From: Policy MailIn
To: [redacted]
Subject: FW: Feedback on the Privacy and Personal Information Protection Amendment Bill 2021
Date: Wednesday, 1 September 2021 9:39:38 AM
Attachments: image008.jpg
image001.png
image002.jpg
image004.png
image010.jpg
image011.jpg

From: [redacted]
Sent: Tuesday, 31 August 2021 5:09 PM
To: Policy MailIn <policy@justice.nsw.gov.au>
Subject: RE: Feedback on the Privacy and Personal Information Protection Amendment Bill 2021

Good afternoon,

If the submission is to be made public, could it please be a combination of the two emails, as follows:

Dear Sir/Madam,

The Mandatory Notification of Data Breach (MNDB) Scheme introduced by this bill formalises the current voluntary notification of privacy breaches to the Privacy Commissioner.

The Department of Regional NSW welcomes this bill and provide the following feedback for consideration:

- Suggest that the data breach definition (s.59C), in addition to 'unauthorised access to, or disclosure of, personal information', to also include 'modification, loss of, misuse or other interference with personal information'

- Continue the current voluntary notification of privacy breaches in cases where the breach is not likely to result in 'serious harm', or require agencies to report on these in their annual report, as these breaches may offer insight into certain trends

- To prevent delays, allow the designated (delegated) Privacy Officer to initially notify the Privacy Commissioner of an eligible data breach rather than the 'head of a public sector agency'

- Notifying affected individuals should take priority over notifying the Privacy Commissioner. Section 59L(2)(a)-(i) includes lots of details that would necessarily require affected individuals to be notified first (particularly 59L(2)(h)) and it would seem pertinent that individuals be advised of the breach as soon as possible to take any necessary action

- Provide that the Privacy Commissioner report on the number **and types** of data breaches, mitigation and controls used by the agency to prevent future such breaches, and use this to assist other agencies in preventing similar types of breaches in the future

- That the Privacy Commissioner, or the legislation, provides details of what should be included in a data breach policy as mentioned in section 59ZD

- Change the word 'may' in section 59ZH, to 'must' and ensure that such Guidelines created by the Privacy Commissioner use examples and a pragmatic approach to assist agencies

- That the Guidelines include what is meant by 'secrecy provisions' (s. 59U), 'certain actions taken' (s. 59T), risk of harm (s. 59V), and 'cyber security' (s. 59W) including examples

- Provide details of what is meant by 'estimated cost of the breach' in section 59ZE(2)(e) as well as what is meant by 'summary' in section 59ZE(3)

- That the minor typo in section 59Q(3)(a) be corrected to state 'a notifiable individual' rather than 'an notifiable individual'.

- Section 59A refers to various sections where certain terms are mentioned. These terms should be defined in the PPIP Act, particularly in respect of the terms mentioned in sections 59C(1), 59(c)(3)(a)-(c), 59D(2)(b), 59G(c), and 59(I) – additional details in respect of this point is set out below

Section 59(c)(3)(a(-(c) - for clarification for agencies, it would be helpful if there is a definition of the following 'terms':
"Data breach within an agency"
"Data breach between agencies"
"Data breach by external person/entity"
One would assume this means unauthorised access, use or disclosure, but may mean more than that and often staff of agencies do not see that access to personal information within an agency may be a use or disclosure or even a breach. If it is defined, privacy officers within agencies will then have something tangible to refer to when explaining and educating staff on what it means. The use of an example, similar to that used in section 59F(2)(c) would be extremely helpful for Privacy Officers.

Section 59D(2)(b)
Section 59A defines the word assessment by referring to section 59D(2)(b)). Section 59D(2)(b) defines Assessment as a data breach that is an 'eligible data breach'. Section 59A defines an 'eligible data breach' By referring to section 59C(1). Section 59C(1)(a)(ii) further defines it as resulting in 'serious harm', yet 'serious harm' is not defined anywhere. It would be helpful if these circular references to define what things mean could provide a full picture of the definitions, by including a definition of 'serious harm'. Even more helpful would be if the definition section at 59A contained the full description, rather than the Privacy officer having to wade through various sections to obtain the definition.

Section 59G(c)
This section mentions the word 'security measures' yet this term is not defined anywhere. A definition of what that may include, for example a mix of physical, administrative or technical. Some examples would be password protection, two factor authentication, application of security

controls (including physical controls where relevant), restricting access to personal information, securing data in transit and at rest, avoiding enumerations on website that require logins, use HTTPs rather than HTTP, warning of use of cookies, having policies, procedures and staff training on how to ensure data security practices are followed to protect personal information.

Section 59(I)
This section again mentions 'eligible data breach' and reference is made to comments above in respect of 59D(2)(b).

Thank you for the opportunity to give feedback on the proposed introduction of the MNDB.

Thanks,

[redacted]

[redacted]

The Department of Regional New South Wales acknowledges that it stands on Country which always was and always will be Aboriginal land. We acknowledge the Traditional Custodians of the land and waters, and we show our respect for Elders past, present and emerging. We are committed to providing places in which Aboriginal people are included socially, culturally and economically through thoughtful and collaborative approaches to our work.

[redacted]