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.