2013-2014-2015

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

EXPOSURE DRAFT (30/11/2015)

Privacy Amendment (Notification of Serious Data Breaches) Bill 2015

No. , 2015

(Attorney-General)

A Bill for an Act to amend the *Privacy Act 1988*, and for related purposes

Contents

A Bill for an Act to amend the *Privacy Act 1988*, and for related purposes

The Parliament of Australia enacts:

1 Short title

This Act may be cited as the *Privacy Amendment (Notification of Serious Data Breaches) Act 2015*.

2 Commencement

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	
2. Schedule 1	A single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 12 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

(2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

3 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1—Amendments

Privacy Act 1988

1 Subsection 6(1)

Insert:

serious data breach has the meaning given by section 26WB.

2 After subsection 13(4)

Insert:

Notification of serious data breaches

(4A) If an entity (within the meaning of Part IIIC) contravenes section 26WC or 26WD, the contravention is taken to be an act that is an ***interference with the privacy of an individual***.

3 After Part IIIB

Insert:

Part IIIC—Notification of serious data breaches

Division 1—Introduction

26WA Simplified outline of this Part

- This Part sets up a scheme for notification of serious data breaches.
- A serious data breach occurs if:
  - (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information (or certain other information) held by an entity; and
  - (b) as a result, there is a real risk of serious harm to any of the individuals to whom the information relates.

- A serious data breach also occurs if:
  - (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information (or certain other information) held by an entity; and
  - (b) any of the information is of a kind specified in the regulations.
- An entity must give a notification if:
  - (a) it has reasonable grounds to believe that a serious data breach has occurred; or
  - (b) it is directed to do so by the Commissioner.

Division 2—Serious data breach

26WB Serious data breach

Scope

(1) This section applies if:

(a) both:

(i) an APP entity holds personal information relating to one or more individuals; and

(ii) the APP entity is required under section 15 not to do an act, or engage in a practice, that breaches Australian Privacy Principle 11.1 in relation to the personal information; or

(b) both:

(i) a credit reporting body holds credit reporting information relating to one or more individuals; and

(ii) the credit reporting body is required to comply with section 20Q in relation to the credit reporting information; or

(c) both:

(i) a credit provider holds credit eligibility information relating to one or more individuals; and

(ii) the credit provider is required to comply with subsection 21S(1) in relation to the credit eligibility information; or

(d) both:

(i) a file number recipient holds tax file number information relating to one or more individuals; and

(ii) the file number recipient is required under section 18 not to do an act, or engage in a practice, that breaches a section 17 rule that relates to the tax file number information.

Serious data breach

(2) If:

(a) there is unauthorised access to, or unauthorised disclosure of, the information, and:

(i) the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the information relates; or

(ii) any of the information is of a kind specified in the regulations; or

(b) the information is lost in circumstances where:

(i) unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and:

(ii) assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, the access or disclosure will result in a real risk of serious harm to any of the individuals to whom the information relates; or

(c) the information is lost in circumstances where:

(i) unauthorised access to, or unauthorised disclosure of, the information may occur, and:

(ii) any of the information is of a kind specified in the regulations;

the access or disclosure covered by paragraph (a), or the loss covered by paragraph (b) or (c), is a ***serious data breach*** of the APP entity, credit reporting body, credit provider or file number recipient, as the case may be.

Note 1: For ***harm***, see section 26WF.

Note 2: For ***real risk***, see section 26WG.

Relevant matters

(3) For the purposes of this section, in determining whether there is a real risk of serious harm to an individual as mentioned in subparagraph (2)(a)(i) or (b)(ii), have regard to the following:

(a) the kind or kinds of information concerned;

(b) the sensitivity of the information;

(c) whether the information is in a form that is intelligible to an ordinary person;

(d) if the information is not in a form that is intelligible to an ordinary person—the likelihood that the information could be converted into such a form;

(e) whether the information is protected by one or more security measures;

(f) if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome;

(g) the persons, or the kinds of persons, who have obtained, or who could obtain, the information;

(h) the nature of the harm;

(i) if the entity has taken, is taking, or will take, steps to mitigate the harm:

(i) the nature of those steps; and

(ii) how quickly those steps have been, are being, or will be, taken; and

(iii) the extent to which those steps have mitigated, are mitigating, or are likely to mitigate, the harm;

(j) any other relevant matters.

