PRIVACY AMENDMENT (NOTIFIABLE DATA BREACHES) BILL 2016

PASSES THROUGH BOTH HOUSES

Current as at 28 February 2017

The Privacy Amendment (Notifiable Data Breaches) Bill 2016 (**the Bill**) received Royal Assent on 22 February 2017. The resulting legislation, the Privacy Amendment (Notifiable Data Breaches) Act 2017, amends the *Privacy Act 1988* (***Privacy Act***) to require entities covered by that Act to:

- **undertake an assessment process** if they are aware that there are reasonable grounds to suspect there may have been an ***eligible data breach***, but does not know if there are reasonable grounds to believe that there has been a breach; and

- **notify both the Office of the Australian Information Commissioner (OAIC) and affected individuals** if they are aware that there are reasonable grounds to believe there has been an **eligible data breach** (after completing the above assessment or otherwise).

An **eligible data breach** essentially happens if there is unauthorised access to, unauthorised disclosure of, or loss of personal information held by an entity and this is likely to result in serious harm to any of the individuals to whom the information relates.

WHO DO THE OBLIGATIONS APPLY TO?

The changes apply to entities, including insurers, insurance brokers and their agents that are regulated under the *Privacy Act*.

The obligations will not apply to those that are exempt from the *Privacy Act* requirements, such as a small businesses with annual turnover of $3 million or less.

TIMING AND TRANSITIONAL PERIODS

- The amendments will commence on a single day to be fixed by proclamation. However if the provisions do not commence within 12 months from 22 February 2017, they will commence on the day after the end of that period.

- This allows all entities a transitional period of up to one year to ensure their existing policies and procedures are amended comply with the new requirements.

WHAT IS AN ELIGIBLE DATA BREACH?

Generally

An *eligible data breach* occurs where **EITHER**:

- Both of the following conditions are satisfied:
    - there is unauthorised access to, or unauthorised disclosure of personal information held by an entity regulated under the *Privacy Act*; and
    - a reasonable person would conclude that the access or disclosure would be *likely* to result in *serious harm* to any of the individuals to whom the personal information relates;

OR

- the information is lost in circumstances where:
    - unauthorised access to, or unauthorised disclosure of the personal information is *likely* to occur; and
    - assuming that unauthorised access to, or unauthorised disclosure of, the personal information were to occur, a *reasonable person* would conclude that the access or disclosure would be *likely* to result in *serious harm* to any of the individuals to whom the information relates.

(Section 26WE). The above is subject to an exception discussed further below.

Meaning of "reasonable person" and "likely risk"

The terms 'reasonable person' and 'likely risk' are not defined terms. Paragraph 8 of the Explanatory Memorandum (**EM**) to the Bill notes "the 'reasonable person' and 'likely risk' elements of the notification standard, by using commonly-understood legal standards of objectivity and probability, are intended to provide greater certainty for regulated entities while maintaining consistency with the core objective of the ALRC recommendation.

"Likely" is effectively more probable than not.

What is "*serious harm"?*

The term "serious harm" is not defined. Paragraphs 9 and 10 of the EM provide some form of guidance:

9. "Serious harm, in this context, could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach. Though individuals may be distressed or otherwise upset at an unauthorised access to or unauthorised disclosure or loss of their personal information, this would not itself be sufficient to require notification unless a reasonable person in the entity's position would consider that the likely consequences for those individuals would constitute a form of serious harm."

10. “It is expected that a likely risk of serious financial, economic or physical harm would be the most common likely forms of serious harm that may give rise to notification. Nonetheless, a reasonable person may conclude in some cases that a likely risk of serious psychological or emotional harm, serious harm to reputation or other serious harms arising from an unauthorised access, unauthorised disclosure or loss of personal information may exist. For example, this may be the case where an eligible data breach involves health information or other ‘sensitive information’ (in the sense of the definition of that term in existing subsection 6(1) of the *Privacy Act* or otherwise).”

Obligation to take account of certain relevant matters in forming a view

In forming a view on whether a reasonable person would conclude that an access to, or a disclosure of, information would be likely or not to result in serious harm to the individuals, the following must be considered (they are not all inclusive):

- the kind or kinds of information;
- the sensitivity of the information;
- whether the information is protected by one or more security measures;
- if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome;
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information;
- if a security technology or methodology (for example encryption):
    - was used in relation to the information; and
    - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information,

  the likelihood that the persons, or the kinds of persons, who:
    - have obtained, or who could obtain, the information; and
    - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;

  have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology (for example an encryption key);
- the nature of the harm; and
- any other relevant matters.

