Privacy Amendment (Notifiable Data Breaches) Act 2017

No. 12, 2017

An Act to amend the *Privacy Act 1988*, and for related purposes

Note: An electronic version of this Act is available on the Federal Register of Legislation (https://www.legislation.gov.au/)

Contents

Privacy Amendment (Notifiable Data Breaches) Act 2017

No. 12, 2017

An Act to amend the *Privacy Act 1988*, and for related purposes

[*Assented to 22 February 2017*]

The Parliament of Australia enacts:

1 Short title

This Act is the *Privacy Amendment (Notifiable Data Breaches) Act 2017*.

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.	22 February 2017
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Note: This table relates only to the provisions of this Act as originally enacted.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Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.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:

at risk from an eligible data breach has the meaning given by section 26WE.

eligible data breach has the meaning given by Division 2 of Part IIIC.

2 After subsection 13(4)

Insert:

Notification of eligible data breaches etc.

(4A) If an entity (within the meaning of Part IIIC) contravenes subsection 26WH(2), 26WK(2), 26WL(3) or 26WR(10), 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 eligible data breaches

Division 1—Introduction

26WA Simplified outline of this Part

- This Part sets up a scheme for notification of eligible data breaches.
- An eligible data breach happens if:
  (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and

(b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

- An entity must give a notification if:
  (a) it has reasonable grounds to believe that an eligible data breach has happened; or
  (b) it is directed to do so by the Commissioner.

26WB Entity

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

26WC Deemed holding of information

Overseas recipients

(1) 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 Part 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

(2) 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 Part 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.

26WD Exception—notification under the *My Health Records Act 2012*

If:

(a) an unauthorised access to information; or

(b) an unauthorised disclosure of information; or

(c) a loss of information;

has been, or is required to be, notified under section 75 of the *My Health Records Act 2012*, this Part does not apply in relation to the access, disclosure or loss.

Division 2—Eligible data breach

26WE Eligible 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.

Eligible data breach

(2) For the purposes of this Act, if:

(a) both of the following conditions are satisfied:

(i) there is unauthorised access to, or unauthorised disclosure of, the information;

(ii) 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

(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, 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;

then:

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

(d) an individual covered by subparagraph (a)(ii) or (b)(ii) is ***at risk*** from the eligible data breach.

(3) Subsection (2) has effect subject to section 26WF.

26WF Exception—remedial action

Access to, or disclosure of, information

(1) If:

(a) an access to, or disclosure of, information is covered by paragraph 26WE(2)(a); and

(b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the access or disclosure; and

(c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so before the access or disclosure results in serious harm to any of the individuals to whom the information relates; and

(d) as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of those individuals;

the access or disclosure is not, and is taken never to have been:

(e) an ***eligible data breach*** of the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or

(f) an ***eligible data breach*** of any other entity.

(2) If:

(a) an access to, or disclosure of, information is covered by paragraph 26WE(2)(a); and

(b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the access or disclosure; and

(c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so before the

access or disclosure results in serious harm to a particular individual to whom the information relates; and

(d) as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to the individual;

this Part does not require:

(e) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or

(f) any other entity;

to take steps to notify the individual of the contents of a statement that relates to the access or disclosure.

Loss of information

(3) If:

(a) a loss of information is covered by paragraph 26WE(2)(b); and

(b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the loss; and

(c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so before there is unauthorised access to, or unauthorised disclosure of, the information; and

(d) as a result of the action, there is no unauthorised access to, or unauthorised disclosure of, the information;

the loss is not, and is taken never to have been:

(e) an ***eligible data breach*** of the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or

(f) an ***eligible data breach*** of any other entity.

(4) If:

(a) a loss of information is covered by paragraph 26WE(2)(b); and

(b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the loss; and

(c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so:

(i) after there is unauthorised access to, or unauthorised disclosure of, the information; and

(ii) before the access or disclosure results in serious harm to any of the individuals to whom the information relates; and

(d) as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of those individuals;

the loss is not, and is taken never to have been:

(e) an ***eligible data breach*** of the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or

(f) an ***eligible data breach*** of any other entity.

(5) If:

(a) a loss of information is covered by paragraph 26WE(2)(b); and

(b) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, takes action in relation to the loss; and

(c) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be, does so:

(i) after there is unauthorised access to, or unauthorised disclosure of, the information; and

(ii) before the access or disclosure results in serious harm to a particular individual to whom the information relates; and

(d) as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to the individual;

this Part does not require:

(e) the APP entity, credit reporting body, credit provider or file number recipient, as the case may be; or

(f) any other entity;

to take steps to notify the individual of the contents of a statement that relates to the loss.

