2025-2026

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

EXPOSURE DRAFT

Privacy Amendment (Personal Data Protection) Bill 2026

No. , 2026

(Attorney-General)

A Bill for an Act to amend legislation relating to privacy, and for related purposes

Contents

EXPOSURE DRAFT

A Bill for an Act to amend legislation relating to privacy, and for related purposes

The Parliament of Australia enacts:

1 Short title

This Act is the *Privacy Amendment (Personal Data Protection) Act 2026*.

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.		
2.		
3.		
4.		

Note: This table relates only to the provisions of this Act as originally enacted.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Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.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

Privacy Act 1988

1 Subsection 6(1) (definition of *collects*)

Repeal the definition, substitute:

collects has the meaning given by section 6AAA.

2 Subsection 6(1) (definition of *consent*)

Repeal the definition, substitute:

consent has a meaning affected by section 6AAB.

3 Subsection 6(1) (definition of *de-identified*)

Repeal the definition, substitute:

de-identified has the meaning given by section 6FG.

4 Subsection 6(1)

Insert:

discloses: an entity ***discloses*** personal information if the entity makes the personal information accessible to another person or body.

5 Subsection 6(1) (definition of *personal information*)

Repeal the definition, substitute:

personal information has the meaning given by section 6FD.

6 Subsection 6(1)

Insert:

precise geolocation tracking data means personal information that:

(a) is generated by or derived from a device or other technology; and

(b) identifies an individual's location within a radius of 500 metres; and

(c) is collected and held by reference to the individual's location over time (whether location is identified at points in time, by reference to an aggregation of information or in any other way).

7 Subsection 6(1)

Insert:

reasonably identifiable has a meaning affected by section 6FF.

8 Subsection 6(1) (definition of *sensitive information*)

Repeal the definition, substitute:

sensitive information has the meaning given by section 6FE.

9 After section 6

Insert:

6AAA Meaning of *collects*

Meaning of collects

(1) An entity ***collects*** personal information only if the entity collects the personal information for inclusion in a record or generally available publication (regardless of the source from which or means by which the information is collected).

Note: Examples of sources from which an entity might collect information include the individual to whom the information relates, another person or a website. Examples of means by which an entity might collect information include generating the information itself using its own processes, systems, observations or measurements, or deriving it from other information.

Collection time for sensitive information that can be derived from personal information

(2) An entity is not taken to collect sensitive information only because the entity collects personal information from which the sensitive information can be derived.

(3) However, if an entity collects personal information from which sensitive information can be derived, the entity is taken to collect the sensitive information:

(a) if the entity collects the personal information for a purpose that involves using or disclosing the sensitive information—at the time the entity collects the personal information; or

(b) otherwise—at the earlier of:

(i) the time the entity uses or discloses the sensitive information; or

(ii) the time the entity derives the sensitive information for inclusion in a record or generally available publication.

(4) To avoid doubt, references in paragraphs (3)(a) and (b) to use and disclosure of sensitive information include references to use and disclosure of personal information from which sensitive information can be derived, if the circumstances indicate that the personal information is being used or disclosed as sensitive information.

10 Before section 6AA

Insert:

6AAB What constitutes consent

(1) For the purposes of this Act, an individual's consent may be express or implied, but must be all of the following:

(a) voluntary;

(b) informed;

(c) current;

(d) specific;

(e) unambiguous.

(2) However, paragraphs (1)(c) and (d) do not apply in relation to an act done in the course of human research that is reviewed, approved and monitored in accordance with the applicable national statement on ethical conduct in human research.

11 Paragraph 6FA(d)

Omit "genetic information about", substitute "genetic or genomic information that relates to".

12 After Division 1 of Part II

Insert:

Division 1A—Key definitions relating to personal information

6FD Meaning of *personal information*

Personal information means information or an opinion that relates to an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

Note 1: An individual can be identified, or reasonably identifiable, even if the individual's name or legal identity is not known. This can be the case if, for example, information allows an individual to be recognised, singled out, or otherwise dealt with as a distinct individual in practice. This could be information such as the following:

(a) a name, date of birth or address;

(b) contact information (such as a phone number or email address);

(c) a pseudonym or identifier;

(d) location data or geolocation data;

(e) characteristics, behaviours, traits, preferences or patterns of activity.

Note 2: Section 187LA of the *Telecommunications (Interception and Access) Act 1979* extends the meaning of personal information to cover information kept under Part 5-1A of that Act.

6FF When an individual is *reasonably identifiable*

An individual is ***reasonably identifiable*** from information or an opinion if the individual could be identified by combining the information or opinion with other information or opinions that are reasonably available.

6FE Meaning of sensitive information

The following information is ***sensitive information***:

(a) information or an opinion about an individual's:
  (i) racial or ethnic origin; or
  (ii) political opinions; or
  (iii) membership of a political association; or
  (iv) religious beliefs or affiliations; or
  (v) philosophical beliefs; or
  (vi) membership of a professional or trade association; or
  (vii) membership of a trade union; or
  (viii) sexual orientation or practices; or
  (ix) criminal record;
  that is also personal information;

(b) health information;

(c) genetic or genomic information that relates to an individual that is not otherwise health information;

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification;

(e) biometric templates;

(f) precise geolocation tracking data.

6FG Meaning of *de-identified*

Information or an opinion is ***de-identified*** at a particular time, or in particular circumstances, if, at that time or in those circumstances, the information or opinion has ceased to be information or an opinion that relates to an identifiable individual or an individual who is reasonably identifiable.

13 Application and transitional provisions

(1) The amendments made by this Schedule to the definition of ***collects*** in the *Privacy Act 1988* apply in relation to collections made on or after the commencement of this item.

(2) The amendments made by this Schedule to the definitions of ***de-identified***, ***health information***, ***personal information*** and ***sensitive information*** in the *Privacy Act 1988* apply, on and after the

commencement of this item, in relation to information held by an entity on or after that commencement, whether the information was acquired or created before, on or after that commencement.

Schedule 2—Handling personal information

Part 1—Fair and reasonable handling of personal information, consent and notice requirements

Privacy Act 1988

1 Subsection 6(1)

Insert:

publicly available document:

(a) means any document that is publicly available; and

(b) includes a document that is publicly available subject to a barrier to access (for example, a requirement to pay a fee, register or create an account), as long as the barrier can be overcome by any ordinary member of the public.

trade, in relation to personal information, has the meaning given by section 6FC.

