Five practical things you need to know about Mandatory Data Breach Reporting

AUTHOR // Peter Karcher

February 2018

After 10 years and numerous Federal Governments Australia has finally caught up with the rest of the world in terms of mandatory data breach notification (the US first introduced mandatory data breach reporting over 15 years ago). To mark the commencement of the laws which kicked off on 23 February 2018, we take a look at five things you need to know about the regime (one for every two years since the Australian Law Reform Commission first recommended the idea back in 2008!)

1. IT DOES NOT APPLY TO ALL KINDS OF DATA, ONLY PERSONAL INFORMATION

The mandatory data breach laws come within the framework of Australia's Federal *Privacy Act*, which regulates the collection, handling and disclosure of *personal information* such as names, addresses, phone numbers and personal financial details including bank account and credit card details. The rules do not apply to unauthorised access to or disclosure of sensitive business information including financial data, unless it also includes personal information relating to identifiable individuals. So while a hack which targets confidential business information may be an event of serious consequences for a commercial organisation, it may have nothing to do with the notifiable data breach laws. Keep in mind that employee records kept by a private sector employer are also not regulated by the *Privacy Act*, therefore a breach involving personal information of an organisation's employees may not trigger the notification laws either.

2. IT MAY NOT APPLY TO YOUR BUSINESS

The *Privacy Act* does not apply to all businesses. There is a small business exemption whereby if you are a private sector business or a not-for-profit organisation and your annual turnover is $3 million or less, you are not an "APP Entity" and therefore the Privacy Act, including the mandatory notification requirements, does not apply to you. There are exceptions to this exemption for certain types of businesses if you operate in the Health Care, Child Care, Education or Credit Reporting industries, or if your business involves buying or selling personal information (e.g. if you commercialise a customer data base). Interestingly State and Territory Government bodies (as opposed to Federal Government bodies) are also not subject to the new laws, given that privacy laws are separately regulated in the public sector at the State level. So the laws may not apply to you because you are too small. Of course there is the law, and then there is best practice. Reporting of data breaches may well be a best practice course of action to mitigate reputational damage and loss of customer goodwill. Whether small businesses with limited resources available for compliance are in a position to address this will depend on the nature of the business itself.

3. IT'S NOT JUST ABOUT MALICIOUS ATTACKS BY ENEMY HACKERS

The term "data breach" brings to mind first and foremost a cyber attack by nameless ghosts out there in the Internet,

an extraordinary circumstance affecting high profile businesses or big corporates. However the definition of a data breach is where there is "*unauthorised access to, or unauthorised disclosure of, personal information…, or where such information is lost in circumstances that are likely to give rise to unauthorised access or unauthorised disclosure*". A far more common data breach, for example, is the employee who mistakenly discloses customer information to the wrong person at another organisation, when the employee was not actually authorised to disclose it. Or a disgruntled employee who leaves and takes customer personal information with him or her in circumstances where it may be disclosed to damage the organisation. Or simply leaving a portable device on the bus! Businesses will need to be alive to the fact that such events could trigger their investigation and breach reporting obligations.

4. CONTEXT IS EVERYTHING

The new laws require a data breach to be notified only where there is a "likely risk of serious harm" to any of the individuals whose information is affected. The law doesn't set out all the circumstances in which "serious harm" may occur or what type of data may trigger this threshold. So while the disclosure of customers' credit card details, for example, has the clear potential for serious harm, will the disclosure of a database of names, email addresses, phone numbers etc. be a notifiable breach? In this regard context is everything. Think of the infamous *Ashley Madison* data breach. While the disclosure of names or addresses could be mundane in many contexts, *Ashley Madison* was a scenario in which the disclosure of such simple personal information could very well lead to the conclusion of "serious harm" occurring to the individuals concerned.

5. A BREACH CAN BE REMEDIED

All is not lost if you discover that a data breach has occurred. In fact, some of the more mundane data breaches such as losing information can be remedied, even if the event would otherwise have been a reportable breach. If you are able to take steps such that "serious harm" is ultimately not likely to occur, you have a get-out. So for example if you are able to recover lost data before it is likely to have been used or copied, if you can reign in that recalcitrant employee before he or she goes to Wikileaks, or if you are savvy enough to have put in place the tech to remotely wipe the data from a lost device, you may still be in the clear!

FOR MORE INFORMATION, PLEASE CONTACT:

PETER KARCHER //
Partner

T 61 2 8235 1218

E P.Karcher@clarkekann.com.au