Mandatory data breach reporting comes to Australia — new notification requirements under the Privacy Act — (2018) 15(4) PRIVLB 54

Privacy Law Bulletin (newsletter)

Daniel Kovacs and Alex Garfinkel KCL LAW

Editor's Note: This article was originally published in Volume 15 Number 4 of the LexisNexis *Privacy Law Bulletin*.

Mandatory data breach reporting comes to Australia — new notification requirements under the Privacy Act

Daniel Kovacs and Alex Garfinkel KCL LAW

Abstract

On 22 February 2018, the Privacy Act 1988 (Cth) (the Act) was amended to introduce a mandatory data breach notification regime, the Notifiable Data Breaches scheme (NDB scheme). Australian Privacy Principle (APP) entities bound by the Act must now report specified breaches of privacy.

Such data breaches must be notified to the Office of the Australian Information Commissioner (OAIC). In addition, individuals that are likely to suffer serious harm as a result of that breach must also be notified. Businesses need to act quickly to contain and address such privacy breaches, and practitioners need to be aware of the requirements and the time frames for action.

Introduction

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) amended the Act to bring into force the NDB scheme. The legislation introduces a set of onerous reporting obligations for those already bound by privacy obligations under the Act. The OAIC is already reporting a flurry of activity in this area. This article outlines the provisions of the NDB scheme and provides examples of how it may apply in practice.

Who is bound?

The new data breach notification regime will apply to those already bound by the Act, including businesses with an annual turnover of $3 million or more. Such entities are called APP entities.

What is a data breach?

The Act protects "personal information", being information about an individual from which their identity can be ascertained.[1] A data breach is an unauthorised access or disclosure of such information, which typically occurs when personal information held by a business is, through accident, theft or malicious action, disclosed to or accessed by a third party.

The types of personal information covered by the Act include an individual's name, address, email, photograph, passport and/or driver's licence details, and financial information such as bank account details, tax file numbers, credit eligibility information and health information.

Data breaches can occur in various scenarios. A laptop may be lost or stolen, leaving personal data vulnerable. A client file could be left behind on public transport. A database may be hacked into. Paper records may be stolen from unsecured bins. Technical or administrative errors may result in a business accidentally providing details about an individual (such as a client) to a third party without the individual's authorisation, for example by sending an email to the wrong person.

What is an eligible data breach?

Under the NDB scheme, the obligations to notify the OAIC and any individuals affected by a data breach only apply in circumstances where the data breach is an *eligible* data breach.[2]

In summary, an eligible data breach occurs when:[3]

- there is unauthorised access to, or unauthorised disclosure of, personal information held by an APP entity in circumstances where a reasonable person would conclude that this would be likely to result in serious harm to any of the individuals to whom the personal information relates *or*
- personal information is lost in circumstances where unauthorised access to or unauthorised disclosure of the information is likely to occur, and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates *and*
- in either case, the APP entity has been unable to prevent the likely risk of serious harm with remedial action

Serious harm

A breach is only notifiable if there is a likelihood of serious harm to the individual to whom the information relates.

"Serious harm" is not defined in the legislation, but the Explanatory Memorandum to the Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) states that serious harm could include serious physical, psychological, emotional, economic and financial harm, as well as serious reputational damage and other forms of serious harm. Examples of serious harm could include identity theft, significant financial loss, loss of business or employment opportunities, humiliation or damage to reputation, workplace or social bullying, or marginalisation.

In assessing whether serious harm is likely, APP entities are required to make an assessment from the perspective of "a reasonable person in the [APP] entity's position"[4] — being properly informed and basing it on information immediately available or after making reasonable enquiries about the circumstances of each individual whose information is involved in the breach.[5]

When is serious harm "likely"?

The term "likely" in the context of an eligible data breach is intended to mean that "more probable than not", the information will be subject to unauthorised access, loss or unauthorised disclosure,[6] and that serious harm would occur as a result.

Section 26WG of the Act provides a non-exhaustive list of matters to be considered in determining whether access or disclosure of information would be likely to result in serious harm.

This list includes:

- the kind and sensitivity of information involved
- whether the information is protected by security measures and if so, the likelihood that any of those security measures could be overcome
- the persons or the kinds of persons who have obtained or who could obtain the information, and the likelihood that would have the intention of causing harm to any of the individuals to whom the information relates
- whether recipients have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
- the nature of the likely harm

The government's "Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)"[7] notes that certain types of personal information may be more likely to cause harm if compromised, such as medical information, documents that might be used for identity fraud (such as a Medicare card or passport details), and financial information.

Consideration should also be given to *whose* information has been compromised (are they at a particular risk or particularly vulnerable?), the number of individuals who have been involved, and the length of time the information has been accessible.