26WG Whether access or disclosure would be likely, or would not be likely, to result in serious harm—relevant matters

For the purposes of this Division, in determining whether a reasonable person would conclude that an access to, or a disclosure of, information:

(a) would be likely; or

(b) would not be likely;

to result in serious harm to any of the individuals to whom the information relates, have regard to the following:

(c) the kind or kinds of information;

(d) the sensitivity of the information;

(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) if a security technology or methodology:

(i) was used in relation to the information; and

(ii) 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:

(iii) have obtained, or who could obtain, the information; and

(iv) 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;

(i) the nature of the harm;

(j) any other relevant matters.

Note: If the security technology or methodology mentioned in paragraph (h) is encryption, an encryption key is an example of information required to circumvent the security technology or methodology.

Division 3—Notification of eligible data breaches

Subdivision A—Suspected eligible data breaches

26WH Assessment of suspected eligible data breach

Scope

(1) This section applies if:

(a) an entity is aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity; and

(b) 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.

Assessment

(2) The entity must:

(a) 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

(b) take all reasonable steps to ensure that the assessment is completed within 30 days after the entity becomes aware as mentioned in paragraph (1)(a).

Note: Section 26WK applies if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity.

26WJ Exception—eligible data breaches of other entities

If:

(a) an entity complies with section 26WH in relation to an eligible data breach of the entity; and

(b) 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;

that section does not apply in relation to those eligible data breaches of those other entities.

Subdivision B—General notification obligations

26WK Statement about eligible data breach

Scope

(1) This section applies if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity.

Statement

(2) The entity must:
  (a) both:
    (i) prepare a statement that complies with subsection (3); and
    (ii) give a copy of the statement to the Commissioner; and
  (b) do so as soon as practicable after the entity becomes so aware.

(3) The statement referred to in subparagraph (2)(a)(i) must set out:
  (a) the identity and contact details of the entity; and
  (b) a description of the eligible 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 eligible data breach that the entity has reasonable grounds to believe has happened.

(4) 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 in subparagraph (2)(a)(i) may also set out the identity and contact details of those other entities.

26WL Entity must notify eligible data breach

Scope

(1) This section applies if:

(a) an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity; and

(b) the entity has prepared a statement that:

(i) complies with subsection 26WK(3); and

(ii) relates to the eligible data breach that the entity has reasonable grounds to believe has happened.

Notification

(2) The entity must:

(a) 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—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals to whom the relevant information relates; or

(b) 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—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals who are at risk from the eligible data breach; or

(c) if neither paragraph (a) nor (b) applies:

(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.

Note: See also subsections 26WF(2) and (5), which deal with remedial action.

(3) The entity must comply with subsection (2) as soon as practicable after the completion of the preparation of the statement.

Method of providing a statement to an individual

(4) If the entity normally communicates with a particular individual using a particular method, the notification to the individual under paragraph (2)(a) or (b) may use that method. This subsection does not limit paragraph (2)(a) or (b).

26WM Exception—eligible data breaches of other entities

If:

(a) an entity complies with sections 26WK and 26WL in relation to an eligible data breach of the entity; and

(b) 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;

those sections do not apply in relation to those eligible data breaches of those other entities.

26WN Exception—enforcement related activities

If:

(a) an entity is an enforcement body; and

(b) the chief executive officer of the enforcement body believes on reasonable grounds that there has been an eligible data breach of the entity; and

(c) the chief executive officer of the enforcement body believes on reasonable grounds that compliance with section 26WL in relation to the eligible data breach would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, the enforcement body;

paragraph 26WK(3)(d) and section 26WL do not apply in relation to:

(d) the eligible data breach of the entity; and

(e) if 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—such an eligible data breach of those other entities.

26WP Exception—inconsistency with secrecy provisions

Secrecy provisions

(1) For the purposes of this section, ***secrecy provision*** means a provision that:

(a) is a provision of a law of the Commonwealth (other than this Act); and

(b) prohibits or regulates the use or disclosure of information.

(2) If compliance by an entity with subparagraph 26WK(2)(a)(ii) in relation to a statement would, to any extent, be inconsistent with a secrecy provision (other than a prescribed secrecy provision), subsection 26WK(2) does not apply to the entity, in relation to the statement, to the extent of the inconsistency.