2 Subsection 6D(4)

After "or trust", insert "(the ***body***)".

3 Subsection 6D(4)

Omit "he, she or it" (wherever occurring), substitute "the body".

4 Paragraph 6D(4)(b)

Omit "another individual", substitute "an individual (other than the body)".

5 Paragraphs 6D(4)(c) and (d)

Repeal the paragraphs, substitute:

(c) trades personal information that relates to an individual (other than the body); or

(d) collects personal information that relates to an individual (other than the body) from a third party, in circumstances

where the third party's disclosure of the information to the body is a trade of the information; or

6 Subsection 6D(8)

Repeal the subsection, substitute:

Collection with consent or under legislation

(8) Paragraph (4)(d) does not prevent the body referred to in that paragraph from being a small business operator only because the disclosure, to the body, of personal information that relates to an individual (other than the body) is a trade of the information by the discloser of the information, if the body collects the information:

(a) with the consent of the other individual; or

(b) as required or authorised by or under legislation.

7 At the end of Division 1 of Part II

Add:

6FC Meaning of *trade*

(1) A disclosure of personal information by an organisation is a ***trade*** of that information if the organisation discloses the information:

(a) for money or other consideration; or

(b) for the purposes of direct marketing.

(2) Despite subsection (1), a disclosure of personal information by an organisation is not a ***trade*** of that information if:

(a) the disclosure is for the purposes of the recipient of the information providing the individual to whom the information relates with a product or service that the individual requested from the recipient; or

(b) both:

(i) the disclosure is incidental to a transaction, or group of related transactions, in which a person or body takes over the business or part of the business of the organisation; and

(ii) the disclosure of the information for money or other consideration is not a substantial purpose of that transaction or group of related transactions; or

Note: A transaction, or group of related transactions, in which a person or body takes over the business or part of the business of an organisation could include a merger or acquisition.

(c) the disclosure is made to a processor by a controller for the purpose of the processor doing an act, or engaging in a practice, on behalf of the controller in relation to the information.

(3) Despite subsection (1), a disclosure of personal information by an organisation is not a ***trade*** of that information if:

(a) either:

(i) the functions or activities of the recipient of the information include enabling or facilitating the disclosure of information for the prevention, detection, investigation or remedying of unlawful activity, or wrongdoing of a serious nature, involving fraud; or

(ii) the recipient of the information suspects that unlawful activity, or wrongdoing of a serious nature, involving fraud, that relates to the recipient's functions or activities, has been, is being or may be engaged in (whether engaged in by a person owing a duty to the recipient or any other person); and

(b) the organisation reasonably believes that the disclosure is necessary for the prevention, detection, investigation or remedying of the unlawful activity or wrongdoing.

8 After subsection 13(3)

Insert:

Health information collected for research etc.

(3A) An act or practice is an ***interference with the privacy of an individual*** if the act or practice contravenes subsection 16B(2A).

Note: Subsection 16B(2A) requires an organisation to take reasonable steps to de-identify health information before disclosing it, if the organisation collected the health information in the permitted health situation described in subsection 16B(2) (research etc.).

9 After subsection 16B(2)

Insert:

(2A) If an organisation collects health information that relates to an individual in the situation described in subsection (2), the organisation must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the organisation discloses it.

10 Part 2 of Schedule 1

Repeal the Part, substitute:

Part 2—Handling of personal information

3 Australian Privacy Principle 3—fair, reasonable and lawful collection, use and disclosure of personal information

3.1 An APP entity must not collect personal information, or use or disclose personal information held by the APP entity, unless the collection, use or disclosure of the information is:

(a) fair and reasonable in the circumstances; and

(b) lawful.

Note: For exceptions, see subclauses 3.3 (for paragraph 3.1(a) only) and subclause 3.4 (for both paragraphs 3.1(a) and (b)).

Fair and reasonable in the circumstances

3.2 An APP entity must have regard to the following matters in determining whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances:

(a) whether a reasonable person would expect the collection, use or disclosure of the information in the circumstances;

(b) whether the collection, use or disclosure of the information relates to one or more of the APP entity's functions or activities;

(c) whether the APP entity is transparent about the means and the purposes of the collection, use or disclosure of the information;

(d) whether the purpose for which the information is being collected, used or disclosed could be met by collecting, using or disclosing less information, or information that is not personal information;

(e) whether the individual to whom the information relates is provided with genuine choice in relation to the collection, use or disclosure of the information;

(f) the impact on the privacy of the individual to whom the information relates, and any risk of harm to the individual, arising from the collection, use or disclosure of the information (including whether that impact or risk of harm is proportionate having regard to any benefits to the individual or the APP entity arising from the collection, use or disclosure);

(g) if the individual to whom the information relates is a child, the best interests of the child as a primary consideration.

Exceptions to fair and reasonable requirement

3.3 Paragraph 3.1(a) does not apply to a collection, use or disclosure of personal information by an APP entity if:

(a) the collection, use or disclosure is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection, use or disclosure; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection, use or disclosure.

Note 1: For ***permitted general situation***, see section 16A. For ***permitted health situation***, see section 16B.

Note 2: The exceptions in this subclause are also exceptions to the requirement for consent to collection of sensitive information in subclause 4.1 (see paragraph 4.2(a)) and the requirement for consent to trading in personal information in subclause 4.2 (see paragraph 4.6(a)).

Exception for government related identifiers

3.4 Subclause 3.1 does not apply to the use or disclosure by an organisation of government related identifiers.

4 Australian Privacy Principle 4—consent to collection of sensitive information or trading of personal information

4.1 An APP entity must not collect sensitive information that relates to an individual unless the individual has consented to the collection of the information.

Note: For exceptions, see subclause 4.3.

4.2 An organisation that holds personal information that relates to an individual must not trade the information unless the individual has consented to the trading of the information.

Note: For exceptions, see subclause 4.6.

Exceptions to consent for collection of sensitive information

4.3 Subclause 4.1 does not apply to the collection of sensitive information by an APP entity if:

(a) one or more of the following applies:

(i) the collection is required or authorised by or under an Australian law or a court/tribunal order;

(ii) a permitted general situation exists in relation to the collection;

(iii) the APP entity is an organisation and a permitted health situation exists in relation to the collection; or

Note 1: For ***permitted general situation***, see section 16A. For ***permitted health situation***, see section 16B.