(Section 26WG).

Examples of types of data breaches that may trigger the above

The EM in paragraph 61 in explaining the types of conduct often giving rise to issues provides the following examples:

- lost or stolen laptops, removable storage devices, or paper records containing personal information;
- hard disk drives and other digital storage media being disposed of or returned without the contents first being erased;
- databases containing personal information being ‘hacked' into or otherwise illegally accessed by individuals outside of the entity;
- employees accessing or disclosing personal information outside the requirements or authorisation of their employment;
- paper records stolen from insecure recycling or garbage bins;
- mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address; and
- an individual deceiving an entity into improperly releasing the personal information of another person.

In each case it needs to be considered whether it falls within the eligible data breach criteria referred to above.

EXCEPTIONS

Remedial action exception

In the event that there is unauthorised access to, or unauthorised disclosure or loss of information, and the entity:

- takes action in relation to the access, disclosure or loss before any serious harm to an individual arises; and
- as a result of that action, a reasonable person would conclude that the access, disclosure or loss would not be likely to result in serious harm to any of those individuals,

then the unauthorised access, disclosure or loss of information is taken to never have been an eligible data breach.

Consequently in this case the entity is not required to take steps to notify the individual of the contents of a statement that relates to the access or disclosure.

This highlights the importance of effective and immediate action in response to data breaches.

(Section 26WF).

ASSESSMENT OBLIGATION

What do I do if I suspect an eligible data breach has occurred but don't know for sure?

If:

- an entity is aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity, and:

- the entity is not aware that there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity,

the entity must:

- carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity; and

- take all reasonable steps to ensure the assessment is completed within 30 days after the entity becomes aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity.

(Section 26WH).

If an entity complied with the above in relation to a breach by it and the access, disclosure or loss that constituted the eligible data breach of the entity is a breach by one or more other entities, the section i.e. the assessment obligation is not applicable in relation to the eligible data breaches of the other entities (s26WJ).

In the event an eligible data breach has occurred, notification to the OAIC and effected individuals is then required.

NOTIFICATION OBLIGATION

Notification to the OAIC

If an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach, the entity must prepare statement to the OAIC Commissioner setting out:

- the identity and contact details of the entity;
- a description of the eligible data breach that the entity has reasonable grounds to believe has happened;
- the kind or kinds of information concerned; and
- recommendations about the steps that individuals should take in response to the eligible data breach that the entity has reasonable grounds to believe has happened.

(**Statement**) (s26WK).

If the entity has reasonable grounds to believe that the access, disclosure or loss that constituted the eligible data breach of the entity is an eligible data breach of one or more

other entities, the statement referred to above may also set out the identity and contact details of those other entities (s26WK(4)).

Notification to affected persons

Where an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity and it has prepared a Statement the entity must:

- **Group type notification** - If it is practicable for the entity to notify the contents of the statement to each of the individuals to whom the relevant information relates, the entity must take reasonable steps in the circumstances to notify each individual affected of the contents of the statement (s26WL(2)(a));

  Paragraph 16 of the EM notes that in some cases "it may be impracticable for an entity to consider the circumstances of each affected individual to determine which individuals are at risk from an eligible data breach and which are not. In these circumstances notifying the entire cohort of affected individuals may be appropriate."

  OR

- **individuals at risk type notification** - If it is practicable for the entity to notify the contents of the statement to each of the individuals who are '*at risk'* from the eligible data breach, the entity must take reasonable steps in the circumstances to notify the contents of the statement to each of the individuals who are at risk from the eligible data breach (s26WL(2)(b)).

  Section 26WE(2)(d) provides an individual will be 'at risk' of serious harm from an eligible data breach if:

  - a reasonable person would conclude that the access, loss or disclosure of information would be likely to result in serious harm to any of the individuals to whom the information relates; and
  - assuming that unauthorised access to, loss of or unauthorised disclosure of the information were to occur, a reasonable person would conclude that the access, loss or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

  Paragraph 16 of the EM notes that in some cases "it may be practicable for an entity to determine with a high degree of confidence that only some individuals from a broader group of affected individuals are 'at risk', meaning that notification to the broader group may not be necessary from a harm mitigation perspective." In these cases, it is practicable for the entity to contact the selected individuals who are 'at risk' of being affected, not the entire group.

  In either of the above cases notification may be by the method in which the entity ordinarily communicates with that individual.

- ***Not practicable to notify all individuals or only those at risk***

  Where neither of the above notification triggers apply the entity must publish a copy of the statement on the entity's website (if any) and take reasonable steps to publicise the contents of the statement (s26WL(2)(c)).

