NEW SOUTH WALES

DRAFT GOVERNMENT BILL

Privacy and Personal Information Protection Amendment Bill 2021

Contents

NEW SOUTH WALES

DRAFT GOVERNMENT BILL

Privacy and Personal Information Protection Amendment Bill 2021

No , 2020

A Bill for

An Act to amend the *Privacy and Personal Information Protection Act 1998* to require public sector agencies to notify certain individuals and the Privacy Commissioner if there is a particular data breach relating to personal information; to extend its application to State owned corporations that are not subject to the *Privacy Act 1988* of the Commonwealth; and for other purposes.

The Legislature of New South Wales enacts—

1 Name of Act

This Act is the *Privacy and Personal Information Protection Amendment Act 2021*.

2 Commencement

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

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 59C(2).

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

assessors, for Part 6A—see section 59F(1).

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

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) of the definition—

(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 "paragraphs (a)–(f1)".

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

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

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

Insert after section 33(2)(c)—

(c1) the obligations and responsibilities the agency has in relation to the mandatory notification of data breach scheme and how the agency will comply with the obligations and responsibilities,

[6] 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,

[7] 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 59ZC,

[8] 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.

[9] 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 59C(2)

approved form means a form approved under section 59ZG.

assessment—see section 59D(2)(b).

assessors—see section 59F(1).

eligible data breach—see section 59C(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.

public notification register—see section 59ZD.

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 eligible data breach and affected individual

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

(a) both of the following are satisfied—

(i) there is unauthorised access to, or unauthorised disclosure of, personal information,

(ii) 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 is lost in circumstances where—

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

(ii) if the access or 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)(ii) 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 an 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 or on behalf of an agency without authorisation.

Division 2 Assessment of data breaches

59D Requirements for public sector agency

(1) This section applies if an officer or employee of a public sector agency reasonably suspects that an eligible data breach has occurred.

(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 reasonable suspicion was formed about the data breach—assess 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 59J.

59E Mitigation of harm

An officer or employee of a public sector agency that reasonably suspects an eligible data breach has occurred must, during an assessment, make all reasonable attempts to mitigate the harm done by the breach.

59F Assessors

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

(2) An assessor may be—

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

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

(c) a person acting on behalf of the public sector agency the subject of the breach.

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 may be an assessor.

(3) A person who the head of the public sector 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 agency first held the reasonable suspicion about the breach.

(5) In this section—

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

59G Assessment of data breach—factors for consideration

Without limiting the factors that may be considered by the assessors in the assessment of a data breach, the following factors may be considered—

(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 protected by security measures,

(d) the persons who have obtained, or who could obtain, the personal information,

(e) the likelihood that persons who have obtained, or could obtain, the personal information—

(i) have the intention of causing harm, or

(ii) could circumvent the security measures,

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

(g) any 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 information relates.

59H 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 59ZH in relation to guidelines made under this Part.

59I Decision about data breach

(1) Following an assessment, the assessor must advise the head of the public sector agency of whether the assessment found, or there are reasonable grounds to believe, the data breach is an eligible data breach.

(2) The head of the agency must decide whether the breach is an eligible data breach.

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

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

(2) For an extension approved under subsection (1), the head of the agency must, within 30 days after the agency first held the reasonable suspicion that an eligible data breach has occurred, give written notice to the Privacy Commissioner that—

(a) the assessment has started, and

(b) the head of the agency has approved an extension of the period for the assessment.

(3) The head of the public sector agency must give the Privacy Commissioner an update on the progress of the assessment each month.

(4) The Privacy Commissioner may ask the head of the public sector agency to provide further information or updates about the progress of the assessment.

Division 3 Notification of data breaches to Privacy Commissioner

Subdivision 1 Application

59K Application of Division

This Division applies if the head of the public sector agency decides, under Division 2, that a data breach is an eligible data breach.

