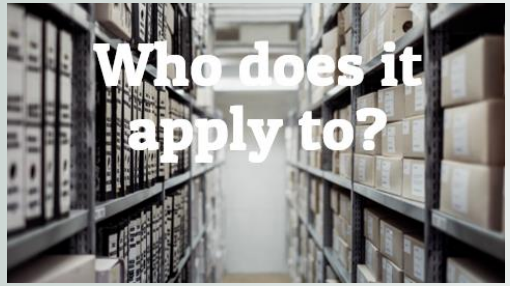
DWYER HARRIS

Notifiable data breaches in Australia



Click on an icon for details

Background

DWYER HARRIS

Background

- Until now there has not been a general requirement in Australia at a Commonwealth level to report data breaches to the individual or the Government, except in the case of e-health records under the *My Health Records Act* 2012.
- The Australian Law Reform Commission recommended a reporting requirement in its 2008 review of Australian privacy law.
- The Government consulted on this proposal in 2012 and 2013.
- In 2015 the Parliamentary Joint Committee on Intelligence and Security supported mandatory data breach notification.
- The Government released draft legislation for comment in December 2015.
- The *Privacy Amendment (Notifiable Data Breaches) Act* 2017 was enacted in February 2017 and **commences on 22 February 2018**.

Overview

DWYER HARRIS

Overview

- An eligible data breach will have to be reported to the affected individual and notified to the Australian Information Commissioner.
- An eligible data breach will be where a reasonable person concludes there is a likely risk of serious harm from unauthorised access or disclosure.
- Organisations suspecting an eligible data breach will have to conduct an assessment.
- If remedial action is taken, the breach may not have to be reported.
- The Commissioner will also have the power to grant exemptions from notifying an individual.

Who does it apply to?

DWYER HARRIS

Who does it apply to?

- Entities subject to the Australian Privacy Principles (APP entities), including government agencies and private sector organisations.
- Credit reporting bodies holding credit reporting information.
- Credit providers holding credit eligibility information.
- Tax file number recipients holding tax file numbers.
- Will not apply to entities exempt from the Privacy Act –
  - Small businesses.
  - Intelligence agencies.

DWYER HARRIS

Overseas recipients

- In some cases an APP entity will retain accountability for an eligible data breach involving personal information when the personal information has been disclosed to (and is held by) an overseas recipient –
  - Where APP 8.1 applies to the disclosure to an overseas recipient. (APP 8.1 says that before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information.)
  - Where a credit provider has disclosed credit eligibility information about one or more individuals to a company or person that does not have an Australian link.


Notifiable
breaches

DWYER HARRIS

Notifiable breaches

- An “eligible data breach” will have to be notified.
- Data includes –
  - Personal information held by an entity subject to the Australian Privacy Principles.
  - Credit reporting information held by a credit reporting body.
  - Credit eligibility information held by a credit provider.
  - Tax file number information held by a file number recipient.

DWYER HARRIS

Notifiable breaches

- Eligible data breaches are of 2 kinds –
  - **Unauthorised access or disclosure** of the information where a reasonable person would likely conclude that the access or disclosure would result in **serious harm** to any of the individuals to whom the information relates.
  - **Loss** of the information in circumstances where unauthorised access or disclosure is likely to occur and if that were to occur, a reasonable person would likely conclude that the access or disclosure would result in **serious harm** to any of the individuals to whom the information relates.

DWYER HARRIS

Exemptions

- It is not an eligible data breach if –
  - The entity takes action in relation to the access or disclosure, or loss.
  - It does so before it results in serious harm to any affected individuals.
  - A reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of the affected individuals.
- A particular individual does not need to be notified of the access, disclosure or loss (even if it is an eligible data breach) if –
  - The entity takes action in relation to the access or disclosure, or loss.
  - It does so before it results in serious harm to the particular individual.
  - A reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to the particular individual.

Serious harm

DWYER HARRIS

Serious harm

- Relevant factors in determining if a reasonable person would conclude that access to or disclosure of information would be likely to result in **serious harm** to an individual –
  - Kind of information.
  - Sensitivity of the information.
  - Whether information is protected by security measures – and if it is, the likelihood that those measures could be overcome.
  - The persons or kinds of persons who have obtained (or could obtain) the information.
  - If a security technology or methodology was used and designed to make the information unintelligible or meaningless for unauthorised users – the likelihood that persons who obtain the information and who have the intention of causing harm to the individuals have the information or knowledge required to circumvent the technology or methodology.
  - Nature of the harm.
  - Any other relevant matters.

Making an assessment

DWYER HARRIS

Making an assessment

- If an entity has reasonable grounds to **suspect** an eligible data breach but is not aware of reasonable grounds to **believe** that the circumstances amount to an eligible data breach –
  - Entity must carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that there is an eligible data breach.
  - Entity must take all reasonable steps to ensure the assessment is completed within 30 days.
- Where more than one entity jointly and simultaneously holds the same particular record of personal information, only one assessment needs to be undertaken into a single eligible data breach, regardless of how many entities hold the record of the information.

Notifying breaches

DWYER HARRIS

Reporting to the Commissioner

- If the entity is aware of reasonable grounds to believe there has been an eligible data breach in the entity, it must prepare a statement and give a copy to the Australian Information Commissioner as soon as practicable.
- The statement must set out –
  - Identity and contact details of the entity (and may identify other entities involved).
  - Description of the eligible data breach.
  - Kind or kinds of information concerned.
  - Recommendation about steps that individuals should take in response.

DWYER HARRIS

Notifying individuals

- When an entity has prepared a statement to the Commissioner following an eligible data breach it must as soon as practicable –
  - Take such steps as are reasonable to notify the content of the statement to each affected individual (if it is practicable to do this).
  - Take such steps as are reasonable to notify the content of the statement to each individual at risk from the breach (if it is practicable to do this).
  - If neither or the above applies, publish the statement on its website and take reasonable steps to publicise the contents of the statement.

DWYER HARRIS

Exceptions

- Enforcement bodies – if it would be likely to prejudice enforcement activities.
- Where inconsistent with secrecy provisions in other legislation.
- Declaration by Commissioner – having regard to the public interest and any relevant advice from enforcement bodies.

DWYER HARRIS

Multiple entities

- Where more than one entity holds the same particular record of personal information, only one statement must be prepared and notified for a single eligible data breach, regardless of how many entities hold the information compromised in the eligible data breach.


Help

DWYER HARRIS

Help

- We are experienced in all privacy law matters and can help you prepare for mandatory data breach notification.
- We have worked with clients on privacy since the Privacy Act was first extended to private sector organisations in 1992.
- Patrick Dwyer is a member of the International Association of Privacy Professionals (ANZ).
- Contact us if you need our help:

  Dwyer Harris
  02 8912 2500
  admin@dwyerharris.com
  www.dwyerharris.com