mercury
Information Technology

Notifiable Data Breach (NDB)

Commencing 22 February 2018

Overview

16 November 2017

Summary

- The Notifiable Data Breach NDB legislation is coming into effect on February 22, 2018
- It will affect a significant number of businesses including all those who have turned over $3million in revenue since 2001, it captures a number of other businesses regardless of turnover based on a number of different criteria
- Data breaches that cause serious harm to individuals are reportable
- In the event of non-compliance, the Office of the Information Commissioner (OAIC) can:
    - Apply for civil penalty orders of up to $340,000 for individuals (such as directors and sole traders) and $1.7million for organisations and;
    - The Commissioner can also make organisations pay compensation for damages and issue a public apology

What is the Notifiable Data Breaches scheme?

The *Privacy Amendment (Notifiable Data Breaches) Act 2017*, also known as Notifiable Data Breach (NDB) legislation is an amendment to the Privacy Act 1988 that comes into effect on February 22, 2018. The legislation is regulated by the Office of the Australian Information Commissioner (OAIC).

he NDB scheme requires organisations covered by the Australian *Privacy Act 1988* (Privacy Act) to notify any individuals likely to be at risk of serious harm by a data breach.

What is a Notifiable Data Breach?

A Notifiable Data Breach is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.[1]

Identifying whether an eligible data breach has occurred involves considering whether there has been a data breach; that is, unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information (s 26WE(2)). The *Privacy Act 1988* (Cth) (Privacy Act) does not define these terms.[2] The OAIC does provide some examples of what the *ordinary* meaning of what those terms mean:

- Unauthorised Access: someone *gains* access to information that they should not have access
- Unauthorised Disclosure: is someone *gives* access to information to an unauthorised person
- Loss: is *losing* control of information, i.e. losing a laptop with data or disposing of a hard drive incorrectly

[1] OAIC 2017, oaic.gov.au
[2] https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/draft-identifying-eligible-data-breaches

What is Serious Harm?

Serious harm may include: serious physical, psychological, emotional, financial, or reputational harm[3]. Understanding whether serious harm is likely or not will generally rely on an evaluation of the context of a data breach — including the types of personal information involved, who has access to it, whether the data breach can be contained, and more.[4]
To determine serious harm, a 'reasonable person' from the entity breached, who is properly informed, must from their perspective determine if 'serious harm' has or is likely to occur.[5] The likelihood of harm increases based on a number of factors:

- The number of people impacted – the greater the number the more likely harm will occur to at least one of the people increases
- The type of information – sensitive or financial information for instance has a higher chance of causing harm
- Whether the information has security protection like encryption, obscurity through diversity
- The type of people who have the information – a hacker who has deliberately obtained the data is more likely to use the information than someone that has received the information by mistake for instance
- The OAIC also very helpfully notes that the 'nature of the harm' and the 'other relevant matters' also increases the likelihood of harm[6]

Who must comply with the NDB scheme?

Generally, organisations and entities that are already covered by the *Privacy Act 1988 (Cth)* must comply with the NDB scheme[7] and more precisely it applies to those entities covered under the Australian Privacy Principles (APP).[8] This covers any business, sole trader, body corporate, partnership, unincorporated association or trust that has an annual turnover of more than $3million in **any** financial year since 2001. Additionally, if a business falls into any of the following categories the $3million turnover threshold does not apply, so every organisation in these categories is captured under the scheme regardless of turnover:

- entities that provide health services[9]
- entities related to an APP entity
- entities that trade in personal information
- credit reporting bodies
- employee associations registered under the *Fair Work (Registered Organisations) Act 2009*

[3] https://www.oaic.gov.au/media-and-speeches/news/retailers-check-out-mandatory-data-breach-reporting-obligations-and-prepare-for-2018
[4] OAIC 2017, oaic.gov.au
[5] https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/draft-identifying-eligible-data-breaches
[6] https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/draft-identifying-eligible-data-breaches
[7] https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/draft-entities-covered-by-the-ndb-scheme
[8] https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#app-entity
[9] Health Services also includes naturopaths, chiropractors, gyms, weight loss clinics, child care centres and schools - https://www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/health-service-providers/is-my-organisation-a-health-service-provider

- entities that 'opt-in' to APP coverage under s 6EA of the Privacy Act

If a Small Business Operator (SBO) carries on any of the following activities it must comply with the APPs, and therefore must comply with the NDB scheme, but only in relation to personal information held by the entity for the purpose of, or in connection with, those activities:

- providing services to the Commonwealth under a contract
- operating a residential tenancy data base
- reporting under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
- conducting a protected action ballot, and
- information retained under the mandatory data retention scheme, as per Part 5-1A of the *Telecommunications (Interception and Access) Act 1979*.

Complying with the Legislation

If you have information that is subject to unauthorised access or disclosure or loss, and it has the potential to create serious harm, organisations captured under the scheme must:

- Notify the individuals effected **or;**
- All individuals at risk of serious harm **and;**
- The Commissioner of the OAIC
- If you cannot practically contact the individuals, you have to publish the notice you sent to the OAIC on the organisation's website

Non-compliance

The Commissioner has a range of enforcement powers including:

- Applying for civil penalty orders of up to $340,000 for individuals (such as directors and sole traders) and $1.7million for organisations[10] **and**;
- The Commissioner can also make organisations pay compensation for damages and issue a public apology

[10] https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