(3) If compliance by an entity with section 26WL in relation to a statement would, to any extent, be inconsistent with a secrecy provision (other than a prescribed secrecy provision), section 26WL does not apply to the entity, in relation to the statement, to the extent of the inconsistency.

Prescribed secrecy provisions

(4) For the purposes of this section, ***prescribed secrecy provision*** means a secrecy provision that is specified in the regulations.

(5) For the purposes of a prescribed secrecy provision:
   (a) subparagraph 26WK(2)(a)(ii); and
   (b) section 26WL;

are taken not to be provisions that require or authorise the use or disclosure of information.

(6) If compliance by an entity with subparagraph 26WK(2)(a)(ii) in relation to a statement would, to any extent, be inconsistent with a prescribed secrecy provision, subsection 26WK(2) does not apply to the entity in relation to the statement.

(7) If compliance by an entity with section 26WL in relation to a statement would, to any extent, be inconsistent with a prescribed secrecy provision, section 26WL does not apply to the entity in relation to the statement.

26WQ Exception—declaration by Commissioner

(1) If the Commissioner:
   (a) is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity; or
   (b) is informed by an entity that the entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity;

the Commissioner may, by written notice given to the entity:

(c) declare that sections 26WK and 26WL do not apply in relation to:
  (i) the eligible data breach of the entity; and
  (ii) if 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—such an eligible data breach of those other entities; or

(d) declare that subsection 26WL(3) has effect in relation to:
  (i) the eligible data breach of the entity; and
  (ii) if 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—such an eligible data breach of those other entities;

as if that subsection required compliance with subsection 26WL(2) before the end of a period specified in the declaration.

(2) The Commissioner's power in paragraph (1)(d) may only be used to extend the time for compliance with subsection 26WL(2) to the end of a period that the Commissioner is satisfied is reasonable in the circumstances.

(3) The Commissioner must not make a declaration under subsection (1) unless the Commissioner is satisfied that it is reasonable in the circumstances to do so, having regard to the following:
  (a) the public interest;
  (b) any relevant advice given to the Commissioner by:
    (i) an enforcement body; or
    (ii) the Australian Signals Directorate of the Defence Department;
  (c) such other matters (if any) as the Commissioner considers relevant.

(4) Paragraph (3)(b) does not limit the advice to which the Commissioner may have regard.

(5) The Commissioner may give a notice of a declaration to an entity under subsection (1):
  (a) on the Commissioner's own initiative; or
  (b) on application made to the Commissioner by the entity.

Applications

(6) An application by an entity under paragraph (5)(b) may be expressed to be:

(a) an application for a paragraph (1)(c) declaration; or

(b) an application for a paragraph (1)(d) declaration; or

(c) an application for:

(i) a paragraph (1)(c) declaration; or

(ii) in the event that the Commissioner is not disposed to make such a declaration—a paragraph (1)(d) declaration.

(7) If an entity applies to the Commissioner under paragraph (5)(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.

(8) If:

(a) an application for a paragraph (1)(d) declaration nominates a period to be specified in the declaration; and

(b) the Commissioner makes the declaration, but specifies a different period in the declaration;

the Commissioner is taken not to have refused the application.

(9) If an entity applies to the Commissioner under paragraph (5)(b) for a declaration that, to any extent, relates to an eligible data breach of the entity, sections 26WK and 26WL do not apply in relation to:

(a) the eligible data breach; or

(b) if 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—such an eligible data breach of those other entities;

until the Commissioner makes a decision in response to the application for the declaration.

(10) An entity is not entitled to make an application under paragraph (5)(b) in relation to an eligible data breach of the entity if:

(a) 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; and

(b) one of those other entities has already made an application under paragraph (5)(b) in relation to the eligible data breach of the other entity.

Extension of specified period

(11) If notice of a paragraph (1)(d) declaration has been given to an entity, the Commissioner may, by written notice given to the entity, extend the period specified in the declaration.

Subdivision C—Commissioner may direct entity to notify eligible data breach

26WR Commissioner may direct entity to notify eligible data breach

(1) If the Commissioner is aware that there are reasonable grounds to believe that there has been an eligible 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 (4); and

(b) give a copy of the statement to the Commissioner.

(2) The direction must also require the entity to:

(a) 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—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals to whom the relevant information relates; or

(b) 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—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals who are at risk from the eligible data breach; or

(c) if neither paragraph (a) nor (b) applies:

(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.

