Privacy and Personal Information Protection Act 1998 No 133

[1998-133]

New South Wales

Status Information

Currency of version

Current version for 28 November 2023 to date (accessed 29 February 2024 at 7:47)

Legislation on this site is usually updated within 3 working days after a change to the legislation.

Provisions in force

The provisions displayed in this version of the legislation have all commenced.

Authorisation

This version of the legislation is compiled and maintained in a database of legislation by the Parliamentary Counsel's Office and published on the NSW legislation website, and is certified as the form of that legislation that is correct under section 45C of the Interpretation Act 1987.

File last modified 28 November 2023

Privacy and Personal Information Protection Act 1998 No 133

New South Wales

Contents

Privacy and Personal Information Protection Act 1998 No 133

New South Wales

An Act to provide for the protection of personal information, and for the protection of the privacy of individuals generally; to provide for the appointment of a Privacy Commissioner; to repeal the *Privacy Committee Act 1975*; and for other purposes.

Part 1 Preliminary

1 Name of Act

This Act is the *Privacy and Personal Information Protection Act 1998*.

2 Commencement

This Act commences on a day or days to be appointed by proclamation.

3 Definitions

(1) In this Act—

affected individual, for Part 6A—see section 59D(2).

approved form, for Part 6A—see section 59A.

assessment, for Part 6A—see section 59E(2)(b).

assessor, for Part 6A—see section 59G(1).

Commonwealth agency means an entity referred to in paragraph (a)–(h) of the definition of ***agency*** in the *Privacy Act 1988* of the Commonwealth.

convicted inmate has the same meaning as it has in the *Crimes (Administration of Sentences) Act 1999*.

eligible data breach, for Part 6A—see section 59D(1).

exercise a function includes perform a duty.

function includes a power, authority or duty.

head, for Part 6A—see section 59A.

health privacy code of practice, for Part 6A—see section 59A.

Health Privacy Principle, for Part 6A—see section 59A.

held, in relation to personal information—

(a) for Part 6A—see section 59C, or

(b) otherwise—see section 4(4).

Information Commissioner means the Information Commissioner under the *Government Information (Information Commissioner) Act 2009*.

information protection principle or ***principle*** means a provision set out in Division 1 of Part 2.

investigative agency means—

(a) any of the following—

(i) the Ombudsman's Office,

(ii) the Independent Commission Against Corruption,

(iii) the Inspector of the Independent Commission Against Corruption,

(iv) the Law Enforcement Conduct Commission,

(v) the Inspector of the Law Enforcement Conduct Commission and any staff of the Inspector,

(vi) the Health Care Complaints Commission,

(vii) the Office of the Legal Services Commissioner,

(viia) the Ageing and Disability Commissioner,

(viib) the Children's Guardian,

(viii) a person or body prescribed by the regulations for the purposes of this definition, or

(b) any other public sector agency with investigative functions if—

(i) those functions are exercisable under the authority of an Act or statutory rule (or where that authority is necessarily implied or reasonably contemplated under an Act or statutory rule), and

(ii) the exercise of those functions may result in the agency taking or instituting

disciplinary, criminal or other formal action or proceedings against a person or body under investigation, or

(c) a public sector agency conducting an investigation for or on behalf of an agency referred to in paragraph (a) or (b).

law enforcement agency means any of the following—

(a) the NSW Police Force, or the police force of another State or a Territory,

(b) the New South Wales Crime Commission,

(c) the Australian Federal Police,

(d) the Australian Crime Commission,

(e) the Director of Public Prosecutions of New South Wales, of another State or a Territory, or of the Commonwealth,

(f) the Department of Justice,

(f1) the Independent Gaming and Liquor Authority under the *Gaming and Liquor Administration Act 2007*,

(g) the NSW Independent Casino Commission under the *Casino Control Act 1992*,

(g1) the Office of the Sheriff of New South Wales,

(h) a person or body prescribed by the regulations for the purposes of this definition.

local government authority means a council, a county council or a joint organisation, within the meaning of the *Local Government Act 1993*.

mandatory notification of data breach scheme means the scheme under Part 6A for assessing and notifying data breaches.

personal information is defined in section 4.

privacy code of practice or ***code*** means a privacy code of practice made under Part 3.

Privacy Commissioner means the Privacy Commissioner appointed under this Act.

public register means a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee).

public sector agency means any of the following—

(a) a Public Service agency or the Teaching Service,

(a1) the office of a political office holder within the meaning of the *Members of Parliament Staff Act 2013*, being the office comprising the persons employed by the political office holder under Part 2 of that Act,

(b) a statutory body representing the Crown,

(c) (Repealed)

(d) an auditable entity within the meaning of the *Government Sector Audit Act 1983* or any other entity within the meaning of that Act (or entity of a kind) prescribed by the regulations, but excluding an entity (or entity of a kind) prescribed by the regulations,

(e) the NSW Police Force,

(e1) (Repealed)

(f) a local government authority,

(f1) a State owned corporation that is not subject to the *Privacy Act 1988* of the Commonwealth,

(g) a person or body that—

(i) provides data services (being services relating to the collection, processing, disclosure or use of personal information or that provide for access to such information) for or on behalf of a body referred to in paragraph (a)–(f1) of this definition, or that receives funding from any such body in connection with providing data services, and

(ii) is prescribed by the regulations for the purposes of this definition.

Note—

Section 4B enables the regulations to declare that a public sector agency is to be regarded as being part of another public sector agency for the purposes of this Act. It also enables the regulations to declare that a part of a public sector agency is to be regarded as being a separate public sector agency from the public sector agency of which it forms part for the purposes of this Act.

public sector official means any of the following—

(a) a person appointed by the Governor, or a Minister, to a statutory office,

(b) a judicial officer within the meaning of the *Judicial Officers Act 1986*,

(c) a person employed in the Public Service, the Transport Service of New South Wales, the Teaching Service, the NSW Health Service or the NSW Police Force,

(c1) a person employed by a political office holder under Part 2 of the *Members of Parliament Staff Act 2013*,

(c2) a person employed by a member of Parliament under Part 3 of the *Members of Parliament Staff Act 2013*,

(d) a local government councillor or a person employed by a local government authority,

(e) a person who is an officer of the Legislative Council or Legislative Assembly or who is employed by (or who is under the control of) the President of the Legislative Council or the Speaker of the Legislative Assembly, or both,

(f) a person who is employed or engaged by—

(i) a public sector agency, or

(ii) a person referred to in paragraph (a)–(e),

(g) a person who acts for or on behalf of, or in the place of, or as deputy or delegate of, a public sector agency or person referred to in paragraph (a)–(e).

publicly available publication does not include any publication or document declared by the regulations not to be a publicly available document for the purposes of this Act.

staff of the Inspector of the Independent Commission Against Corruption means—

(a) any staff employed under section 57E (1) or (2) of the *Independent Commission Against Corruption Act 1988*, and

(b) any consultants engaged under section 57E (3) of that Act.

staff of the Inspector of the Law Enforcement Conduct Commission means—

(a) any staff employed under section 128 (1) of the *Law Enforcement Conduct Commission Act 2016*, and

(b) any consultants engaged under section 128 (4) (c) of that Act.

State record has the same meaning as in the *State Records Act 1998*.

Tribunal means the Civil and Administrative Tribunal.

Note—

The *Interpretation Act 1987* contains definitions and other provisions that affect the interpretation and application of this Act.

(2) Notes included in this Act are explanatory notes and do not form part of this Act.

4 Definition of "personal information"

(1) In this Act, ***personal information*** means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

(2) Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

(3) Personal information does not include any of the following—

(a) information about an individual who has been dead for more than 30 years,

(b) information about an individual that is contained in a publicly available publication,

(c) information about a witness who is included in a witness protection program under the *Witness Protection Act 1995* or who is subject to other witness protection arrangements made under an Act,

(d) information about an individual arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* of the Commonwealth,

(e) information about an individual that is contained in a public interest disclosure within the meaning of the *Public Interest Disclosures Act 2022*, or that has been collected while dealing with a voluntary public interest disclosure in accordance with that Act, Part 5, Division 2,

(f) information about an individual arising out of, or in connection with, an authorised operation within the meaning of the *Law Enforcement (Controlled Operations) Act 1997*,

(g) information about an individual arising out of a Royal Commission or Special Commission of Inquiry,

(h) information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990*,

(i) information about an individual that is contained in Cabinet information or Executive Council information under the *Government Information (Public Access) Act 2009*,

(j) information or an opinion about an individual's suitability for appointment or employment as a public sector official,

(ja) information about an individual that is obtained about an individual under Chapter 8 (Adoption information) of the *Adoption Act 2000*,

(k) information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations for the purposes of this subsection.

(4) Personal information is ***held*** by a public sector agency if—

(a) the agency is in possession or control of the information, or

(b) the information is in the possession or control of a person employed or engaged by the agency in the course of such employment or engagement, or

(c) the information is contained in a State record in respect of which the agency is responsible under the *State Records Act 1998*.

(5) For the purposes of this Act, personal information is not ***collected*** by a public sector agency if the receipt of the information by the agency is unsolicited.

4A Exclusion of health information from definition of "personal information"

Except as provided by this Act or the *Health Records and Information Privacy Act 2002*, the definition of ***personal information*** in section 4 does not include health information within the meaning of the *Health Records and Information Privacy Act 2002*.

4B Regulations may declare whether agency is part of or separate from a public sector agency

(1) The regulations may declare that—

(a) a specified public sector agency is not to be regarded as a separate public sector agency and instead is to be regarded for the purposes of this Act as part of and included in another specified public sector agency in respect of specified functions, or

(b) a specified office, branch or other part of a public sector agency is for the purposes of this Act to be regarded as being a separate public sector agency to the public sector agency of which it forms part in respect of specified functions that it exercises.

(2) The regulations may make provision for or with respect to the application of this Act (with such modifications, if any, as may be prescribed) for the purposes of a declaration under this section.

(3) The Minister must, before recommending the making of a regulation under this section, consider whether the making of a declaration under this section will permit the sharing of personal information between public sector agencies and, if so, whether the sharing of that information would be appropriate in the circumstances.

5 Government Information (Public Access) Act 2009 not affected

(1) Nothing in this Act affects the operation of the *Government Information (Public*

Access) Act 2009.

(2) In particular, this Act does not operate to lessen any obligations under the *Government Information (Public Access) Act 2009* in respect of a public sector agency.

6 Courts, tribunals and Royal Commissions not affected

(1) Nothing in this Act affects the manner in which a court or tribunal, or the manner in which the holder of an office relating to a court or tribunal, exercises the court's, or the tribunal's, judicial functions.

(2) Nothing in this Act affects the manner in which a Royal Commission, or any Special Commission of Inquiry, exercises the Commission's functions.

(3) In this section, ***judicial functions*** of a court or tribunal means such of the functions of the court or tribunal as relate to the hearing or determination of proceedings before it, and includes—

(a) in relation to a Magistrate—such of the functions of the Magistrate as relate to the conduct of committal proceedings, and

(b) in relation to a coroner—such of the functions of the coroner as relate to the conduct of inquests and inquiries under the *Coroners Act 2009*.

7 Crown bound by Act

This Act binds the Crown in right of New South Wales and also, in so far as the legislative power of Parliament permits, the Crown in all its other capacities.

Part 2 Information protection principles

Division 1 Principles

8 Collection of personal information for lawful purposes

(1) A public sector agency must not collect personal information unless—

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and

(b) the collection of the information is reasonably necessary for that purpose.

(2) A public sector agency must not collect personal information by any unlawful means.

9 Collection of personal information directly from individual

A public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless—

(a) the individual has authorised collection of the information from someone else, or

(b) in the case of information relating to a person who is under the age of 16 years—the information has been provided by a parent or guardian of the person.

10 Requirements when collecting personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following—

(a) the fact that the information is being collected,

(b) the purposes for which the information is being collected,

(c) the intended recipients of the information,

(d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided,

(e) the existence of any right of access to, and correction of, the information,

(f) the name and address of the agency that is collecting the information and the agency that is to hold the information.

11 Other requirements relating to collection of personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that—

(a) the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete, and

(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

12 Retention and security of personal information

A public sector agency that holds personal information must ensure—

(a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

(b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and

(c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

(d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.

13 Information about personal information held by agencies

A public sector agency that holds personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain—

(a) whether the agency holds personal information, and

(b) whether the agency holds personal information relating to that person, and

(c) if the agency holds personal information relating to that person—

(i) the nature of that information, and

(ii) the main purposes for which the information is used, and

(iii) that person's entitlement to gain access to the information.

14 Access to personal information held by agencies

A public sector agency that holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

15 Alteration of personal information

(1) A public sector agency that holds personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information—

(a) is accurate, and

(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

(2) If a public sector agency is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the agency must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If personal information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the public sector agency.

(4) This section, and any provision of a privacy code of practice that relates to the requirements set out in this section, apply to public sector agencies despite section 25 of this Act and section 21 of the *State Records Act 1998*.

(5) The Privacy Commissioner's guidelines under section 36 may make provision for or with respect to requests under this section, including the way in which such a request should be made and the time within which such a request should be dealt with.