Note 2: The exceptions in this paragraph are also exceptions to the fair and reasonable requirement in Australian Privacy Principle 3 (see subclause 3.3) and to the requirement for consent to trading in personal information in subclause 4.2 (see paragraph 4.6(a)).

(b) the information is collected from a publicly available document; or

(c) all of the following apply:

(i) the APP entity is a non-profit organisation;

(ii) the information relates to the activities of the entity;

(iii) the information relates solely to the members of the entity, or to other individuals who have regular contact with the entity in relation to its activities; or

(d) collecting the information is strictly necessary within the meaning of subclause 4.4.

4.4 A collection of sensitive information that relates to an individual by an APP entity is strictly necessary within the meaning of this subclause if:

(a) collecting the information is strictly necessary in order for the APP entity to provide or deliver goods or services that the individual has requested the APP entity to provide the individual; and

(b) if the individual is a child—the provision of those goods or services is necessary:

(i) to protect the child from neglect or physical, mental or emotional harm; or

(ii) to protect the child's physical, mental or emotional well-being.

4.5 A collection of sensitive information for the purposes of direct marketing is never strictly necessary within the meaning of subclause 4.4 (regardless of whether an individual has requested the provision of direct marketing).

Exceptions to consent for trading of personal information

4.6 Subclause 4.2 does not apply to the trading of personal information by an organisation if:

(a) one or more of the following applies:

(i) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order;

(ii) a permitted general situation exists in relation to the disclosure of the information;

(iii) the APP entity is an organisation and a permitted health situation exists in relation to the disclosure of the information; or

Note 1: For ***permitted general situation***, see section 16A. For ***permitted health situation***, see section 16B.

Note 2: These exceptions are also exceptions to the fair and reasonable requirement in Australian Privacy Principle 3 (see subclause 3.3)

and to the requirement for consent to collection of sensitive information in subclause 4.1 (see paragraph 4.2(a)).

(b) the disclosure is of a government related identifier.

5 Australian Privacy Principle 5—notification of the collection of personal information

5.1 If an APP entity collects personal information that relates to an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of:

(i) the fact of, and circumstances of, the collection; and

(ii) the purposes for which the entity intends to use or disclose the information; or

(b) to otherwise ensure that the individual is aware of those matters.

5.2 The APP entity must take those steps at or before the time the entity collects the information, or, if that is not practicable, as soon as practicable after.

5.3 Notification for the purposes of paragraph 5.1(a) must be:

(a) in clear and plain language; and

(b) readily understandable by the individual; and

(c) up-to-date; and

(d) concise.

11 Clause 6 of Schedule 1

Repeal the clause.

12 Part 3 of Schedule 1 (heading)

Repeal the heading.

13 Application of amendments

The amendments made by this Part apply in relation to the collection, use, disclosure or holding of information on or after the commencement of this item, whether the information was acquired or created before, on or after that commencement.

Part 2—Permitted general situations

Privacy Act 1988

14 Subparagraph 13K(1)(b)(iv)

Repeal the subparagraph.

15 After subsection 13K(1)

Insert:

Civil penalty provision for not complying with subsection 16A(3)

(1A) An entity contravenes this subsection if:

(a) the entity uses or discloses personal information in the situation set out in item 10 of the table in subsection 16A(1); and

(b) the entity does not comply with subsection 16A(3) in relation to the use or disclosure.

Note: Item 10 of the table in subsection 16A(1) sets out a permitted general situation for an APP entity to use or disclose personal information as reasonably necessary for enforcement related activities of an enforcement body. Subsection 16A(3) requires the entity to make a written note of the use or disclosure.

16 Subsections 13K(3) and (4)

After "(1)", insert ", (1A)".

17 Subsection 16A(1)

Repeal the subsection, substitute:

(1) A ***permitted general situation*** exists in relation to the collection, use or disclosure by an APP entity of personal information that relates to an individual, or of a government related identifier of an individual, if:

(a) the entity is the kind specified in an item in column 1 of the table; and

(b) the item applies to collection, use or disclosure of the information or identifier in accordance with that item in column 2; and

(c) the conditions specified in that item in column 3 are met.

Permitted general situations

Item	Column 1 Kind of entity	Column 2 Item applies to	Column 3 Condition(s)
1	APP entity	Collection, use or disclosure of: (a) personal information; or (b) a government related identifier.	(a) for sensitive information—it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure; and (b) in any case—the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
2	APP entity	Collection, use or disclosure of: (a) personal information; or (b) a government related identifier.	(a) the entity has reason to suspect that unlawful activity, or wrongdoing of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in (whether engaged in by a person owing a duty to the entity or any other person); and (b) the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.
3	APP entity	Collection, use or disclosure of personal information	(a) the entity reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing; and

Permitted general situations			
Item	**Column 1** **Kind of entity**	**Column 2** **Item applies to**	**Column 3** **Condition(s)**
			(b) the collection, use or disclosure complies with the rules made under subsection (2).
4	APP entity	Collection, use or disclosure of personal information (other than a government related identifier)	(a) for a disclosure—the recipient of the information is not an overseas recipient; and (b) in any case—the collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.
5	APP entity	Collection, use or disclosure of personal information (other than a government related identifier)	(a) for a disclosure—the recipient of the information is not an overseas recipient; and (b) in any case—the collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.
6	Agency	Collection, use or disclosure of personal information	The entity reasonably believes that the collection, use or disclosure is necessary for the entity's diplomatic or consular functions or activities.
7	Defence Force	Collection, use or disclosure of personal information	The entity reasonably believes that the collection, use or disclosure is necessary for any of the following occurring outside Australia and the external Territories: (a) war or warlike operations; (b) peacekeeping or peace enforcement; (c) civil aid, humanitarian assistance, medical or civil emergency or disaster relief.
8	Immigration Department	Collection of personal	The entity reasonably believes that the collection is reasonably

Permitted general situations			
Item	**Column 1** **Kind of entity**	**Column 2** **Item applies to**	**Column 3** **Condition(s)**
		information	necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity.
9	Enforcement body (other than the Immigration Department)	Collection of personal information	The entity reasonably believes that the collection is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.
10	APP entity	Use or disclosure of personal information	(a) the recipient of the information is not an overseas recipient; and (b) the entity reasonably believes that the use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.
11	Agency (other than an enforcement body)	Disclosure of biometric information or biometric templates	(a) the recipient of the information is not an overseas recipient; and (b) the recipient of the information is an enforcement body; and (c) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.
12	Agency	Disclosure of personal information	(a) the recipient of the information is an overseas recipient; and (b) the disclosure is required or authorised by or under an international agreement relating to information sharing to which Australia is a party.
13	Agency	Disclosure of personal information	(a) the recipient of the information is an overseas recipient; and (b) the recipient is a body that performs functions, or exercises powers, that are similar to those

Permitted general situations			
Item	**Column 1** **Kind of entity**	**Column 2** **Item applies to**	**Column 3** **Condition(s)**
			performed or exercised by an enforcement body; and (c) the entity reasonably believes that the disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: The Commissioner's power to make guidelines for the purposes of paragraph (c) of table item 11 is set out in paragraph 28(1)(b).

