law Committee of the Business Law Section, the Law Society of South Australia, and the Law Society of New South Wales in the preparation of this submission.
3. The Law Council considers that the draft resources will be helpful for agencies and organisations because they summarise the law. However, the Law Council considers that the draft resources should provide clearer direction on what organisations are subject to the NDB scheme, what types of breaches must be notified, and the manner of notification. For example, as most law practices hold data they would fall within the scope of the NDB scheme. Therefore, the issue to consider is under what circumstances they are required to report breaches of that data.
4. The Law Council has the following general suggestions on how to enhance the draft resources:
 - add a paragraph addressed to individuals explaining that they may expect to receive notifications and how to respond;
 - make it clear to organisations that they are not expected to make external enquiries to assess impact on individuals and can rely on the knowledge they have of the customer (e.g. a bank will have financial details, a hospital will have health information, etc.);
 - add a flow chart that demonstrates the process (especially of the notifications to the OAIC);
 - add a checklist for organisations based on the criteria with steps to be taken if notification is necessary;

- add a comment about the status of voluntary notifications;
 - add a comment to help address notifications under other schemes or jurisdictions; and
 - add additional examples as to what is notifiable.
5. The Law Council provides the following two examples that could help illustrate the operation of the NDB scheme:

Client lists

Happy Recruitment Company is in the process of transferring its very sizable candidate database to a new service provider. In the course of the transfer Happy Recruitment Company learns that one of its very senior recruiters is leaving to join a competitor and has made a copy of the candidate contact list (in breach of his contract of employment and restraint of trade). The unauthorised copying was brought to your attention by the service provider.

You have taken the following steps:

- instructed the service provider not to provide access to the departing recruiter;
- instructed the recruiter to return the list to you; and
- requested that the new employer (who has received the list) not use and disclose the information and securely destroy the list.

In this example, the Happy Recruitment Company has taken remedial action and the breach is not an eligible data breach, and is therefore not reportable.

Service provider

You are a popular provider of online financial services and regularly process a large volume of personal information. Your business is growing very quickly. You rely heavily on third party service providers, including public cloud providers. Your provider has just notified you (as they are required under the Security Incident Clause) that they have an incident impacting on some 30 other customers in Australia and Europe. They have assured you that they have it in hand and that they are merely letting you know because they are required under the contract and because they value our business. You are concerned that your customer data may have been impacted but have no reason to suspect that the incident as described may cause harm let alone serious harm. You are keeping a watching brief and have asked for daily updates. The incident is not reportable under the NDB scheme.

6. The Law Council also has suggestions specific to some of the materials. Please find attached a marked up version of 'Identifying eligible data breaches' and the website content, with some suggestions to improve clarity.
7. In relation to 'Entities covered by the NDB scheme', the Law Council suggests that the NDB resources:

- provide clarification of the obligations on state government agencies to notify OAIC in relation to breaches concerning tax file numbers, and provide an example to cover this scenario; and
 - incorporate a fuller definition of ‘entities that provide health services’, as there are many entities (both not-for-profits and private businesses) that may hold health records but do not necessarily provide a health service as defined in section 6FB of the *Privacy Act 1988* (Cth).
8. In relation to ‘Notifying individuals about an eligible data breach’, the Law Council suggests that the NDB resources:
- add information on the timeframe that OAIC would consider a reasonable time for a notification to be made, and provide an example of notification and appropriate timeframes; and
 - provide guidance as to whether, and how, notifications should be made in circumstances where the notification itself is likely to result in serious harm to the individual concerned.
9. The Law Council also suggests that the guidance address expressly the ramifications for entities that are caught under the NDB scheme of failure to comply with the notification requirements of the scheme. While this is set out in ‘Australian Information Commissioner’s role in the NDB scheme’, entities may not think to look at that resource for this information. We therefore suggest that the guidance is set out in the description of the NDB scheme and its scope under a specific heading dealing with sanctions.
10. I trust that this information is of assistance. Please contact Dr Natasha Molt, Senior Legal Advisor, at natasha.molt@lawcouncil.asn.au or (02) 6246 3754 with any questions.

Yours sincerely



Fiona McLeod SC
President