(6) In this section (and in any other provision of this Act in connection with the operation of this section), ***public sector agency*** includes a Minister and a Minister's personal staff.

16 Agency must check accuracy of personal information before use

A public sector agency that holds personal information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

17 Limits on use of personal information

A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless—

(a) the individual to whom the information relates has consented to the use of the information for that other purpose, or

(b) the other purpose for which the information is used is directly related to the purpose for which the information was collected, or

(c) the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

18 Limits on disclosure of personal information

(1) A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless—

(a) the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or

(b) the individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or

(c) the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

(2) If personal information is disclosed in accordance with subsection (1) to a person or body that is a public sector agency, that agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

19 Special restrictions on disclosure of personal information

(1) A public sector agency must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person.

(2) A public sector agency that holds personal information about an individual must not disclose the information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless—

(a) the public sector agency reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the information protection principles, or

(b) the individual expressly consents to the disclosure, or

(c) the disclosure is necessary for the performance of a contract between the individual and the public sector agency, or for the implementation of pre-contractual measures taken in response to the individual's request, or

(d) the disclosure is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the public sector agency and a third party, or

(e) all of the following apply—

(i) the disclosure is for the benefit of the individual,

(ii) it is impracticable to obtain the consent of the individual to that disclosure,

(iii) if it were practicable to obtain such consent, the individual would be likely to give it, or

(f) the disclosure is reasonably believed by the public sector agency to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person, or

(g) the public sector agency has taken reasonable steps to ensure that the information that it has disclosed will not be held, used or disclosed by the recipient of the information inconsistently with the information protection principles, or

(h) the disclosure is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

(3)–(5) (Repealed)

Division 2 General provisions relating to principles

20 General application of information protection principles to public sector agencies

(1) The information protection principles apply to public sector agencies.

(2) The application of the principles to public sector agencies—

(a) may be modified by privacy codes of practice, and

(b) is otherwise subject to this Act.

(3) Sections 8–11 do not apply in respect of personal information collected by a public sector agency before the commencement of this Part.

(4) (Repealed)

(5) Without limiting the generality of section 5, the provisions of the *Government Information (Public Access) Act 2009* that impose conditions or limitations (however expressed) with respect to any matter referred to in section 13, 14 or 15 are not affected by this Act, and those provisions continue to apply in relation to any such matter as if those provisions were part of this Act.

21 Agencies to comply with principles

(1) A public sector agency must not do any thing, or engage in any practice, that contravenes an information protection principle applying to the agency.

(2) The contravention by a public sector agency of an information protection principle that applies to the agency is conduct to which Part 5 applies.

Division 3 Specific exemptions from principles

22 Operation of Division

Nothing in this Division authorises a public sector agency to do any thing that it is otherwise prohibited from doing.

23 Exemptions relating to law enforcement and related matters

(1) A law enforcement agency is not required to comply with section 9 if compliance by

the agency would prejudice the agency's law enforcement functions.

(2) A public sector agency (whether or not a law enforcement agency) is not required to comply with section 9 if the information concerned is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal.

(3) A public sector agency (whether or not a law enforcement agency) is not required to comply with section 10 if the information concerned is collected for law enforcement purposes. However, this subsection does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.

(4) A public sector agency (whether or not a law enforcement agency) is not required to comply with section 17 if the use of the information concerned for a purpose other than the purpose for which it was collected is reasonably necessary for law enforcement purposes or for the protection of the public revenue.

(5) A public sector agency (whether or not a law enforcement agency) is not required to comply with section 18 if the disclosure of the information concerned—

(a) is made in connection with proceedings for an offence or for law enforcement purposes (including the exercising of functions under or in connection with the *Confiscation of Proceeds of Crime Act 1989* or the *Criminal Assets Recovery Act 1990*), or

(b) is to a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

(c) is authorised or required by subpoena or by search warrant or other statutory instrument, or

(d) is reasonably necessary—

(i) for the protection of the public revenue, or

(ii) in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed.

(6) Nothing in subsection (5) requires a public sector agency to disclose personal information to another person or body if the agency is entitled to refuse to disclose the information in the absence of a subpoena, warrant or other lawful requirement.

(6A) A public sector agency is not required to comply with the information protection principles with respect to the collection, use or disclosure of personal information if—

(a) the agency is providing the information to another public sector agency or the agency is being provided with the information by another public sector agency,

and

(b) the collection, use or disclosure of the information is reasonably necessary for law enforcement purposes.

(7) A public sector agency (whether or not a law enforcement agency) is not required to comply with section 19 if the disclosure of the information concerned is reasonably necessary for the purposes of law enforcement in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed.

(8) In this section—

(a) a reference to law enforcement purposes includes a reference to law enforcement purposes of another State or a Territory or the Commonwealth, and

(b) a reference to an offence includes a reference to an offence against a law of another State or a Territory or the Commonwealth, and

(c) a reference to the protection of the public revenue includes a reference to the protection of the public revenue of another State or a Territory or the Commonwealth.

23A Exemptions relating to ASIO

(1) A public sector agency is not required to comply with section 13 or 14 if compliance would reveal to the public that ASIO had requested, or been provided with, information about a person.

(2) A public sector agency is not required to comply with section 18 if—

(a) the disclosure of the information concerned has been requested by the Director-General of ASIO for a purpose connected with the exercise of ASIO's functions under the *Australian Security Intelligence Organisation Act 1979* of the Commonwealth, and

(b) the information is disclosed to an officer or employee of ASIO who is authorised in writing by the Director-General to receive the information, and

(c) the authorised officer or employee certifies in writing that the information sought is reasonably necessary for ASIO to exercise its functions under the *Australian Security Intelligence Organisation Act 1979* of the Commonwealth.

(3) To avoid doubt, this section permits (but does not require) a public sector agency to disclose any information requested by the Director-General of ASIO.

(4) The Minister may enter into arrangements with the Director-General of ASIO concerning the provision of reports by the Director-General to the Minister concerning requests for information from public sector agencies made by the Director-General.

(5) The regulations may make provision for or with respect to the tabling of such reports (or parts of such reports) in Parliament, including authorising the Minister to omit information in the reports that is confidential.

(6) In this section—

ASIO means the Australian Security Intelligence Organisation continued in existence by the *Australian Security Intelligence Organisation Act 1979* of the Commonwealth.

24 Exemptions relating to investigative agencies

(1) An investigative agency is not required to comply with section 9, 10, 13, 14, 15, 18 or 19 (1) if compliance with those sections might detrimentally affect (or prevent the proper exercise of) the agency's complaint handling functions or any of its investigative functions.

(2) An investigative agency is not required to comply with section 17 if the use of the information concerned for a purpose other than the purpose for which it was collected is reasonably necessary in order to enable the agency to exercise its complaint handling functions or any of its investigative functions.

(3) An investigative agency is not required to comply with section 18 or 19 (1) if the information concerned is disclosed to another investigative agency.

(4) A public sector agency (whether or not an investigative agency) is not required to comply with section 18 or 19 (1) if non-compliance is reasonably necessary to assist another public sector agency that is an investigative agency in exercising its investigative functions.

(5) An investigative agency is not required to comply with section 18 if—

(a) the information concerned is disclosed to a complainant, and

(b) the disclosure is reasonably necessary for the purpose of—

(i) reporting the progress of an investigation into the complaint made by the complainant, or

(ii) providing the complainant with advice as to the outcome of the complaint or any action taken as a result of the complaint.

(6) The exemptions provided by subsections (1)–(5) extend to—

(a) any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency, and

(b) the Office of Local Government, or any person employed in that Office, who is

investigating or otherwise handling (formally or informally) a complaint or other matter even though it is or may be the subject of a right of appeal conferred by or under an Act.

(7) The Ombudsman's Office is not required to comply with section 9 or 10.

(8) An investigative agency is not required to comply with section 12 (a).

25 Exemptions where non-compliance is lawfully authorised or required

A public sector agency is not required to comply with section 9, 10, 13, 14, 15, 17, 18 or 19 if—

(a) the agency is lawfully authorised or required not to comply with the principle concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

26 Other exemptions where non-compliance would benefit the individual concerned

(1) A public sector agency is not required to comply with section 9 or 10 if compliance by the agency would, in the circumstances, prejudice the interests of the individual to whom the information relates.

(2) A public sector agency is not required to comply with section 10, 18 or 19 if the individual to whom the information relates has expressly consented to the agency not complying with the principle concerned.

27 Specific exemptions for certain law enforcement agencies

(1) Despite any other provision of this Act, the following are not required to comply with the information privacy principles—

(a) the Independent Commission Against Corruption,

(b) the Inspector of the Independent Commission Against Corruption and the staff of the Inspector,

(c) the Independent Gaming and Liquor Authority under the *Gaming and Liquor Administration Act 2007*,

(d) the Law Enforcement Conduct Commission,

(e) the Inspector of the Law Enforcement Conduct Commission and the staff of the Inspector,

(f) the New South Wales Crime Commission,

(g) the NSW Independent Casino Commission,

(h) the NSW Police Force.

(2) However, the information protection principles do apply to a public sector agency mentioned in subsection (1) in connection with the exercise of the agency's administrative and educative functions.

27A Exemptions relating to information exchanges between public sector agencies

A public sector agency is not required to comply with the information protection principles with respect to the collection, use or disclosure of personal information if—

(a) the agency is providing the information to another public sector agency or the agency is being provided with the information by another public sector agency, and

(b) the collection, use or disclosure of the information is reasonably necessary—

(i) to allow any of the agencies concerned to deal with, or respond to, correspondence from a Minister or member of Parliament, or

(ii) to enable inquiries to be referred between the agencies concerned, or

(iii) to enable the auditing of the accounts or performance of a public sector agency or group of public sector agencies (or a program administered by an agency or group of agencies).

27B Exemptions relating to research

A public sector agency is not required to comply with the information protection principles with respect to the collection, use or disclosure of personal information if—

(a) the collection, use or disclosure of the information is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest, and

(b) in the case where the agency would otherwise contravene section 9 in respect of the collection of the information—it is unreasonable or impracticable for the information to be collected directly from the individual to whom the information relates, and

(c) in the case of the use or disclosure of the information—either—

(i) the purpose referred to in paragraph (a) cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the agency to seek the consent of the individual for the use or disclosure, or

(ii) reasonable steps are taken to de-identify the information, and

(d) in the case where the use or disclosure of the information could reasonably be expected to identify individuals—the information is not published in a publicly

available publication, and

(e) the collection, use or disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph.

27C Exemptions relating to credit information

(1) A courts agency is not required to comply with section 17 or 18 if—

(a) compliance would prevent the courts agency from disclosing to a credit reporting body that an individual is a default judgment debtor and the amount of the debt, and

(b) the courts agency is satisfied that the credit reporting body has given an enforceable undertaking not to retain the information disclosed to it after the expiry of the applicable retention period.

(2) The ***applicable retention period*** for the purposes of subsection (1) (b) is—

(a) if the debt of the default judgment debtor is satisfied—the period of 2 years commencing on the date that the debt was satisfied, or

(b) if the debt of the default judgment debtor remains unsatisfied—the period of 5 years commencing on the date the judgment was given,

whichever is the earlier.

(3) In this section—

courts agency means—

(a) the Department of Justice (including any Public Service executive agency that is related to the Department for the purposes of the *Government Sector Employment Act 2013*), and

(b) any court or tribunal referred to in Schedule 1 to the *Civil Procedure Act 2005*.

credit reporting body has the same meaning as in the *Privacy Act 1988* of the Commonwealth.

default judgment debtor means an individual against whom a default judgment has been given by a court or tribunal under the uniform rules within the meaning of the *Civil Procedure Act 2005*.

27D Exemptions relating to emergency situations

(1) A public sector agency is not required to comply with the information protection principles in relation to the collection, use or disclosure of personal information if—

(a) the collection, use or disclosure of the information is reasonably necessary to

assist in a stage of an emergency, and

(b) the collection, use or disclosure is only for the purpose of assisting in the stage of the emergency, and

(c) it is impracticable or unreasonable to seek the consent of the individual to whom the information relates to the collection, use or disclosure for the purpose of assisting in the stage of the emergency.

(2) In this section—

emergency has the same meaning as in the *State Emergency and Rescue Management Act 1989*.

stage, of an emergency, means a stage in relation to an emergency mentioned in the *State Emergency and Rescue Management Act 1989*, section 5.

(3) If personal information is collected, used or disclosed under this section—

(a) the public sector agency must not hold the information for longer than 18 months, unless extenuating circumstances apply or consent has been obtained, and

(b) if the public sector agency is a law enforcement agency—the agency must not use the information for the purpose of a prosecuting an offence.

28 Other exemptions

(1) The Ombudsman's Office, Children's Guardian, Health Care Complaints Commission, Anti-Discrimination Board, Ageing and Disability Commissioner and Guardianship Board are not required to comply with section 19.