18 At the end of section 16A

Add:

(3) If an APP entity uses or discloses personal information in the situation set out in item 10 of the table in subsection (1), the entity must make a written note of the use or disclosure.

Note: An APP entity may be liable to a civil penalty if it does not comply with this requirement (see subsection 13K(1A)).

19 Paragraph 28(1)(b)

Omit "paragraph (d) of Australian Privacy Principle 6.3", substitute "paragraph (c) of column 3 of item 11 of the table in subsection 16A(1)".

20 Paragraph 8.2(d) of Schedule 1

Omit "(other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or", substitute "exists in relation to the disclosure of the information by the APP entity."

21 Paragraphs 8.2(e) and (f) of Schedule 1

Repeal the paragraphs.

22 Paragraph 9.2(d) of Schedule 1

Omit "other than the situation referred to in item 4 or 5 of the table in subsection 16A(1))".

23 Paragraph 9.2(e) of Schedule 1

Repeal the paragraph.

24 Subparagraph 12.3(h)(i) of Schedule 1

Omit "misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in", substitute "wrongdoing of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in (whether engaged in by a person owing a duty to the entity or any other person)".

Part 3—Direct marketing

Privacy Act 1988

25 Subsection 6(1)

Insert:

ad-supported service has the meaning given by subclause 7.6 of Schedule 1.

direct marketing means the communication, by any means, of advertising or marketing material to an individual, if:

(a) the individual is selected, identified or otherwise targeted (whether as an individual or as a member of a class) for receipt of the material; and

(b) the selecting, identification or other targeting is done using personal information that relates to the individual.

26 Subparagraphs 13K(1)(b)(v), (vi) and (vii)

Repeal the subparagraphs, substitute:

(v) Australian Privacy Principle 7.3;

27 Clause 7 of Schedule 1

Repeal the clause, substitute:

7 Australian Privacy Principle 7—direct marketing

7.1 An organisation must not make a direct marketing communication to an individual unless the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation.

7.2 If an individual makes a request not to receive direct marketing communications from an organisation, the organisation must take such steps as are reasonable in the circumstances to give effect to the request.

7.3 If an organisation makes a direct marketing communication to an individual, the communication must be accompanied by

information that sets out how the individual may request not to receive direct marketing communications from the organisation.

7.4 The information mentioned in subclause 7.3 must be:

(a) set out in clear and plain language; and

(b) readily understandable by an ordinary person; and

(c) up-to-date; and

(d) concise.

7.5 If:

(a) an organisation provides an ad-supported service to an individual; and

(b) the individual has requested not to receive direct marketing communications from the organisation;

the organisation may offer the service, or an element of the service, to the individual on terms that differ from the terms on which the service or element is offered to individuals who receive direct marketing, as long as the different terms provide the individual with a genuine choice to continue to use the service without receiving direct marketing communications.

7.6 A service provided by an organisation is an ***ad-supported service*** if the making of direct marketing communications to individuals who use the service is itself a source of revenue for the organisation. For this purpose, have regard only to revenue from the actual making of communications (disregard any revenue from sales of the goods or services marketed by the communications).

7.7 This principle does not apply to the extent that any of the following apply:

(a) Division 5 of Part 7B of the *Interactive Gambling Act 2001*;

(b) the *Do Not Call Register Act 2006*;

(c) the *Spam Act 2003*;

(d) any other Act of the Commonwealth, or a law in force in an external Territory, prescribed by the regulations.

28 Application of amendments

The amendments of the *Privacy Act 1988* made by this Part apply in relation to direct marketing communications made on or after the commencement of this item.

Schedule 3—Data security

Part 1—Notifiable data breaches

Privacy Act 1988

1 Subsection 6(1) (definition of *at risk*)

Omit "section 26WE", substitute "subsection 26WE(3)".

2 Subsection 6(1)

Insert:

data breach has the meaning given by section 26WBA.

3 Subsection 13(4A)

Repeal the subsection (not including the heading), substitute:

(4A) An act or practice of an entity (within the meaning of Part IIIC) is an ***interference with the privacy of an individual*** if the act or practice contravenes any of the following provisions:

(a) subsection 26WDA(2);
(b) section 26WDB;
(c) subsection 26WH(2);
(d) subsection 26WK(2);
(e) subsection 26WK(6);
(f) subsection 26WK(7);
(g) subsection 26WL(3);
(h) subsection 26WR(10).

4 Subsection 13K(2)

Repeal the subsection, substitute:

Civil penalty provision for failure to give eligible data breach statement within required timeframe

(2) An entity (within the meaning of Part IIIC) contravenes this subsection if:

(a) the 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 fails to give the Commissioner a statement relating to the eligible data breach, in compliance or purported compliance with subsection 26WK(2), within the period referred to in that subsection.

5 Section 26WA

Repeal the section, substitute:

26WA Guide to this Part

This Part deals with data breaches.

A data breach happens if there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity.

An entity must take reasonable steps to prevent or reduce harm to individuals to whom information involved in an actual or suspected data breach relates. In addition, entities must take reasonable steps to implement practices, procedures and systems to ensure that the entity complies with all the obligations in this Part.

This Part also sets up a scheme for notification of eligible data breaches. An eligible data breach is a data breach that is likely to result in serious harm to any of the individuals to whom the information involved in the data breach 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.

The Commissioner may obtain information or documents in relation to actual or suspected eligible data breaches.

This Part also deals with the collection, use and disclosure of personal information involved in eligible data breaches.

