Community Underwriting

MANDATORY DATA BREACH REPORTING

A Resource to Help Not for Profits Manage The Impact of Data Breach Laws

On 22 February 2018 new mandatory data breach reporting obligations were imposed on Australian entities through the passage of the Privacy Amendment (Notifiable Data Breaches) Act 2017 which established the Notifiable Data Breaches (NDB) scheme in Australia.

The potential impacts to an organisation as a result of the new legislation include significant costs, compensation to individuals and civil penalties.

Which Not for Profit Organisations are captured by the legislation:

- Organisations that have an annual turnover of more than $3m and possess or control information that identifies an individual (APP entities);
- An individual, body corporate, partnership, unincorporated association or trust with an annual turnover of less than $3m (a Small Business Operator – SBO) that:
  - is related to an APP entity;
  - provide any services in relation to the physical, emotional, psychological and mental health of any individual including hospitals, day surgeries, medical practitioners and allied health professionals; complementary therapists, child care centres, private schools and private tertiary educational institutions;
  - operate a residential tenancy data base;
  - collect or disclose personal information about individuals to anyone else for a benefit, service or advantage;
  - is a “tax file number recipient” by being in possession or control of a record that contains tax file number information of an individual;
  - participates in the credit reporting system by disclosing personal information to or collecting information from a credit reporting body;
  - employee associations registered under the Fair Work (Registered Organisations) Act 2009 and /or conduct any protected action ballot; and
  - voluntarily ‘opt-in’ to APP coverage under the Privacy Act.

What is an Eligible Data Breach

An organisation has an obligation to notify where there is an "eligible data breach" which occurs where:

1. There has been (or is likely to be) unauthorised access or disclosure of information; and
2. A "reasonable person" would conclude that the access or disclosure would 'likely' result in "serious harm" to the affected individuals

A loss or erroneous disclosure of information does not automatically trigger the operation of the Act.

Organisations must be prepared to conduct an objective assessment of a suspected data breach to determine:

Has there been unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation holds, e.g:

- an employee or contractor browses sensitive records without authority;
- a computer network is compromised by an external hacker;
- an employee publishes a confidential data file on the internet;
- an employee leaves hard copy documents, unsecured electronic equipment or storage devices in a public place.

Is the access or disclosure likely to result in serious harm to any of the individuals to whom the information relates:

- is the risk of serious harm more probable than not;
- what are the anticipated consequences of the harm and could physical, psychological, emotional, financial or reputational harm be suffered by any individual, e.g:

    - identity theft;
    - significant financial loss by the individual;
    - threats to an individual's physical safety;
    - loss of business or employment opportunities;
    - humiliation, damage to reputation or relationships;
    - workplace or social bullying or marginalisation.

Has the organisation has been able to prevent the likely risk of serious harm through prompt remedial action.

If an organisation acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to report.

When an Eligible Data Breach has been Identified by your Organisation:

Once an organisation is aware that there are reasonable grounds to believe that there has been an eligible data breach – whether during the course of an assessment, or when the assessment is complete (all reasonable steps must be taken to complete an assessment within 30 calendar days) – it must promptly notify affected individuals and the Commissioner about the breach.

A Notifiable Data Breach Statement must be provided:

- to the Information Commissioner as soon as practicable after becoming aware of the suspected eligible data breach; and
- to the individuals about whom the relevant information relates, or those who are at risk from the eligible data breach, as soon as practicable after completion of the Statement.

The Statement must include the name and contact details of the organisation, a description of the eligible data breach, the kind or kinds of information involved, and what steps the organisation recommends that individuals at risk of serious harm take in response to the eligible data breach.

The Notifiable Data Breaches scheme provides three options for notifying individuals at risk of serious harm, depending on what is 'practicable' for the organisation. Practicable considers the time, effort, and cost of notifying individuals at risk as well as the capabilities and capacity of the organisation:

- Option 1 – notify all individuals whose personal information was part of the eligible data breach.
- Option 2 - If it is practicable, notify only those individuals who are at risk of serious harm from the eligible data breach.
- Option 3 - If neither option 1 or 2 are practicable (for e.g. where there is no up to date contact details for individuals) then the statement must be published on a website and proactive steps taken to publicise the substance of the breach.

Consequences of a Failure to Comply

The Information Commissioner's powers if an organisation fails to comply are the same as those currently available for failing to comply with the Privacy Act, including:

- Declaring sanctions such as public apologies;
- Investigative powers, including the power to enter premises or compel the provision of information;
- Conduct of a hearing, including examination of witnesses;
- Seeking enforceable undertakings, such as updating security systems on a regular basis or obtaining an independent review of a party's dealings with third party providers;
- Making determinations including declarations that a complainant is entitled to compensation for loss or damage;
- Applying to the Federal Court for an order for penalty of up to $360,000 for individuals and $1,800,000 for organisations.

Risk Mitigation

If your organisation is subject to the Act it is critical to implement policies and procedures that will:

- identify and classify / rank the types of data your organisation holds which might result in an eligible data breach;
- mitigate the potential of a data breach; and
- ensure that you are compliant with the new regime should a breach occur.

There are a range of experts that can provide professional advice in this area. Some of the high-level points relevant to risk mitigation have included:

- undertake an annual privacy and security vulnerability assessment to identify and close gaps in policies and procedures and adjust resource needs in areas such as:
  - intrusion detection and prevention
  - web access restrictions
  - patching procedures
  - cloud based hosting
  - back up of data
  - third party access (due diligence, contractual agreements and ongoing oversight)
- review the effective use of encryption technology for information that needs to be protected and the devices on which it is stored;
- consider how your organisation's present insurance coverage responds to cyber events and whether obtaining specialised cyber insurance coverage is necessary;
- implement a data breach response plan (the Office of the Australian Information Commissioner has an example plan on its website);
- develop an appropriate and adequately trained breach response team.

Making a real difference to the way insurance is provided to the Not for Profit sector