(2) The information protection principles do not apply in respect of personal information collected or held by Multicultural NSW if—

(a) the information is collected or held by Multicultural NSW for the purpose only of translating the information, and

(b) all documents held by Multicultural NSW in which the information is contained are destroyed or returned to the person who submitted the information for translation when Multicultural NSW is satisfied that the documents are no longer required for the provision of the translation service, and

(c) in a case where it is necessary for the information to be given to another person in connection with the provision of the translation service, everything reasonably within the power of Multicultural NSW is done to prevent unauthorised disclosure of the information by that other person.

(3) Nothing in section 17, 18 or 19 prevents or restricts the disclosure of information—

(a) by a public sector agency to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

(b) by a public sector agency to any public sector agency under the administration of the Premier if the disclosure is for the purposes of informing the Premier about any matter.

Part 3 Privacy codes of practice and management plans

Division 1 Privacy codes of practice

29 Operation of privacy codes of practice

(1) Privacy codes of practice may be made for the purpose of protecting the privacy of individuals.

(2) A privacy code of practice may regulate the collection, use and disclosure of, and the procedures for dealing with, personal information held by public sector agencies.

(3) In particular, a privacy code of practice may provide for the protection of personal information contained in a record that is more than 30 years old, and any such provision has effect despite the provisions of any other Act that deals with the disclosure of, or access to, personal information of that kind. Any such code must, to the extent that it relates to personal information contained in a State record that is more than 30 years old, be consistent with any relevant guidelines issued under section 52 of the *State Records Act 1998*.

(4) A privacy code of practice may also provide for the disclosure of personal information to persons or bodies outside New South Wales.

(5) A privacy code of practice can apply to any one or more of the following—

(a) any specified class of personal information,

(b) any specified public sector agency or class of public sector agency,

(c) any specified activity or specified class of activity.

(6) Except in the case of a privacy code of practice that is referred to in subsection (3), a code cannot affect the operation of any exemption provided under Division 3 of Part 2.

(7) A code—

(a) must provide standards of privacy protection that operate to protect public sector agencies from any restrictions in relation to the importation of personal information into New South Wales, and

(b) must not impose on any public sector agency any requirements that are more

stringent (or of a higher standard) than the information protection principles.

30 Modification of information protection principles

(1) A privacy code of practice may modify the application to any public sector agency of any one or more of the information protection principles or the application to any public sector agency of the provisions of Part 6.

(2) A code may—

(a) specify requirements that are different from the requirements set out in the principles, or exempt any activity or conduct of or by the public sector agency from compliance with any such principle, and

(b) specify the manner in which any one or more of the information protection principles are to be applied to, or are to be followed by, the public sector agency, and

(c) exempt a public sector agency, or class of public sector agency, from the requirement to comply with any information protection principle.

31 Preparation and making of privacy codes of practice

(1) The Privacy Commissioner, or any public sector agency, may—

(a) initiate the preparation of a draft privacy code of practice, and

(b) develop the draft code in consultation with such other persons or bodies as the Commissioner, or agency, thinks appropriate, and

(c) submit the draft code to the Minister.

(2) If a draft code is initiated and prepared by a public sector agency, the agency must consult with the Privacy Commissioner on the draft code before it is submitted to the Minister.

(3) The Privacy Commissioner may make such submissions to the Minister in respect of a draft code as the Privacy Commissioner thinks appropriate.

(4) Once a draft code is submitted to the Minister, the Minister may, after taking into consideration any submissions by the Privacy Commissioner, decide to make the code.

(5) A code of practice is made by an order of the Minister published in the Gazette.

(6) A code takes effect when the order making the code is published (or on such later date as may be specified in the order).

(7) The procedures specified in this section extend to any amendment of a privacy code of practice.

Editorial note—

For the *Privacy Code of Practice (General) 2003* and amendments to that Code, see www.legislation.nsw.gov.au. For other codes of practice published under this section see Gazettes No 84 of 23.7.1999, p 5152; No 81 of 30.6.2000, pp 5981, 5993, 6004, 6007, 6020, 6024; No 83 of 30.6.2000, p 6035; No 143 of 3.11.2000, p 11568; No 170 of 29.12.2000, p 14069; No 46 of 2.3.2001, p 1133; No 93 of 1.6.2001, p 3395; No 199 of 28.12.2001, p 10853; No 104 of 25.6.2004, p 4812; No 85 of 24.8.2012, p 3781; No 17 of 5.3.2015, p 632; No 34 of 6.5.2016, p 1009; No 57 of 2.6.2017, p 1826; No 36 of 29.3.2018, p 1862; No 76 of 3.8.2018, p 5127; No 82 of 24.8.2018, p 5574 and No 179 of 20.12.2019, n2019-4051. From April 2021, PCO is no longer updating notes in provisions of in force titles about related gazette notices. To search for related gazette notices, please use the Gazette Search functionality.

32 Agencies to comply with privacy codes of practice

(1) A public sector agency must comply with any privacy code of practice applying to the agency.

(2) The contravention by a public sector agency of a privacy code of practice applying to the agency is conduct to which Part 5 applies.

Division 2 Privacy management plans

33 Preparation and implementation of privacy management plans

(1) Each public sector agency must have and implement a privacy management plan.

(2) The privacy management plan of a public sector agency must include provisions relating to the following—

(a) the devising of policies and practices to ensure compliance by the agency with the requirements of this Act or the *Health Records and Information Privacy Act 2002*, if applicable,

(b) the dissemination of those policies and practices to persons within the agency,

(c) the procedures that the agency proposes to provide in relation to internal review under Part 5,

(c1) the procedures and practices used by the agency to ensure compliance with the obligations and responsibilities set out in Part 6A for the mandatory notification of data breach scheme,

(d) such other matters as are considered relevant by the agency in relation to privacy and the protection of personal information held by the agency.

(3) (Repealed)

(4) An agency may amend its privacy management plan from time to time.

(5) An agency must provide a copy of its privacy management plan to the Privacy Commissioner as soon as practicable after it is prepared and whenever the plan is

amended.

(6) The regulations may make provision for or with respect to privacy management plans, including exempting certain public sector agencies (or classes of agencies) from the requirements of this section.

Part 4 Privacy Commissioner

Division 1 Appointment of Privacy Commissioner

34 Appointment of Privacy Commissioner

(1) The Governor may appoint a Privacy Commissioner.

(2) The Privacy Commissioner holds office for such term not exceeding 5 years as may be specified in the instrument of appointment, but is eligible (if otherwise qualified) for re-appointment.

(3) A person is not eligible to be appointed for more than 2 terms of office as Privacy Commissioner (whether or not consecutive terms).

(4) A person is not eligible to be appointed as Privacy Commissioner or to act in that office if the person is the Information Commissioner.

(5) A person is not eligible to be appointed as Privacy Commissioner or to act in that office if the person is a member of the Legislative Council or of the Legislative Assembly or is a member of a House of Parliament or legislature of another State or Territory or of the Commonwealth.

(6) The Privacy Commissioner may be appointed on a full-time or part-time basis. If the Privacy Commissioner is appointed to office on a full-time basis, the Privacy Commissioner is required to hold the office on that basis except to the extent permitted by the Governor.

35 Veto of proposed appointment of Privacy Commissioner

(1) A person is not to be appointed as Privacy Commissioner until—

(a) a proposal that the person be so appointed has been referred to the Joint Committee under section 31BA of the *Ombudsman Act 1974*, and

(b) the period that the Committee has under that section to veto the proposed appointment has ended without the Committee having vetoed the proposed appointment or the Committee notifies the Minister that it has decided not to veto the proposed appointment.

(2) A person may be proposed for appointment on more than one occasion.

(3) In this section, ***appointment*** includes re-appointment.

35A Remuneration

(1) The Privacy Commissioner is entitled to be paid—

(a) remuneration in accordance with the *Statutory and Other Offices Remuneration Act 1975*, and

(b) such travelling and subsistence allowances as the Minister may from time to time determine.

(2) The Privacy Commissioner is not, if a Judge of a New South Wales Court and while receiving remuneration as such a Judge, entitled to remuneration under this Act.

35B Vacancy in office

The office of Privacy Commissioner becomes vacant if the holder—

(a) dies, or

(b) completes a term of office and is not re-appointed, or

(c) resigns the office by instrument in writing addressed to the Governor, or

(d) is nominated for election as a member of the Legislative Council or of the Legislative Assembly or as a member of a House of Parliament or a legislature of another State or Territory or of the Commonwealth, or

(e) becomes bankrupt, applies to take the benefit of any law for the relief of bankrupt or insolvent debtors, compounds with his or her creditors or makes an assignment of his or her remuneration for their benefit, or

(f) becomes a mentally incapacitated person, or

(g) is convicted in New South Wales of an offence that is punishable by imprisonment for 12 months or more or is convicted elsewhere than in New South Wales of an offence that, if committed in New South Wales, would be an offence so punishable, or

(h) is removed from office under section 35C.

35C Removal from office

(1) The Governor may remove the Privacy Commissioner from office on the address of both Houses of Parliament.

(2) The Governor may suspend the Privacy Commissioner from office—

(a) for misbehaviour, or

(b) for incapacity, or

(c) if the Privacy Commissioner is absent from duty for a period in excess of his or her leave entitlement as approved by the Governor unless the absence is caused by illness or other unavoidable cause.

(3) The Minister is to lay or cause to be laid before each House of Parliament, within 7 sitting days of that House after the Privacy Commissioner has been suspended from office, a full statement of the grounds for the suspension.

(4) The suspension is to be lifted unless each House of Parliament, within 21 sitting days from the time when the statement was laid before it, declares by resolution that the Privacy Commissioner ought to be removed from office.

(5) If each House does so declare within that period, the Privacy Commissioner is to be removed from office by the Governor.

(6) For the purposes of this section, sitting days are to be counted whether or not they occur in the same session.

35D Filling of vacancy

If the office of Privacy Commissioner becomes vacant, a person is, subject to this Act, to be appointed to fill the vacancy.

35E Privacy Commissioner a statutory officer and not Public Service employee

The office of Privacy Commissioner is a statutory office and the provisions of the *Government Sector Employment Act 2013* relating to the employment of Public Service employees do not apply to that office.

35F Appointment of acting Privacy Commissioner

(1) The Minister may, from time to time, appoint a person to act in the office of the Privacy Commissioner during the illness or absence of the Privacy Commissioner or during a vacancy in the office of the Privacy Commissioner. The person, while so acting, has all the functions of the Privacy Commissioner and is taken to be the Privacy Commissioner.

(2) The Minister may, at any time, remove a person from office as acting Privacy Commissioner.

(3) An acting Privacy Commissioner is entitled to be paid such remuneration (including travelling and subsistence allowances) as the Minister may from time to time determine.

35G Staff of Privacy Commissioner

Persons may be employed in the Public Service under the *Government Sector Employment Act 2013* to enable the Privacy Commissioner to exercise his or her

functions.

Note—

Section 59 of the *Government Sector Employment Act 2013* provides that the persons so employed (or whose services the Privacy Commissioner makes use of) may be referred to as officers or employees, or members of staff, of the Privacy Commissioner. Section 47A of the *Constitution Act 1902* precludes the Privacy Commissioner from employing staff.

35H Delegation

The Privacy Commissioner may delegate the exercise of any function of the Privacy Commissioner (other than this power of delegation) to—

(a) any member of staff of the Privacy Commissioner, or

(b) any person, or any class of persons, authorised for the purposes of this section by the regulations.

Division 2 Functions of Privacy Commissioner

36 General functions

(1) The Privacy Commissioner has such functions as are conferred or imposed on the Commissioner by or under this or any other Act.

(2) In particular, the Privacy Commissioner has the following functions—

(a) to promote the adoption of, and monitor compliance with, the information protection principles,

(b) to prepare and publish guidelines relating to the protection of personal information and other privacy matters, and to promote the adoption of such guidelines,

(c) to initiate and recommend the making of privacy codes of practice,

(d) to provide assistance to public sector agencies in adopting and complying with the information protection principles, privacy codes of practice and the mandatory notification of data breach scheme,

(e) to provide assistance to public sector agencies in preparing and implementing—

(i) privacy management plans under section 33, and

(ii) data breach policies under section 59ZD,

(f) to conduct research, and collect and collate information, about any matter relating to the protection of personal information and the privacy of individuals,

(g) to provide advice on matters relating to the protection of personal information and the privacy of individuals,

(h) to make public statements about any matter relating to the privacy of individuals generally,

(i) to conduct education programs, and to disseminate information, for the purpose of promoting the protection of the privacy of individuals,

(j) to prepare and publish reports and recommendations about any matter (including developments in technology) that concerns the need for, or the desirability of, legislative, administrative or other action in the interest of the privacy of individuals,

(k) to receive, investigate and conciliate complaints about privacy related matters (including conduct to which Part 5 applies),

(l) to conduct such inquiries, and make such investigations, into privacy related matters as the Privacy Commissioner thinks appropriate,

(m) to investigate, monitor, audit and report on a public sector agency's compliance with Part 6A, including the agency's data handling systems, policies and practices.

(3) The Privacy Commissioner must consult with the Information Commissioner before preparing any guidelines concerning the information protection principle set out in section 18 (Limits on disclosure of personal information).