6 After section 26WB

Insert:

26WBA Data breach

Scope

(1) This section applies if:

(a) an APP entity:

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

(ii) 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) a credit reporting body:

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

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

(c) a credit provider:

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

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

(d) a file number recipient:

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

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

Data breach

(2) If:

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

(b) the information is lost in circumstances where there is likely to be unauthorised access to or disclosure of the information;

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

7 After Division 1 of Part IIIC

Insert:

Division 1A—Responding to data breaches

26WDA Practices etc. to enable effective responses to data breaches

(1) The object of this section is to ensure that an entity:

(a) effectively responds to data breaches, or suspected data breaches, of the entity; and

(b) prevents or reduces harm to individuals to whom information involved in such an actual or suspected data breach relates or may relate.

(2) An entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that will ensure that the entity complies with this Part.

26WDB Mitigation of data breaches

(1) This section applies if an entity becomes aware that there are reasonable grounds to believe, or to suspect, that there has been a data breach of the entity.

(2) The entity must, as soon as practicable, take reasonable steps to prevent or reduce harm to the individuals to whom the information involved in the actual or suspected data breach relates or may relate.

Note: Steps taken in accordance with this section may also constitute action for the purposes of section 26WF or subsection 26WL(6) or (7) or 26WR(12) or (13) (which deal with remedial action).

8 Section 26WE

Repeal the section, substitute:

26WE Eligible data breach

Eligible data breach

(1) A data breach of an entity is an ***eligible data breach*** if:

(a) for a data breach constituted by unauthorised access to, or disclosure of, information—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) for a data breach constituted by a loss of information—a reasonable person would conclude that any unauthorised access to, or unauthorised disclosure of, the information would be likely to result in serious harm to any of the individuals to whom the information relates.

(2) Subsection (1) has effect subject to section 26WF.

At risk from an eligible data breach

(3) An individual is ***at risk*** from an eligible data breach if:

(a) information that relates to the individual is involved in the data breach; and

(b) a reasonable person would conclude that the data breach would be likely to result in serious harm to the individual.

9 Section 26WF

Repeal the section, substitute:

26WF Exception—remedial action

(1) A data breach of an entity is not, and is taken never to have been, an ***eligible data breach*** of that, or any other entity, if the first-mentioned entity takes action in relation to the data breach in accordance with subsection (2) or (3).

(2) Action taken in relation to a data breach constituted by unauthorised access to, or unauthorised disclosure of, information is taken in accordance with this subsection if:

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

(b) 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.

(3) Action taken in relation to a data breach constituted by a loss of information is taken in accordance with this subsection if:

(a) both of the following apply:

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

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

(b) both of the following apply:

(i) the action is taken after there is unauthorised access to, or unauthorised disclosure of, the information but before the access or disclosure results in serious harm to any of the individuals to whom the information relates;

(ii) 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.

10 Sections 26WK and 26WL

Repeal the sections, substitute:

26WK Statement about eligible data breach

Scope

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

Statement

(2) The entity must, within 72 hours, give the Commissioner a statement that sets out the matters referred to in subsection (3).

Note: A statement that does not fully set out the matters referred to in subsection (3) may initially be provided in certain circumstances: see subsections (5) and (6).

(3) The matters that the statement must set out for the purposes of subsection (2) are the following:

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

(b) a description of the eligible data breach;

(c) the particular kind or kinds of information involved in the eligible data breach;

(d) recommendations about the steps that individuals should take in response to the eligible data breach;

(e) information about any steps that the entity has taken, or proposes to take, in response to the eligible data breach (including any steps to reduce harm to any of the individuals to whom information involved in the eligible data breach relates).

(4) If the entity has reasonable grounds to believe that the access, disclosure or loss that constituted the eligible data breach is also an eligible data breach of one or more other entities, the statement may also set out the identity and contact details of those other entities.

When an incomplete statement may initially be provided

(5) Despite subsection (2), the statement need not set out, or fully set out, certain matters referred to in subsection (3), if:

(a) the entity considers it impossible or impracticable to give the Commissioner a statement within the period referred to in subsection (2) setting out, or fully setting out, those matters; and

(b) at the same time the entity gives the statement to the Commissioner, the entity gives the Commissioner notice in writing:

(i) stating that the statement is incomplete by reason of it being impossible or impracticable for the entity to set out, or fully set out, certain matters; and

(ii) identifying those matters; and

(iii) setting out the reasons why it is impossible or impracticable for those matters to be set out, or fully set out, in the statement.

(6) If the entity gives the Commissioner an incomplete statement in accordance with subsection (5), the entity must, as soon as practicable, give the Commissioner written notice of those matters.

Notice of material changes or errors

(7) If an entity becomes aware of a material change to, or a material error in, any matter set out in a statement or a notice given by the entity in accordance with subsection (2) or (6), the entity must, as soon as practicable, give the Commissioner written notice of the change or necessary correction (as the case may be).

26WL Entity must notify eligible data breach

Scope

(1) This section applies if:

(a) an entity becomes 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 in accordance with subsection 26WK(2) relating to the eligible data breach.

Notification

(2) The entity must give notification of the eligible data breach in accordance with the following table.

Notifications relating to eligible data breach

Item	If…	the entity must…
1	it is practicable for the entity to notify the contents of the	take such steps as are reasonable in the circumstances to notify the contents of the

Notifications relating to eligible data breach		
Item	**If…**	**the entity must…**
	statement to each of the individuals to whom the information involved in the eligible data breach relates	following to each of those individuals: (a) the statement; (b) any notice given by the entity under subsection 26WK(6) or (7) in relation to the statement.
2	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 following to each of those individuals: (a) the statement; (b) any notice given by the entity under subsection 26WK(6) or (7) in relation to the statement.
3	neither item 1 nor item 2 applies	(a) publish a copy of each of the following on the entity's website (if any): (i) the statement; (ii) any notice given by the entity under subsection 26WK(6) or (7) in relation to the statement; and (b) take reasonable steps to publicise the contents of the statement.

Note: The taking of remedial action may affect the obligations under this subsection: see subsection (5).

When notification must be given

(3) The entity must comply with subsection (2):

(a) in respect of the statement:

(i) if practicable—at the same time the entity gives the statement to the Commissioner; or

(ii) otherwise—as soon as practicable after the entity gives the statement to the Commissioner; and

(b) in respect of a notice given under subsection 26WK(6) or (7)—as soon as practicable after the notice is given.

Method of giving notification

(4) If the entity normally communicates with a particular individual using a particular method, a notification to the individual in accordance with item 1 or 2 of the table in subsection (2) may use that method. This subsection does not limit those table items.

