Mandatory Data Breach Reporting Becomes Law

Privacy Amendment (Notifiable Data Breaches) Bill 2016

Alexandra Nash & Paul Angus | February 2017 | Insurance & Financial Services

Summary

On 13 February 2017, a Bill to amend the *Privacy Act 1988* was passed by Federal Parliament. The amendment will become effective twelve months after the Bill is given Royal Assent, which is likely to be in the next few days. This change means that Australian legislation will come to reflect the position in similar jurisdictions, such as the UK, EU, USA, and Japan, where mandatory breach reporting has been a legislative requirement for many years.

Under the amendment, organisations will need to report to the Australian Information Commissioner incidents such as loss, interference or unauthorised disclosure of information that would be likely to result in serious harm to the individuals concerned.

Responding to a data breach

The Australian Privacy Principles (APPs) in the Privacy Act apply to most Australian Government agencies, as well as to private sector organisations – including insurers – with an annual turnover of more than $3 million (subject to some exceptions).

APP 11 requires entities to take reasonable steps to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. However, prior to the amendment, there was no general legal data breach notification requirement.[1]

The Office of the Australian Information Commissioner's (OAIC's) current 2014 Data Breach Notification Guide (the Guide)[2] was drafted to assist entities to manage data breaches, and it provides guidance on how to assess the risk of harm to individuals following a data breach.

The Guide will likely be updated by OAIC in coming months to reflect the Amendments.

There are four steps outlined in the Guide when responding to a data breach:

- Step 1 - Contain the breach and do a preliminary assessment
- Step 2 - Evaluate the risks associated with the breach
- Step 3 - Notification
- Step 4 - Prevent future breaches

The Amendment

The Bill's mandatory data breach notification scheme will commence in 12 months, and will amend the Privacy Act to insert a new 'Part IIIC', which will define when a 'serious data breach' occurs and explain when and in what form notification of serious data breaches is required.

Notification to the Commissioner and affected individuals would only be required following a 'serious data breach'.

A serious data breach would occur if:

- personal information (which includes health information),
- credit reporting information,
- credit eligibility information, or
- tax file number information,

that an entity holds about individuals, is:

- subject to unauthorised access or unauthorised disclosure that,
- puts any of the individuals to whom the information relates at 'real risk of serious harm'.

There are also provisions in the Bill which note that if the organisation takes action before any serious harm is caused (such as retrieving or deleting the information before the unintended third party can access the information), then the 'eligible data breach' is treated as never having occurred. In such instances the breach is not reportable and does not trigger the notification obligations.

Data breach notification allows individuals whose personal information has been compromised following a data breach to take remedial steps to avoid potential adverse consequences, such as financial loss or identity theft.

Examples might include cancelling a credit card, or changing an online password.

The penalties for not reporting 'eligible data breaches' include fines of up to $1.8 million for organisations.

What needs to be done?

Over the next twelve months, before the amendments take effect, organisations should:

1. familiarise themselves with the 2014 Breach Notification Guide, (the Guide can be found at https://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-notification-guide-august-2014.pdf)
2. keep up to date on any changes OAIC may make to the Guide to reflect the amendment to the Act,
3. review internal data breach policies, and
4. if necessary, implement internal policies which incorporate the Guide's 4 Steps noting, of course, that 'Step 3 Notification' for 'eligible data breaches' will soon be mandatory.

If you or your organisation have any questions in relation to mandatory data breach notification, or any other privacy issue, please contact Alexandra Nash.

[1] Mandatory data breach notification was previously only required in the event of unauthorised access to eHealth information under the My Health Records Act 2012, and other provisions of the Privacy Act create equivalent obligations in relation to credit reporting information, credit eligibility information and tax file number information.

[2] 'Data breach notification guide: A guide to handling personal information security breaches". The Guide can be found at https://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-notification-guide-august-2014.pdf

For more information, please contact:

Paul Angus
Partner
T: 02 8257 5780
M: 0408 188 808
paul.angus@turkslegal.com.au

Alexandra Nash
Lawyer
T: 02 8257 5790
alexandra.nash@turkslegal.com.au