

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

1	Short title	1
2	Commencement	1
3	Schedule(s)	2
Schedule 1—Amendments		3
	<i>Privacy Act 1988</i>	3

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

3 The Parliament of Australia enacts:

4 **1 Short title**

5 This Act may be cited as the *Privacy Amendment (Privacy Alerts)*
6 *Act 2014*.

7 **2 Commencement**

8 (1) Each provision of this Act specified in column 1 of the table
9 commences, or is taken to have commenced, in accordance with
10 column 2 of the table. Any other statement in column 2 has effect
11 according to its terms.
12

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.	

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

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

7 **3 Schedule(s)**

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9 repealed as set out in the applicable items in the Schedule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

1 **Schedule 1—Amendments**
2

3 ***Privacy Act 1988***

4 **1 Subsection 6(1)**

5 Insert:

6 *serious data breach* has the meaning given by section 26X, 26Y,
7 26Z or 26ZA.

8 **2 Subsection 6(1)**

9 Insert:

10 *significantly affected*, in relation to an individual and in relation to
11 a serious data breach, has the meaning given by section 26X, 26Y,
12 26Z or 26ZA.

13 **3 After subsection 13(4)**

14 Insert:

15 *Data breach notification*

16 (4A) If an entity (within the meaning of Part IIIC) contravenes
17 section 26ZB or 26ZC, the contravention is taken to be an act that
18 is an *interference with the privacy of an individual*.

19 **4 After Part IIIB**

20 Insert:

21 **Part IIIC—Data breach notification**

22 **Division 1—Serious data breach**

23 **26X Serious data breach—APP entities**

24 *Unauthorised access or disclosure of personal information*

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

- 1 (a) an APP entity holds personal information relating to one or
2 more individuals; and
3 (b) the APP entity is required under section 15 not to do an act,
4 or engage in a practice, that breaches Australian Privacy
5 Principle 11.1 in relation to the personal information; and
6 (c) there is unauthorised access to, or unauthorised disclosure of,
7 the personal information; and
8 (d) either:
9 (i) the access or disclosure will result in a real risk of
10 serious harm to any of the individuals to whom the
11 personal information relates; or
12 (ii) any of the personal information is of a kind specified in
13 the regulations;
14 then:
15 (e) the access or disclosure is a *serious data breach* of the APP
16 entity in relation to the personal information; and
17 (f) if subparagraph (d)(i) applies—an individual is *significantly*
18 *affected* by the serious data breach if, and only if, the
19 individual is an individual to whom the risk mentioned in that
20 subparagraph relates; and
21 (g) if subparagraph (d)(ii) applies—an individual is *significantly*
22 *affected* by the serious data breach if, and only if, the
23 individual is:
24 (i) an individual to whom the personal information relates;
25 and
26 (ii) an individual who, under the regulations, is taken to be
27 significantly affected by the serious data breach.

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

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

30 *Loss of personal information*

- 31 (2) For the purposes of this Act, if:
32 (a) an APP entity holds personal information relating to one or
33 more individuals; and
34 (b) the APP entity is required under section 15 not to do an act,
35 or engage in a practice, that breaches Australian Privacy
36 Principle 11.1 in relation to the personal information; and

- 1 (c) the personal information is lost in circumstances where
- 2 unauthorised access to, or unauthorised disclosure of, the
- 3 personal information may occur; and
- 4 (d) either:
 - 5 (i) assuming that unauthorised access to, or unauthorised
 - 6 disclosure of, the personal information were to occur,
 - 7 the access or disclosure will result in a real risk of
 - 8 serious harm to any of the individuals to whom the
 - 9 personal information relates; or
 - 10 (ii) any of the personal information is of a kind specified in
 - 11 the regulations;
- 12 then:
 - 13 (e) the loss is a *serious data breach* of the APP entity in relation
 - 14 to the personal information; and
 - 15 (f) if subparagraph (d)(i) applies—an individual is *significantly*
 - 16 *affected* by the serious data breach if, and only if, the
 - 17 individual is an individual to whom the risk mentioned in that
 - 18 subparagraph relates; and
 - 19 (g) if subparagraph (d)(ii) applies—an individual is *significantly*
 - 20 *affected* by the serious data breach if, and only if, the
 - 21 individual is:
 - 22 (i) an individual to whom the personal information relates;
 - 23 and
 - 24 (ii) an individual who, under the regulations, is taken to be
 - 25 significantly affected by the serious data breach.