The Explanatory Memorandum expands on how the relevant matters mentioned in s 26WG might be examined. For example:

- If an APP entity's intrusion detection and prevention systems detect an attack on the APP entity's IT networks, the APP entity "could consider whether network security mechanisms were likely to have prevented the attacker from accessing [personal] information".[8]
- Where unauthorised disclosure of the names and addresses of individuals who are accessing a particular government service, or who are a clientele of a particular business, has occurred:

  > … although the data breach would involve information that would generally not be intrinsically sensitive, sensitivity may nonetheless arise if the knowledge that the individual was accessing the service or was a client of the business could cause harm.[9]

- Unauthorised access or disclosure may not be likely, for example, following the loss of an electronic storage device that has been encrypted or contains encrypted information where the probability of the encryption being circumvented is low.[10]

Assessment

APP entities must carry out a "reasonable and expeditious" assessment of whether any suspected breach has occurred, and then ascertain whether any given breach may be "eligible".[11] During this assessment, remedial action to contain the breach and reduce any potential harm to individuals caused by a suspected or eligible data breach should be taken. This may involve notifying individuals who have received the information and/or those to whom the

information relates.

Remedial action

Under s 26WF of the Act, an APP entity that takes action in relation to the access, disclosure or loss of personal information before it results in serious harm may be entitled to conclude that as a result, the access, disclosure or loss would not be likely to result in serious harm to any of those individuals. In those instances, the access, disclosure or loss is not, and is taken to never have been, an eligible data breach.

Statement

If reasonable grounds exist to believe that there has been an eligible data breach, the APP entity must, as soon as practical after becoming aware of it, notify individuals about the breach and prepare and provide a statement in relation to the breach to the OAIC.

The statement must set out, among other things, a description of the breach believed to have occurred, the kind or kinds of information concerned, recommendations about the steps that individuals should take in response to the breach,[12] and details of any other APP entities involved in the breach.

Notification

Having prepared the statement, an APP entity must, as soon as practicable after completion of the preparation of the statement, take steps as are reasonable in the circumstances to (as applicable):[13]

- notify the individuals to whom the information relates
- notify the individuals who are at risk from the eligible date breach
- notify the Commissioner
- publish a copy of the statement on the APP entity's website and/or
- take reasonable steps to publicise the contents of the statement

The APP entity may provide supplementary information to the Commissioner, explaining the circumstances of the breach and its response in further detail. Some of that information may not be intended for a wider dissemination and the APP entity is entitled to request that the Commissioner hold additional supporting information in confidence.

Once notified of an eligible data breach, the Commissioner may make inquiries or offer advice and guidance in response to the notifications. The Commissioner may also decide to take regulatory action on its own initiative. An APP entity must comply with any direction from the Commissioner in respect of the notification.

Enforcement of the NDB scheme

A failure by an APP entity to comply with the NDB scheme is regarded as an interference with the privacy of an individual. Although "the Commissioner's priority when responding to notifications is to provide guidance to the entity and to assist individuals at risk of serious harm",[14] the Commissioner has powers to require enforceable undertakings and bring proceedings to enforce such undertakings, to make determinations and bring proceedings to enforce such determinations, to seek injunctions, and to apply to a court for a civil penalty. Serious or repeated interferences with

privacy can give rise to civil penalties of up to $2.1 million.

Conclusion

The NDB scheme imposes a relatively onerous set of obligations on APP entities. Practitioners should endeavour to ensure that their clients are aware of their obligations under the NDB scheme and their privacy policies and practices are compliant.

Having a purpose-drafted and properly enforced privacy policy and security procedures will assist clients in avoiding privacy breaches at the outset. Existing privacy procedures should also be closely reviewed and amended to include a comprehensive data breach response plan.

Businesses need to know when to investigate a suspected breach, how to contain a breach, and how to respond quickly, effectively and within the requirements of the law, in the event that an eligible data breach does occur. Employees should also be made aware of what personal information the organisation deals with and be equipped with strategies for protecting that information.

Daniel Kovacs, *Principal Lawyer*, *KCL Law*

dkovacs@kcllaw.com.au

www.kcllaw.com.au

Alex Garfinkel, *Lawyer, KCL Law*

agarfinkel@kcllaw.com.au

www.kcllaw.com.au

1 Privacy Act 1988 (Cth), s 6.
2 See above n 1, s 26WE.
3 Above n 1, s 26WE.
4 Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth).
5 OAIC "Australian Privacy Principles guidelines" (as at 2 March 2018) 23 para B.105.
6 Above n 4, at 72 at para 41.
7 OAIC "Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)" (February 2018) www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response.
8 Above n 4, at 77 para 67.
9 Above n 4, at 77 para 66.
10 Above n 4, at 72 para 39.
11 Above n 1, s 26WH(2)(a).
12 Above n 1, s 26WK.
13 Above n 1, s 26WK(3).
14 Above n 7, at 57.

End of Document