37 Requirement to give information

(1) The Privacy Commissioner may, in connection with the exercise of the Privacy Commissioner's functions, require any person or public sector agency—

(a) to give the Privacy Commissioner a statement of information, or

(b) to produce to the Privacy Commissioner any document or other thing, or

(c) to give the Privacy Commissioner a copy of any document.

(2) The Privacy Commissioner is not to make any such requirement if it appears to the Privacy Commissioner that—

(a) the person or public sector agency concerned does not consent to compliance with the requirement, and

(b) the person or public sector agency would not, in court proceedings, be required to comply with a similar requirement on the grounds of public interest, privilege against self-incrimination or legal professional privilege.

(3) A requirement under this section must be in writing, must specify or describe the information, document or thing required, and must specify the time and manner for complying with the requirement.

(4) This section does not confer any function on the Privacy Commissioner that may be exercised in relation to the Independent Commission Against Corruption.

38 Inquiries and investigations

(1) For the purposes of any inquiry or investigation conducted by the Privacy Commissioner under this Act (including in relation to a complaint made under Division 3 of this Part), the Privacy Commissioner has the powers, authorities, protections and immunities conferred on a commissioner by Division 1 of Part 2 of the *Royal Commissions Act 1923*, and that Act (section 13 and Division 2 of Part 2 excepted) applies (subject to this section) to any witness summoned by or appearing before the Privacy Commissioner in the same way as it applies to a witness summoned by or appearing before a commissioner.

(2) Subsection (1) does not confer any function on the Privacy Commissioner that may be exercised in relation to the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the staff of the Inspector of the Independent Commission Against Corruption, Law Enforcement Conduct Commission, Inspector of the Law Enforcement Conduct Commission, staff of the Inspector of the Law Enforcement Conduct Commission or New South Wales Crime Commission.

(3) Any inquiry or investigation conducted by the Privacy Commissioner under this Act is to be conducted in the absence of the public, except as otherwise directed by the Privacy Commissioner.

(4) The Privacy Commissioner, in the course of conducting an inquiry or investigation under this Act, must set aside any requirement—

(a) to give any statement of information, or

(b) to produce any document or other thing, or

(c) to give a copy of any document, or

(d) to answer any question,

if it appears to the Privacy Commissioner that the person concerned does not consent to compliance with the requirement and the person would not, in court proceedings, be required to comply with a similar requirement on the grounds of public interest, privilege against self-incrimination or legal professional privilege. However, the person must comply with any such requirement despite any duty of secrecy or other restriction on disclosure.

(5) A person is not entitled to be represented by another person at an inquiry or investigation conducted by the Privacy Commissioner except with the leave of the Privacy Commissioner.

(6) The Privacy Commissioner may allow any person appearing before the Privacy Commissioner to have the services of an interpreter.

39 General procedure for inquiries and investigations

The Privacy Commissioner—

(a) may determine the procedures to be followed in exercising the Privacy Commissioner's functions under this Act, including the procedures to be followed at an inquiry or investigation conducted by the Privacy Commissioner, and

(b) is to act in an informal manner (including avoiding conducting formal hearings) as far as possible, and

(c) is not bound by the rules of evidence and may inform himself or herself on any matter in any way that the Privacy Commissioner considers to be just, and

(d) is to act according to the substantial merits of the case without undue regard to technicalities.

40 Personal information digest

(1) The Privacy Commissioner may, from time to time, prepare and publish a personal information digest setting out the nature and source of personal information held by public sector agencies.

(2) Any such personal information digest is to be made publicly available.

(3) The Privacy Commissioner may, from time to time, require a public sector agency to provide the Privacy Commissioner with such details relating to the personal information held by the agency as the Commissioner may require. The public sector agency must comply with the requirement.

(4) This section does not apply to personal information held by the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the staff of the Inspector of the Independent Commission Against Corruption, the Law Enforcement Conduct Commission, the Inspector of the Law Enforcement Conduct Commission, the staff of the Inspector of the Law Enforcement Conduct Commission or the New South Wales Crime Commission.

41 Exempting agencies from complying with principles and codes

(1) The Privacy Commissioner, with the approval of the Minister, may make a written direction that—

(a) a public sector agency is not required to comply with an information protection principle or a privacy code of practice, or

(b) the application of a principle or a code to a public sector agency is to be modified

as specified in the direction.

(2) Any such direction has effect despite any other provision of this Act.

(3) The Privacy Commissioner is not to make a direction under this section unless the Privacy Commissioner is satisfied that the public interest in requiring the public sector agency to comply with the principle or code is outweighed by the public interest in the Privacy Commissioner making the direction.

42 Information about compliance arrangements

(1) The Privacy Commissioner may require a public sector agency to provide the Commissioner with information concerning the arrangements that have been made by the agency to enable the agency to comply with the information protection principles, and any privacy code of practice, applying to the agency.

(2) Any such requirement must be in writing and specify a time for complying with the requirement.

(3) This section does not confer any function on the Privacy Commissioner that may be exercised in relation to the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the staff of the Inspector of the Independent Commission Against Corruption, Law Enforcement Conduct Commission, Inspector of the Law Enforcement Conduct Commission, staff of the Inspector of the Law Enforcement Conduct Commission, New South Wales Crime Commission or Ombudsman's Office.

43 Disclosure of Cabinet or Executive Council information

(1) Nothing in this Act or the *Health Records and Information Privacy Act 2002* authorises the Privacy Commissioner to require any person or public sector agency to disclose Cabinet information or Executive Council information.

(2) The Secretary or General Counsel of the Cabinet Office may certify that information is Cabinet information. Any such certificate—

(a) is conclusive of that fact, and

(b) authorises any person or agency who would otherwise be required under this Act or the *Health Records and Information Privacy Act 2002* to disclose the information concerned to refuse to disclose it.

(3) In this section—

Cabinet information means information that is Cabinet information under the *Government Information (Public Access) Act 2009*.

Executive Council information means information that is Executive Council

information under the *Government Information (Public Access) Act 2009*.

44 (Repealed)

44A Oversight of functions by Joint Committee

(1) The Joint Committee has the following functions under this Act—

(a) to monitor and review the exercise by the Privacy Commissioner of the Privacy Commissioner's functions,

(b) to report to both Houses of Parliament, with such comments as it thinks fit, on any matter appertaining to the Privacy Commissioner or connected with the exercise of the Privacy Commissioner's functions to which, in the opinion of the Joint Committee, the attention of Parliament should be directed,

(c) to examine each annual and other report of the Privacy Commissioner and report to both Houses of Parliament on any matter appearing in, or arising out of, any such report,

(d) to recommend to both Houses of Parliament any changes to the functions of the Privacy Commissioner that the Joint Committee thinks desirable,

(e) to inquire into any question in connection with its functions which is referred to it by both Houses of Parliament, and report to both Houses on that question.

(2) Nothing in this section authorises the Joint Committee—

(a) to investigate a matter relating to any particular conduct, or

(b) to reconsider any decision to investigate, not to investigate or to discontinue investigation of any particular matter, or

(c) to reconsider the findings, recommendations or other decisions of the Privacy Commissioner in relation to any particular matter.

(3) The provisions of Part 4A of the *Ombudsman Act 1974* apply in relation to the Joint Committee's functions under this Act in the same way as they apply in relation to the Joint Committee's functions under that Act.

(4) In this section—

Joint Committee means the Committee on the Ombudsman, the Law Enforcement Conduct Commission and the Crime Commission constituted under the *Ombudsman Act 1974* or such other joint committee of members of Parliament as may be appointed to exercise the functions of the Joint Committee under this Act.

Division 3 Complaints relating to privacy

45 Making of privacy related complaints

(1) A complaint may be made to (or by) the Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual.

(2) The subject-matter of a complaint may relate to conduct to which Part 5 applies (unless it is conduct that is alleged to have occurred before the commencement of that Part).

Note—

Section 21 of the *Health Records and Information Privacy Act 2002* provides that certain conduct under that Act by public sector agencies is conduct to which Part 5 of this Act applies.

(2A) A complaint about a matter referred to in section 42 of the *Health Records and Information Privacy Act 2002* is not to be dealt with under this Division but is to be dealt with by the Privacy Commissioner as a complaint under Part 6 of that Act.

Note—

Section 42 of that *Health Records and Information Privacy Act 2002* provides that a complaint may be made to the Privacy Commissioner about the alleged contravention by a private sector person of a Health Privacy Principle, a provision of Part 4 (Provisions for private sector persons) of that Act or a health privacy code of practice.

(3) A complaint may be in writing or verbal, but the Privacy Commissioner may require a verbal complaint to be put in writing.

(4) The Privacy Commissioner may require information about a complaint to be provided by the complainant in a particular manner or form, and may require a complaint to be verified by statutory declaration.

(5) A complaint must be made within 6 months (or such later time as the Privacy Commissioner may allow) from the time the complainant first became aware of the conduct or matter the subject of the complaint.

(6) A complainant may amend or withdraw a complaint.

46 Preliminary assessment of privacy related complaints

(1) The Privacy Commissioner may conduct a preliminary assessment of a complaint made under this Division for the purpose of deciding whether to deal with the complaint.

(2) If the subject-matter of the complaint relates to conduct to which Part 5 applies, the Privacy Commissioner must inform the complainant of the review process under that Part and the remedial action that may be available if the complainant decides to make an application under section 53 in respect of that conduct.

(3) The Privacy Commissioner may decide not to deal with a complaint if the Privacy Commissioner is satisfied that—

(a) the complaint is frivolous, vexatious or lacking in substance, or is not in good faith, or

(b) the subject-matter of the complaint is trivial, or

(c) the subject-matter of the complaint relates to a matter permitted or required by or under any law, or

(d) there is available to the complainant an alternative, satisfactory and readily available means of redress, or

(e) it would be more appropriate for the complainant to make an application under section 53.

47 Referring privacy related complaints to other authorities

(1) The Privacy Commissioner may refer a complaint made under this Division for investigation or other action to any person or body (***the relevant authority***) considered by the Privacy Commissioner to be appropriate in the circumstances.

(2) The Privacy Commissioner may communicate to the relevant authority any information that the Privacy Commissioner has obtained in relation to the complaint.

(3) The Privacy Commissioner may only refer a complaint to a relevant authority after appropriate consultation with the complainant and the relevant authority, and after taking their views into consideration.

48 Dealing with privacy related complaints

(1) If the Privacy Commissioner decides to deal with a complaint made under this Division, the Privacy Commissioner may—

(a) deal with the complaint, and

(b) make such inquiries and investigations in relation to the complaint as the Privacy Commissioner thinks appropriate.

(2) If the Privacy Commissioner declines to deal with a complaint, the Privacy Commissioner must advise the complainant of the reasons for declining to deal with the complaint.

49 Resolution of privacy related complaints by conciliation

(1) In dealing with a complaint made under this Division, the Privacy Commissioner must endeavour to resolve the complaint by conciliation.

(2) The Privacy Commissioner may by written notice request the complainant, and the person or body against whom the complaint is made (***the respondent***), to appear before the Privacy Commissioner in conciliation proceedings.

(3) If a respondent that is a public sector agency receives any such notice, the agency must comply with the terms of the notice.

Maximum penalty (subsection (3)): 50 penalty units.

(4) The parties to any such conciliation proceedings before the Privacy Commissioner are not entitled to be represented by any other person except by leave of the Privacy Commissioner.

(5) The procedures for conciliation are to be determined by the Privacy Commissioner.

50 Reports and recommendations of Privacy Commissioner

(1) The Privacy Commissioner may make a written report as to any findings or recommendations by the Privacy Commissioner in relation to a complaint dealt with by the Commissioner under this Division.

(2) The Privacy Commissioner may give a copy of any such report to the complainant, and to such other persons or bodies as appear to be materially involved in matters concerning the complaint.

51 Effect of dealing with privacy related complaints under this Division

Even though the Privacy Commissioner declines to deal with a complaint under this Division, or decides to refer the complaint to a relevant authority, the Privacy Commissioner may conduct an inquiry or investigation into any general issues or matters raised in connection with the complaint.

Part 5 Review of certain conduct

52 Application of Part

(1) This Part applies to the following conduct—

(a) the contravention by a public sector agency of an information protection principle that applies to the agency,

(b) the contravention by a public sector agency of a privacy code of practice that applies to the agency,

(c) the disclosure by a public sector agency of personal information kept in a public register.

(2) A reference in this Part to conduct includes a reference to alleged conduct.

(3) This Part does not apply to any conduct that occurred before the commencement of this Part.

(4) Section 53 (Internal reviews) of the *Administrative Decisions Review Act 1997* does not apply to or in respect of conduct to which this Part applies.

53 Internal review by public sector agencies

(1) A person (***the applicant***) who is aggrieved by the conduct of a public sector agency is entitled to a review of that conduct.

(1A) There is no entitlement under this section to the review of the conduct of a Minister (or a Minister's personal staff) in respect of a contravention of section 15 (Alteration of personal information).

Note—

Any such conduct can still be administratively reviewed by the Tribunal. See section 55 (1A).

(2) The review is to be undertaken by the public sector agency concerned.

