AON
Empower Results®

CLYDE&CO

Webinar

New privacy law: How your organisation can prepare

Agenda

- Overview of legislation
- Why preparation is key
- Clarifying the terms “eligible data breach” and “serious harm”
- Notification requirements and statement content
- Exceptions to the notification requirement
- Penalties for non-compliance
- OAIC guidance
- Cyber incident response
- Q&A

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)

- Legislation requiring mandatory reporting of ‘eligible data breaches’ passed in February 2017
- Requirement to notify the Privacy Commissioner and (in some circumstances) affected individuals of eligible data breaches
- Expected implementation date: 23 February 2018
- Legislation applies to APP entities, entities deemed to hold information disclosed to overseas recipients, credit reporting bodies, credit providers and organisations that hold tax file information
- A number of steps to take before the legal requirement to notify is triggered
- Many broad brush terms to consider: "eligible data breach“, "reasonable person", "practicable", “likely to result in”, "serious harm“
- Statutory timelines apply and so preparation is key

Why is preparation key?

- ***30 day*** incident investigation period:
  - An incident has occurred which ***may*** have been an eligible data breach
  - Within 30 days (of becoming aware), you must carry out a ***reasonable and expeditious assessment*** as to whether there are ***reasonable grounds*** to believe that the data breach ***has been*** an eligible data breach
  - If there are no such reasonable grounds, no notification required
  - If there are such reasonable grounds, the notification requirement is triggered
- ***Reasonable grounds***: common legal standard referring to an objective entity in the position of the entity
- Need to have a system in place to make and document this determination within 30 days

What is an 'Eligible Data Breach'?

- An ***Eligible Data Breach*** occurs when:
  - there has been:
    - unauthorised access to information; or
    - disclosure of information; or
    - loss of information in circumstances where that access to that 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"*

- A ***reasonable person****:* common legal standard referring to an objective bystander in the position of the entity

- A ***likely*** risk: a risk that is not a 'remote risk'; is it more probably than not?

What is likely to result in 'serious harm'?

- Each incident must be considered
- Must consider: ***any of the individuals to whom the information relates***
- ***Harm*** includes physical, psychological, emotional, economic and financial harm
- Is it likely to result in ***serious harm***: consider the following:

The type of information	Sensitivity and volume of the information	Who is likely to have obtained the information	Whether there are security measures to protect the information	Whether the information is (or could be converted into) a form that is intelligible to an ordinary person

What notification is required?

- Prepare a prescribed statement

- Provide a copy to the Privacy Commissioner/OAIC ***as soon as practicable***

- Provide a copy of the contents of the statement ***as soon as practicable*** after completion of the statement to:
    - ***if practicable*** to notify each, individuals to whom the relevant information relates; or
    - ***if practicable*** to notify each, individuals who are at risk from the Eligible Data Breach; or
    - if neither of the above applies, ***reasonable*** steps must be taken to publicise the contents of the statement and publish the statement on the entity's website.
- How? Notification can be in the same way the entity normally communicates with the intended recipients

What must the statement say?

- The prescribed statement must contain the following:
    - the entity's identity and contact details and
    - a description of the Eligible Data Breach believed to have occurred;
    - the kind of information that has been lost;
    - recommendations that effected individuals can take in response to the eligible data breach; and
    - if the breach is also an eligible data breach of other entities, the identity and contact details of those entities.
- Key: ensure that your advisors assist in drafting the statement to ensure it is drafted using appropriate language

Are there exceptions to the notification requirement?

- Yes: a number of exceptions to the notification requirement:

  - *My Health Records Act 2012* notifications
  - Remedial action – what steps were taken
  - Eligible data breaches of other entities – multiple notices
  - Secrecy provision
  - OAIC discretion

Penalties for non-compliance

- Non-compliance is a breach of privacy and Privacy Act penalties apply

Order the respondent to take specified steps within a specified period to ensure that such conduct is not repeated or continued

