Australian Government
Office of the Australian Information Commissioner

The Notifiable Data Breaches (NDB) scheme

Presented by Angelene Falk, Deputy Commissioner
Office of the Australian Information Commissioner

OAIC

Data breach notification — why?

- Formalises long-standing community expectations.
  - 94% of Australians said that they should be told if a business loses their personal information.
  - 58% of people have avoided a business due to privacy concerns.
- Notification provides individuals with the opportunity to take steps to reduce the chance they will experience serious harm.
- Encourages higher standards of privacy protection and security — which supports greater public trust in the management of personal information.

Data breach notification laws around the world

- USA: 48 states and DC have data breach notification laws.
- Canada has passed a mandatory notification law for the private sector (yet to commence).
- The Netherlands introduced mandatory breach reporting in January 2016.
- New Zealand and Singapore have announced that they will introduce mandatory data breach notification.
- Europe: GDPR Article 33 will introduce mandatory notification for personal data breaches from May 2018.
- Other countries seeking to maintain or achieve ‘adequacy’ recognition under European privacy law are likely to follow.

Australian Government
Office of the Australian Information Commissioner

Identifying an eligible data breach

OAIC

Eligible data breaches

- An eligible data breach occurs when (in summary) (s 26WE):
  - there is unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds, and
  - the access, disclosure or loss is **likely to result in serious harm** to any of the individuals to whom the information relates (emphasis added).
- 'Harm' is undefined in the legislation, but can include psychological, emotional, physical, reputational, or other forms of harm.
- Whether serious harm is likely is an objective assessment, based on the view of a reasonable person in the position of the entity that has experienced the data breach (s 26WE(2)).
- Effective remedial action can result in notification being unnecessary (s 26WF).

Australian Government
Office of the Australian Information Commissioner

Assessing a suspected eligible data breach

OAIC

Conducting an assessment of a suspected eligible data breach

- If an entity suspects a data breach may meet the threshold of 'likely to result in serious harm' (s 26WH), it must conduct:

  '*a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity*' (s 26WH(2)(a)).

- Generally, there is a maximum of 30 days to conduct this assessment (s 26WH(2)(b)).

- See OAIC resource *Assessing a suspected data breach*:
  - Initiate: Who will do the assessment? How will it be conducted?
  - Investigate: Make inquiries and gather information.
  - Evaluate: Consider the information and make a decision.

Australian Government
Office of the Australian Information Commissioner

How to notify

OAIC

Notification to affected individuals

There are three options for notifying the affected individuals (s 26WL(2)):

- Notify all individuals whose personal information was involved
- Notify only those who are at likely risk of serious harm; or
- If direct notification is not practicable: publish the notification, and take reasonable steps to publicise it.

Notification can be via your normal methods of communication (s 26WL(4)).

