PRIVACY AMENDMENT (NOTIFIABLE DATA BREACHES) BILL 2016

Current as at 4 November 2016

BACKGROUND

The Privacy Amendment (Notifiable Data Breaches) Bill 2016 ("Privacy Data Breaches Bill") has been introduced to Parliament and is currently before the House of Representatives.

The Privacy Data Breaches Bill implements recommendations of:

- the Parliamentary Joint Committee on Intelligence and Security's Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014; and
- the Australian Law Reform Commission's report "For Your Information: Australian Privacy Law and Practice",

by amending the Privacy Act 1988 ("Privacy Act") to require agencies, organisations and certain other entities to provide notice to the Office of the Australian Information Commissioner ("OAIC") and affected individuals of an eligible data breach.

KEY OBJECTIVES OF THE PRIVACY DATA BREACHES BILL

The key objectives of the Privacy Data Breaches Bill are to:

- implement a mandatory data breach notification scheme to promote the protection of privacy of individuals, and provide certainty and consistency to organisations and agencies when responding to data breaches;
- allow individuals whose personal information has been compromised in a data breach to take remedial steps to lessen the adverse impact that might arise from the breach;
- encourage consumers to more fully engage in e-commerce, thereby boosting Australia's digital economy by providing greater assurance about the safety of personal information;
- provide the OAIC with information about trends in data breaches that may assist in the development of useful guidance material for entities about information security; and
- improve compliance with privacy obligations - the reputational damage that can follow a high-profile data breach, and the commercial consequences of such a breach, can provide powerful incentives to improve security.

WHO THE CHANGES WILL APPLY TO

The Privacy Data Breaches Bill apply to entities that are regulated under the Privacy Act.

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

EXAMPLES OF A DATA BREACH

A data breach could arise where there is unauthorised access to, or unauthorised disclosure of personal information such as:

- 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.

Where a data breach occurs an entity then needs to consider whether this is an "eligible data breach" to which notification requirements may apply.

WHAT IS AN ELIGIBLE DATA BREACH?

An eligible data breach happens if:

- both of the following conditions are satisfied:
  - there is unauthorised access to, or unauthorised disclosure of, the information; 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 information relates; or
- the information is lost in circumstances where:
  - unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
  - assuming that unauthorised access to, or unauthorised disclosure of, the 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.

This definition provides an objective test as to what a "reasonable person" would conclude as to whether the unauthorised access or disclosure may result in "serious harm" to an individual requiring the regulated entity to assess each data breach on its facts.

An entity must complete an assessment of a suspected eligible data breach within 30 days of becoming aware of such suspected breach.

WHEN IS THERE LIKELY TO BE A RISK OF SERIOUS HARM?

The Privacy Data Breaches Bill outlines a number of factors to consider in order to determine whether a data breach would be likely to result in serious harm to any individuals (and thus be an eligible data breach to which the notification provisions apply).

These factors include, but are not limited to, the following:

- 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:
  - 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;
- the nature of the harm; and
- any other relevant matters.

These factors need to be considered in the event of a data breach in order to determine whether the matter is an eligible data breach to which the notification provisions apply.

NOTIFICATION OF ELIGIBLE DATA BREACHES

Where an entity has reasonable grounds to believe there has been an eligible data breach the entity must as soon as practicable:

- prepare a statement which sets out:
  - the identity and contact details of the entity (and any other entities involved if applicable);
  - 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,

and give a copy of the statement to the OAIC Commissioner.

An entity is then required as soon as practicable to either:

- notify the individuals who are at risk from the serious data breach or to whom the information relates of the contents of the statement referred to above if it is practicable; or
- publish a copy of the statement on the entity's website (if any) and take reasonable steps to publicise the contents of the statement.

An entity may notify an individual by the method in which it ordinarily communicates with that individual.

EXCEPTIONS

There are limited exceptions to the notification provisions.

The proposed exceptions are:

- 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);
- 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;
- where compliance would be inconsistent with a secrecy provision that prohibits or regulates the use or disclosure of information; or
- where the OAIC Commissioner has issued a written notice declaring the provisions do not apply.

PENALTY PROVISIONS

At this stage no new penalty provisions are proposed as part of the Privacy Data Breaches Bill.

Failure to comply with an obligation included in the Privacy Data Breaches Bill will be deemed to be an interference with the privacy of an individual for the purposes of the Privacy Act. This will engage the Commissioner's existing powers to investigate, make determinations and provide remedies in relation to non-compliance with the Privacy Act. This includes the capacity to undertake initiated investigations, make determinations, seek enforceable undertakings, and pursue civil penalties for serious or repeated interferences with privacy.

A civil penalty for serious or repeated interferences with the privacy of an individual can only be issued by the Federal Court or Federal Circuit Court of Australia following an application by the Commissioner. 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 bodies corporate.

TRANSITION PERIOD

If passed, the Privacy Data Breaches Bill is expected to take effect 12 months after the amendment receives Royal Assent to allow entities time to transition to the new regime.

HOW THIS AFFECTS YOU

Entities that are regulated under the Privacy Act will need to review and consider the following:

- 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 data breaches;
- its 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.