Legal Insight

K&L GATES

www.klgates.com

27 May 2013

Practice Group:

Commercial Transactions & Outsourcing

Mandatory Notification a Step Closer to Reality for Serious Privacy Breaches

By Miranda Skelley, Rob Pulham, Andrea Beatty and Cameron Abbott

On 2 May 2013, the Australian Government released, to a limited number of key stakeholders, a confidential Exposure Draft Bill for an Australian mandatory data breach notification scheme. This is the strongest indication yet that mandatory privacy breach notifications will come into force.

In the same week, Commonwealth Attorney-General Mark Dreyfus commented at the launch of Privacy Awareness Week 2013 that there is a "strong case" to move to a mandatory data breach notification scheme.

Background

For some time, privacy lawyers have advised clients to expect some form of mandatory notification requirements. When it did not make it into the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* most thought it would not be addressed until after organisations digested and implemented the changes for the Australian Privacy Principles, before 12 March 2014. The implementation of a mandatory data breach notification scheme is however more imminent than ever, with the considerable rise in personal information stored in the cloud and the rise in reported instances of improper access to personal information.

A mandatory data breach notification scheme increases the pressure on organisations to adequately protect personal information that they collect, store, use and disclose.

Data breach notification laws have already been adopted by many countries including Germany, almost all states of the US, Russia, India, Chile, Brazil and Mexico. The European Union (EU) currently requires telecommunications companies to adhere to data breach notification laws and has included a data breach notification law covering all sectors in its proposed cyber security directive, which is subject to EU parliamentary approval.

The Australian Government received submissions on a discussion paper released in October 2012 on a proposed mandatory notification scheme. It has looked at overseas models to assist in designing an Australian data breach notification scheme.

For further information on the discussion paper see our October 2012 Legal Insight.

The Exposure Draft Bill

Although the Exposure Draft Bill has only been released "confidentially", initial reports indicate that the Government has taken a conservative approach to mandatory notification.

The reports note that as currently drafted, only "serious breaches" would require mandatory notification. A serious breach is said to occur if a data breach results in a customer being exposed to a real risk of serious harm or if an organisation does not take reasonable steps to secure a customer's personal information as required under the current National Privacy Principles or as will be required under the Australian Privacy Principles, which come into force on 12 March 2014.

Mandatory Notification a Reality for Serious Privacy Breaches

Under the proposed mandatory notification scheme, when a serious data breach occurs, organisations would be required to notify the individual customers affected by the breach as well as notifying the Privacy Commissioner.

It is proposed that the Privacy Commissioner will be able to apply for or enforce a range of penalties including:

- public notification of the breach (by posting a public statement to organisations' websites or informing media outlets about the breach)
- apply for court appearance and financial penalties for small-scale offenders (fines of up to AUD34,000 for individuals or AUD170,000 for organisations)
- apply for court appearance and financial penalties for repeat or serious offenders (fines of up to AUD340,000 for individuals or AUD1.7 million for organisations).

Law enforcement agencies are exempt under the Exposure Draft Bill which was deemed necessary to avoid damaging the reputation and public confidence in the police service. The Privacy Commissioner also has the power to provide exemptions to other organisations if it is deemed to be in the public interest.

Finally, the reforms also introduce a new requirement to protect information from "interference", not just misuse or loss, which is an element organisations will need to consider.

There are some reports that the mandatory data breach notification scheme could come into force as soon as July this year (with a grace period), although other reports consider the changes will come into effect at around the same time as the amendments to the *Privacy Act 1988 (Cth)* in March 2014. However, until there is a clear indication from the Government as to its intention, this remains to be seen.

We wait with interest for the public release of the Exposure Draft Bill and the Government's next steps in implementing a mandatory data breach notification scheme in Australia.

What Does This Mean for Organisations

Together with the reforms to come into effect in March next year, these proposals introduce greater financial penalties but, more importantly, give the Privacy Commissioner an increased range of powers to investigate privacy practices. In 2011/2012, the Privacy Commissioner instigated seven high profile own motion investigations with data breach elements. They related to:

- data security issues, including compromise of personal information due to malware (the Privacy Commissioner found no failure to take reasonable steps)
- exposure to hacking (the Privacy Commissioner found a failure to take adequate steps to protect personal information)
- a customer management tool becoming publically available (the Privacy Commissioner found privacy failure at all stages, including failure to classify the project as involving privacy and failure to follow privacy procedures).

With the enhanced powers we would expect a significantly expanded list of investigations in 2014.

At the Privacy Awareness Week Business Breakfast 2013, the Privacy Commissioner stated that the *Guide to Information Security* released in April 2013 will be used in investigating data breaches.

If the mandatory notification scheme is implemented as proposed, organisations will need to ensure that in addition to their current privacy obligations under the *Privacy Act 1988 (Cth)*, they

Mandatory Notification a Reality for Serious Privacy Breaches

have adequate privacy practices and incident response mechanisms in place to identify and deal with data breaches.

An emerging message appears to be that if organisations embed privacy impact assessments as an integral part of projects and new product or service development, then they will meet the privacy requirements by design and will be able to show that they have made "reasonable efforts".

To minimise the event of a data breach or risk of reputational damage, we recommend organisations ensure data breach incident response mechanisms include a comprehensive communications policy to enable an organisation to effectively communicate with the media and customers.

Authors:

Cameron Abbott
Cameron.Abbott@klgates.com
+61.3.9640.4261

Andrea Beatty
Andrea.Beatty@klgates.com
+61.2.9513.2333

Rob Pulham
Rob.Pulham@klgates.com
+61.3.9640.4414

Miranda Skelley
Miranda.Skelley@klgates.com
+61.3.9640.4392