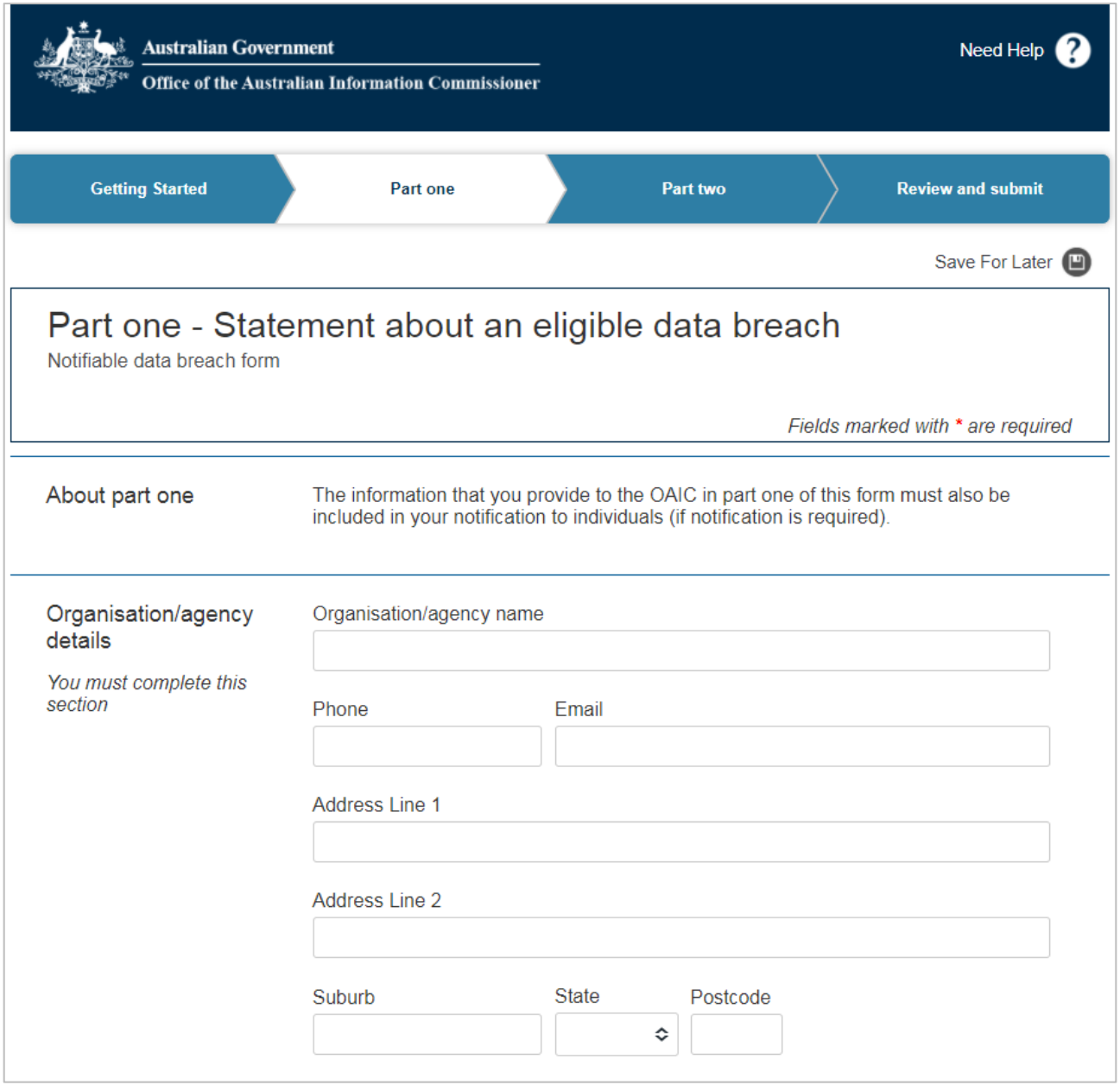


Information to include in your notification to individuals

The notification must include four mandatory pieces of information:

1. the identity and contact details of the entity (s 26WK(3)(a))
2. a description of the eligible data breach that the entity has reasonable grounds to believe has happened (s 26WK(3)(b))
3. the kind, or kinds, of information concerned (s 26WK(3)(c))
4. recommendations about the steps that individuals should take in response to the eligible data breach (s 26WK(3)(d)).

It may also include other information. For example, an apology, or a description of what you have done to prevent reoccurrence.


Australian Government
Office of the Australian Information Commissioner
Need Help
Getting Started
Part one
Part two
Review and submit
Save For Later
Part one - Statement about an eligible data breach
Notifiable data breach form
Fields marked with * are required
About part one
The information that you provide to the OAIC in part one of this form must also be included in your notification to individuals (if notification is required).
Organisation/agency details
You must complete this section
Organisation/agency name
Phone
Email
Address Line 1
Address Line 2
Suburb
State
Postcode

Visit www.oaic.gov.au/ndb

- We have recently published *Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988.*

- The guide consolidates the guidance we have published in recent years on data breach notification and developing a data breach response plan, as well as our guidance on the Notifiable Data Breaches scheme.

Australian Government
Office of the Australian Information Commissioner

Other considerations

OAIC

1. Know your data

   - This will enable you to identify potential privacy risks.

2. Prepare to notify individuals — what will you say and how will you communicate with them?

   - Your notification can build confidence in your handling of a data breach.

3. Have a practice run

   - This will ensure staff know what to do if a data breach occurs.

oaic.gov.au