The Notifiable Data Breaches Scheme: What You Need to Know

February 21, 2018

Written by JHK Legal Lawyer, Matthew Paul

From 23 February 2018, amendments to the *Privacy Act 1988 (Cth)* ("Privacy Act") will come into effect. These amendments create a new Notifiable Data Breaches scheme ("NDB scheme") for many businesses and organisations in Australia, overseen by the Office of the Australian Information Commissioner ("OAIC").

This article provides an overview of the new obligations on businesses and organisations under the NDB scheme. It provides general information only and is not intended as legal advice.

Who does the NDB scheme apply to?

The NDB scheme applies to an "APP Entity", which is defined as an agency or organisation.[1]

An "organisation" includes:[2]

- An individual person (including a sole trader);
- A body corporate
- A partnership
- Any other unincorporated association, or
- A Trust

However, there are exceptions:

- Small business operators (defined as having annual turnover of three million dollars or less in a financial year), *unless* they provide certain health services, provide information about individuals for profit, or are contracted by the Australian government;

[1] s 6 Privacy Act.
[2] s 6C Privacy Act.

JHK LEGAL

- Registered political parties; or
- State or Territory authorities

Which data breaches have to be notified?

A notification obligation arises when an APP Entity is aware of reasonable grounds to believe that there has been an "eligible data breach".[3]

This is where:

1. There is a data breach.

This includes unauthorised access to or an unauthorised disclosure of personal information, or a loss of personal information, that an APP Entity holds.[4]

Data breaches can arise in many different ways. For example, it will be a data breach where:

- file servers are accessed by unauthorised parties over the internet (such as by hacking);
- an employee of the entity leaves a folder with personal information on public transport;
- an email with personal information is sent to the wrong person outside the entity; or
- a filing cabinet containing personal files is sold to third parties.

2. The data breach is likely to cause "serious harm" to one or more individuals

This assessment is an objective assessment, based on the perspective of a reasonable person in the position of the APP entity.[5]
The APP entity must consider the following factors (which are not an exhaustive list):[6]

- The kind of information;
- The sensitivity of the information;
- Whether the information is protected by security measures, and if so the likelihood that any of those security measures could be overcome;
- The people or kind of people who have obtained (or could obtain) the information
- Where measures were taken to make the information meaningless to unauthorised third parties (e.g. encryption) – whether it is likely that the people who have obtained (or could obtain) the information will be able to counter these measures.
- The nature of the harm or potential harm

Exception - the APP entity takes remedial action before any "serious harm" occurs

This exception is designed to provide entities with an incentive to take positive steps to address a data breach in a timely manner.

The assessment of whether such action is sufficient is again an objective one, based on whether a reasonable person would consider that the acts would prevent serious harm.[7]

[3] ss 26WK & 26WL Privacy Act.
[4] s 26WE(2) Privacy Act.
[5] Ibid.
[6] s 21WG Privacy Act. Further guidance on assessing the likelihood of "serious harm" can be found on the OAIC website at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches.

JHK LEGAL

What if a data breach is only suspected?

If an entity merely *suspects* an eligible data breach has occurred it must conduct an assessment within 30 calendar days to determine whether there are reasonable grounds to believe an eligible data breach has occurred. If so, the APP entity must then follow the notification procedure. [8]

What is the notification procedure?

As soon as practicable after there are reasonable grounds to believe an eligible data breach has occurred, an APP entity must prepare a statement containing prescribed information about the data breach and provide it to the OAIC.[9]

The entity must also notify the individuals at risk of harm. Depending on the circumstances, the APP entity may either:[10]

- Notify all individuals whose personal information was part of the eligible data breach; or
- Notify only individuals at risk of serious harm from the eligible data breach; or
- If the above isn't practicable, then publish a copy of the statement on the entity's website (if it has one) and take reasonable steps to publicise the contents of the statement.

How is the NDB Scheme enforced?

Enforcement of the NDB scheme falls under the Privacy Act's existing framework. The Information Commissioner has the power to investigate non-compliance, issue binding determinations, seek injunctions, and (in the event of serious or repeated non-compliance) apply to the Federal Court or Federal Circuit Court to impose a civil penalty on an APP entity.[11]

Conclusion

Under the NDB framework, many businesses and organisations in Australia will have new proactive obligations in the event of a data breach. It is recommended that affected entities audit their current information security processes and procedures to ensure they are adequate, and prepare a data breach response plan to ensure compliance.

If you have any concerns about your privacy obligations, JHK Legal would be pleased to assist. You may contact our office on 07 3859 4500

---

[7] s 26WF Privacy Act. Examples of satisfactory remedial action can be found on the OAIC website at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches.
[8] s 26WH Privacy Act.
[9] s 26WK Privacy Act.
[10] s 26WL Privacy Act.
[11] ss 13G, 33E, 33F, 36, 55A, 62, 80W, 98 Privacy Act.