No notification obligations for individuals if remedial action taken

(5) A reference to an individual in item 1 or 2 of the table in subsection (2) does not include a reference to an individual to whom subsection (6) or (7) applies.

(6) This subsection applies in relation to an individual if:
- (a) the data breach is constituted by unauthorised access to, or unauthorised disclosure of, information; and
- (b) the entity takes action in relation to the data breach before the access or disclosure results in serious harm to the individual; and
- (c) 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.

(7) This subsection applies in relation to an individual if:
- (a) the data breach is constituted by a loss of information; and
- (b) the entity takes action in relation to the data breach:
  - (i) after there is unauthorised access to, or unauthorised disclosure of, the information; and
  - (iii) before the access or disclosure results in serious harm to the individual; and
- (c) 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.

11 Section 26WN

Omit "paragraph 26WK(3)(d)", substitute "paragraphs 26WK(3)(d) and (e)".

12 Subsections 26WP(2) and (3)

Repeal the subsections, substitute:

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

13 Subsections 26WP(5) to (7)

Repeal the subsections, substitute:

(5) For the purposes of a prescribed secrecy provision, sections 26WK and 26WL are taken not to be provisions that require or authorise the use or disclosure of information.

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

14 Paragraph 26WR(1)(a)

Omit "a copy of".

15 Paragraphs 26WR(2)(a) and (b)

Repeal the paragraphs, substitute:

(a) if it is practicable for the entity to notify the contents of the statement to each of the individuals to whom the information involved in the eligible data breach relates—take such steps as are reasonable in the circumstances to notify the contents of the statement to each of those individuals; 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 those individuals; or

16 Subsection 26WR(2) (note)

Repeal the note, substitute:

Note: See also subsection (11) (which deals with remedial action).

17 Paragraphs 26WR(4)(b) to (d)

Repeal the paragraphs, substitute:

(b) a description of the eligible data breach; and

(c) the particular kind or kinds of information involved in the eligible data breach; and

(d) recommendations about the steps that individuals should take in response to the eligible data breach; and

(e) information about steps that the entity has taken, or proposes to take, in response to the eligible data breach (including steps to reduce harm to any of the individuals to whom the information involved in the eligible data breach relates).

18 Subsection 26WR(5)

Repeal the subsection, substitute:

(5) A direction under subsection (1) may also:

(a) require the statement referred to in paragraph (1)(a) to set out specified matters that relate to the eligible data breach; or

(b) require that, if the entity becomes aware of a material change to, or a material error in, any matter set out in the statement referred to in paragraph (1)(a), the entity must give the Commissioner written notice of the change or necessary correction (as the case may be).

19 Subsection 26WR(10)

Repeal the subsection, substitute:

Compliance with direction

(10) If an entity is given a direction under subsection (1):

(a) the entity must give the statement referred to in paragraph (1)(a) to the Commissioner within:

(i) 72 hours after receiving notice of the direction; or

(ii) such longer period as the Commissioner allows; and

(b) the entity must comply with the requirements referred to in subsection (2):

(i) if practicable—at the same time the entity gives the statement to the Commissioner; or

(ii) otherwise—as soon as practicable after the entity gives the statement to the Commissioner; and

(c) if the direction includes a requirement of the kind referred to in paragraph (5)(b)—the entity must comply with that requirement as soon as practicable after the entity becomes aware of a change or error of the kind referred to in that paragraph.

No notification obligations for individuals if remedial action taken

(11) Despite paragraph (10)(b), an entity is not required to comply with the requirements referred to in subsection (2) to the extent that the requirements relate to an individual to whom subsection (12) or (13) applies.

(12) This subsection applies in relation to an individual if:

(a) the data breach is constituted by unauthorised access to, or unauthorised disclosure of, information; and

(b) the entity takes action in relation to the data breach before the access or disclosure results in serious harm to the individual; and

(c) 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.

(13) This subsection applies in relation to an individual if:

(a) the data breach is constituted by a loss of information; and

(b) the entity takes action in relation to the data breach:

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

(iii) before the access or disclosure results in serious harm to the individual; and

(c) 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.

20 Paragraph 33C(1)(ca)

Repeal the paragraph, substitute:

(ca) the ability of an entity subject to Part IIIC to comply with that Part, including the extent to which the entity has

implemented practices, procedures and systems of the kind referred to in subsection 26WDA(2);

Part 2—Security of personal information

Privacy Act 1988

21 Schedule 1 (overview of the Australian Privacy Principles)

Omit:

> Australian Privacy Principle 11—security of personal information

substitute:

> Australian Privacy Principle 11—security and destruction of personal information

22 Clause 11 of Schedule 1

Repeal the clause, substitute:

11 Australian Privacy Principle 11—security and destruction of personal information

Security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification and disclosure.

Destruction etc. of personal information

11.2 If an APP entity holds personal information that the entity no longer needs for any purpose for which the entity may use or disclose the information under this Schedule, the entity must:

(a) consider whether to destroy the personal information; and

(b) take such steps as are reasonable in the circumstances to either:

(i) destroy the information; or
(ii) ensure that the information is de-identified.

11.3 Subclause 11.2 does not apply if:
(a) the information is contained in a Commonwealth record; or
(b) the entity is required by or under an Australian law or a court/tribunal order to retain the information.

Nature of steps to be taken

11.4 For the purposes of subclauses 11.1 and 11.2:
(a) steps taken by an APP entity may include technical or organisational measures; and
(b) the APP entity must take any steps needed to ensure that the APP entity is able to identify personal information to which those subclauses apply.

Ongoing evaluation

11.5 An APP entity must regularly evaluate the effectiveness of its compliance with subclauses 11.1 and 11.2.

23 Application of amendments

Clause 11 of Schedule 1 to the *Privacy Act 1988*, as inserted by this Part, applies in relation to information held on or after the commencement of this item, whether the information was acquired or created before, on or after that commencement.

Schedule 4—Data access and erasure

Part 1—Technically impossible or infeasible

Privacy Act 1988

1 After subclause 12.3 of Schedule 1

Insert:

Exception to access—all APP entities

12.3A If the APP entity:

(a) takes reasonable steps to give access to the personal information; and

(b) despite taking those steps, giving access remains unreasonable or impracticable due to technical impossibility or infeasibility;

then, despite subclause 12.1, the entity is not required to give access to the personal information to the extent that giving access remains so unreasonable or impracticable.

2 Paragraph 12.4(b) of Schedule 1

Before "give", insert "subject to subclauses 12.2, 12.3 and 12.3A,".