Subdivision 2 Immediate notification to Privacy Commissioner

59L 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 an 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 59N,

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

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

(d) whether the breach is a cyber incident,

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

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

(g) the total number, or estimated total number, of individuals affected or likely to be affected by the breach,

(h) the total number, or estimated total number, of individuals notified of the breach,

(i) whether the individuals notified under section 59M(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

59M Public sector agencies must notify certain individuals

(1) As soon as practicable after the head of the public sector agency decides an eligible data breach has occurred, the head of the agency must—

(a) if it is reasonably practicable to notify each individual to whom the personal information the subject of the breach relates—take the steps that are reasonable in the circumstances to notify each individual to whom the information relates, or

(b) if it is reasonably practicable to notify each affected individual—take the steps that are reasonable in the circumstances to notify each affected individual.

(2) If the head of the public sector agency is unable to identify, or it is not reasonably practicable to identify, any or all of the individuals specified in subsection (1) for the purposes of notifying the individuals, the head of the agency must—

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

(b) take reasonable steps to publicise the notification.

59N Information to be notified to certain individuals

A notification given under section 59M(1) must, if it is reasonably practicable for the information to be provided, include the following information—

(a) the date the eligible data breach occurred,

(b) a description of the eligible data breach,

(c) how the eligible data breach occurred,

(d) the type of eligible data breach that occurred,

Examples of a type of 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 eligible data breach,

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

(l) contact details for the agency the subject of the eligible data breach, or another person nominated by the agency for the individual to contact in relation to the breach.

59O Public notification

A notification given under section 59M(2) must, if it is reasonably practicable for the information to be provided—

(a) include the information specified in section 59N, except to the extent the information—

(i) contains personal information, or

(ii) would prejudice the agency's functions, and

(b) be published on the public notification register for at least 12 months after the date the notification is published.

59P Further information to be provided to the Privacy Commissioner

Following notification under section 59M(1) or (2), the head of the 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 59L.

Subdivision 4 Information sharing

59Q Information sharing for notification

(1) An officer or employee of a public sector agency the subject of an eligible data breach is not required to comply with an information protection principle or a privacy code of practice for the purposes of sharing personal information—

(a) within the agency, or

(b) with an officer or employee of another public sector agency.

(2) Also, an officer or employee of a public sector agency is not required to comply with an information protection principle or a privacy code of practice for the purposes of sharing relevant personal information with an officer or employee of the public sector agency the subject of an eligible data breach.

(3) Information may be shared under this section only if it is reasonably necessary for the purposes of—

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

(b) confirming whether a notifiable individual is deceased.

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

(5) In this section—

notifiable individual means an individual specified in section 59M(1).

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

Division 4 Exemptions from certain eligible data breach requirements

59R 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 one 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 head of each of the public sector agencies involved in the breach has notified the Privacy Commissioner under section 59L.

(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 that Subdivision.

59S Exemption relating to ongoing investigations and certain proceedings

(1) This section applies if the head of a public sector agency believes on reasonable grounds that there has been an eligible data breach of the agency.

(2) The head of the public sector agency is exempt from Division 3, Subdivision 3 if the head of the agency reasonably believes that notification of the 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.

59T 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—

(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 or disclosure of information results in serious harm to an individual, and

(iii) as a result 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—

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

59U Exemption if inconsistent with secrecy provisions

(1) The head of a public sector agency is exempt from Division 3, Subdivision 3, if notification would be inconsistent with a secrecy provision.

(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.

59V 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 if 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 whether 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 cause or permit the search of data held by the agency, that were not affected by the breach, to assess the impact of the notification, unless the head of the agency knows, or reasonably believes, that 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 of—

(a) reliance on an exemption under this section, and

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

(c) if the exemption is temporary—the specified or expected time the exemption is to have effect.

59W 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 public sector agency the subject of the eligible data breach must, by written notice given to the Privacy Commissioner, notify the Privacy Commissioner of—

(a) reliance on an exemption under this section, and

(b) when the exemption is expected to cease having effect, and

(c) the way 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.

(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 for Part

59X Privacy Commissioner may make directions and recommendations

(1) This section applies if there are reasonable grounds for the Privacy Commissioner to believe that 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 individuals should take in response to the suspected 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 individuals under sections 59M(1) or (2), as if the suspected breach were an eligible data breach.

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

(5) In deciding whether to make the direction or recommendation to the head of the agency, 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 of the agency involved one 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.

59Y 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 one or more public sector agencies, including the systems, policies and practices of an agency, that relate to this Part.

