NOT LONG TO GO UNTIL THE NEW NOTIFIABLE DATA BREACH SCHEME BEGINS

Date: 13 December 2017

Australia Privacy Alert

By: Cameron Abbott, Rob Pulham

The long awaited commencement of the notifiable data breach scheme (**NDB Scheme**) is just around the corner.

Prior to the introduction of the NDB Scheme in Australia, notification of a data breach to the Australian Information Commissioner was not mandatory under the *Privacy Act 1988* (Cth) (**Privacy Act**).

From 22 February 2018, an entity that is bound by the Australian Privacy Principles, as well as credit reporting bodies, credit providers and file number recipients, will be required to comply with this new scheme. Entities will also need to notify the Commissioner and affected individuals when a data breach is likely to result in serious harm to those affected individuals.

WHY IS IT IMPORTANT TO PREPARE FOR THE SCHEME?

You may be asking yourself, so what does this all mean and why should I care?

Well for starters, compliance with the NDB Scheme will be mandatory for many businesses. Failure to comply with the scheme may attract a civil penalty (currently up to AUD420,000 for individuals and AUD2.1 million for corporations). The Commissioner has also evidenced a willingness to pursue enforceable undertakings.

The recent data breaches such as those affecting Adobe, Equifax and Uber among others over the past few years is a constant reminder that data breaches are costly and can have significant wide reaching operational, financial, legal and reputational consequences.

WHAT DO I NEED TO DO TO PREPARE FOR THE SCHEME?

If you are required to comply with the NDB Scheme, at a minimum, you should make an upfront investment to:

- review your current privacy and data security policies and procedures and incident/breach response plans
- assess whether your policy and procedures set out a plan you can follow in the event you suffer a data breach. We recommend all clients work up a clear breach response plan. The Commissioner expects it and our clients have all found it so much more effective to have pre-thought out a crisis response. If you do not have a data breach response plan, we recommend you prepare one in time for the start of the NDB Scheme

©2005-2026 K&L Gates LLP. All Rights Reserved.

- increase staff awareness of your information security policies and procedures and conduct staff training to inform all staff members of the new NDB Scheme. Remember, it is everyone's responsibility to remain vigilant and know what to do if they become aware of a data breach
- create a communication plan that sets out a process you will follow in the event you must notify the Commissioner, affected individuals (if necessary) and other interested parties (such as your insurer and third party advisers) of a data breach
- review your contracts with existing suppliers that collect and handle personal information on your behalf. Assess if those contracts need updating to include data breach response and notification obligations that your suppliers must comply with in the event your suppliers suffer a data breach that includes the personal information it collects or handles on your behalf.

KEY CONTACTS



CAMERON ABBOTT
PARTNER

MELBOURNE
+61.3.9640.4261
CAMERON.ABBOTT@KLGATES.COM



ROB PULHAM
SPECIAL COUNSEL

MELBOURNE
+61.3.9640.4414
ROB.PULHAM@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.