Data Breach Law Obligations: Are You Ready

On the 22nd of February 2018, *the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)* comes into effect, establishing the Notifiable Data Breaches (NDB) scheme in Australia; which requiring all organisations identified under the *Privacy Act 1988 (Cth)* to notify the Office of the Australian Information Commissioner (OAIC) and any impacted parties about significant data breaches. As of the 1st of February 2018, a significant number of Australian organisations are still not ready to address the new obligations placed on them. Many don't realise the law will apply to them; others haven't even started to identify their data risks.

Background

The *Privacy Act 1988* regulates how personal information must be handled. The Privacy Act defines personal information as "*information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable".* Some examples of personal information include (*but are not limited to*) an individual's name, signature, address, telephone number, birth date, medical records, bank account details and commentary or opinion about a person.

The Privacy Act 1988 (Schedule 1) describes thirteen Australian Privacy Principles (APPs). The 13 AAPs are:

- APP 1 'Open and transparent management of personal information';
- APP 2 'Anonymity and pseudonymity';
- APP 3 'Collection of solicited personal information';
- APP 4 'Dealing with unsolicited personal information';
- APP 5 'Notification of the collection of personal information';
- APP 6 'Use or disclosure of personal information';
- APP 7 'Direct marketing';
- APP 8 'Cross-border disclosure of personal information';
- APP 9 'Adoption, use or disclosure of government related identifiers';
- APP 10 'Quality of personal information';
- APP 11 'Security of personal information';
- APP 12 'Access to personal information'; and
- APP 13 'Correction of personal information'

All entities regulated under the *Privacy Act 1988* and the associated Australian Privacy Principles (APP) are known as APP entities. All APP entities are captured by the NDB scheme.

The status of many AAP entities is very clear as they are Australian Government (*or Norfolk Island Government*) agencies; businesses and not-for-profit organisations with an annual turnover of $3 million or more; credit reporting bodies; health service providers; and TFN recipients.

Most small business operators (SBOs) believe they are exempt. To be clear, an SBO is considered as an individual (including a sole trader), body corporate, partnership, unincorporated association, or trust that has not had an annual turnover of more than $3 million in any financial year since 2001. Many small organisations, currently under the threshold, are not aware of the 'any financial year' statement and are captured by previous annual turnover(s). Also a number of SBOs undertaking a range of activities (including: providing any health services; trading in personal information; credit reporting; acting as an employee associations registered under the *Fair Work (Registered Organisations) Act 2009 (Cth);* providing services to the Commonwealth under a contract; operating a residential tenancy data base; reporting under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)*; conducting a protected action ballot; or retaining information retained under the mandatory data retention scheme (S 5-1A) of the *Telecommunications (Interception and Access) Act 1979 (Cth)*) may be considered an AAP entity and therefore have obligations to report data breaches under the NDB scheme..

Managing data under the NDB scheme

Under Section 6(1) of the *Privacy Act 1988*, an AAP entity is taken to 'hold' personal information if it has possession or control of a record that contains personal information. The terminology 'hold' extends beyond the actual physical possession of a record to include a record that an entity has a right or power to deal with, even if it does not physically possess the record or own the medium on which it is stored. An entity still 'holds' a record if it is stored on their behalf by a third party (e.g. a cloud server, record storage facility, service provider or subcontractor). Based on contractual arrangements, joint ventures or outsourcing, two or more entities may be deemed to 'hold' the same information

The NDB scheme will extend to the overseas activities of an Australian Government agency (S 5-B (1)) and it will also applies to organisations (including small businesses covered by the Act) that have an 'Australian link' (S 5-B (2)). An organisation is considered to have an Australian link either because it is incorporated or formed in Australia (S 5-B (1A)), or where it:

- Carries on business in Australia or an external Territory, and
- Collected or held personal information in Australia or an external Australian Territory, either before or at the time of the act or practice (s 5-B (3)).

Importantly, an APP entity which discloses any personal information to an overseas recipient, in line with the requirements of APP 8, then the APP entity is deemed to 'hold' the information for the purposes of the NDB scheme (s 26WC(1)). An APP entity that discloses personal information to an overseas recipient must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. This means that if the personal information held by the overseas recipient is subject to loss, unauthorised access, or disclosure, the APP entity is still responsible for assessing whether it is an eligible data breach under the Privacy Act 1988, and if it is, for notifying individuals at risk of serious harm and providing a statement to the OAIC.

The NDB scheme applies to incidents where personal information is subject to unauthorised access or disclosure, or is lost, following the scheme's commencement. This is an important statement as a data breach before 22 February 2018 is not subject to the NDB scheme or if an organisation discovers the breach after 22 February 2018, but the breach occurred prior to that date, the breach is not an 'eligible data breach' for the purposes of the NDB scheme.

Organisations need to understand what constitutes an 'eligible data breach'. In the simplest of terms, an 'eligible data breach' arises when all the following three criteria are satisfied:

1. There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds (S 26-WE(2)); and
2. This event is likely to result in serious harm to one or more individuals; and
3. The AAP entity has not been able to prevent the likely risk of serious harm with remedial action.