  Paragraph 17 of the EM notes that "there may be circumstances in which it is impracticable to provide a notification to affected individuals, either collectively or only to those at risk. The Bill provides that, in these circumstances, an entity will not be required to provide notice directly to each affected individual but will rather be required to provide the information described above on its website (if any) and to take reasonable steps to publicise the information."

Deemed holding of information regarding overseas entities

An entity that has disclosed personal information to an overseas recipient that holds the information, retains accountability for an eligible data breach involving personal information even though that APP entity might not otherwise be responsible for the breach due to the fact that the personal information has been disclosed to an overseas recipient pursuant to Australian Privacy Principle 8 .

In effect, the data breach notification obligations will continue to apply in the same way as if the information were still held by the Australian entity (s26WC).

The practical effect of this is that entities will need to ensure their agreements with overseas processors include strict obligations to notify the Australian entity whenever the overseas processor has reason to believe an eligible data breach has occurred as the Australian entity will breach its obligation if this is not done.

Notification exceptions

The following limited exceptions also apply in relation to the notification obligations:

- where the eligible data breach of the entity is also an eligible data breach of another entity (for example a data warehouse facility) the requirements do not apply to the breaches of those other entities (an entity must still comply with its own breach requirements for its breach) (section 26WM);

- where the entity is an enforcement body and compliance would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, the enforcement body (section 26WN);

- where compliance would be inconsistent with a secrecy provision that prohibits or regulates the use or disclosure of information (section 26WP); or

- where the OAIC has issued a written notice declaring the provisions do not apply (section 26WQ).

CONSEQUENCES OF ANY FAILURE TO COMPLY

Any failure to:

- carry out an assessment of a suspected eligible data breach within 30 days of becoming aware of it;
- prepare a statement and give a copy to the Commissioner as soon as practicable after becoming aware of an eligible data breach;
- notify the individuals affected of the contents of the statement or publish a copy of the statement; or
- comply with a direction of the Commissioner if the Commissioner is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity, and the Commissioner directs the entity to:
    - prepare a statement relating to the eligible data breach; and
    - give a copy of the statement to the Commissioner

constitutes an interference with the privacy of an individual.

This will engage the Commissioner's existing powers to:

- investigate;
- make determinations;
- provide remedies in relation to non-compliance;
- seek enforceable undertakings; and
- pursue civil penalties for serious or repeated interferences with privacy.

As noted in paragraph 29 of the EM, this approach will permit the use of less severe sanctions before elevating to a civil penalty. These less severe penalties could include public or personal apologies, compensation payments or enforceable undertakings.

In circumstances where the Commissioner believes that an eligible data breach has occurred and no notification has been given by the entity that suffered the breach, the Commissioner may give a written direction to the entity requiring it to provide notification of the data breach.

Before giving a direction, the Commissioner must invite the entity concerned to make a submission to the Commissioner about the direction, and consider any response from the entity.

The Commissioner has discretion to decide on the manner in which the invitation is made and the time the entity has to respond, given that in some cases a long period of time may not be appropriate.

Civil penalties

Serious or repeated interferences with the privacy of an individual may attract a maximum penalty of $360,000 for individuals and $1,800,000 for corporations.

A civil penalty would only be applicable where there has been a serious or repeated non-compliance with mandatory notification requirements. Civil penalties can only be imposed by the Federal Court or Federal Circuit Court of Australia on application by the Commissioner.

SOME EXAMPLES OF HOW THIS MAY AFFECT YOU

Consider the following:

- reviewing agreements with third parties to whom the entity may disclose personal information, in order to ensure that there are requirements for the third party providers to notify the entity of any suspected eligible data breaches (this also applies to organisations who outsource aspects of their operations dealing with personal information to overseas providers, i.e. call centres and IT management firms);
- current processes for reviewing any suspected data breaches and implementing procedures to notify any eligible data breaches to the OAIC and affected individuals;
- current procedures and processes relating to the security and safety of data, including employee access and use of such information; and
- IT security procedures and mechanisms to prevent a breach arising.
- developing a data breach response plan;
- ensuring you have a current IT and data security policy;
- ensuring you monitor compliance with IT and data security polices; and
- the appropriateness of a cyber insurance policy to assist in covering potential exposures.

FOR FURTHER INFORMATION

It is anticipated that the Commissioner will update the current *OAIC Data Breach Notification: A guide to handling personal information security breaches* or release other guidance material to reflect the passage of this Bill and to assist entities in preventing, identifying, notifying and containing eligible data breaches.

You can also refer to the Explanatory Memorandum available on Parliament's website.