3 Subclauses 12.5 to 12.10 of Schedule 1

Repeal the subclauses, substitute:

Refusals to give access

12.5 If the APP entity refuses to give access to all or some of the personal information because of subclause 12.2, 12.3 or 12.3A, or to give access to all or some of the personal information in the manner requested by the individual, the entity must:

(a) take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual; and

(b) give the individual a written notice that sets out:

(i) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(ii) the mechanisms available to complain about the refusal; and

(iii) any other matter prescribed by the regulations.

12.6 Without limiting paragraph 12.5(a), access may be given through the use of a mutually agreed intermediary.

12.7 If the APP entity refuses to give access to all or some of the personal information because of paragraph 12.3(j), the reasons referred to in subparagraph 12.5(b)(i) may include an explanation for the commercially sensitive decision.

Access charges

12.8 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.9 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

4 Application of amendments

The amendments of clause 12 of Schedule 1 to the *Privacy Act 1988* made by this Part apply in relation to requests for access to personal information made on or after the commencement of this item, whether the information was acquired or created before, on or after that commencement.

Part 2—Right to erasure on large digital platforms

Privacy Act 1988

5 Subsection 6(1)

Insert:

business group has the meaning given by subsection 6EB(4).

control has the meaning given by subsection 6EB(6).

gross revenue has the meaning given by subsection 6EB(3).

large digital platform has the meaning given by subsection 6EB(1).

parent entity has the meaning given by subsection 6EB(5).

6 After section 6EA

Insert:

6EB Large digital platforms

(1) An organisation is a ***large digital platform*** at a time if, at that time:

(a) the organisation is a provider of a social media service, relevant electronic service or designated internet service (all within the meaning of the *Online Safety Act 2021*); and

(b) either:

(i) the organisation passes one or both of the tests in subsections (2) and (8); or

(ii) the organisation is prescribed by the regulations.

Note: For specification by class in the regulations, see subsection 13(3) of the *Legislation Act 2003*.

Gross revenue test

(2) The organisation passes the test in this subsection if the gross revenue of the organisation's business group for the previous financial year was at least $500 million.

(3) The ***gross revenue*** of an organisation's business group for a financial year is the sum of each member of the business group's gross revenue for the financial year, worked out in accordance with any of the accounting standards mentioned in subsection (7). For this purpose, it does not matter whether revenue has an Australian source.

(4) An organisation's ***business group*** has the following members:

(a) the organisation;

(b) if the organisation has a parent entity—the parent entity and all other entities (if any) controlled by the parent entity;

(c) if the organisation does not have a parent entity—all other entities (if any) controlled by the organisation.

(5) An entity is an organisation's ***parent entity*** if:

(a) the entity is not controlled by any other entity; and

(b) the entity controls the organisation.

(6) An entity ***controls*** another entity if it controls the other entity within the meaning of any of the accounting standards mentioned in subsection (7).

(7) For the purposes of subsections (3) and (6), the accounting standards are the following:

(a) accounting standards within the meaning of the *Corporations Act 2001*;

(b) international accounting standards made or adopted by the International Accounting Standards Board;

(c) accounting standards made by a body of a foreign country that correspond to, and are equivalent to, standards covered by paragraph (a) or (b).

Note: For paragraph (b), in 2026 the international accounting standards can be accessed from the IFRS website (www.ifrs.org).

End users test

(8) The organisation passes the test in this subsection if the number worked out, using the following method statement, for the service provided by the organisation as mentioned in paragraph (1)(a) for the previous financial year is at least 2.5 million.

Method statement	
Step 1.	For each whole calendar month in the financial year in which the organisation provided the service (an ***active calendar month***), work out the number of end-users of the service in Australia.
Step 2.	Add up the numbers worked out under step 1.
Step 3.	Divide the result of step 2 by the number of active calendar months.

7 After subparagraph 13K(1)(b)(ix)

Insert:

(ixa) Australian Privacy Principle 14.4(c) (notice of response to request for destruction);

8 At the end of section 100

Add:

(4) Before the Governor-General makes regulations for the purposes of subparagraph 6EB(1)(b)(ii) prescribing an entity as a large digital platform, the Minister must:

(a) be satisfied that doing so is desirable in the public interest; and

(b) consult the Commissioner about the desirability of regulating the entity as a large digital platform under this Act.

9 Schedule 1 (overview paragraph beginning "Part 5")

After "correction", insert "and destruction".

10 Part 5 of Schedule 1 (heading)

After "**correction**", insert "**and destruction**".

11 At the end of Schedule 1

Add:

14 Australian Privacy Principle 14—destruction on request of personal information held by large digital platform

14.1 If an organisation that is a large digital platform holds personal information that relates to an individual, the organisation must, on request by the individual, destroy the information.

Note: For ***large digital platform***, see section 6EB.

Exceptions to requirement to destroy personal information

14.2 Subclause 14.1 does not apply in relation to a request that is frivolous or vexatious.

14.3 Subclause 14.1 does not apply in relation to personal information covered by a request to the extent that one or more of the following applies in relation to the information:

(a) at the time the request is made, a permitted general situation exists in relation to the use or disclosure of the personal information by the organisation; or

Note: For ***permitted general situation***, see section 16A.

(b) at the time the request is made, a permitted health situation exists in relation to the use or disclosure of the personal information by the organisation; or

Note: For ***permitted health situation***, see section 16B.

(c) the organisation is required to retain the information under an Australian law or a court/tribunal order;

(d) despite the organisation taking reasonable steps to destroy the information in response to the request, destroying the information is unreasonable or impracticable due to technical impossibility or infeasibility;

(e) the information is strictly necessary in order for the organisation to continue to provide or deliver goods or services that the individual has requested the organisation to provide to the individual.

Dealing with requests for destruction

14.4 If a request is made under subclause 14.1, the organisation must, within a reasonable period after the request is made:

(a) assess whether subclause 14.1 applies in relation to some or all of the information covered by the request; and

(b) after the assessment:

(i) to the extent (if any) that subclause 14.1 applies in relation to the information—destroy the information to which subclause 14.1 applies; and

(ii) give the individual a written notice that sets out the matters required by subclause 14.5.