59Z Entry of premises

(1) This section applies—

(a) for the purposes of investigating, monitoring, auditing and reporting on a public sector agency under this Part, or

(b) to a complaint made under Part 4, Division 3, in relation to this Part.

(2) The Privacy Commissioner may—

(a) enter and inspect premises occupied or used by a public sector agency, and

(b) inspect a record or thing in or on the premises that the Privacy Commissioner reasonably believes relates to compliance with this Part.

(3) The Privacy Commissioner must, by written notice given to the head of the public sector agency occupying or using the premises—

(a) notify the head of the public sector agency to request consent to enter the premises, and

(b) if consent is not given—provide reasonable notice of the time for entry and inspection of premises.

59ZA Limits on entry powers because of privilege

(1) The Privacy Commissioner must not exercise a power of entry under section 59Z if it appears to the Privacy Commissioner that a person has a ground of privilege where, in proceedings in a court of law, the person might resist a similar requirement or the exercise of a similar power, unless—

(a) the privilege is a privilege of an agency, or

(b) it appears to the Commissioner that the person has waived the privilege.

(2) However, the Privacy Commissioner may exercise the power of entry despite—

(a) a rule of law that, in proceedings in a court of law, might justify an objection to compliance with a similar requirement or the exercise of a like power on grounds of public interest, or

(b) a duty of secrecy or other restriction on disclosure applying to an agency.

59ZB Reports and recommendations of Privacy Commissioner

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

(2) If the Privacy Commissioner considers that there are grounds for adverse comment about a person or a public sector agency in a report, the Privacy Commissioner must, as far as it is practicable before making the comment—

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

(b) give the person an opportunity to make submissions.

(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 public sector 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

59ZC 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.

59ZD Public notification register

(1) The head of a public sector agency must keep a register if the agency gives a notification under section 59M(2) (a ***public notification register***).

(2) The public notification register must be available on the public sector agency's website.

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 the actions taken to prevent future breaches,

(e) the estimated cost of the breach.

(3) If the agency is required to prepare an annual report under a relevant Act, the report must include a summary of the information specified in subsection (2).

(4) In this section—

relevant Act means the following—

(a) the *Annual Reports (Departments) Act 1985*,

(b) the *Annual Reports (Statutory Bodies) Act 1984*,

(c) the *Local Government Act 1993.*

Division 7 Miscellaneous

59ZF Confidentiality

(1) Information given to the Privacy Commissioner under this Part is confidential and is not to be released by the Privacy Commissioner—

(a) without consent from the head of the public sector agency, or

(b) except as permitted, authorised or required by—

(i) subsection (2), or

(ii) section 59Q, or

(iii) another provision of this Act or another law.

(2) The Privacy Commissioner is not required to comply with an information protection principle for the purposes of sharing information with Cyber Security NSW to enable Cyber Security NSW to exercise its functions.

59ZG Approval of forms

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

(2) A copy of the approved forms must be available on the Information and Privacy Commission's website.

59ZH 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) conducting an assessment in relation to whether access, disclosure or loss that occurs by way of a data breach would be likely, or would not be likely, to result in serious harm,

(b) deciding whether to give an exemption for serious risk of harm for health or safety reasons,

(c) deciding whether to given an exemption for 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.

Schedule 2 Amendment of other instruments

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

Schedule 2 Excluded information of particular agencies

Omit "The office of Privacy Commissioner—review, complaint handling, investigative and reporting functions." from clause 2 of the Schedule.

Insert instead—

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

2.3 Government Sector Finance Legislation (Repeal and Amendment) Act 2018 No 70

Schedule 4 Other amendments to legislation

Insert at the end of Schedule 4.85—

[2] Section 59ZE Eligible data breach incident register

Omit section 59ZE(3) and (4). Insert instead—

(3) A reporting GSF agency within the meaning of the *Government Sector Finance Act 2018* must include a summary of the information specified in subsection (2) in the agency's annual reporting information under the *Government Sector Finance Act 2018*.

(4) A local government authority required to prepare an annual report under the *Local Government Act 1993* must include a summary of the information specified in subsection (2) in the authority's annual report under that Act.