# Data Privacy Amendments – February 2018

## Background

- The Australian Privacy Principles (APP) are **Guidelines** produced by the 'Office of the Australian Information Commissioner' (OAIC) and are not Legislative
- The Notifiable Data Breach (NDB) scheme form part of the APP and come into effect on **22 Feb 2018**
- The NDB dictates that organisations that any organisation considered an **APP entity** needs to notify the OAIC and customers affected of a data breach.
- The reason is fairly clear – with so much personal information stored digitally, Australians need to be comfortable that their information is **secure** and that if there is a breach, that they are **notified**.

## What can happen if I don't comply?

- The Privacy Act gives the OAIC the ability to work with entities to facilitate legal compliance and best privacy practice, as well as **investigative and enforcement powers** to use in cases where a privacy breach has occurred including:
  - investigate a matter following a complaint
  - attempt to conciliate a complaint
  - decide whether or not to hold a hearing in response to a request from a complainant
  - bring proceedings to enforce an enforceable undertaking
  - apply to the court for a **civil penalty** order for a breach of a civil penalty

## How do I know if I need to comply?

- If you store any personal information for clients or staff **AND** your revenue was greater than **$3 million** in any year since 2002
- If you are a **small healthcare provider**, regardless of revenue.
- If your small business is **related to a larger body corporate** that is subject to the Privacy Act
- If you provide services to Australian or Norfolk Island government agencies under a **commonwealth contract or subcontract**
- If your small business operates a **residential tenancy database**
- If your small business an **employee association registered**
- If your small business only trades in personal information **without the consent of the individual** and without being required or authorised by law

## So what do I need to do to comply?

- Only store personal information that is **necessary**. If you have old clients data or you don't use the data, delete it
- Ensure that you have **strict access controls** in place. Only employees who need access to private data should be granted it.
- Reduce human error through **training and security awareness** sessions. Develop stringent security policies.
- Put appropriate **monitoring** in place which will alert you if there is a data breach
- If you have control of your infrastructure, **encrypt** your data and even your backups to reduce the risk of a breach.
- Review your **firewall policies and Anti-Virus effectiveness** to reduce the likelihood of a breach

* Note that this document combines extracts from official sources with Integr8IT's recommendations and interpretations. For more comprehensive information, please visit the OAIC website

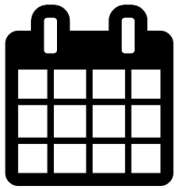
INTEGR8IT

# Quick reference guide

## THE POLICY CHANGES

### DATE OF ENFORCEMENT

- 22 February 2018



### WHO NEEDS TO COMPLY

- Any Organisation storing private data (phone numbers, TFN's, Health records etc.)
- Organisations >$ 3 mil TO

### YOUR OBLIGATIONS

- Secure your data to the best of your ability
- Monitor for breaches so that you know when one occurs

### NOTIFICATION

- Notify OAIC of a data breach
- Notify the affected client of a data breach

## WHAT TO CONSIDER FOR YOUR ORGANISATION

### POLICIES/ PROCEEDURES

- Staff training
- Develop a culture of privacy

### USE WHAT YOU NEED

- Don't collect unnecessary data
- Remove unused private data

### SECURITY

- Data Access Controls, Physical Security, Threat Management, Data Encryption

### MONITORING

- Access breaches
- Notification on data breach