(4) For the purposes of the application of paragraphs (3)(c) and (d) to information in an electronic form, assume that the person has access to software, or other technology, that:

(a) is publicly available; and

(b) is commonly used.

Overseas recipients

(5) If:

(a) an APP entity has disclosed personal information about one or more individuals to an overseas recipient; and

(b) Australian Privacy Principle 8.1 applied to the disclosure of the personal information; and

(c) the overseas recipient holds the personal information;

this section has effect as if:

(d) the personal information were held by the APP entity; and

(e) the APP entity were required under section 15 not to do an act, or engage in a practice, that breaches Australian Privacy Principle 11.1 in relation to the personal information.

Bodies or persons with no Australian link

(6) If:

(a) either:

(i) a credit provider has disclosed, under paragraph 21G(3)(b) or (c), credit eligibility information about one or more individuals to a related body corporate, or person, that does not have an Australian link; or

(ii) a credit provider has disclosed, under subsection 21M(1), credit eligibility information about one or more individuals to a body or person that does not have an Australian link; and

(b) the related body corporate, body or person holds the credit eligibility information;

this section has effect as if:

(c) the credit eligibility information were held by the credit provider; and

(d) the credit provider were required to comply with subsection 21S(1) in relation to the credit eligibility information.

Note: See section 21NA.

Division 3—Notification of serious data breaches

26WC Entity must notify serious data breach

(1) If an entity is aware, or ought reasonably to be aware, that there are reasonable grounds to believe that there has been a serious data breach of the entity, the entity must, as soon as practicable after the entity becomes so aware, or ought reasonably to have become so aware, as the case may be:

(a) prepare a statement that complies with subsection (3); and

(b) give a copy of the statement to the Commissioner; and

(c) take such steps (if any) as are reasonable in the circumstances to notify the contents of the statement to each of the individuals to whom the relevant information relates; and

(d) if it is not practicable for the entity to notify the contents of the statement to each of the individuals to whom the relevant information relates:

(i) publish a copy of the statement on the entity's website (if any); and

(ii) take reasonable steps to publicise the contents of the statement.

(2) For the purposes of subsection (1), ***as soon as practicable*** includes time taken by the entity in carrying out a reasonable assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to a serious data breach of the entity, so long as that assessment is carried out within 30 days after the entity becomes so aware, or ought reasonably to have become so aware, as the case may be.

(3) The statement referred to in paragraph (1)(a) must set out:

(a) the identity and contact details of the entity; and

(b) a description of the serious data breach that the entity has reasonable grounds to believe has happened; and

(c) the kind or kinds of information concerned; and

(d) recommendations about the steps that individuals should take in response to the serious data breach that the entity has reasonable grounds to believe has happened.

Method of providing the statement to an individual

(4) If the entity normally communicates with an individual using a particular method, the notification to the individual under paragraph (1)(c) may use that method. This subsection does not limit paragraph (1)(c).

Exception—enforcement related activities

(5) Paragraphs (1)(c) and (d) and (3)(d) do not apply if:

(a) the entity is an enforcement body; and

(b) the enforcement body believes on reasonable grounds that compliance with those paragraphs would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, the enforcement body.

Exception—Commissioner's notice

(6) The Commissioner may, by written notice given to an entity, exempt the entity from subsection (1) in such circumstances as are specified in the notice.

(7) The Commissioner must not give a notice under subsection (6) unless the Commissioner is satisfied that it is in the public interest to do so.

(8) The Commissioner may give a notice under subsection (6) to an entity:

(a) on the Commissioner's own initiative; or

(b) on application made to the Commissioner by the entity.

(9) An entity is not entitled to apply to the Commissioner under paragraph (8)(b) for an exemption that relates to particular circumstances unless the entity believes, on reasonable grounds, that there has been a serious data breach of the entity that involves those circumstances.

(10) If an entity applies to the Commissioner under paragraph (8)(b):

(a) the Commissioner may refuse the application; and

(b) if the Commissioner does so—the Commissioner must give written notice of the refusal to the entity.

(11) If an entity applies to the Commissioner under paragraph (8)(b) for an exemption that relates to particular circumstances, subsection (1) does not apply to the entity in relation to a serious data breach that involves those circumstances until the Commissioner makes a decision in response to the application for the exemption.

Exception—inconsistency with secrecy provisions

(12) If compliance by an entity with paragraph (1)(b), (c) or (d) would, to any extent, be inconsistent with a provision of a law of the Commonwealth (other than a provision of this Act) that prohibits or regulates the use or disclosure of information, subsection (1) does not apply to the entity to the extent of the inconsistency.