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

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

28 *Overseas recipients*

- 29 (3) If:
 - 30 (a) an APP entity has disclosed personal information about one
 - 31 or more individuals to an overseas recipient; and
 - 32 (b) Australian Privacy Principle 8.1 applied to the disclosure of
 - 33 the personal information; and
 - 34 (c) the overseas recipient holds the personal information;
 - 35 this section has effect as if:
 - 36 (d) the personal information were held by the APP entity; and

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

4 **26Y Serious data breach—credit reporting bodies**

5 *Unauthorised access or disclosure of credit reporting information*

- 6 (1) For the purposes of this Act, if:
7 (a) a credit reporting body holds credit reporting information
8 relating to one or more individuals; and
9 (b) the credit reporting body is required to comply with
10 section 20Q in relation to the credit reporting information;
11 and
12 (c) there is unauthorised access to, or unauthorised disclosure of,
13 the credit reporting information; and
14 (d) either:
15 (i) the access or disclosure will result in a real risk of
16 serious harm to any of the individuals to whom the
17 credit reporting information relates; or
18 (ii) any of the credit reporting information is of a kind
19 specified in the regulations;

20 then:

- 21 (e) the access or disclosure is a *serious data breach* of the credit
22 reporting body in relation to the credit reporting information;
23 and
24 (f) if subparagraph (d)(i) applies—an individual is *significantly*
25 *affected* by the serious data breach if, and only if, the
26 individual is an individual to whom the risk mentioned in that
27 subparagraph relates; and
28 (g) if subparagraph (d)(ii) applies—an individual is *significantly*
29 *affected* by the serious data breach if, and only if, the
30 individual is:
31 (i) an individual to whom the credit reporting information
32 relates; and
33 (ii) an individual who, under the regulations, is taken to be
34 significantly affected by the serious data breach.

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

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

Loss of credit reporting information

- 1
- 2 (2) For the purposes of this Act, if:
- 3 (a) a credit reporting body holds credit reporting information
- 4 relating to one or more individuals; and
- 5 (b) the credit reporting body is required to comply with
- 6 section 20Q in relation to the credit reporting information;
- 7 and
- 8 (c) the credit reporting information is lost in circumstances
- 9 where unauthorised access to, or unauthorised disclosure of,
- 10 the credit reporting information may occur; and
- 11 (d) either:
- 12 (i) assuming that unauthorised access to, or unauthorised
- 13 disclosure of, the credit reporting information were to
- 14 occur, the access or disclosure will result in a real risk
- 15 of serious harm to any of the individuals to whom the
- 16 credit reporting information relates; or
- 17 (ii) any of the credit reporting information is of a kind
- 18 specified in the regulations;
- 19 then:
- 20 (e) the loss is a ***serious data breach*** of the credit reporting body
- 21 in relation to the credit reporting information; and
- 22 (f) if subparagraph (d)(i) applies—an individual is ***significantly***
- 23 ***affected*** by the serious data breach if, and only if, the
- 24 individual is an individual to whom the risk mentioned in that
- 25 subparagraph relates; and
- 26 (g) if subparagraph (d)(ii) applies—an individual is ***significantly***
- 27 ***affected*** by the serious data breach if, and only if, the
- 28 individual is:
- 29 (i) an individual to whom the credit reporting information
- 30 relates; and
- 31 (ii) an individual who, under the regulations, is taken to be
- 32 significantly affected by the serious data breach.

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

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

1 **26Z Serious data breach—credit providers**

2 *Unauthorised access or disclosure of credit eligibility information*

- 3 (1) For the purposes of this Act, if:
- 4 (a) a credit provider holds credit eligibility information relating
- 5 to one or more individuals; and
- 6 (b) the credit provider is required to comply with
- 7 subsection 21S(1) in relation to the credit eligibility
- 8 information; and
- 9 (c) there is unauthorised access to, or unauthorised disclosure of,
- 10 the credit eligibility information; and
- 11 (d) either:
- 12 (i) the access or disclosure will result in a real risk of
- 13 serious harm to any of the individuals to whom the
- 14 credit eligibility information relates; or
- 15 (ii) any of the credit eligibility information is of a kind
- 16 specified in the regulations;
- 17 then:
- 18 (e) the access or disclosure is a **serious data breach** of the credit
- 19 provider in relation to the credit eligibility information; and
- 20 (f) if subparagraph (d)(i) applies—an individual is **significantly**
- 21 **affected** by the serious data breach if, and only if, the
- 22 individual is an individual to whom the risk mentioned in that
- 23 subparagraph relates; and
- 24 (g) if subparagraph (d)(ii) applies—an individual is **significantly**
- 25 **affected** by the serious data breach if, and only if, the
- 26 individual is:
- 27 (i) an individual to whom the credit eligibility information
- 28 relates; and
- 29 (ii) an individual who, under the regulations, is taken to be
- 30 significantly affected by the serious data breach.

