2013-2014

The Parliament of the
Commonwealth of Australia

THE SENATE

Presented and read a first time

Privacy Amendment (Privacy Alerts) Bill 2014

No. , 2014

(Senator Singh)

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 (Privacy Alerts) Act 2014*.

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**
Provision(s)	**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 provision(s) do not commence within the period of 6 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Note: This table relates only to the provisions of this Act as originally enacted.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 Schedule(s)

Each Act that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.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 26X, 26Y, 26Z or 26ZA.

2 Subsection 6(1)

Insert:

significantly affected, in relation to an individual and in relation to a serious data breach, has the meaning given by section 26X, 26Y, 26Z or 26ZA.

3 After subsection 13(4)

Insert:

Data breach notification

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

4 After Part IIIB

Insert:

Part IIIC—Data breach notification

Division 1—Serious data breach

26X Serious data breach—APP entities

Unauthorised access or disclosure of personal information

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

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

(b) 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; and

(c) there is unauthorised access to, or unauthorised disclosure of, the personal information; and

(d) either:

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

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

then:

(e) the access or disclosure is a ***serious data breach*** of the APP entity in relation to the personal information; and

(f) if subparagraph (d)(i) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is an individual to whom the risk mentioned in that subparagraph relates; and

(g) if subparagraph (d)(ii) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is:

(i) an individual to whom the personal information relates; and

(ii) an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

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

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

Loss of personal information

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

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

(b) 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; and

(c) the personal information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the personal information may occur; and

(d) either:

(i) assuming that unauthorised access to, or unauthorised disclosure of, the personal 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 personal information relates; or

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

then:

(e) the loss is a ***serious data breach*** of the APP entity in relation to the personal information; and

(f) if subparagraph (d)(i) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is an individual to whom the risk mentioned in that subparagraph relates; and

(g) if subparagraph (d)(ii) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is:

(i) an individual to whom the personal information relates; and

(ii) an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

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

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

Overseas recipients

(3) 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.

26Y Serious data breach—credit reporting bodies

Unauthorised access or disclosure of credit reporting information

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

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

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

(c) there is unauthorised access to, or unauthorised disclosure of, the credit reporting information; and

(d) either:

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

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

then:

(e) the access or disclosure is a ***serious data breach*** of the credit reporting body in relation to the credit reporting information; and

(f) if subparagraph (d)(i) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is an individual to whom the risk mentioned in that subparagraph relates; and

(g) if subparagraph (d)(ii) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is:

(i) an individual to whom the credit reporting information relates; and

(ii) an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

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

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

Loss of credit reporting information

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

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

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

(c) the credit reporting information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the credit reporting information may occur; and

(d) either:

(i) assuming that unauthorised access to, or unauthorised disclosure of, the credit reporting 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 credit reporting information relates; or

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

then:

(e) the loss is a ***serious data breach*** of the credit reporting body in relation to the credit reporting information; and

(f) if subparagraph (d)(i) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is an individual to whom the risk mentioned in that subparagraph relates; and

(g) if subparagraph (d)(ii) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is:

(i) an individual to whom the credit reporting information relates; and

(ii) an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

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

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

26Z Serious data breach—credit providers

Unauthorised access or disclosure of credit eligibility information

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

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

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

(c) there is unauthorised access to, or unauthorised disclosure of, the credit eligibility information; and

(d) either:

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

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

then:

(e) the access or disclosure is a ***serious data breach*** of the credit provider in relation to the credit eligibility information; and

(f) if subparagraph (d)(i) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is an individual to whom the risk mentioned in that subparagraph relates; and

(g) if subparagraph (d)(ii) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is:

(i) an individual to whom the credit eligibility information relates; and

(ii) an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

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

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

Loss of credit eligibility information

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

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

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

(c) the credit eligibility information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the credit eligibility information may occur; and

(d) either:

(i) assuming that unauthorised access to, or unauthorised disclosure of, the credit eligibility 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 credit eligibility information relates; or

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

then:

(e) the loss is a ***serious data breach*** of the credit provider in relation to the credit eligibility information; and

(f) if subparagraph (d)(i) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is an individual to whom the risk mentioned in that subparagraph relates; and

(g) if subparagraph (d)(ii) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is:

(i) an individual to whom the credit eligibility information relates; and

(ii) an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

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

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

Bodies or persons with no Australian link

(3) 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.

26ZA Serious data breach—file number recipients

Unauthorised access or disclosure of tax file number information

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

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

(b) 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; and

(c) there is unauthorised access to, or unauthorised disclosure of, the tax file number information; and

(d) either:

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

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

then:

(e) the access or disclosure is a ***serious data breach*** of the file number recipient in relation to the tax file number information; and

(f) if subparagraph (d)(i) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is an individual to whom the risk mentioned in that subparagraph relates; and

(g) if subparagraph (d)(ii) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is:

(i) an individual to whom the tax file number information relates; and

(ii) an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

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

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

Loss of tax file number information

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

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

(b) 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; and

(c) the tax file number information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the tax file number information may occur; and

(d) either:

(i) assuming that unauthorised access to, or unauthorised disclosure of, the tax file number 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 tax file number information relates; or

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

then:

(e) the loss is a ***serious data breach*** of the file number recipient in relation to the tax file number information; and

(f) if subparagraph (d)(i) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the

individual is an individual to whom the risk mentioned in that subparagraph relates; and

(g) if subparagraph (d)(ii) applies—an individual is ***significantly affected*** by the serious data breach if, and only if, the individual is:

(i) an individual to whom the tax file number information relates; and

(ii) an individual who, under the regulations, is taken to be significantly affected by the serious data breach.

