INTERNATIONAL PRIVACY AND DATA BREACH LEGISLATION

NOBODY WANTS TO EXPERIENCE A DATA BREACH

At TIMG we are the information management specialists. We understand the importance of protecting personal data. Around the world, rigorous privacy and data breach regulations are being implemented, imposing many new obligations on organisations that collect, handle or analyse personal data (an overview of Australia's Notifiable Data Breach legislation follows).

New Zealand is not exempt from this. The New Zealand Government is currently working to refresh our privacy laws to better protect information gathered and stored digitally by way of a new Privacy Bill due to come into effect in 2019. Talk to TIMG now about how we can assist your business or organisation with secure information storage and destruction to avoid incurring hefty penalties in the future, which could be in the millions of dollars.

New Privacy Bill for New Zealand

The Privacy Bill is intended to replace the current Privacy Act 1993, which is 25 years old and ready for modernisation. The Bill seeks to bring New Zealand's privacy law into the digital era, and better align our law with other international privacy developments.

The key changes proposed in the Privacy Bill are based on the Law Commission's recommendations from its 2011 review.

- ***Mandatory reporting of privacy breaches:*** privacy breaches (unauthorised or accidental access to, or disclosure of, personal information) that pose a risk of harm to people must be notified to the Privacy Commissioner and to affected individuals
- ***Compliance notices:*** the Commissioner will be able to issue compliance notices that require an agency to do something, or stop doing something, in order to comply with privacy law. The Human Rights Review Tribunal will be able to enforce compliance notices and hear appeals
- ***Strengthening cross-border data flow protections:*** New Zealand agencies will be required to take reasonable steps to ensure that personal information disclosed overseas will be subject to acceptable privacy standards. The Bill also clarifies the application of our law when a New Zealand agency engages an overseas service provider
- ***New criminal offences:*** it will be an offence to mislead an agency in a way that affects someone else's information and to knowingly destroy documents containing personal information where a request has been made for it. The penalty is a fine not exceeding $10,000
- ***Commissioner making binding decisions on access requests:*** this reform will enable the Commissioner to make decisions on complaints relating to access to information, rather than the Human Rights Review Tribunal. The Commissioner's decisions will be able to be appealed to the Tribunal
- ***Strengthening the Privacy Commissioner's information gathering power:*** the Commissioner's existing investigation power is strengthened by allowing him or her to shorten the time frame within which an agency must comply, and increasing the penalty for non-compliance.

As part of the process, John Edwards the Privacy Commissioner, will be pointing to his report put forward to the Government in 2016 in which there were six recommendations made including a power to apply for fines of up to $1 million for organisations, and $100,000 for individuals who seriously breach their obligations. This would bring NZ into line with Australia and would begin to approach the sanctions available to the Privacy Commissioners counterparts in Europe, Asia and elsewhere in the world.

Next Steps

The Bill is proposed to come into effect on 1 July 2019. However, this date and the content of the Bill, are subject to change as it progresses through Parliament.

timg

THE INFORMATION MANAGEMENT GROUP

Australia's Notifiable Data Breach Legislation

What is the NDB?

The NDB legislation, which came into effect on 22nd February 2018, is an addition to the Australian Privacy Act 1988 and aims to increase the level of responsibility an organisation has with securing personal information of staff, stakeholders, and customers. Businesses and organisations need to maximise their data security. Under the new laws, a business has a legal obligation to notify an individual when information regarding them is breached. Data breaches that can cause serious harm to individuals must also be reported to the Office of the Information Commissioner (OAIC)

What are the penalties?

Failure to uphold the obligations of the NDB will result in heavy consequences. If there's an eligible data breach and no notifications are sent, the penalty can reach $1.7 million for organisations and $340,000 for individuals. In addition to this, it's difficult to quantify the cost of loss of trust for a business or organisation and therefore the impact on a brand. The Commissioner also has the power to make organisations pay compensation for damages and issue a public apology.

Who does the NDB apply to?

The NDB scheme applies to any agency, organisation or entity that is covered by the Australian Privacy Act 1988 (Cth). Businesses, organisations and entities (with a $3 million or higher turnover per annum in any financial year since 2001) are also covered. Any business that is included in the following categories are also captured under the scheme, regardless of their turnover.

These entities include:

- Health service providers
- Credit reporting bodies
- Entities related to an APP entity
- Entities that trade in personal information
- Employee associations registered under the Fair Work (Registered Organisations) ACT 2009
- Entities that 'opt-in' to APP coverage under the Privacy Act

How to protect your business

Regardless of what personal information you store, the risk of a data breach is increasing. That's why it's essential to maintain a strong defence against cybercrime and have steps in place to safely store and destroy information.

The best way to protect your business from the consequences of a data breach is to protect the information from the beginning.

Here are some tips to prevent a data breach:

- Store only essential and relevant personal information
- Make sure the process of data collection & storage is secure. TIMG offer secure document and media storage
- Keep your staff educated on dealing with suspicious emails that may contain viruses
- Keep information on a trusted platform and have cyber defence systems in place. TIMG offers a secure online cloud backup service
- Implement procedures to monitor the storage and destruction of information. TIMG can do this for you
- Outsource your information storage and destruction needs to a certified and secure provider such as TIMG

What to do if a data breach occurs

Time is critical with any sort of data breach, and the actions you take will determine the success of your recovery. Initially you should secure the information and contain the breach. Securing information online is an ongoing pursuit, however, physical data breaches are easier to contain.

TIMG's secure document and media storage, e-Waste/data destruction and online cloud backup services guarantee you absolute data protection. TIMG will partner with you to establish and maintain effective and secure information storage and once the information is no longer required, TIMG can ensure certified destruction takes place.

To better understand how the new NZ privacy laws will affect your business or to discuss a secure storage or destruction solution, contact TIMG today.

TIMG's CERTIFICATIONS & ACCREDITATIONS

PRISM INTERNATIONAL Professional Records & Information Services Management

AAA CERTIFIED APPROVED SITE

R·I·M Professionals Australasia

CEMARS ORGANISATION

PCI Security Standards Council

timg THE INFORMATION MANAGEMENT GROUP

0800 SECURITY

salesenquiries@timg.co.nz

timg.co.nz