14.5 The matters required are the following, as applicable:

(a) if the organisation destroyed some or all of the information—that fact;

(b) if the organisation did not destroy all of the information on the ground that subclause 14.1 does not apply to some or all of the information:

(i) that fact and the reasons the organisation is satisfied that subclause 14.1 does not apply, except to the extent that, having regard to those reasons, it would be unreasonable to give the individual notice of them; and

(ii) the mechanisms available to the individual to complain about the organisation's decision; and

(iii) any other matter prescribed by the regulations.

12 Application of amendments

Australian Privacy Principle 14, as inserted by this Act, applies on and after the commencement of this item:

(a) in relation to an organisation that is a large digital platform within the meaning of the *Privacy Act 1988* as in force from that commencement, regardless of whether the organisation became a large digital platform before, on or after that commencement; and

(b) in relation to information held on or after that commencement, regardless of whether the information was acquired or created before, on or after that commencement.

Schedule 5—Exception for research

Part 1—Main amendments

Privacy Act 1988

1 Subsection 6(1)

Insert:

applicable national statement on ethical conduct in human research, in relation to human research, means the national statement on ethical conduct in human research that is most recent at the time the human research starts.

human research means research that:

(a) is conducted with or about individuals; and

(b) involves personal information.

Example: Research conducted with individuals includes surveys, interviews and focus groups of individuals.

human research guidelines means guidelines made under subsection 94B(2).

national statement on ethical conduct in human research means any statement jointly developed by the National Health and Medical Research Council, the Australian Research Council and Universities Australia (ACN 008 502 930) setting out national standards for the ethical design, review and conduct of human research.

Note: The national statement on ethical conduct in human research could in 2026 be viewed on the National Health and Medical Research Council's website (https://www.nhmrc.gov.au/).

2 After section 94A

Insert:

94B Human research does not breach Australian Privacy Principles if alternative requirements are met

(1) If:

(a) but for this subsection, an act done by an APP entity would breach an Australian Privacy Principle; and
(b) the act is done in the course of human research; and
(c) the human research is reviewed, approved and monitored in accordance with the applicable national statement on ethical conduct in human research; and
(d) the human research meets the requirements (if any) in the human research guidelines; and
(e) the act is in accordance with the human research guidelines;

the act does not breach that Australian Privacy Principle.

Human research guidelines

(2) The Commissioner may, by legislative instrument, make guidelines (the ***human research guidelines***) that do the following:
(a) set out requirements human research must meet for subsection (1) to apply;
(b) provide for the protection of the privacy of individuals in the conduct of human research by APP entities.

(3) Without limiting any other subsection in this section, human research guidelines made for the purposes of paragraph (2)(a) may have the effect of limiting the kinds of human research to which subsection (1) applies.

(4) Before the Commissioner makes human research guidelines, the Commissioner must:
(a) prepare a draft of the guidelines; and
(b) publish a notice on the Commissioner's website:
(i) containing a summary of the draft guidelines; and
(ii) stating where copies of the draft guidelines can be obtained; and
(iii) inviting persons or bodies to make submissions relating to the draft guidelines in accordance with the procedures, and within the period, specified in the notice; and
(iv) including the information prescribed by the regulations; and

(c) have regard to any submissions received as a result of the invitation referred to in subparagraph (b)(iii).

Part 2—Consequential amendments

Privacy Act 1988

3 Subsection 6(1) (definition of *medical research*)

Repeal the definition.

4 Paragraph 16B(2)(d)

Omit "any of the following apply", substitute "either of the following applies".

5 Subparagraph 16B(2)(d)(ii)

Omit "organisation;", substitute "organisation.".

6 Subparagraph 16B(2)(d)(iii)

Repeal the subparagraph.

7 Subsection 16B(3)

Repeal the subsection.

8 After paragraph 28(1)(b)

Insert:

(ba) making, by legislative instrument, guidelines for the purposes of subsection 94B(2) (human research guidelines);

9 Subsection 28(2)

Omit "and (b)", substitute ", (b) and (ba)".

10 Sections 95 and 95A

Repeal the sections.

11 Paragraph 96(1)(d)

Omit "an application;", substitute "an application.".

12 Paragraphs 96(1)(e) to (g)

Repeal the paragraphs.

Schedule 6—Exception for information processors

Privacy Act 1988

1 Subsection 6(1)

Insert:

controller, in relation to an act or practice, has the meaning given by subsection 16D(1).

processor, in relation to an act or practice, has the meaning given by subsection 16D(1).

2 After subsection 6A(2)

Insert:

No breach—processor acting on behalf of controller

(2A) An act or practice does not ***breach*** an Australian Privacy Principle, other than Australian Privacy Principle 1 or 11, if the act is done, or the practice is engaged in, by a processor on behalf of a controller.

Note: See subsection 16D(1) for when an act is done, or a practice is engaged in, by a processor on behalf of a controller.

3 Subsection 6A(5)

After "(2),", insert "(2A),".

4 After subsection 6B(2)

Insert:

No breach—processor acting on behalf of controller

(2A) An act or practice does not ***breach*** a registered APP code if the act is done, or the practice is engaged in, by a processor on behalf of a controller.

Note: See subsection 16D(1) for when an act is done, or a practice is engaged in, by a processor on behalf of a controller.

5 Subsection 6B(5)

After "(2),", insert "(2A),".

6 After section 16C

Insert:

16D Acts and practices of processors done on behalf of controllers

(1) An APP entity (a ***processor***), other than a contracted service provider for a Commonwealth contract, does an act, or engages in a practice, on behalf of another APP entity (a ***controller***) if:

(a) the act is done, or the practice is engaged in:

(i) in accordance with instructions given to the processor by the controller; and

(ii) for one or more purposes of the controller specified in the instructions; and

(b) the instructions are documented in writing by the controller.

(2) If an act done, or a practice engaged in, by a processor on behalf of a controller does not breach an Australian Privacy Principle only because of subsection 6A(2A) and the act or practice would breach the Australian Privacy Principle if it were done or engaged in by the controller, then the controller is taken:

(a) to have done the act or engaged in the practice; and

(b) to have breached the Australian Privacy Principle.

(3) If an act done, or a practice engaged in, by a processor on behalf of a controller does not breach a registered APP code only because of subsection 6B(2A) and the act or practice would breach the registered APP code if it were done or engaged in by the controller, then the controller is taken:

(a) to have done the act or engaged in the practice; and

(b) to have breached the registered APP code.

7 Application of amendments

The amendments of the *Privacy Act 1988* made by this Schedule apply in relation to acts done, and practices engaged in, on or after the commencement of this item.

EXPOSURE DRAFT