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

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

Division 2—Notifying serious data breaches

26ZB Entity must notify serious data breach

(1) If an entity believes on reasonable grounds that there has been a serious data breach of the entity in relation to:

(a) personal information; or

(b) credit reporting information; or

(c) credit eligibility information; or

(d) tax file number information;

the entity must, as soon as practicable after forming that belief:

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

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

(g) if the general publication conditions are not satisfied—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals significantly affected by the serious data breach that the entity believes has happened; and

(h) if the general publication conditions are satisfied:

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

(ii) cause a copy of the statement to be published in each State by being published in at least one newspaper circulating generally in that State.

Note: For ***general publication conditions***, see subsection (12).

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

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

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

(c) the kinds of information concerned; and

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

(e) such other information (if any) as specified in the regulations.

Method of providing the statement to an individual

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

Exception—enforcement related activities

(4) Paragraphs (1)(g) and (h) 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

(5) 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.

(6) The Commissioner must not give a notice under subsection (5) unless the Commissioner is satisfied that it is in the public interest to do so.

(7) The Commissioner may give a notice under subsection (5) to an entity:

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

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

(8) If:

(a) an entity applies to the Commissioner under paragraph (7)(b); and

(b) the Commissioner decides to refuse the application;

the Commissioner must give written notice of the refusal to the entity.

(9) If:

(a) an entity forms a belief about a serious data breach as mentioned in subsection (1); and

(b) as soon as practicable after forming that belief, the entity applies to the Commissioner for a notice under subsection (5) in relation to the serious data breach;

then:

(c) subsection (1) does not apply to the entity in relation to the serious data breach during the period:

(i) beginning when the entity formed the belief; and

(ii) ending when the Commissioner makes a decision in relation to the application for the notice; and

(d) if the Commissioner makes a decision to refuse to give the notice—subsection (1) has effect as if the entity had formed the belief when the Commissioner made the decision.

Exception—inconsistency with secrecy provisions

(10) If compliance by an entity with paragraph (1)(f), (g) or (h) 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—data breach notified under the Personally Controlled Electronic Health Records Act 2012

(11) Subsection (1) does not apply to a serious data breach if the breach has been notified under section 75 of the *Personally Controlled Electronic Health Records Act 2012*.

General publication conditions

(12) The regulations may declare that one or more specified conditions are ***general publication conditions*** for the purposes of this section.

26ZC 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 in relation to:

(a) personal information; or

(b) credit reporting information; or

(c) credit eligibility information; or

(d) tax file number information;

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

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

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

(g) if the general publication conditions are not satisfied—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of the individuals significantly affected by the serious data breach that the Commissioner believes has happened; and

(h) if the general publication conditions are satisfied:

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

(ii) cause a copy of the statement to be published in each State by being published in at least one newspaper circulating generally in that State.

Note: For ***general publication conditions***, see subsection (8).

(2) The statement referred to in paragraph (1)(e) 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 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; and

(e) such other information (if any) as specified in the regulations.

Method of providing the statement to an individual

(3) If the entity normally communicates with an individual using a particular method, the notification to the individual mentioned in

paragraph (1)(g) may use that method. This subsection does not limit paragraph (1)(g).

Compliance with direction

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

Exception—enforcement related activities

(5) 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

(6) If compliance by an entity with so much of a direction under subsection (1) as is covered by paragraph (1)(f), (g) or (h) 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)(f), (g) or (h), as the case may be, does not apply to the entity to the extent of the inconsistency.

Exception—data breach notified under the Personally Controlled Electronic Health Records Act 2012

(7) The Commissioner must not give a direction under subsection (1) in relation to a serious data breach if the breach has been notified under section 75 of the *Personally Controlled Electronic Health Records Act 2012*.

General publication conditions

(8) The regulations may declare that one or more specified conditions are ***general publication conditions*** for the purposes of this section.

Division 3—General

26ZD Entity

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

26ZE Harm

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

(a) harm to reputation; and

(b) economic harm; and

(c) financial harm.

26ZF Real risk

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

5 After paragraph 96(1)(b)

Insert:

(ba) a decision under section 26ZB to refuse to give a notice under subsection 26ZB(5);

(bb) a decision under subsection 26ZC(1) to give a direction;

6 Application of amendments—serious data breaches

(1) Paragraphs 26X(1)(c), 26Y(1)(c), 26Z(1)(c) and 26ZA(1)(c) of the *Privacy Act 1988* (as amended by this Schedule) apply to an access or disclosure that happens after the commencement of this item.

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