Planning, Industry & Environment

Our ref: EF21/8629

Ms [redacted]
A/Director, Courts, Access to Justice
Policy Reform and Legislation
Department of Communities and Justice

Via email: policy@justice.nsw.gov.au

Dear Ms [redacted]

RE: **Submission on the Privacy and Personal Information Protection Amendment Bill 2021**

I refer to the proposed changes to NSW privacy laws and provide this response on behalf of the Department of Planning, Industry and Environment (the Department).

The Department supports the introduction of the proposed mandatory notification of data breach scheme (MNDB). The MNDB will standardise what and how to report, and set out how to notify affected individuals. The Department submits the changes will result in better outcomes for agencies and members of the public.

The Department makes the following observations about the draft Bill.

Division 2 - Assessment of data breaches

Section 59D(2) requires the 'head of the agency' to be notified by any officer who reasonably suspects that an eligible data breach has occurred, to immediately take all reasonable steps to mitigate that breach, and to assess whether the breach is an eligible data breach.

Section 59F provides for another person to be directed to undertake the required assessment under 59D(2)(b), but there is no provision for delegating the responsibility for notification and mitigation. While the Department understands the importance of the head of any agency being aware of a serious privacy breach, requiring all notifications and mitigation steps to be carried out by the head of the agency has issues with practical application.

Most, if not all, agencies have dedicated privacy officers or privacy governance units. These officers are best placed to triage and notify senior management of serious breaches, and to understand the steps needed to mitigate the risk. The inability to delegate the functions of 59D(2) may, in practice, result in heads of agencies being responsible for receiving and assessing notifications from officers across an agency who are not in a position to determine whether a breach is serious or not. This is a particular concern in the Planning, Industry and Environment cluster, which has approximately 10,000 employees.

The Department recommends a provision be added to 59D that allows the functions of 59D(2) to be delegated.

Division 3 – Notification of breaches

Section 59L(2)(d) and (e) require a breach notification to include whether it is a 'cyber incident'. There is no definition or any other reference to a 'cyber incident' in the Bill.

The Department recommends that if a breach notification must include whether the breach is a 'cyber incident', a definition or explanation of the term is included. Alternatively, this requirement should be removed.

Division 5 – Powers of Privacy Commissioner

Section 59X gives the Privacy Commissioner (the Commissioner) the power to make recommendations or directions to an agency if the Commissioner has reason to believe there has been an eligible data breach. It is unclear as to whether these powers apply only when the Commissioner has not been notified by an agency, or whether they apply regardless of what notification or steps an agency has already taken.

The Department recommends some clarification be added as to when this section applies.

Section 59ZB allows the Commissioner to make a report that may make adverse comment about a person or an agency. Subsection (2) requires the person or the head of the agency to be notified prior to the publication of the report and given the opportunity to make submissions. Given that the naming of an individual is likely to affect the agency's processes and reputation, the Department believes that the head of the agency and the affected person should be contacted in every case.

The Department recommends that the word "or" in section 59ZB(2)(b) be changed to "and", so that the person and the head of the agency are contacted.

Resourcing

The Department acknowledges that the Bill has been drafted with an expectation that there will be significant guidance material produced by the Information and Privacy Commission (IPC), as well as increased monitoring and investigation functions for the IPC.

The Department notes the increased requirements on agencies for recording of breaches, annual reporting, a public register of notifications made under 59M(2), and amendments to privacy management plans to include processes to meet requirements for the scheme. The Department looks forward to reviewing guidance material developed by the IPC and suggests a transition period for Departments to fully implement and be able to demonstrate compliance, as there will be a resourcing impact.

Contact

Thank you for the opportunity for commenting on the Bill. If you would like to discuss this submission, please contact Ms [redacted], Management Information Access & Privacy at [redacted] or on [redacted].

Yours sincerely,

[redacted]

Date: 12 July 2021