(3) An application for such a review must—

(a) be in writing, and

(b) be addressed to the public sector agency concerned, and

(c) specify an address in Australia to which a notice under subsection (8) may be sent, and

(d) be lodged at an office of the public sector agency within 6 months (or such later date as the agency may allow) from the time the applicant first became aware of the conduct the subject of the application, and

(e) comply with such other requirements as may be prescribed by the regulations.

(4) Except as provided by section 54 (3), the application must be dealt with by an individual within the public sector agency who is directed by the agency to deal with the application. That individual must be, as far as is practicable, a person—

(a) who was not substantially involved in any matter relating to the conduct the subject of the application, and

(b) who is an employee or officer of the agency, and

(c) who is otherwise suitably qualified to deal with the matters raised by the application.

(5) In reviewing the conduct the subject of the application, the individual dealing with the application must consider any relevant material submitted by—

(a) the applicant, and

(b) the Privacy Commissioner.

(6) The review must be completed as soon as is reasonably practicable in the circumstances. However, if the review is not completed within 60 days from the day on which the application was received, the applicant is entitled to make an application under section 55 to the Tribunal for an administrative review of the conduct concerned.

(7) Following the completion of the review, the public sector agency whose conduct was the subject of the application may do any one or more of the following—

(a) take no further action on the matter,

(b) make a formal apology to the applicant,

(c) take such remedial action as it thinks appropriate (eg the payment of monetary compensation to the applicant),

(d) provide undertakings that the conduct will not occur again,

(e) implement administrative measures to ensure that the conduct will not occur again.

(7A) A public sector agency may not pay monetary compensation under subsection (7) if—

(a) the applicant is a convicted inmate or former convicted inmate or a spouse, partner (whether of the same or the opposite sex), relative, friend or an associate of a convicted inmate or former convicted inmate, and

(b) the application relates to conduct of a public sector agency in relation to the convicted inmate or former convicted inmate, and

(c) the conduct occurred while the convicted inmate or former convicted inmate was a convicted inmate, or relates to any period during which the convicted inmate or former convicted inmate was a convicted inmate.

(8) As soon as practicable (or in any event within 14 days) after the completion of the review, the public sector agency must notify the applicant in writing of—

(a) the findings of the review (and the reasons for those findings), and

(b) the action proposed to be taken by the agency (and the reasons for taking that action), and

(c) the right of the person to have those findings, and the agency’s proposed action, administratively reviewed by the Tribunal.

54 Role of Privacy Commissioner in internal review process

(1) A public sector agency that receives an application under section 53 must—

(a) as soon as practicable after receiving the application notify the Privacy Commissioner of the application, and

(b) keep the Privacy Commissioner informed of the progress of the internal review, and

(c) inform the Privacy Commissioner of the findings of the review and of the action proposed to be taken by the agency in relation to the matter.

(2) The Privacy Commissioner is entitled to make submissions to the agency in relation to the subject matter of the application.

(3) The Privacy Commissioner may, at the request of the agency concerned—

(a) undertake the internal review on behalf of the agency, and

(b) make a report to the agency in relation to the application.

(4) The Privacy Commissioner is entitled to charge an appropriate fee for that service.

(5) Section 53 (7), (7A) and (8) apply in respect of an internal review that is undertaken by the Privacy Commissioner on behalf of an agency.

55 Administrative review of conduct by Tribunal

(1) If a person who has made an application for internal review under section 53 is not satisfied with—

(a) the findings of the review, or

(b) the action taken by the public sector agency in relation to the application,

the person may apply to the Civil and Administrative Tribunal for an administrative review under the *Administrative Decisions Review Act 1997* of the conduct that was the subject of the application under section 53.

(1A) A person (***the applicant***) who is aggrieved by the conduct of a Minister (or a Minister's personal staff) constituting a contravention of section 15 (Alteration of personal information) may apply to the Civil and Administrative Tribunal for an administrative review under the *Administrative Decisions Review Act 1997* of the conduct.

(2) On reviewing the conduct of the public sector agency concerned, the Tribunal may decide not to take any action on the matter, or it may make any one or more of the following orders—

(a) subject to subsections (4) and (4A), an order requiring the public sector agency to pay to the applicant damages not exceeding $40,000 by way of compensation for any loss or damage suffered because of the conduct,

(b) an order requiring the public sector agency to refrain from any conduct or action in contravention of an information protection principle or a privacy code of practice,

(c) an order requiring the performance of an information protection principle or a privacy code of practice,

(d) an order requiring personal information that has been disclosed to be corrected by the public sector agency,

(e) an order requiring the public sector agency to take specified steps to remedy any loss or damage suffered by the applicant,

(f) an order requiring the public sector agency not to disclose personal information contained in a public register,

(g) such ancillary orders as the Tribunal thinks appropriate.

(3) Nothing in this section limits any other powers that the Tribunal has under Division 3 of Part 3 of Chapter 3 of the *Administrative Decisions Review Act 1997*.

(4) The Tribunal may make an order under subsection (2) (a) only if—

(a) the application relates to conduct that occurs after the end of the 12 month period following the date on which Division 1 of Part 2 commences, and

(b) the Tribunal is satisfied that the applicant has suffered financial loss, or psychological or physical harm, because of the conduct of the public sector agency.

(4A) The Tribunal may not make an order under subsection (2) (a) if—

(a) the applicant is a convicted inmate or former convicted inmate or a spouse, partner (whether of the same or the opposite sex), relative, friend or an associate of a convicted inmate or former convicted inmate, and

(b) the application relates to conduct of a public sector agency in relation to the convicted inmate or former convicted inmate, and

(c) the conduct occurred while the convicted inmate or former convicted inmate was a convicted inmate, or relates to any period during which the convicted inmate or former convicted inmate was a convicted inmate.

(5) If, in the course of an administrative review, the Tribunal is of the opinion that the

chief executive officer or an employee of the public sector agency concerned has failed to exercise in good faith a function conferred or imposed on the officer or employee by or under this Act (including by or under a privacy code of practice), the Tribunal may take such measures as it considers appropriate to bring the matter to the attention of the responsible Minister (if any) for the public sector agency.

(6) The Privacy Commissioner is to be notified by the Tribunal of any application for an administrative review. The Privacy Commissioner has a right to appear and be heard in any proceedings before the Tribunal in relation to an administrative review.

(7) The Information Commissioner is to be notified by the Tribunal of any application for a review under this section that concerns the provision of government information by an agency (within the meaning of the *Government Information (Public Access) Act 2009*). The Information Commissioner has a right to appear and be heard in any proceedings before the Tribunal in relation to such a review.

56 (Repealed)

Part 6 Public registers

56A Personal information includes health information

In this Part—

personal information includes health information within the meaning of the *Health Records and Information Privacy Act 2002*.

57 Disclosure of personal information contained in public registers

(1) The public sector agency responsible for keeping a public register must not disclose any personal information kept in the register unless the agency is satisfied that it is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept.

(2) In order to enable the responsible agency to comply with subsection (1), the agency may require any person who applies to inspect personal information contained in the public register to give particulars, in the form of a statutory declaration, as to the intended use of any information obtained from the inspection.

58 Suppression of personal information

(1) A person about whom personal information is contained (or proposed to be contained) in a public register may request the public sector agency responsible for keeping the register to have the information—

(a) removed from, or not placed on, the register as publicly available, and

(b) not disclosed to the public.

(2) If the public sector agency is satisfied that the safety or well-being of any person would be affected by not suppressing the personal information as requested, the agency must suppress the information in accordance with the request unless the agency is of the opinion that the public interest in maintaining public access to the information outweighs any individual interest in suppressing the information.

(3) Any information that is removed from, or not placed on, a public register under this section may be kept on the register for other purposes.

59 Provisions of this Part prevail

The provisions of this Part prevail to the extent of any inconsistency with the requirements of the law under which the public register concerned is established.

Part 6A Mandatory notification of data breaches

Division 1 Preliminary

59A Definitions

In this Part—

affected individual—see section 59D(2).

approved form means a form approved under section 59ZH.

assessment—see section 59E(2)(b).

assessor—see section 59G(1).

eligible data breach—see section 59D(1).

head, of a public sector agency, means—

(a) for a Public Service agency—the person who is the head of the Public Service agency within the meaning of the *Government Sector Employment Act 2013*, or

(b) otherwise—the person who is the chief executive officer, however described, of the agency or otherwise responsible for the agency's day to day management.

health privacy code of practice has the same meaning as in the *Health Records and Information Privacy Act 2002*.

Health Privacy Principle has the same meaning as in the *Health Records and Information Privacy Act 2002* and a reference in this Part to a Health Privacy Principle by number is a reference to the clause of Schedule 1 of that Act with that number.

held, in relation to personal information—see section 59C.

59B Personal information includes health information

In this Part, ***personal information*** includes health information within the meaning of the *Health Records and Information Privacy Act 2002*.

59C Meaning of information "held" by public sector agency for Part

For the purposes of this Part, personal information is ***held*** by a public sector agency if—

(a) the agency is in possession or control of the information, or

(b) the information is contained in a State record in respect of which the agency is responsible under the *State Records Act 1998*.

59D Meaning of eligible data breach and affected individual

(1) For the purposes of this Part, an ***eligible data breach*** means—

(a) there is unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency and a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates, or

(b) personal information held by a public sector agency is lost in circumstances where—

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

(ii) if the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.

(2) An individual specified in subsection (1)(a) or (1)(b)(ii) is an ***affected individual***.

(3) To avoid doubt, an eligible data breach may include the following—

(a) a data breach that occurs within a public sector agency,

(b) a data breach that occurs between public sector agencies,

(c) a data breach that occurs by an external person or entity accessing data held by a public sector agency without authorisation.

Division 2 Assessment of data breaches

59E Requirements for public sector agency

(1) This section applies if an officer or employee of a public sector agency is aware that

there are reasonable grounds to suspect there may have been an eligible data breach of the agency.

(2) The officer or employee must report the data breach to the head of the public sector agency and the head of the agency must—

(a) immediately make all reasonable efforts to contain the data breach, and

(b) within 30 days after the officer or employee of the agency becomes aware as mentioned in subsection (1)—carry out an assessment of whether the data breach is, or there are reasonable grounds to believe the data breach is, an eligible data breach (an ***assessment***).

(3) An assessment must be carried out in an expeditious way.

(4) Subsection (2)(b) is subject to an extension approved under section 59K.

59F Mitigation of harm

During an assessment, the head of the public sector agency the subject of the suspected breach must make all reasonable attempts to mitigate the harm done by the suspected breach.

59G Assessors

(1) The head of a public sector agency may direct one or more persons to carry out the assessment (each an ***assessor***).

(2) An assessor may be—

(a) an officer or employee of the agency the subject of the data breach, or

(b) an officer or employee of another public sector agency acting on behalf of the public sector agency the subject of the data breach, or

(c) a person acting on behalf of the public sector agency the subject of the data breach, or a person employed by that person.

Example for paragraph (c)—

An individual employed by a third party to carry out the assessment for the public sector agency the subject of the data breach.

(3) However, a person who the head of the agency reasonably suspects was involved in an action or omission that led to the breach is not permitted to be an assessor.

(4) An assessor must take all reasonable steps to ensure the assessment is completed within 30 days after the officer or employee of the agency becomes aware under section 59E(1).

(5) In this section—

employee includes an individual engaged by the public sector agency under a contract.

59H Assessment of data breach—factors for consideration

Without limiting the factors that may be considered by the assessor carrying out the assessment, the assessor may consider the following—

(a) the types of personal information involved in the breach,

(b) the sensitivity of the personal information involved in the breach,

(c) whether the personal information is or was protected by security measures,

(d) the persons to whom the unauthorised access to, or unauthorised disclosure of, the personal information involved in the breach was, or could be, made or given,

(e) the likelihood the persons specified in paragraph (d)—

(i) have or had the intention of causing harm, or

(ii) could or did circumvent security measures protecting the information,

(f) the nature of the harm that has occurred or may occur,

(g) other matters specified in guidelines issued by the Privacy Commissioner about whether the disclosure is likely to result in serious harm to an individual to whom the personal information relates.

59I Guidelines about process for assessing data breach

An assessor must have regard to the guidelines, prepared by the Privacy Commissioner, about the process for carrying out an assessment.

Note—

See section 59ZI in relation to guidelines made under this Part.

59J Decision about data breach

(1) Following an assessment, the assessor must advise the head of the public sector agency whether the assessment found—

(a) the data breach is an eligible data breach, or

(b) there are reasonable grounds to believe the data breach is an eligible data breach.

(2) After receiving the assessor’s advice, the head of the agency must decide whether—

(a) the data breach is an eligible data breach, or

(b) there are reasonable grounds to believe the data breach is an eligible data breach.

59K Extension of assessment period by head of public sector agency

(1) If the head of a public sector agency is satisfied an assessment cannot reasonably be conducted within 30 days, the head of the agency may approve an extension of the period to conduct the assessment.

(2) The extension may be approved for an amount of time reasonably required for the assessment to be conducted (an ***extension period***).