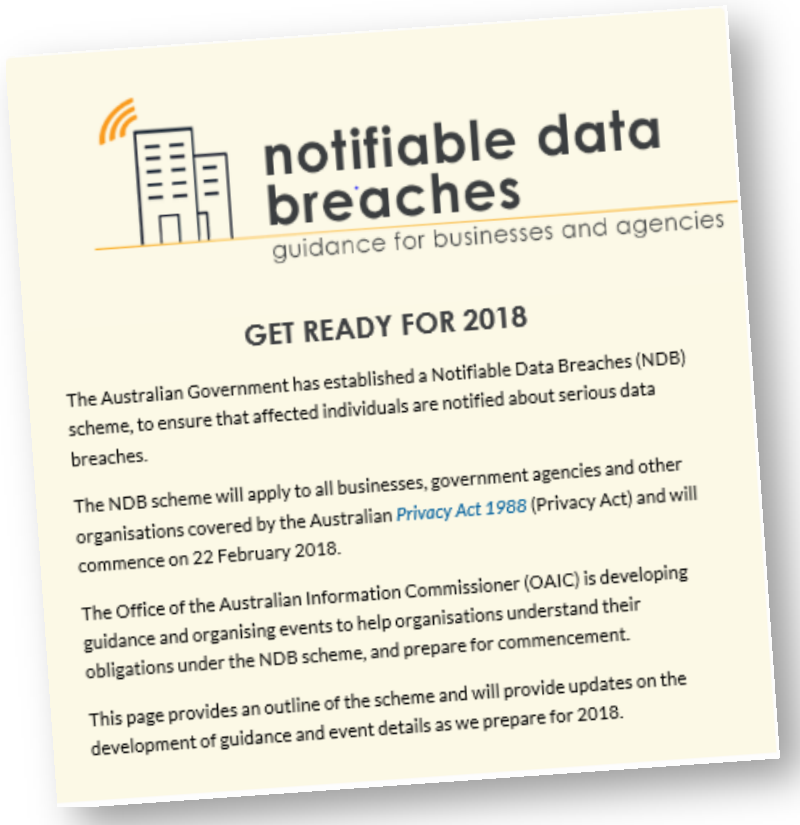
Make a determination requiring the payment of compensation for damages or other remedies

Accept an enforceable undertaking

Seek civil penalties of up to (or apply for civil penalty orders of up to) $340,000 for individuals and $1.8m for companies

Seek an injunction regarding conduct that would contravene the Privacy Act

OAIC Guidance: https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/



notifiable data breaches

guidance for businesses and agencies

GET READY FOR 2018

The Australian Government has established a Notifiable Data Breaches (NDB) scheme, to ensure that affected individuals are notified about serious data breaches.

The NDB scheme will apply to all businesses, government agencies and other organisations covered by the Australian *Privacy Act 1988* (Privacy Act) and will commence on 22 February 2018.

The Office of the Australian Information Commissioner (OAIC) is developing guidance and organising events to help organisations understand their obligations under the NDB scheme, and prepare for commencement.

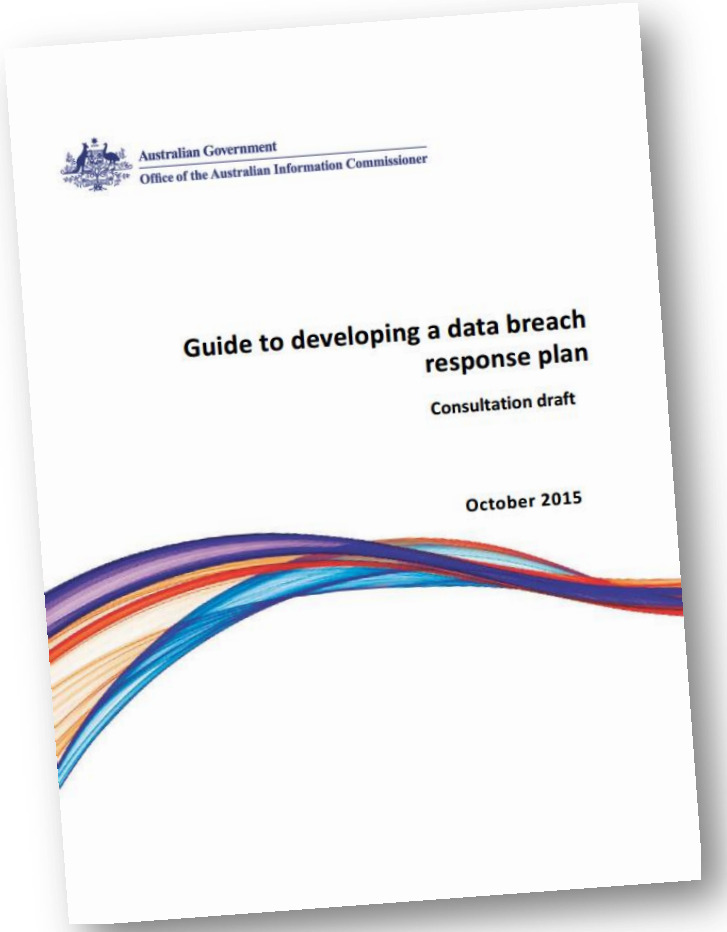
This page provides an outline of the scheme and will provide updates on the development of guidance and event details as we prepare for 2018.

