BUDDLE FINDLAY

Legal update - Mandatory reporting of data breaches - the New Zealand position

Philip Wood, Allan Yeoman, Amy Ryburn

19 March 2015

Australia is the latest in a growing list of countries to introduce mandatory reporting of data breaches, with a scheme to be introduced by the end of this year. The Australian announcement took some by surprise, as it had previously been signalled that mandatory reporting would apply only to those organisations caught by the upcoming Telecommunications (Interception and Access) Amendment (Data Retention) Bill – ie, telecommunications services providers who will be required to retain metadata for two years.

The decision to take a broader approach, and require any organisation which is subject to the Australian Privacy Act to report breaches involving personal information, reflects a worldwide trend towards the view that both regulators and affected individuals have a right to know when personal information has been compromised. The United States, many EU countries, parts of Canada, Dubai, Indonesia, Mexico, Norway, and South Africa have all – to varying degrees – introduced, or plan to introduce, mandatory reporting obligations, which apply either generally or to certain industries only (typically telcos, ISPs and financial institutions).

For the time being, New Zealand falls into a group of countries in which breach reporting is not mandatory, but is very strongly encouraged by regulatory guidelines. The Privacy Commissioner (the Commissioner) has issued Privacy Breach Guidelines which encourage notification and provide guidance on when and how entities should notify the Commissioner and affected individuals. Compliance with the Guidelines is voluntary, but failing to report a breach could put organisations on the back foot with both the Commissioner and the public generally if the breach later came to light.

In the longer term, it looks highly likely that mandatory breach notification will be among the changes introduced by reforms to the Privacy Act. The Law Commission, in its 2011 privacy law review, recommended mandatory reporting, and a Cabinet Paper released in May 2014 largely agreed with that recommendation, among others that the Law Commission had made.

The regime outlined in the Cabinet Paper would involve two tiers or notification:

- Entities would be required to notify the Commissioner of material breaches
- More serious breaches (where "there is a real risk of harm") would require notification to the Commissioner and to affected individuals.

The distinction between the two tiers would inevitably require judgement, influenced by guidance that the Commissioner makes available. However, many organisations already voluntarily notify both the Commissioner and affected individuals following a breach, so there is a range of 'good practice' examples that might be relevant to that judgement.

Failing to notify the Commissioner of a breach would be a criminal offence, and private entities would be liable for a fine of up to $10,000. The Cabinet Paper notes that public sector agencies cannot be subjected to a fine under the Privacy Act, and that instead, 'naming and shaming' would be the most effective deterrent.

The timing of these reforms is currently unclear – there appears to be support and willing for privacy law reform across the political spectrum, but there have been no firm indications on when a draft Bill may be prepared or when any changes would come into force.

The policy reasons behind encouraging (or mandating) reporting of serious and harmful data breaches are clear – if affected individuals can take steps to minimise harm that might result from unauthorised access to their information (eg, by changing passwords), then they should be notified so that they have the opportunity to do so. Regulators take the view that they should also be notified so that they can work with the reporting organisation to mitigate potential harm, respond to media and public enquiries, and no doubt prepare for any investigatory action that might follow.

However, for organisations whose focus is on minimising reputational damage, mandatory reporting might not be welcomed. The proposed regime recognises that fear of reputational harm may act as a disincentive to compliance, by proposing that notifications to the Commissioner of material breaches under the first tier are kept confidential, unless the notifying entity consents to publication, or wider notification would be in the public interest.

In a broader sense, many would argue that managing reputational impact is best dealt with on the front foot – reporting obligations aside, stories about privacy breaches have a habit of surfacing sooner or later, and accusations of attempting a cover-up are difficult to avoid. In planning how to respond to a data breach, having a communications plan in place (including template documents) could be just as critical for a firm as engaging forensic IT experts, lawyers and other specialists.

There are a range of other practical steps that organisations can take to guard against data breaches, and prepare their response should one occur – please see the Guide referenced below for a discussion of what those steps should involve.

Safe and sound - a guide to keeping information secure

Against a growing background of cyber-security threats and sensitivity to privacy issues, Buddle Findlay has produced a Guide to help organisations understand their obligations to keep personal information secure, the regulatory and practical guidance that is available both in New Zealand and overseas, and the steps that can be taken to implement and maintain an effective security plan. The Guide is available here.

New unfair contract terms provisions now in force

The new unfair contract terms provisions of the Fair Trading Act have come into force (as of 17 March 2015). As outlined in our December 2014 ICT update, the changes require that all standard form consumer contracts meet a basic requirement of 'fairness' and carry significant penalties for businesses that continue to include terms which have been declared unfair ($200,000 for individuals and $600,000 for body corporates).

The Commerce Commission has now finalised its Guidelines of how it intends to interpret and apply the new provisions, and has warned that there will be no grace period for businesses to update their terms. The Commerce Commission has indicated that it will initially focus on industries that have historically given rise to complaints or proved problematic overseas.

If you're unsure of whether your terms are caught by the new provisions, or whether they meet the 'fairness' requirement, please get in touch.

Auckland

188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659