(3) If an extension is approved, the head of the agency must, within the 30-day period referred to in section 59E(2)—

(a) start the assessment, and

(b) give written notice to the Privacy Commissioner—

(i) that the assessment has started, and

(ii) that the head of the agency has approved an extension of the period for the assessment, and

(iii) specifying the extension period.

(4) If the assessment is not conducted within the extension period, the head of the agency must, before the end of the extension period, give written notice to the Privacy Commissioner—

(a) that the assessment is ongoing, and

(b) that the head of the agency has approved a new extension period for the assessment, and

(c) specifying the new extension period.

(5) The Privacy Commissioner may ask the head of the agency for further information about the progress of the assessment.

Division 3 Notification of data breaches to Privacy Commissioner

Subdivision 1 Application

59L Application of Division

(1) This Division applies if the head of the public sector agency decides under Division 2 that an eligible data breach occurred.

(2) For the purposes of subsection (1), an eligible data breach is taken to have occurred if the head of the agency decides under Division 2 there are reasonable grounds to believe the data breach is an eligible data breach.

Subdivision 2 Immediate notification to Privacy Commissioner

59M Public sector agencies must immediately notify eligible data breach

(1) The head of a public sector agency must, in the approved form, immediately notify the Privacy Commissioner of the eligible data breach.

(2) The approved form must request the following information be provided in relation to the eligible data breach—

(a) the information specified in section 59O, other than the information specified in section 59O(e),

(b) a description of the personal information that was the subject of the breach,

(c) whether the head of the agency is reporting on behalf of other agencies involved in the same breach,

(d) if the head of the agency is reporting on behalf of other agencies involved in the same breach—the details of the other agencies,

(e) whether the breach is a cyber incident,

(f) if the breach is a cyber incident—details of the cyber incident,

(g) the estimated cost of the breach to the agency,

(h) the total number, or estimated total number, of individuals—

(i) affected or likely to be affected by the breach, and

(ii) notified of the breach,

(i) whether the individuals notified under section 59N(1) have been advised of the complaints and internal review procedures under the Act.

(3) The information requested by the approved form must be completed unless it is not reasonably practicable for the information to be provided.

Subdivision 3 Notification of eligible data breach

59N Public sector agencies must notify certain individuals

(1) As soon as practicable after the head of a public sector agency decides an eligible data breach occurred, the head of the agency must, to the extent that it is reasonably practicable, take the steps that are reasonable in the circumstances to notify—

(a) each individual to whom the personal information the subject of the breach relates, or

(b) each affected individual.

(2) However, if the head of the agency is unable to notify, or if it is not reasonably practicable for the head of the agency to notify, any or all of the individuals specified in subsection (1), the head of the agency must—

(a) publish a notification under section 59P, and

(b) take reasonable steps to publicise the notification.

59O Information to be notified to certain individuals

A notification given under section 59N(1) must, if it is reasonably practicable for the information to be provided, include the following information in relation to each eligible data breach—

(a) the date the breach occurred,

(b) a description of the breach,

(c) how the breach occurred,

(d) the type of breach that occurred,

Examples of a type of eligible data breach—

1 unauthorised disclosure

2 unauthorised access

3 loss of information

(e) the personal information that was the subject of the breach,

(f) the amount of time the personal information was disclosed for,

(g) actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to the individual,

(h) recommendations about the steps the individual should take in response to the eligible data breach,

(i) information about—

(i) the making of privacy related complaints under Part 4, Division 3, and

(ii) internal reviews of certain conduct of public sector agencies under Part 5,

(j) the name of the public sector agency the subject of the breach,

(k) if more than 1 public sector agency was the subject of the breach—the name of each other agency,

(l) contact details for—

(i) the agency the subject of the breach, or

(ii) a person nominated by the agency for the individual to contact about the breach.

59P Public notification

(1) This section applies if—

(a) a notification is required to be given under section 59N(2), or

(b) the head of an agency decides to give a notification under this section.

(2) The head of a public sector agency must keep a register that is available on the public sector agency's website (a ***public notification register***).

(3) The notification must, if it is reasonably practicable for the information to be provided—

(a) be published on the public notification register for at least 12 months after the date the notification is published, and

(b) include the information specified in section 59O, except to the extent the information—

(i) contains personal information, or

(ii) would prejudice the agency's functions.

(4) As soon as practicable after the notification is published, the agency must provide the Privacy Commissioner with information about how to access the notification on the public notification register.

(5) The Privacy Commissioner must publish on the Privacy Commissioner's website information about how to access the notification for at least 12 months after the date the notification is published.

Example of information about how to access a notification—

A link to the website on which the notification is published.

Subdivision 4 Other matters for notification

59Q Further information to be provided to the Privacy Commissioner

(1) The head of a public sector agency must, in the approved form, notify the Privacy Commissioner of the information that was not given to the Privacy Commissioner as part of the immediate notification under section 59M.

(2) The further information must be given—

(a) following notification under section 59N(1) or (2), or

(b) if an exemption under Division 4 applies—following the head of the agency determining that an exemption applies.

59R Collecting, using and disclosing information for notification

(1) A public sector agency the subject of an eligible data breach may do the following—

(a) use relevant personal information,

(b) collect relevant personal information from another public sector agency,

(c) disclose relevant personal information to another public sector agency.

(2) Also, a public sector agency may disclose relevant personal information to a public sector agency the subject of an eligible data breach.

(3) Information may be collected, used or disclosed under this section only if it is reasonably necessary for the purpose of confirming—

(a) the name and contact details of a notifiable individual, or

(b) whether a notifiable individual is deceased.

(4) A public sector agency is not required to comply with an information protection principle, a Health Privacy Principle, a privacy code of practice or a health privacy code of practice in relation to the use, collection or disclosure of relevant personal information in accordance with subsection (1) or (2).

(5) In this section, a reference to an eligible data breach extends to a suspected breach within the meaning of section 59Y(1), if the Privacy Commissioner makes a recommendation under the section.

(6) This section applies despite any other provision of this Act.

(7) In this section—

identifier means an identifier, not being an identifier that consists only of the individual's name, which is usually, but need not be, a number, that is—

(a) assigned to an individual in conjunction with or in relation to the individual's personal information by an organisation for the purpose of uniquely identifying that individual, whether or not it is subsequently used other than in conjunction with or in relation to personal information, or

(b) adopted, used or disclosed in conjunction with or in relation to the individual's personal information by an organisation for the purpose of uniquely identifying the individual.

***notifiable individual*—**

(a) means an individual specified in section 59N(1), and

(b) includes a notifiable individual within the meaning of section 59Y.

relevant personal information means the following—

(a) the name of an individual,

(b) the contact details of the individual,

(c) the date of birth of the individual,

(d) an identifier for the individual,

(e) if the individual is deceased—the date of death of the individual.

Division 4 Exemptions from certain requirements for an eligible data breach

59S Exemption for eligible data breaches of multiple public sector agencies

(1) This section applies if—

(a) the access, disclosure or loss that constituted an eligible data breach of the public sector agency is a breach of at least 1 other public sector agency, and

(b) an assessment has been carried out for each of the public sector agencies involved in the breach under Division 2, and

(c) the heads of each of the public sector agencies involved in the breach have notified the Privacy Commissioner under section 59M.

(2) The head of a public sector agency is exempt from Division 3, Subdivision 3 if the head of another public sector agency involved in the same breach undertakes to notify the eligible data breach under the Subdivision.

59T Exemption relating to ongoing investigations and certain proceedings

The head of a public sector agency is exempt from Division 3, Subdivision 3 to the extent that the head of the agency reasonably believes notification of the eligible data breach under the Subdivision would be likely to prejudice—

(a) an investigation that could lead to the prosecution of an offence, or

(b) proceedings before a court or a tribunal, or

(c) another matter prescribed by the regulations for the purposes of this section.

59U Exemption if public sector agency has taken certain action

The head of a public sector agency is exempt from Division 3, Subdivision 3 if—

(a) for an eligible data breach involving unauthorised access to, or disclosure of, personal information held by the agency—

(i) the agency the subject of the breach takes action to mitigate the harm done by the breach, and

(ii) the action is taken before the access to or disclosure of information results in serious harm to an individual, and

(iii) because of the action taken, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to an individual, or

(b) for an eligible data breach involving the loss of personal information held by the agency—

(i) the agency the subject of the breach takes action to mitigate the loss, and

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

(iii) because of the action taken, there is no unauthorised access to, or unauthorised disclosure of, the information.

59V Exemption if inconsistent with secrecy provisions

(1) If compliance with Division 3, Subdivision 3 by the head of a public sector agency would be inconsistent with a secrecy provision, the head of the agency is exempt from Division 3, Subdivision 3 to the extent of the inconsistency.

(2) In this section—

secrecy provision means a provision—

(a) of an Act or statutory rule, other than this Act, and

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

59W Exemption if serious risk of harm to health and safety

(1) The head of a public sector agency may decide to exempt the agency from Division 3, Subdivision 3 for an eligible data breach to the extent that the head of the agency reasonably believes notification would create a serious risk of harm to an individual's health or safety.

(2) In making a decision under subsection (1), the head of the agency—

(a) must consider the extent to which the harm of notifying the breach is greater than

the harm of not notifying the breach, and

(b) must consider the currency of the information relied on in assessing the serious risk of harm to an individual, and

(c) must not search data held by the agency, or require or permit the search of data held by the agency, that was not affected by the breach, to assess the impact of notification, unless the head of the agency knows, or reasonably believes, there is information in the data relevant to whether an exemption under this section applies.

(3) The head of the agency must have regard to the guidelines, prepared by the Privacy Commissioner, in making a decision to exempt the agency under this section.

(4) The exemption may be—

(a) permanent, or

(b) for a specified period, or

(c) until the happening of a particular thing.

(5) The head of the agency must, by written notice given to the Privacy Commissioner, notify the Privacy Commissioner—

(a) that the exemption under this section is relied on, and

(b) the details about whether the exemption is permanent or temporary, and

(c) if the exemption is temporary—of the specified or expected time the exemption is to be relied on.

59X Exemption for compromised cyber security

(1) The head of a public sector agency may decide to exempt the agency from Division 3, Subdivision 3 for an eligible data breach if the head of the agency reasonably believes notification would—

(a) worsen the agency's cyber security, or

(b) lead to further data breaches.

(2) The head of the agency must have regard to the guidelines, prepared by the Privacy Commissioner, in making a decision to exempt the agency under this section.

(3) The head of the agency must, by written notice given to the Privacy Commissioner, notify the Privacy Commissioner—

(a) that the exemption under this section is relied on, and

(b) when the exemption is expected to end, and

(c) of the way in which the agency will review the exemption.

(4) The head of the agency must—

(a) review the use of the exemption each month, and

(b) provide an update to the Privacy Commissioner on the review of the exemption.

(5) The exemption applies only for the period of time the head of the agency reasonably believes the notification would—

(a) worsen the agency's cyber security, or

(b) lead to further data breaches.

Division 5 Powers of Privacy Commissioner

59Y Privacy Commissioner may make directions and recommendations

(1) This section applies if there are reasonable grounds for the Privacy Commissioner to believe there has been an eligible data breach of a public sector agency (a ***suspected breach***).

(2) The Privacy Commissioner may, by written notice given to the head of the public sector agency, direct the head of the agency to—

(a) prepare a statement that includes the following—

(i) the name and contact details of the agency,

(ii) a description of the suspected breach,

(iii) the kind of information involved in the suspected breach,

(iv) recommendations about the steps a notifiable individual should take in response to the breach,

(v) information, specified by the Privacy Commissioner, that relates to the suspected breach, and

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

(3) The Privacy Commissioner may recommend the head of the public sector agency notify notifiable individuals under section 59N(1), or publish a notification under section 59N(2), as if the suspected breach were an eligible data breach.

Note—

See section 59R in relation to the collection, use and disclosure of information by public sector agencies for the purpose of confirming particular details of a notifiable individual.

(4) Before making a direction or recommendation, the Privacy Commissioner must invite the head of the agency to make a submission to the Privacy Commissioner within a specified period.

(5) In deciding whether to make a direction or recommendation, the Privacy Commissioner must have regard to the following—

(a) advice, if any, given to the Privacy Commissioner by a law enforcement agency,

(b) a submission, if any, made by the head of the agency within the period specified by the Privacy Commissioner in response to the invitation under subsection (4),

(c) other matters the Privacy Commissioner considers relevant.

(6) Subsection (5)(a) does not limit the advice to which the Privacy Commissioner may have regard.

(7) If the Privacy Commissioner is aware there are reasonable grounds to believe the access, disclosure or loss that constituted the suspected breach involved 1 or more other public sector agencies, a direction may also require the statement specified in subsection (2)(a) to include the name and contact details of the other agencies.

(8) In this section—

notifiable individual means a person who, if the suspected breach were an eligible data breach—

(a) would be notified under section 59N(1), or

(b) may be notified by operation of section 59N(2).

59Z Investigation and monitoring

Without limiting sections 38 and 39, the Privacy Commissioner may investigate, monitor, audit and report on the exercise of a function of 1 or more public sector agencies, including the systems, policies and practices of an agency, that relate to this Part.