"[We] strongly recommend that all organisations review their practices, procedures and systems for securing personal information…"

"Organisations should also prepare or update their data breach response plan to ensure that they are able to respond quickly to suspected data breaches…"

"… [we] will work with businesses, agencies and other stakeholders to develop practical guidance on complying with the NDB scheme."

OAIC Guide: Data breach response & notification planning

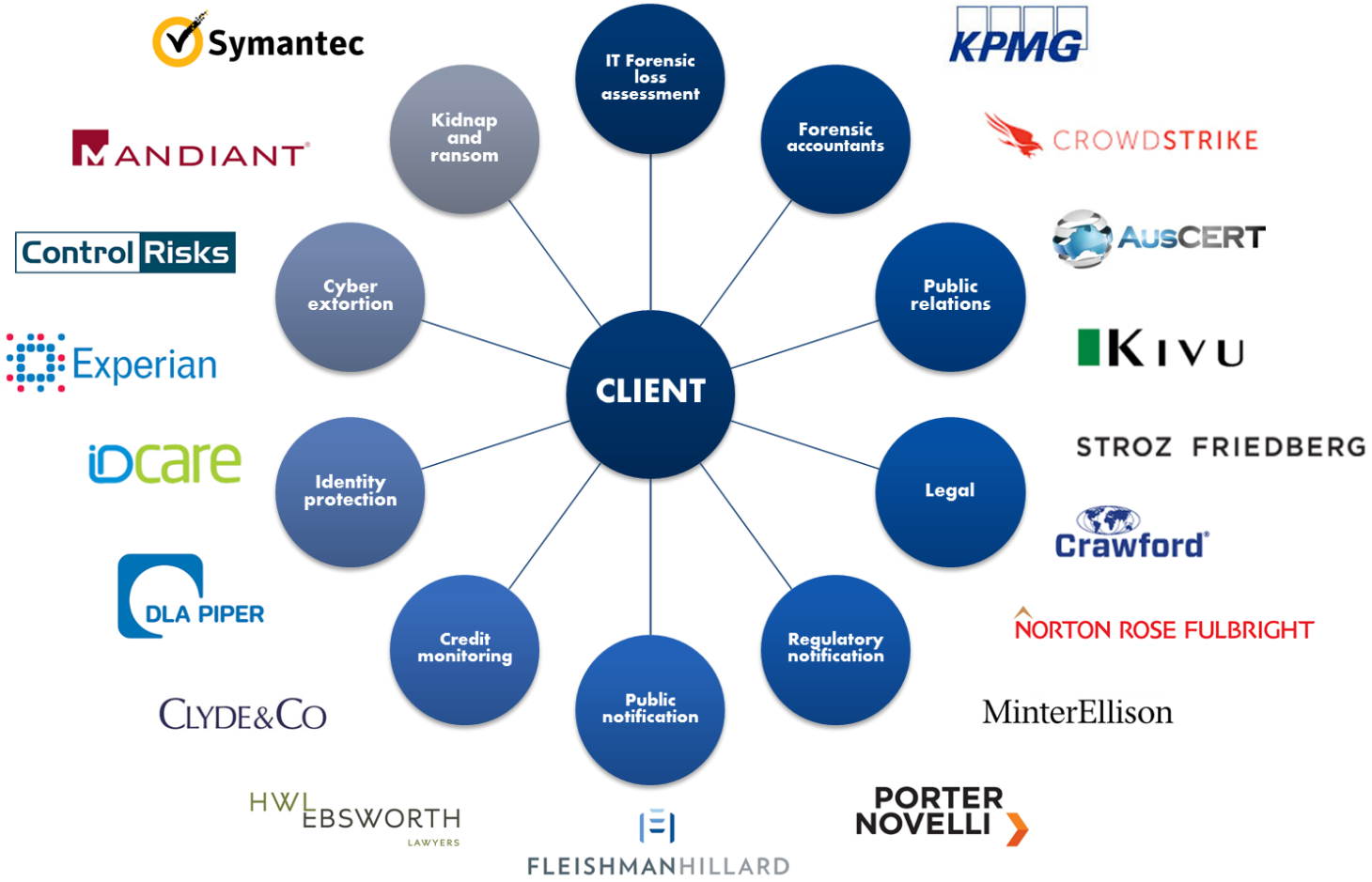


"Your actions in the first 24 hours after discovering a data breach are often critical to the success of your response…"

"You should create and test your plan before a data breach occurs…"

"Response team membership: ensure that the relevant staff, roles and responsibilities are identified and documented…"

Cyber incident breach response



Questions?

Type your question in the question section of the webinar panel

Thankyou for attending our webinar