First print

New South Wales

Privacy and Personal Information Protection Amendment Bill 2022

Explanatory note

This explanatory note relates to this Bill as introduced into Parliament.

Overview of Bill

The object of this Bill is to amend the *Privacy and Personal Information Protection Act 1998* (***the Act***) to—

(a) extend the Act to State owned corporations that are not subject to the *Privacy Act 1988* of the Commonwealth, and

(b) introduce a scheme for the assessment of data breaches and the mandatory notification of certain data breaches that occur in relation to the access, disclosure or loss of personal information held by public sector agencies, and

(c) provide for exemptions from mandatory notification in particular circumstances, and

(d) give the Privacy Commissioner the power to investigate, monitor, audit and report on public sector agencies in relation to the scheme for the mandatory notification of data breaches, including the power to observe the systems, policies and procedures of a public sector agency, and

(e) give the Privacy Commissioner the power to give directions to, and make guidelines, recommendations and reports about, public sector agencies in relation to data breaches, and

(f) require public sector agencies to publish a data breach policy and keep a data breach register.

Outline of provisions

Clause 1 sets out the name, also called the short title, of the proposed Act.

Clause 2 provides for the commencement of the proposed Act.

Schedule 1 Amendment of Privacy and Personal Information Protection Act 1998 No 133

Schedule 1[1] inserts definitions relating to proposed Part 6A, including a definition of ***mandatory notification of data breach scheme***.

Schedule 1[2]–[4] remove the exclusion of State owned corporations from the Act and extend the Act to State owned corporations that are not subject to the *Privacy Act 1988* of the Commonwealth.
Schedule 1[5] makes a consequential amendment.

Schedule 1[6] and [7] insert a requirement that a public sector agency have and implement a privacy management plan. The privacy management plan must include provisions about the procedures and practices used by the agency to ensure compliance with the mandatory notification of data breach scheme inserted by proposed Part 6A.

Schedule 1[8]–[10] insert additional functions of the Privacy Commissioner relating to the mandatory notification of data breach scheme, including functions to—

(a) investigate, monitor, audit and report on a public sector agency's compliance with the scheme, and

(b) provide assistance to agencies in—

  (i) adopting and complying with the scheme, and

  (ii) preparing data breach policies for the scheme.

Schedule 1[11] inserts proposed Part 6A. The proposed Part introduces a mandatory notification of data breach scheme, which provides for the following—

(a) the types of data breaches that are eligible data breaches and must be notified to the Privacy Commissioner,

(b) the persons who are affected individuals under the scheme and who must be notified of eligible data breaches,

(c) when, and the way in which, a public sector agency must assess a data breach to decide whether the breach is an eligible data breach,

(d) the information to be provided, and the way information must be provided, to the Privacy Commissioner if an eligible data breach has occurred,

(e) the notification of information about an eligible data breach to affected individuals, or the requirement of public notification in certain circumstances, and the information that is required to be provided as part of a notification,

(f) the type of information that may be collected, used and disclosed by officers or employees of public sector agencies to confirm particular information about individuals affected by certain data breaches,

(g) exemptions from particular requirements of the mandatory data breach scheme.

The proposed Part provides for the powers of the Privacy Commissioner in relation to the scheme, including the power to—

(a) direct certain information be provided to the Commissioner, and

(b) recommend the public sector agency notify certain individuals about a suspected data breach.

The Privacy Commissioner is empowered to investigate, monitor, audit and report on the exercise of functions of public sector agencies in relation to the scheme. This includes a power to observe the systems, policies and procedures of a public sector agency for the purpose of monitoring and reporting on the agency's compliance with the Part. For that purpose, the Privacy Commissioner is empowered to direct the head of an agency to allow the Privacy Commissioner to enter premises to observe a demonstration of the agency's data handling systems, policies and procedures and

inspect particular documents shown to the Commissioner. The Privacy Commissioner may make reports and recommendations, issue guidelines and approve forms in relation to the proposed Part.