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

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

33 *Loss of credit eligibility information*

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

- 1 (a) a credit provider holds credit eligibility information relating
- 2 to one or more individuals; and
- 3 (b) the credit provider is required to comply with
- 4 subsection 21S(1) in relation to the credit eligibility
- 5 information; and
- 6 (c) the credit eligibility information is lost in circumstances
- 7 where unauthorised access to, or unauthorised disclosure of,
- 8 the credit eligibility information may occur; and
- 9 (d) either:
 - 10 (i) assuming that unauthorised access to, or unauthorised
 - 11 disclosure of, the credit eligibility information were to
 - 12 occur, the access or disclosure will result in a real risk
 - 13 of serious harm to any of the individuals to whom the
 - 14 credit eligibility information relates; or
 - 15 (ii) any of the credit eligibility information is of a kind
 - 16 specified in the regulations;
- 17 then:
 - 18 (e) the loss is a *serious data breach* of the credit provider in
 - 19 relation to the credit eligibility information; and
 - 20 (f) if subparagraph (d)(i) applies—an individual is *significantly*
 - 21 *affected* by the serious data breach if, and only if, the
 - 22 individual is an individual to whom the risk mentioned in that
 - 23 subparagraph relates; and
 - 24 (g) if subparagraph (d)(ii) applies—an individual is *significantly*
 - 25 *affected* by the serious data breach if, and only if, the
 - 26 individual is:
 - 27 (i) an individual to whom the credit eligibility information
 - 28 relates; and
 - 29 (ii) an individual who, under the regulations, is taken to be
 - 30 significantly affected by the serious data breach.

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

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

33 *Bodies or persons with no Australian link*

- 34 (3) If:
 - 35 (a) either:
 - 36 (i) a credit provider has disclosed, under
 - 37 paragraph 21G(3)(b) or (c), credit eligibility information

- 1 about one or more individuals to a related body
2 corporate, or person, that does not have an Australian
3 link; or
4 (ii) a credit provider has disclosed, under
5 subsection 21M(1), credit eligibility information about
6 one or more individuals to a body or person that does
7 not have an Australian link; and
8 (b) the related body corporate, body or person holds the credit
9 eligibility information;

10 this section has effect as if:

- 11 (c) the credit eligibility information were held by the credit
12 provider; and
13 (d) the credit provider were required to comply with
14 subsection 21S(1) in relation to the credit eligibility
15 information.

16 Note: See section 21NA.

17 **26ZA Serious data breach—file number recipients**

18 *Unauthorised access or disclosure of tax file number information*

- 19 (1) For the purposes of this Act, if:
20 (a) a file number recipient holds tax file number information
21 relating to one or more individuals; and
22 (b) the file number recipient is required under section 18 not to
23 do an act, or engage in a practice, that breaches a section 17
24 rule that relates to the tax file number information; and
25 (c) there is unauthorised access to, or unauthorised disclosure of,
26 the tax file number information; and
27 (d) either:
28 (i) the access or disclosure will result in a real risk of
29 serious harm to any of the individuals to whom the tax
30 file number information relates; or
31 (ii) any of the tax file number information is of a kind
32 specified in the regulations;

33 then:

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

- 1 (f) if subparagraph (d)(i) applies—an individual is *significantly*
2 *affected* by the serious data breach if, and only if, the
3 individual is an individual to whom the risk mentioned in that
4 subparagraph relates; and
- 5 (g) if subparagraph (d)(ii) applies—an individual is *significantly*
6 *affected* by the serious data breach if, and only if, the
7 individual is:
- 8 (i) an individual to whom the tax file number information
9 relates; and
- 10 (ii) an individual who, under the regulations, is taken to be
11 significantly affected by the serious data breach.

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

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

14 *Loss of tax file number information*

- 15 (2) For the purposes of this Act, if:
- 16 (a) a file number recipient holds tax file number information
17 relating to one or more individuals; and
- 18 (b) the file number recipient is required under section 18 not to
19 do an act, or engage in a practice, that breaches a section 17
20 rule that relates to the tax file number information; and
- 21 (c) the tax file number information is lost in circumstances
22 where unauthorised access to, or unauthorised disclosure of,
23 the tax file number information may occur; and
- 24 (d) either:
- 25 (i) assuming that unauthorised access to, or unauthorised
26 disclosure of, the tax file number information were to
27 occur, the access or disclosure will result in a real risk
28 of serious harm to any of the individuals to whom the
29 tax file number information relates; or
- 30 (ii) any of the tax file number information is of a kind
31 specified in the regulations;
- 32 then:
- 33 (e) the loss is a *serious data breach* of the file number recipient
34 in relation to the tax file number information; and
- 35 (f) if subparagraph (d)(i) applies—an individual is *significantly*
36 *affected* by the serious data breach if, and only if, the

- 1 individual is an individual to whom the risk mentioned in that
2 subparagraph relates; and
3 (g) if subparagraph (d)(ii) applies—an individual is *significantly*
4 *affected* by the serious data breach if, and only if, the
5 individual is:
6 (i) an individual to whom the tax file number information
7 relates; and
8 (ii) an individual who, under the regulations, is taken to be
9 significantly affected by the serious data breach.