Exception—My Health Records Act 2012

(13) Subsection (1) does not apply to a serious data breach if the breach has been, or is required to be, notified under section 75 of the *My Health Records Act 2012*.

Exception—no serious data breach

(14) If:

(a) at a particular time, an entity was aware, or ought reasonably to have been aware, that there were reasonable grounds to believe that there had been a serious data breach of the entity; and

(b) the entity subsequently carries out a reasonable assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to a serious data breach of the entity; and

(c) the assessment was carried out within 30 days after the entity becomes so aware, or ought reasonably to have become so aware, as the case may be; and

(d) as a result of the carrying out of the assessment, the entity does not have reasonable grounds to believe that the relevant circumstances amount to a serious data breach of the entity;

subsection (1) does not apply, and is taken never to have applied, to the entity in relation to the relevant circumstances.

26WD Commissioner may direct entity to notify serious data breach

(1) If the Commissioner believes on reasonable grounds that there has been a serious data breach of an entity, the Commissioner may, by written notice given to the entity, direct the entity to:

(a) prepare a statement that complies with subsection (2); and

(b) give a copy of the statement to the Commissioner; and

(c) take such steps (if any) as are reasonable in the circumstances to notify the contents of the statement to each of the individuals to whom the relevant information relates; and

(d) if it is not practicable for the entity to notify the contents of the statement to each of the individuals to whom the relevant information relates:

(i) publish a copy of the statement on the entity's website (if any); and

(ii) take reasonable steps to publicise the contents of the statement.

(2) The statement referred to in paragraph (1)(a) must set out:

(a) the identity and contact details of the entity; and

(b) a description of the serious data breach that the Commissioner believes has happened; and

(c) the kind or kinds of information concerned; and

(d) recommendations about the steps that individuals should take in response to the serious data breach that the Commissioner believes has happened.

(3) A direction under subsection (1) may also require that the statement referred to in paragraph (1)(a) must set out specified information that relates to the serious data breach that the Commissioner believes has happened.

Method of providing the statement to an individual

(4) If the entity normally communicates with an individual using a particular method, the notification to the individual mentioned in paragraph (1)(c) may use that method. This subsection does not limit paragraph (1)(c).

Compliance with direction

(5) An entity must comply with a direction under subsection (1) as soon as practicable after the direction is given.

Exception—enforcement related activities

(6) The Commissioner must not give a direction under subsection (1) to an entity if:

(a) the entity is an enforcement body; and

(b) the chief executive officer of the enforcement body has given the Commissioner a certificate stating that the enforcement body believes on reasonable grounds that compliance with the direction would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, the enforcement body.

Exception—inconsistency with secrecy provisions

(7) If compliance by an entity with so much of a direction under subsection (1) as is covered by paragraph (1)(b), (c) or (d) would, to any extent, be inconsistent with a provision of a law of the Commonwealth (other than a provision of this Act) that prohibits or regulates the use or disclosure of information, paragraph (1)(b), (c) or (d), as the case may be, does not apply to the entity to the extent of the inconsistency.

Exception—My Health Records Act 2012

(8) The Commissioner must not give a direction under subsection (1) in relation to a serious data breach if the breach has been, or is required to be, notified under section 75 of the *My Health Records Act 2012*.

Division 4—General

26WE Entity

For the purposes of this Part, ***entity*** includes a person who is a file number recipient.

26WF Harm

For the purposes of this Part, ***harm*** includes:

(a) physical harm; and
(b) psychological harm; and
(c) emotional harm; and
(d) harm to reputation; and
(e) economic harm; and
(f) financial harm.

26WG Real risk

For the purposes of this Part, ***real risk*** means a risk that is not a remote risk.

4 After paragraph 96(1)(b)

Insert:

(ba) a decision under subsection 26WC(10) to refuse an application;
(bb) a decision under subsection 26WD(1) to give a direction;

5 Application of amendments—serious data breaches

(1) Paragraph 26WB(2)(a) of the *Privacy Act 1988* (as amended by this Schedule) applies to an access or disclosure that happens after the commencement of this item.

(2) Paragraphs 26WB(2)(b) and (c) of the *Privacy Act 1988* (as amended by this Schedule) apply to a loss that happens after the commencement of this item.