The proposed Part also requires public sector agencies to prepare and publish a data breach policy and establish and maintain an internal register for eligible data breaches to support the requirements of the scheme.

Schedule 1[12] inserts transitional provisions.

Schedule 2 Amendment of other Acts

Schedule 2.1 amends the *Fines Act 1996* to remove a provision as a consequence of the mandatory notification of data breach scheme set out in the *Privacy and Personal Information Protection Act 1998*, proposed Part 6A.

Schedule 2.2 amends the *Government Information (Public Access) Act 2009* to insert a conclusive presumption that there is an overriding public interest against the disclosure of information contained in a document prepared for the purposes of an assessment of an eligible data breach under the *Privacy and Personal Information Protection Act 1998*, proposed Part 6A in certain circumstances, and makes a consequential amendment.

First print

New South Wales

Privacy and Personal Information Protection Amendment Bill 2022

Contents

b2020-136.d44

New South Wales

Privacy and Personal Information Protection Amendment Bill 2022

No , 2022

A Bill for

An Act to amend the *Privacy and Personal Information Protection Act 1998* to introduce a mandatory notification of data breach scheme; to extend the Act's application to State owned corporations that are not subject to the *Privacy Act 1988* of the Commonwealth; and for other purposes.

Tabling copy

The Legislature of New South Wales enacts—

1 Name of Act

This Act is the *Privacy and Personal Information Protection Amendment Act 2022*.

2 Commencement

This Act commences on the first anniversary of the date of assent.

Schedule 1 Amendment of Privacy and Personal Information Protection Act 1998 No 133

[1] Section 3 Definitions

Insert in alphabetical order in section 3(1)—

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).

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

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).

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

[2] Section 3(1), definition of "public sector agency"

Insert after paragraph (f)—

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

[3] Section 3(1), definition of "public sector agency"

Omit "paragraph (a)–(f)" from paragraph (g)(i). Insert instead "paragraph (a)–(f1)".

[4] Section 3(1), definition of "public sector agency"

Omit "but does not include a State owned corporation.".

[5] Section 4 Definition of "personal information"

Omit "For the purposes of this Act, personal" from section 4(4). Insert instead "Personal".

[6] Section 33 Preparation and implementation of privacy management plans

Omit "prepare and implement a privacy management plan within 12 months of the commencement of this section" from section 33(1).

Insert instead "have and implement a privacy management plan".

[7] Section 33(2)(c1)

Insert after section 33(2)(c)—

(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,

[8] Section 36 General functions

Omit "and privacy codes of practice," from section 36(2)(d). Insert instead—

, privacy codes of practice and the mandatory notification of data breach scheme,

[9] Section 36(2)(e)

Omit "implementing privacy management plans in accordance with section 33,".

Insert instead—

implementing—

(i) privacy management plans under section 33, and

(ii) data breach policies under section 59ZD,

[10] Section 36(2)(m)

Insert after section 36(2)(l)—

(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.

[11] Part 6A

Insert after Part 6—

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.

[12] Schedule 4 Savings, transitional and other provisions

Insert at the end of Schedule 4, with appropriate clause numbering—

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.

Schedule 2 Amendment of other Acts

2.1 Fines Act 1996 No 99

Section 117C Unlawful disclosure of personal information

Omit the section.

2.2 Government Information (Public Access) Act 2009 No 52

[1] Schedule 1 Information for which there is conclusive presumption of overriding public interest against disclosure

Insert in Schedule 1, with appropriate clause numbering—

Information relating to cyber security and data breaches under the Privacy and Personal Information Protection Act 1998

It is to be conclusively presumed that there is an overriding public interest against disclosure of information contained in a document prepared for the assessment of an eligible data breach under the *Privacy and Personal Information Protection Act 1998*, Part 6A, if the information could worsen a public sector agency's cyber security or lead to further data breaches.

[2] Schedule 2 Excluded information of particular agencies

Omit the matter relating to the office of the Privacy Commissioner from clause 2.

Insert instead—

The office of Privacy Commissioner—review, complaint handling, investigative, auditing, monitoring and reporting functions.