www.klm-audit.com.au info@klm-audit.com.au 0407 690 046

THE PRIVACY AMENDMENT (NOTIFIABLE DATA BREACHES) ACT 2017

Are you compliant?

SUMMARY OF CHANGES

It will require business/organisations to notify affected individuals and the OAIC of any eligible breaches where an individual is likely to experience serious physical, psychological, emotional, financial or reputational harm – for example, the release of credit card details can be seen to create financial harm for the individual.

PENALTIES FOR NON-COMPLIANCE

Fines of up to $340,000 for an individual or $1.7 million for a company

CAN YOU RISK IT?

With the increasing number of organisations that have had their systems breached in recent years, and the personal information they have collected being distributed without consent, the Office of the Australian Information Commissioner (OAIC) have introduced an amendment to the Privacy Act 1988 to add further protection to personal information

The Privacy Amendment (Notifiable Data Breaches) Act 2017

Which came into effect on 22nd February 2018

Do I need to comply?

The official list includes Australian Privacy Principle (APP) entities, credit reporting bodies, credit providers, tax file number recipients and businesses/organisations already required to comply with the Privacy Act.

While businesses with an annual turnover of less than $3 million in any financial year since 2001 are generally seen as not having obligation under the APPs, if you collect any of the following information it is best practices to have appropriate privacy policies in place:

KLM & AUDIT COMPLIANCE

www.klm-audit.com.au info@klm-audit.com.au 0407 690 046

THE PRIVACY AMENDMENT (NOTIFIABLE DATA BREACHES) ACT 2017

Will You Be Ready?

ACTION REQUIRED BY FEBRUARY 22ND 2018

- All privacy policies, including those available on your website, will need to be updated to include Notifiable Data Breaches.
- Data Breach Response plans will need to be developed to outline how you will handle the containment, evaluation and notification of breaches and how it will prevent any future breaches
- The introduction of Privacy Officers and Privacy Champions and updates to position descriptions
- Regular internal and external Privacy Impact Assessments and the creation of a Privacy Impact Assessment Register to be made available internally and, as applicable, publically - for example published on your website
- Ongoing Privacy training and education for all staff

- Financial details (including credit card details)
- Government identifiers (e.g. Centrelink Reference Number, Medicare number)
- Tax File Number (TFN)
- Contact information (e.g. home address, phone number, email address)
- Health information
- Other sensitive information (such as sexual orientation, gender identity, political or religious views)

Although the obvious industries that need to comply with the amendment are health, legal and financial services, other industries may include, but are not limited to, child care, training organisations, Not-For-Profit organisations, fitness, retail and anyone who provides online shopping or subscription services

Are you compliant?

Contact us for a free, no obligation discussion on how the amendment will affect your business and how you can avoid potential fines

KLM & AUDIT COMPLIANCE