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

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

12 **Division 2—Notifying serious data breaches**

13 **26ZB Entity must notify serious data breach**

- 14 (1) If an entity believes on reasonable grounds that there has been a
15 serious data breach of the entity in relation to:
16 (a) personal information; or
17 (b) credit reporting information; or
18 (c) credit eligibility information; or
19 (d) tax file number information;
20 the entity must, as soon as practicable after forming that belief:
21 (e) prepare a statement that complies with subsection (2); and
22 (f) give a copy of the statement to the Commissioner; and
23 (g) if the general publication conditions are not satisfied—take
24 such steps as are reasonable in the circumstances to notify the
25 contents of the statement to each of the individuals
26 significantly affected by the serious data breach that the
27 entity believes has happened; and
28 (h) if the general publication conditions are satisfied:
29 (i) publish a copy of the statement on the entity’s website
30 (if any); and
31 (ii) cause a copy of the statement to be published in each
32 State by being published in at least one newspaper
33 circulating generally in that State.

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

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

-
- 1 (a) the identity and contact details of the entity; and
2 (b) a description of the serious data breach that the entity
3 believes has happened; and
4 (c) the kinds of information concerned; and
5 (d) recommendations about the steps that individuals should take
6 in response to the serious data breach that the entity believes
7 has happened; and
8 (e) such other information (if any) as specified in the regulations.

9 *Method of providing the statement to an individual*

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

14 *Exception—enforcement related activities*

- 15 (4) Paragraphs (1)(g) and (h) do not apply if:
16 (a) the entity is an enforcement body; and
17 (b) the enforcement body believes on reasonable grounds that
18 compliance with those paragraphs would be likely to
19 prejudice one or more enforcement related activities
20 conducted by, or on behalf of, the enforcement body.

21 *Exception—Commissioner’s notice*

- 22 (5) The Commissioner may, by written notice given to an entity,
23 exempt the entity from subsection (1) in such circumstances as are
24 specified in the notice.
- 25 (6) The Commissioner must not give a notice under subsection (5)
26 unless the Commissioner is satisfied that it is in the public interest
27 to do so.
- 28 (7) The Commissioner may give a notice under subsection (5) to an
29 entity:
30 (a) on the Commissioner’s own initiative; or
31 (b) on application made to the Commissioner by the entity.
- 32 (8) If:

- 1 (a) an entity applies to the Commissioner under
2 paragraph (7)(b); and
3 (b) the Commissioner decides to refuse the application;
4 the Commissioner must give written notice of the refusal to the
5 entity.
- 6 (9) If:
7 (a) an entity forms a belief about a serious data breach as
8 mentioned in subsection (1); and
9 (b) as soon as practicable after forming that belief, the entity
10 applies to the Commissioner for a notice under subsection (5)
11 in relation to the serious data breach;
12 then:
13 (c) subsection (1) does not apply to the entity in relation to the
14 serious data breach during the period:
15 (i) beginning when the entity formed the belief; and
16 (ii) ending when the Commissioner makes a decision in
17 relation to the application for the notice; and
18 (d) if the Commissioner makes a decision to refuse to give the
19 notice—subsection (1) has effect as if the entity had formed
20 the belief when the Commissioner made the decision.

21 *Exception—inconsistency with secrecy provisions*

- 22 (10) If compliance by an entity with paragraph (1)(f), (g) or (h) would,
23 to any extent, be inconsistent with a provision of a law of the
24 Commonwealth (other than a provision of this Act) that prohibits
25 or regulates the use or disclosure of information, subsection (1)
26 does not apply to the entity to the extent of the inconsistency.

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

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

32 *General publication conditions*

- 33 (12) The regulations may declare that one or more specified conditions
34 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

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

3 *Compliance with direction*

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

6 *Exception—enforcement related activities*

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

- 9 (a) the entity is an enforcement body; and
- 10 (b) the chief executive officer of the enforcement body has given
11 the Commissioner a certificate stating that the enforcement
12 body believes on reasonable grounds that compliance with
13 the direction would be likely to prejudice one or more
14 enforcement related activities conducted by, or on behalf of,
15 the enforcement body.

16 *Exception—inconsistency with secrecy provisions*

17 (6) If compliance by an entity with so much of a direction under
18 subsection (1) as is covered by paragraph (1)(f), (g) or (h) would,
19 to any extent, be inconsistent with a provision of a law of the
20 Commonwealth (other than a provision of this Act) that prohibits
21 or regulates the use or disclosure of information, paragraph (1)(f),
22 (g) or (h), as the case may be, does not apply to the entity to the
23 extent of the inconsistency.

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

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

30 *General publication conditions*

31 (8) The regulations may declare that one or more specified conditions
32 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.