59ZA Access to premises to observe systems, policies and procedures

(1) The Privacy Commissioner may, by written notice given to the head of a public sector agency, direct the head of the agency to provide access to premises occupied or used by the agency on the day and at the time stated in the notice for the purpose of monitoring and reporting on the agency’s compliance with this Part.

(2) The head of the agency must comply with the notice.

(3) If the Privacy Commissioner gives a direction under subsection (1), the Privacy Commissioner may—

(a) enter the premises on the day and at the time stated in the notice, and

(b) observe a demonstration of the agency's data handling systems, policies and procedures, and

(c) inspect the following—

(i) a document that is part of the agency's data handling policies and procedures,

(ii) another document shown to the Privacy Commissioner by the agency.

(4) The head of the agency or an officer or employee of the agency is not required to comply with an information protection principle, a Health Privacy Principle, a privacy code of practice or a health privacy code of practice if the head of the agency, officer or employee produces a document for inspection by the Privacy Commissioner under this section.

(5) In this section—

premises does not include residential premises.

59ZB Reports

The Privacy Commissioner may make a written report in relation to a function of the Privacy Commissioner under this Part.

59ZC Process applying before publication of particular reports

(1) This section applies if the Privacy Commissioner considers there are grounds for making an adverse comment in a report about—

(a) a person, or

(b) a public sector agency, or

(c) both a person and a public sector agency.

(2) As far as it is practicable before making an adverse comment in a report, the Privacy Commissioner must—

(a) inform the person or the head of the public sector agency, or both, of the substance of the grounds for the adverse comment, and

(b) if the grounds for adverse comment are about a person employed or engaged by a public sector agency—inform the public sector agency that employs or engages the person, and

(c) give the person or the head of the agency informed the opportunity to make a submission to the Privacy Commissioner.

(3) The Privacy Commissioner may do the following—

(a) publish the report,

(b) give a copy of the report to the Minister,

(c) give a copy of the report to the head of the agency.

(4) Before publishing a report that makes an adverse comment about a public sector agency, the Privacy Commissioner must—

(a) inform the Minister responsible for the agency that the Privacy Commissioner proposes to publish the report, and

(b) if requested by the Minister—consult the Minister.

Division 6 Other requirements for public sector agencies

59ZD Public sector agency to publish data breach policy

(1) The head of a public sector agency must prepare and publish a data breach policy.

(2) The policy must be publicly available.

59ZE Eligible data breach incident register

(1) The head of a public sector agency must establish and maintain an internal register for eligible data breaches.

(2) The register must include details of the following, where practicable, for all eligible data breaches—

(a) who was notified of the breach,

(b) when the breach was notified,

(c) the type of breach,

(d) details of steps taken by the public sector agency to mitigate harm done by the breach,

(e) details of the actions taken to prevent future breaches,

(f) the estimated cost of the breach.

Division 7 Miscellaneous

59ZF Exemption for Privacy Commissioner from certain principles

(1) The Information and Privacy Commission is not required to comply with the information protection principles under section 9, 13, 14 or 17 or Health Privacy Principle 3, 6, 7 or 10 in relation to information disclosed by Cyber Security NSW to the

Information and Privacy Commission for the purposes of this Part.

(2) The Information and Privacy Commission is not required to comply with the information protection principles under section 18 or 19 or Health Privacy Principle 11 if the information is disclosed to Cyber Security NSW to enable Cyber Security NSW to exercise its functions.

59ZG Exemption for Cyber Security NSW from certain principles

(1) Cyber Security NSW is not required to comply with the information protection principles under section 9, 13, 14 or 17 or Health Privacy Principle 3, 6, 7 or 10 in relation to information disclosed by the Information and Privacy Commission to Cyber Security NSW for the purposes of this Part.

(2) Cyber Security NSW is not required to comply with the information protection principles under section 18 or 19 or Health Privacy Principle 11 if the information is disclosed to the Information and Privacy Commission to enable the Privacy Commissioner to exercise the Privacy Commissioner's functions under this Part.

59ZH Approval of forms

(1) The Privacy Commissioner may approve forms for use under this Part.

(2) The approved forms must be published on the Information and Privacy Commission's website.

59ZI Privacy Commissioner may make guidelines

(1) The Privacy Commissioner may make guidelines for the purpose of exercising the Privacy Commissioner's functions under this Part.

(2) Without limiting subsection (1), the Privacy Commissioner may make guidelines about the following—

(a) whether access, disclosure or loss that occurs as a result of a data breach would be likely, or would not be likely, to result in serious harm to an individual,

(b) deciding whether to exempt a public sector agency for the following—

(i) reasons relating to serious risk of harm to health or safety,

(ii) cyber security reasons.

(3) The Privacy Commissioner must consult with the Minister responsible for this Act before publishing guidelines.

(4) Guidelines must be published on the Information and Privacy Commission's website.

59ZJ Delegation by head of public sector agency

For the purposes of this Part, the head of a public sector agency may delegate the exercise of a function of the head of the agency, other than this power of delegation, to—

(a) a person employed in or by the public sector agency, or

(b) a person of a class prescribed by the regulations.

Part 7 Information and Privacy Advisory Committee

60 Establishment of Information and Privacy Advisory Committee

(1) There is established by this Act an Information and Privacy Advisory Committee.

(2) The Committee is to consist of the Information Commissioner, the Privacy Commissioner, and the following part-time members appointed by the Governor—

(a) 2 persons who are senior officers of public sector agencies and who are nominated by the Minister in consultation with such other Ministers as the Minister considers appropriate,

(b) 2 persons (not being officers of public sector agencies) who are nominated by the Minister and who, in the opinion of the Minister, have special knowledge of or interest in matters affecting access to government information,

(c) 2 persons (not being officers of public sector agencies) who are nominated by the Minister and who, in the opinion of the Minister, have special knowledge of or interest in matters affecting the privacy of persons.

(3) The Information Commissioner is to be the Chairperson of the Committee and is to preside at meetings of the Committee.

(4) Schedule 2 contains provisions relating to the members and procedure of the Committee.

61 Functions of Information and Privacy Advisory Committee

The Information and Privacy Advisory Committee has the following functions—

(a) to advise on matters relevant to the functions of the Information Commissioner and the Privacy Commissioner,

(b) to advise the Minister on such matters as may be referred to it by the Minister.

Part 7A Reports by Privacy Commissioner

61A Annual report

(1) The Privacy Commissioner is, as soon as practicable after 30 June in each year, to

prepare a report of the Privacy Commissioner's work and activities for the 12 months preceding that date and is to furnish the report to the Presiding Officer of each House of Parliament.

(2) A copy of the report is to be provided to the Minister.

(3) The report is to be included as part of the annual report of the Information and Privacy Commission.

61B Report on operation of Act

(1) The Privacy Commissioner is, as soon as practicable after 30 June in each year, to prepare and publish a report on the operation of this Act (generally, across all public sector agencies) for the 12 months preceding that date and is to furnish the report to the Presiding Officer of each House of Parliament.

(2) A copy of the report is to be provided to the Minister.

61C Special report to Parliament

(1) The Privacy Commissioner may, at any time, make a special report on any matter relating to the functions of the Privacy Commissioner to the Presiding Officer of each House of Parliament and must also provide the Minister with a copy of the report.

(2) The Privacy Commissioner may include in a report under this section a recommendation that the report be made public immediately.

61D Procedure for reporting

(1) **Tabling** A copy of a report made or furnished to the Presiding Officer of a House of Parliament under this Part must be laid before that House on the next sitting day of that House after it is received by the Presiding Officer.

(2) **Public reports** If a report includes a recommendation by the Privacy Commissioner that the report be made public forthwith, the Presiding Officer of a House of Parliament may make it public whether or not that House is in session and whether or not the report has been laid before that House.

(3) **Privileges and immunities** A report that is made public by the Presiding Officer of a House of Parliament before it is laid before that House attracts the same privileges and immunities as it would if it had been laid before that House.

(4) **Report procedures** A Presiding Officer need not inquire whether all or any conditions precedent have been satisfied as regards a report purporting to have been made or furnished in accordance with this Act.

(5) **Reference to Presiding Officer** In this Part, a reference to a Presiding Officer of a House of Parliament is a reference to the President of the Legislative Council or the Speaker

of the Legislative Assembly. If there is a vacancy in the office of President, the reference to the President is taken to be a reference to the Clerk of the Legislative Council and, if there is a vacancy in the office of Speaker, the reference to the Speaker is taken to be a reference to the Clerk of the Legislative Assembly.

Part 8 Miscellaneous

62 Corrupt disclosure and use of personal information by public sector officials

(1) A public sector official must not, otherwise than in connection with the lawful exercise of his or her official functions, intentionally disclose or use any personal information about another person to which the official has or had access in the exercise of his or her official functions.

Maximum penalty—100 penalty units or imprisonment for 2 years, or both.

(2) A person must not induce or attempt to induce a public sector official (by way of a bribe or other similar corrupt conduct) to disclose any personal information about another person to which the official has or had access in the exercise of his or her official functions.

Maximum penalty—100 penalty units or imprisonment for 2 years, or both.

(3) Subsection (1) does not prohibit a public sector official from disclosing information about another person if the disclosure is—

(a) a public interest disclosure within the meaning of the *Public Interest Disclosures Act 2022*, or

(b) made for the purpose of exercising a function under that Act.

(4) In this section, a reference to a public sector official includes a reference to a person who was formerly a public sector official.

63 Offering to supply personal information that has been disclosed unlawfully

(1) A person who offers to supply (whether to a particular person or otherwise), or holds himself or herself out as being able to supply (whether to a particular person or otherwise), personal information that the person knows, or ought reasonably to know, has been or is proposed to be disclosed in contravention of section 62 is guilty of an offence.

Maximum penalty—100 penalty units or imprisonment for 2 years, or both.

(2) If a person is convicted of an offence under section 62 or 63 (1), the court may order the confiscation of any money or other benefit alleged to have been obtained by the person in connection with the offence and for that money or other benefit to be forfeited to the Crown.

64, 65 (Repealed)

66 Personal liability of Privacy Commissioner and others

A matter or thing done (or omitted to be done) by the Privacy Commissioner, a member of the staff of the Privacy Commissioner, a member of the Information and Privacy Advisory Committee or a person acting under the direction of the Privacy Commissioner does not, if the matter or thing was done (or omitted to be done) in good faith for the purpose of executing this Act or any other Act, subject the Privacy Commissioner, the member of staff, the member of the Information and Privacy Advisory Committee or the person so acting personally to any action, liability, claim or demand.

66A Protection from liability

(1) Civil proceedings do not lie against a person in respect of loss, damage or injury of any kind suffered by another person by reason only of any of the following acts done in good faith—

(a) the making of a complaint or application under this Act,

(b) the making of a statement to, or the giving of a document or information to, the Privacy Commissioner, whether or not pursuant to a requirement under section 37.

(2) If a public sector agency provides an individual with access to personal information under this Act, and the access was required by section 14 (Access to personal information held by agencies), or an employee, officer or agent of the public sector agency believed in good faith that the access was required by section 14—

(a) no action for defamation or breach of confidence lies against the public sector agency, any employee, officer or agent of the agency or the Crown by reason of the provision of access, and

(b) no action for defamation or breach of confidence in respect of any publication involved in, or resulting from, the giving of access lies against the person who provided the personal information to the public sector agency by reason of the person having supplied the information to the agency, and

(c) the public sector agency, or any employee, officer or agent of the public sector agency, or any other person concerned in giving access to the personal information is not guilty of an offence merely because of the giving of access.

(3) The provision of access to personal information in the circumstances referred to in subsection (2) must not be taken to constitute, for the purposes of the law relating to defamation or breach of confidence, an authorisation or approval of the publication of the health information by the person to whom access to the information is provided.

66B Fees

(1) A public sector agency may charge a fee for any of the following matters—

(a) giving an individual a copy of health information,

(b) giving an individual an opportunity to inspect and take notes of the health information,

(c) amending health information at the request of an individual,

(d) any other matter prescribed by the regulations.

(2) Any fee charged must not exceed such fee (if any) prescribed by the regulations for the matter concerned.

67 Disclosure by Privacy Commissioner or staff member

(1) The Privacy Commissioner or a member of the staff of the Privacy Commissioner must not disclose any information obtained by him or her in the course of his or her office, unless the disclosure is made—

(a) with the consent of the person the subject of the information, or

(b) for the purpose of discharging functions of the Privacy Commissioner or member of staff under this or any other Act.

Maximum penalty—10 penalty units.

(2) Subsection (1) does not prevent the Privacy Commissioner from furnishing any information relating to—

(a) a matter arising under a law of another State, a Territory or the Commonwealth, or

(b) an undertaking that is or was being carried out jointly by New South Wales and another State, a Territory or the Commonwealth,

to a person exercising under a law of that other State, that Territory or the Commonwealth functions similar to those exercised by the Commissioner under this Act or any other Act.

(3) Subsection (1) does not operate to render admissible in evidence in any proceedings any document that would not have been so admissible if this section had not been enacted.

