

## DATA BREACH NOTIFICATIONS WILL SOON BE MANDATORY – IS YOUR BUSINESS READY FOR THE FALL-OUT?

By Amela Murica, Solicitor

19 May 2017

Once upon a time not too long ago, privacy legislation in Australia was a bit of a toothless tiger really. There was a lot of “you should” about the legislation, and not a lot of “you must”. So, when organisations inadvertently breached the “shoulds”, they could be forgiven for not being overly concerned. However, things started to tighten up with the introduction of the new *Australian Privacy Principles* in 2014, which also brought with them a raft of long overdue enforcement powers for the Office of the Australian Information Commissioner. Now, we see a further change that will give the Australian privacy law framework even more teeth. So, what is the new change and how will it impact you?

### So, what is new?

From 22 February 2018, Australia will have mandatory data breach notification laws applicable to all businesses, government agencies and other organisations covered by the Australian *Privacy Act* 1988 (Cth). While some small businesses will be exempted, most businesses (whether based in Australia or overseas) that collect personal information from Australian residents will be subject to the new regime and need to pay close attention.

### What are mandatory data breach notifications, and what will the new law mean for you?

The new regime will require organisations to notify the Australian Information Commissioner, and any individuals affected, when an ‘eligible data breach’ occurs. Previously, such notifications were only recommended by the Commissioner rather than being mandatory. With the increase in such data breach events of late (eg. Ashley Madison, Red Cross, Optus, Telstra, Vodafone), the legislation is coming at a particularly interesting time.

Generally speaking, an ‘eligible data breach’ will be any breach where there has been unauthorised access to or disclosure of any personal information (either of an individual or a group of people, say an entire database) leading to a likely risk of serious harm to any affected individual. Further, an ‘eligible data breach’ will also occur if personal information is lost in circumstances likely to give rise to the above occurring, and there are some other factors listed in the legislation to consider also. The meaning of ‘serious harm’ is not defined, however, the Explanatory Memorandum to the relevant Bill states that ‘serious harm’ can include physical, psychological, emotional, economic and financial harm, and will depend upon both the circumstances of the individual and the circumstances of the data breach. Note that the ‘serious harm’ test does not require the harm to be suffered by all affected individuals; rather this is assessed on a case-by-case basis.

If it is determined that an ‘eligible data breach’ has occurred (an organisation must take all reasonable steps to get this assessment completed within 30 days of becoming aware of a breach), then a notice must be provided to the Commissioner and the affected individuals as soon as practicable, subject to some exceptions. The notice must take a specific form and contain prescribed information, as required under the new data breach notification laws.

The impact and potential cost of making such a notification, both practically and from a PR perspective, cannot be ignored. Prevention is generally always better than cure, and in this case it certainly is. For example, imagine the fall-out from having to notify the Commissioner and then contact your entire customer database (or worse, your client’s) to advise them that their credit card details and billing addresses may have been compromised by poor database security.

The new regime does allow some exceptions to the notification requirements, including where organisations have taken remedial steps to rectify data breaches, so if there is a data breach but the organisation is able to take remedial action to rectify it, and as a result a reasonable person would conclude that the breach is not likely to result in 'serious harm' to those affected, then the breach will not be an 'eligible data breach' and will not require a notification. Care must be taken with this exception, as the remedial actions must serve to prevent 'serious harm' occurring, and organisations should ensure that their actions do not have scope to cause even greater harm than the original breach.

Failure to notify in respect of any 'eligible data breaches' can lead to significant monetary civil penalties for businesses (the maximum of which is 2,000 civil penalty units for corporations, i.e. \$1.8 million), so these obligations warrant serious consideration by and a compliance mindset for organisations. Again, brands and companies who do not have appropriate safeguards and processes in place to secure the personal information of individuals affected will no doubt find the flow-on effects of the laws to be particularly severe, both due to the applicable financial penalties and the PR outcomes that will inevitably come from having to publicly admit that there has been a problem.

### **What should you do?**

Prepare. Prepare. Prepare.

By now, businesses should already have strong and clear privacy compliance processes in place to ensure that they meet their obligations under the APPs, and this includes appropriate data security. Any business that does not should commence this process as soon as possible, as this will minimise the chance of data breaches occurring in the first place, including 'eligible data breaches', but it is just good business practice regardless, and people sharing their personal information with the business rightly expect their data to be handled with rigid security.

Service providers, including creative and digital agencies for instance, will also start to see provisions relating to data breach notifications appear in their client contracts more and more, if they have not already. As such these providers will need to get a clear handle on what the new laws mean for them and what procedures they need to put in place to meet client needs in this regard.

Getting prepared early to deal with data breaches will go a long way to mitigating the impact of the new laws by reducing the risk of a breach event in the first place. Of course, where an 'eligible data breach' does occur, having a set and effective procedure in place will allow a smooth, quick and efficient process in a time of turmoil, hopefully leading to the lowest possible impact on those affected, and on the business. The last thing you should be doing when a data breach occurs is trying to figure out what to do and developing a procedure at that time, as at that stage, time will certainly be "money".

### **Contact us**

Anisimoff Legal can assist you in developing your privacy policies and procedures, and working through any data breach notification concerns you may have. If you consider that a data breach event may have occurred, you should get in touch with us immediately. In the meantime, if you would like further information about the above or your other privacy obligations or questions, please feel free to get in touch with one of our experts below.

**Amela Murica**  
+61 3 9907 4305  
[amela.murica@anisimoff.com.au](mailto:amela.murica@anisimoff.com.au)

**Clint Fillipou**  
+61 3 9907 4302  
[clint.fillipou@anisimoff.com.au](mailto:clint.fillipou@anisimoff.com.au)



[www.anisimoff.com.au](http://www.anisimoff.com.au)



<https://www.facebook.com/AnisimoffLegal>



<https://twitter.com/AnisimoffLegal>



<http://www.linkedin.com/company/anisimoff-legal>