Note: See also subsections 26WF(2) and (5), which deal with remedial action.

(3) Before giving a direction to an entity under subsection (1), the Commissioner must invite the entity to make a submission to the Commissioner in relation to the direction within the period specified in the invitation.

(4) 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 eligible data breach that the Commissioner 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 eligible data breach that the Commissioner has reasonable grounds to believe has happened.

(5) A direction under subsection (1) may also require the statement referred to in paragraph (1)(a) to set out specified information that relates to the eligible data breach that the Commissioner has reasonable grounds to believe has happened.

(6) In deciding whether to give a direction to an entity under subsection (1), the Commissioner must have regard to the following:
  (a) any relevant advice given to the Commissioner by:
    (i) an enforcement body; or
    (ii) the Australian Signals Directorate of the Defence Department;
  (b) any relevant submission that was made by the entity:
    (i) in response to an invitation under subsection (3); and
    (ii) within the period specified in the invitation;
  (c) such other matters (if any) as the Commissioner considers relevant.

(7) Paragraph (6)(a) does not limit the advice to which the Commissioner may have regard.

(8) If the Commissioner is aware that there are 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, a direction under subsection (1) may also require the statement referred to in paragraph (1)(a) to set out the identity and contact details of those other entities.

Method of providing a statement to an individual

(9) If an entity normally communicates with a particular individual using a particular method, the notification to the individual mentioned in paragraph (2)(a) or (b) may use that method. This subsection does not limit paragraph (2)(a) or (b).

Compliance with direction

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

26WS Exception—enforcement related activities

An entity is not required to comply with a direction under subsection 26WR(1) if:

(a) the entity is an enforcement body; and

(b) the chief executive officer of 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.

26WT Exception—inconsistency with secrecy provisions

Secrecy provisions

(1) For the purposes of this section, ***secrecy provision*** means a provision that:

(a) is a provision of a law of the Commonwealth (other than this Act); and

(b) prohibits or regulates the use or disclosure of information.

(2) If compliance by an entity with paragraph 26WR(1)(b) or subsection 26WR(2) in relation to a statement would, to any extent, be inconsistent with a secrecy provision (other than a prescribed secrecy provision), paragraph 26WR(1)(b) or subsection 26WR(2),

as the case may be, does not apply to the entity, in relation to the statement, to the extent of the inconsistency.

Prescribed secrecy provisions

(3) For the purposes of this section, ***prescribed secrecy provision*** means a secrecy provision that is specified in the regulations.

(4) For the purposes of a prescribed secrecy provision:
   (a) paragraph 26WR(1)(b); and
   (b) subsection 26WR(2);
are taken not to be provisions that require or authorise the use or disclosure of information.

(5) If compliance by an entity with paragraph 26WR(1)(b) or subsection 26WR(2) in relation to a statement would, to any extent, be inconsistent with a prescribed secrecy provision, paragraph 26WR(1)(b) or subsection 26WR(2), as the case may be, does not apply to the entity in relation to the statement.

4 After paragraph 96(1)(b)

Insert:

(ba) a decision under subsection 26WQ(7) to refuse an application for a declaration;

(bb) a decision to make a declaration under paragraph 26WQ(1)(d);

(bc) a decision under subsection 26WR(1) to give a direction;

5 After subsection 96(2)

Insert:

(2A) An application under paragraph (1)(ba) may only be made by:
   (a) the entity that made the application for a declaration; or
   (b) if another entity's compliance with subsection 26WL(2) is affected by the decision to refuse the application for a declaration—that other entity.

(2B) An application under paragraph (1)(bb) may only be made by:
   (a) the entity to whom notice of the declaration was given; or
   (b) if another entity's compliance with subsection 26WL(2) is affected by the declaration—that other entity.

(2C) An application under paragraph (1)(bc) may only be made by the entity to whom the direction was given.

(2D) For the purposes of subsections (2A), (2B) and (2C), ***entity*** has the same meaning as in Part IIIC.

6 Application of amendments—eligible data breaches

(1) Paragraph 26WE(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) Paragraph 26WE(2)(b) of the *Privacy Act 1988* (as amended by this Schedule) applies to a loss that happens after the commencement of this item.

[*Minister's second reading speech made in—*
House of Representatives on 19 October 2016
Senate on 8 February 2017]

(158/16)