

## Introduction

Businesses that experience a breach may have specific obligations depending on whether the Privacy Act applies to them, the type of personal data involved, and the risk of serious harm resulting from the breach. Serious harm does not have to be explicitly financial, it can be psychological, physical or reputational harm.

### Current requirements

A **small business** is defined under the **Privacy Act 1988 (Cth)** as one which has an annual turnover of less than three million Australian dollars (**Section 6D(1)**). This value is inclusive of income from all sources and does not include assets held, capital gains or the proceeds of capital gains (Office of the Australian Information Commissioner [OAIC](#)).

If your small business falls under the Privacy Act and experiences a breach, there are obligations under the Notifiable Data Breach scheme. However, some small businesses qualify for the Privacy Act irrespective of their turnover and **must report a data breach event**, these include businesses:

- That provides a health service, or holds any health information, except an employee record; or
- That disclose personal information about another individual to anyone else for a benefit, service or advantage; or
- Provide a benefit, service or advantage to collect personal information about another individual from anyone else; or
- That are contracted service providers for a Commonwealth contract; or
- That are credit reporting bodies (**Section 6D(4)**; [OAIC](#)).

## What constitutes an eligible data breach?

- ☐ Unauthorised access or disclosure to personal information, or a loss of personal information, held by an agency; or
- ☐ That is likely to result in “serious harm” to one or more individuals; or
- ☐ The organisation or agency has not been able to prevent the likely risk of serious harm with remedial action. ([OAIC](#))

#### Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document,

IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

## How to report a data breach?

- ☐ You should report a data breach to the [OAIC](#) as soon as practicable. However, the maximum amount of time before making a report is 30 days after you believe that you experienced a data breach event. This timeframe is provided for the business to assess the risk of “serious harm” to the individual as a result of the data breach (**Section 26WH (2)(b)**); [OAIC](#)
- ☐ You may also wish to contact the OAIC enquiries line: 1300 363 992

## What do I notify about?

You must notify the OAIC and any affected individuals of:

- ☐ Your organisation’s name and contact details
- ☐ A description of the data breach
- ☐ Types of information involved
- ☐ Recommendations of response steps an individual should take ([OAIC](#))

IDCARE can offer your business additional support in drafting and preparing data breach notifications and supporting impacted individuals.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 170 (Aus) | 0800 121 068 (NZ)

### Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.