In its rawest form, 'unauthorised access' of personal information will be considered to have occurred when personal information held by an entity is accessed by someone who is not permitted to have access. 'Unauthorised disclosure' will be considered to have occurred when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the entity, and releases that information from its effective control in a way that is not permitted by the *Privacy Act 1988*. In general, 'Loss' refers to the accidental or inadvertent loss of personal information held by an entity, in circumstances where is it is likely to result in unauthorised access or disclosure. Under the NDB scheme, if personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there may be no eligible data breach (S 26-WE (2)(b)(ii)) (e.g. the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely)

Some examples of data breaches could be:

- The loss or theft of a device (e.g. laptop, tablet, hard drive, memory card or disk left on public transport or in a cafe) containing customers' personal information;
- The incorrect disposal of records or record containing structures (e.g. records remaining legible and open to reading by an unauthorised third party; or record containing filing cabinets being sold at auction);
- The hacking or uncontrolled access of a database containing personal information (e.g. an employee or contractor browses sensitive customer records without any legitimate purpose); or
- The provision of personal information to the wrong person or organisation (e.g. an employee accidentally publishes a confidential data file containing the personal information of one or more individuals on the internet).

When determining if an 'eligible data breach' has occurred, consideration, from the perspective of a 'reasonable person', must be applied to conclude if the data breach would be likely to result in 'serious harm' to an individual whose personal information was part of the data breach. The NDB scheme considers a 'reasonable person' to be a person in the APP entity's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available or following reasonable inquiries or an assessment of the data breach. In general, APP entities are not expected to external enquire about the circumstances of each individual whose information is involved in the breach.

The phrase 'likely to occur' means the risk of serious harm to an individual is more probable than not (rather than possible). 'Serious harm' is not specifically defined in the Privacy Act 1998. It would be reasonable to consider serious harm to an individual may include serious physical, psychological, emotional, financial, or reputation harm. The NDB scheme includes a non-exhaustive list of 'relevant matters' that may assist APP entities during the assessment of the likelihood of serious harm (S 26-WG)

Some examples of 'significant harm' could be:

- 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; or
- Workplace or social bullying or marginalisation.

APP entities take all reasonable steps to complete a 'reasonable and expeditious' assessment within 30 calendar days after the day the entity became aware of the grounds (or information) that caused it to suspect an eligible data breach (S 26-WH (2)). The OAIC has indicated it expects, wherever possible, APP entities treat the 30 days as a maximum time limit for completing an assessment and the entities endeavour

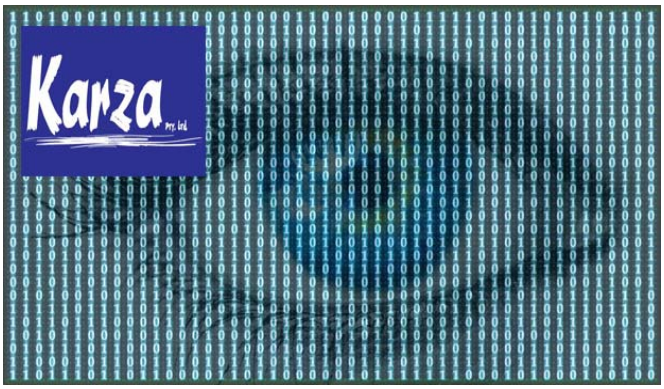
to complete the assessment in a much shorter timeframe to minimise risk of serious harm to individuals.

Base on the OAIC's suggestion, organisations should, as a minimum, consider undertaking an assessment which adequately covers:

1. Deciding whether an assessment is necessary and identify which person or group will be responsible for completing it
2. Quickly gather relevant information about the suspected breach including, for example, what personal information is affected, who may have had access to the information and the likely impacts, and
3. Making a decision, based on the investigation, about whether the identified breach is an eligible data breach

Under the NDB scheme an APP entities is provided with the opportunity to take pro-active steps to address a data breach in a timely manner and thereby avoid the need to notify the OAIC. If the remedial action ensures the data breach would not be likely to result in serious harm, then the breach is not an eligible data breach for that entity or for any other entity (S 26-WF (1), (2) & (3)). If the remedial action prevents the likelihood of serious harm to some individuals within a larger group of individuals whose information was compromised in a data breach, notification to those individuals for whom harm has been prevented is not required.

Certain participants in the *My Health Record* system (e.g. the system operator, a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider) are required to report *My Health Record* data breaches to the either the system operator or the OAIC, or both, depending on the entity reporting the data breach (*My Health Records Act 2012* (Cth), S 75). To prevent duplication, if a data breach has been, or is required to be, notified under the *My Health Records Act 2012*, the NDB scheme does not apply (S 26-WD). This exemption may not apply to a General Practice clinical database (which is not directly a part of the *My Health Record* system).



What steps should an organisation take?

All organisations, irrespective of size (and SBO status) should carefully consider their status relative to the *Privacy Act 1988* and the *Privacy Amendment (Notifiable Data Breaches) Act 2017*. Status consideration needs to cover organisation size, the various activities the organisation undertakes, who the organisation establishes contracts with and the types of data the organisation holds or may potentially hold.

Organisations drawn into the NDB scheme need to promptly identify and clearly understand their data risks before any potential 'notifiable data breach' occurs. As a minimum, effective mitigation measures should be identified, established and maintained to reduce the potential and severity of any breach. A strategic plan should be formulated describing: the risks; the various mitigation measures; how any potential data breaches (incidents) will be managed and reported; any monitoring and measurement requirement; employee training and communication needs; resourcing requirements; and the timing of ongoing reviews. A 'safe data' policy and data breach process should be established and communicated within the organisation. Where data is to be 'held' external to the organisation through outsourcing, clear and measurable contractual requirements should be documented and communicated to ensure the potential for data breaches is minimised and any incidents are prompt reported and effectively managed. All organisations should periodically test and audit their data breach plans and processes; with test and audit outcomes feeding directly into the organisation's continual improvement programme.

Be Ready; Be Prepared