UTS

UTS MEMORANDUM

UTS: UNIVERSITY SECRETARY & DIRECTOR GOVERNANCE SUPPORT UNIT

TO: policy@justice.nsw.gov.au DATE: 18/06/2021

ACTION: FOR INFORMATION

[redacted]

SUBJECT: SUBMISSION ON THE NSW MANDATORY DATA BREACH NOTIFICATION SCHEME

To the Department of Communities and Justice

Please find below our submission as part of public consultation on the *Privacy and Personal Information Protection Amendment Bill 2021* and the introduction of a mandatory data breach notification scheme for NSW.

Overall, we broadly support the approach taken in the Bill and are pleased to see some alignment with the Commonwealth's Privacy Act's Notifiable Data Breach Scheme. Some comments on specific sections of the Bill are set out below for consideration.

Section	Feedback
Various references to "Head of agency" responsibilities	We note there are quite a few references to actions required to be performed by the "head of agency". Some of these are high level and others are more transactional in nature. The *Privacy and Personal Information Protection Act* currently refers primarily to "Agency" or "Entity" responsibilities. We acknowledge the importance of the actions outlined in the Bill and the Head of any agency being fully aware of such matters and the seriousness or them. Managing such a process however does not operate in isolation, and although the Head of any agency has responsibilities in this space, it would be helpful for the legislation to clarify the extent of allowable delegations so that processes can be established to best meet the overall outcomes of the scheme.
s.59O Public notification	This may be appropriate as a sub-section under s.59M(2), as new sections 59M(2)(c) and (d), as it directly relates to it and its action.
s.59P Further information to be provided to the Privacy Commissioner	This may be more appropriate as a sub-section of s.59M, as a new section 59M(3), as it directly relates to it and its action.

s.59Q Information sharing for notification	We view this as a positive inclusion to ensure individuals are notified as soon as possible via the correct contact details. However, this action seems to be limited only to those who need to be notified as a result of an eligible data breach. Under s. 59X(3), the NSW Privacy Commissioner can direct or recommend an agency notify individuals, where the agency itself has not decided that a breach is an eligible data breach. Will clause s.59Q also apply here? It would be helpful for this to be clarified in the legislation.
s.59T Exemption if public sector agency has taken certain action	It is not clear if this section unintentionally contradicts other parts of the Bill. s. 59T exempts an agency from notifying individuals under Division 3, Subdivision3, if the mitigation actions taken, mean that individuals would NOT be subject to serious harm (but not Division 3,Sub Division 2 which related to notifying the Privacy Commissioner). However, action to mitigate harm is required under s.59E when a breach is first suspected. If this mitigation means the breach would not cause serious harm, it would not then be identified as an Eligible Data Breach under Division 2. Section 59K (Division 3, Subdivision 1) states that Division 3 as a whole only applies if a data breach is an eligible data breach under the assessment in division 2. Therefore, s.59T would not seem to apply. It is suggested this apparent inconsistency be resolved or clarified for agencies.
s.59ZC Public Sector Agency to Publish Data Breach Policy	Does this require an agency to have a specific document called a "Data Breach Policy", as opposed to being incorporated in as part of an existing Privacy Policy, or as a Data Breach Plan?

Please contact me if you would like to discuss any of the above comments.

Yours sincerley,

[redacted]