68 Offences relating to dealings with Privacy Commissioner

(1) A person must not—

(a) without lawful excuse, wilfully obstruct, hinder or resist the Privacy Commissioner

or a member of the staff of the Privacy Commissioner in the exercise of functions under this or any other Act, or

(b) without lawful excuse, refuse or wilfully fail to comply with any lawful requirement of the Privacy Commissioner or a member of the staff of the Privacy Commissioner under this or any other Act, or

(c) wilfully make any false statement to or mislead, or attempt to mislead, the Privacy Commissioner or a member of the staff of the Privacy Commissioner in the exercise of functions under this or any other Act.

Maximum penalty—10 penalty units.

(2) A person must not directly or indirectly—

(a) if the person is not the Privacy Commissioner—represent that he or she is the Privacy Commissioner, or

(b) if the person has not been appointed under this Act as acting Privacy Commissioner—represent that he or she has been so appointed, or

(c) if the person is not a person to whom a delegation has been made under this Act or the *Health Records and Information Privacy Act 2002*—represent that he or she is such a person, or

(d) if the person is not a member of the staff of the Privacy Commissioner—represent that he or she is a member of that staff.

Maximum penalty—10 penalty units.

(3) For the purposes of subsection (2), a person represents that a state of affairs exists if the person does or says anything, or causes, permits or suffers anything to be done or said, whereby it is represented, or whereby a belief may be induced, that the state of affairs exists.

69 Legal rights not affected

(1) Nothing in Part 2 or 3 gives rise to, or can be taken into account in, any civil cause of action, and without limiting the generality of the foregoing, nothing in Part 2 or 3—

(a) operates to create in any person any legal rights not in existence before the enactment of this Act, or

(b) affects the validity, or provides grounds for review, of any judicial or administrative act or omission.

(2) Subsection (1) is subject to sections 21 and 32.

70 Proceedings for offences

Proceedings for an offence against this Act are to be dealt with summarily before the Local Court.

71 Regulations

(1) The Governor may make regulations, not inconsistent with this Act, for or with respect to any matter that by this Act is required or permitted to be prescribed or that is necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) Without affecting the generality of subsection (1), the regulations may make provision for or with respect to—

(a) the manner in which privacy codes of practice are to be prepared and developed, and

(b) exempting specified persons or public sector agencies, or classes of persons or public sector agencies, from—

(i) any of the requirements of this Act or the regulations relating to the collection, use or disclosure of specified classes of personal information, or

(ii) any other provision of this Act.

(3) A regulation may create an offence punishable by a penalty not exceeding 50 penalty units.

72 (Repealed)

73 Repeal of Privacy Committee Act 1975 No 37

The *Privacy Committee Act 1975* is repealed.

74 Savings, transitional and other provisions

Schedule 4 has effect.

75 Review of Act

(1) The Minister is to review this Act to determine whether the policy objectives of the Act remain valid and whether the terms of the Act remain appropriate for securing those objectives.

(2) The review is to be undertaken as soon as possible after the period of 5 years from the date of assent to this Act.

(3) A report of the outcome of the review is to be tabled in each House of Parliament within 12 months after the end of the period of 5 years.

Schedule 1 (Repealed)

Schedule 2 Provisions relating to members and procedure of Information and Privacy Advisory Committee

(Section 60 (4))

1 Definition

In this Schedule—

member means a member of the Information and Privacy Advisory Committee other than the Information Commissioner or the Privacy Commissioner.

2 Deputies of members

(1) The Minister may, from time to time, appoint a person to be the deputy of a member, and the Minister may revoke any such appointment.

(2) (Repealed)

(3) In the absence of a member, the member's deputy—

(a) may, if available, act in the place of the member, and

(b) while so acting, has all the functions of the member and is taken to be the member.

(4) A deputy while acting in the place of a member is entitled to be paid such remuneration (including travelling and subsistence allowances) as the Minister may from time to time determine in respect of the person.

3 Term of office of members

Subject to this Schedule, a member holds office for such period (not exceeding 3 years) as is specified in the member's instrument of appointment, but is eligible (if otherwise qualified) for re-appointment.

4 Remuneration of members

A member (other than a member who is an officer of a public sector agency) is entitled to be paid such remuneration (including travelling and subsistence allowances) for attending meetings and transacting the business of the Committee as the Minister may from time to time determine in respect of the member.

5 Vacancy in office of members

(1) The office of a member becomes vacant if the member—

(a) dies, or

(b) completes a term of office and is not re-appointed, or

(c) resigns the office by letter addressed to the Minister, or

(d) is removed from office by the Minister under this clause, or

(e) is absent from 4 consecutive meetings of the Information and Privacy Advisory Committee of which reasonable notice has been given to the member personally or in the ordinary course of post, except on leave granted by the Committee or unless, before the expiration of 4 weeks after the last of those meetings, the member is excused by the Committee for having been absent from those meetings, or

(f) becomes bankrupt, applies to take the benefit of any law for the relief of bankrupt or insolvent debtors, compounds with his or her creditors or makes an assignment of his or her remuneration for their benefit, or

(g) becomes a mentally incapacitated person, or

(h) is convicted in New South Wales of an offence that is punishable by imprisonment for 12 months or more or is convicted elsewhere than in New South Wales of an offence that, if committed in New South Wales, would be an offence so punishable.

(2) The Minister may remove a member from office at any time.

6 Filling of vacancy in office of member

If the office of any member becomes vacant, a person is, subject to this Act, to be appointed to fill the vacancy.

7 Effect of certain other Acts

(1) The provisions of the *Government Sector Employment Act 2013* relating to the employment of Public Service employees do not apply to a member.

(2) If, by or under any Act, provision is made—

(a) requiring a person who is the holder of a specified office to devote the whole of his or her time to the duties of that office, or

(b) prohibiting the person from engaging in employment outside the duties of that office,

the provision does not operate to disqualify the person from holding that office and also the office of a member or from accepting and retaining any remuneration payable to the person under this Act as such a member.

(3) The office of a member is not, for the purposes of any Act, an office or place of profit under the Crown.

8 General procedure

The procedure for the calling of meetings of the Information and Privacy Advisory Committee and for the conduct of business at those meetings, is to be as determined by the Information Commissioner.

Schedule 3 (Repealed)

Schedule 4 Savings, transitional and other provisions

(Section 74)

1 Savings and transitional regulations

(1) The regulations may contain provisions of a savings or transitional nature consequent on the enactment of the following Acts—

this Act

Health Records and Information Privacy Act 2002, but only to the extent that it amends this Act

Privacy and Personal Information Protection Amendment (Prisoners) Act 2002

Privacy and Government Information Legislation Amendment Act 2010

any other Act that amends this Act

(2) Any such provision may, if the regulations so provide, take effect from the date of assent to the Act concerned or a later date.

(3) To the extent to which any such provision takes effect from a date that is earlier than the date of its publication on the NSW legislation website, the provision does not operate so as—

(a) to affect in a manner prejudicial to any person (other than the State or an authority of the State), the rights of that person existing before the date of its publication, or

(b) to impose liabilities on any person (other than the State or an authority of the State) in respect of any thing done or omitted to be done before the date of its publication.

2 Abolition of Privacy Committee

(1) The Privacy Committee is abolished.

(2) A person who, immediately before the repeal of the *Privacy Committee Act 1975*, held office as a member of the Privacy Committee, ceases to hold office on that repeal but is eligible (if otherwise qualified) to be appointed as a member of the Privacy Advisory

Committee under this Act.

(3) A person who ceases to hold office because of subclause (1) is not entitled to any remuneration or compensation because of the loss of that office.

3 Existing complaints

A complaint received by the Privacy Committee, but not concluded immediately before the repeal of the *Privacy Committee Act 1975*, is to be dealt with by the Privacy Commissioner as if that Act had not been repealed by this Act.

4 Existing reports

A publication to which there was a defence of absolute privilege under section 17B of the *Defamation Act 1974*, immediately before the amendment to that section by Schedule 3 to this Act, continues to be subject to that defence.

5 Annual report

The Privacy Commissioner is, in the Privacy Commissioner's first annual report, to report on the activities of the Privacy Committee in the period from the date of the last annual report of the Committee to the date of abolition of the Committee.

6 Provisions consequential on enactment of Health Records and Information Privacy Act 2002

(1) In this clause—

health information has the same meaning as in the HRIP Act.

HRIP Act means the *Health Records and Information Privacy Act 2002*.

(2) A request made under this Act before the commencement of section 4A for access to, or alteration of, health information is to continue to be dealt with by the public sector agency under this Act as if the amendments to this Act by the HRIP Act had not been made.

(3) A complaint concerning health information made to the Privacy Commissioner under Division 3 of Part 4 before the commencement of section 4A and pending immediately before that commencement is to continue to be dealt with under this Act as if the amendments to this Act by the HRIP Act had not been made. This Act (as in force immediately before the commencement of those amendments) continues to apply for that purpose.

(4) An application concerning health information made under section 53 (Internal review by public sector agencies) or section 55 (Review of conduct by Tribunal) before the commencement of section 4A and pending immediately before that commencement is to continue to be dealt with by the public sector agency or the Administrative

Decisions Tribunal under this Act as if the amendments to this Act by the HRIP Act had not been made. This Act (as in force immediately before the commencement of those amendments) continues to apply for that purpose.

(5) For the purpose of allowing a complaint or application to be made in respect of conduct concerning health information that was engaged in before the commencement of section 4A, but in respect of which a complaint or application was not pending immediately before that commencement, this Act (as in force immediately before the commencement of the amendments made by the HRIP Act) continues to apply to conduct engaged in before the commencement of section 4A.

7 Provisions consequent on enactment of Privacy and Government Information Legislation Amendment Act 2010

(1) The group of staff employed in the Department of Justice and Attorney General as staff of the Privacy Commissioner or otherwise to enable the Privacy Commissioner to exercise the Privacy Commissioner's functions are removed from that Department and added to the Information and Privacy Commission.

(2) The Privacy Advisory Committee established under this Act before the substitution of Part 7 by the *Privacy and Government Information Legislation Amendment Act 2010* is abolished.

(3) An appointment of a person as Privacy Commissioner or acting Privacy Commissioner in force immediately before the commencement of Division 1 of Part 4 (as substituted by the *Privacy and Government Information Legislation Amendment Act 2010*) is taken to have been made under that Division as so substituted.

(4) A delegation in force under section 44 immediately before the repeal of that section is taken to have been made under section 35H.

8 Provisions consequent on enactment of Privacy and Personal Information Protection Amendment (Exemptions Consolidation) Act 2015

(1) The following directions made by the Privacy Commissioner under section 41 are revoked—

(a) *Direction on Disclosures of Information by Public Sector Agencies for Research Purposes* as renewed by the Privacy Commissioner on 19 June 2015 for the period 1 July 2015 to 31 December 2015,

(b) *Direction relating to the Disclosure of Information to Credit Reporting Agencies* as renewed by the Privacy Commissioner on 19 June 2015 for the period 1 July 2015 to 31 December 2015,

(c) *Direction on Information Transfers between Public Sector Agencies* as renewed by the Privacy Commissioner on 19 June 2015 for the period 1 July 2015 to 31

December 2015,

(d) *Direction on Processing of Personal Information by Public Sector Agencies in relation to their Investigative Functions* as renewed by the Privacy Commissioner on 19 June 2015 for the period 1 July 2015 to 31 December 2015,

(e) *Direction on Disclosures of Information by the New South Wales Public Sector to the National Coronial Information System (NCIS)* as renewed by the Privacy Commissioner on 19 June 2015 for the period 1 July 2015 to 31 December 2015,

(f) *Direction on the Collection of Personal Information about Third Parties by New South Wales Public Sector (Human Services) Agencies from their Clients* as renewed by the Privacy Commissioner on 19 June 2015 for the period 1 July 2015 to 31 December 2015,

(g) *Direction for the Department of Families and Community Services and Associated Agencies* as renewed by the Privacy Commissioner on 19 June 2015 for the period 1 July 2015 to 31 December 2015,

(h) *Direction on the Disclosure of Information to Victims of Crime* as renewed by the Privacy Commissioner on 19 June 2015 for the period 1 July 2015 to 31 December 2015.

(2) Subclause (1) extends to any direction made before the commencement of this clause that renews a direction referred to in that subclause.

9 Provisions consequent on enactment of Privacy and Personal Information Protection Amendment Act 2022

(1) If an officer or employee of a public sector agency becomes aware, after the commencement of Part 6A, that there may be reasonable grounds to suspect there may have been an eligible data breach of the agency before the commencement of the Part, section 59E applies to the officer or employee in relation to the breach as if the breach had occurred after the commencement of the Part.

(2) Sections 8–11 do not apply in relation to personal information collected by a relevant public sector agency before the commencement of the amending Act, Schedule 1[2].

(3) To avoid doubt, Part 5 does not apply to the conduct of a relevant public sector agency that occurred before the commencement of the amending Act, Schedule 1[2].

(4) In this clause—

amending Act means the *Privacy and Personal Information Protection Amendment Act 2022*.

relevant public sector agency means a public sector agency that is a State owned corporation that is not subject to the *Privacy Act 1988* of the Commonwealth.