THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL: JWap170621

17 June 2021

Mandatory Notification of Data Breaches by NSW Public Sector Agencies
Policy, Reform and Legislation
NSW Department of Communities and Justice
GPO Box 31
Sydney NSW 2001

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

Dear sir / madam,

Mandatory notification of data breach scheme in the Privacy and Personal Information Protection Amendment Bill 2021

The Law Society of New South Wales (NSW) appreciates the opportunity to comment on the Draft Privacy and Personal Information Protection Amendment Bill 2021 (Draft Bill). The Law Society's Privacy and Data Law Committee has contributed to this submission.

General comments

The Law Society strongly supports the introduction of a mandatory notification of data breach (MNDB) scheme in NSW as a mechanism to enhance citizen trust, as well as Government accountability. As noted in our 2019 submission to the Department of Community and Justice's (the Department) Discussion Paper, 'Mandatory notification of data breaches by NSW public sector agencies',[1] breaches relating to data held by public sector agencies can have a detrimental impact on both individuals and government agencies. Government agencies' unauthorised disclosure of data about citizens, whether accidental or through the result of malicious acts, can result in both tangible harms as well as the denigration of public confidence.

We consider members of the public, who may have no choice but to provide public sector agencies with personal information under relevant legislation or to receive a service, should be able to trust that their information will be appropriately protected, used and stored. Where it has not been, there should be an obligation on public sector agencies to notify affected individuals of data breaches as soon as practicable.

[1] Law Society of NSW, *Mandatory notification of data breaches by NSW public sector agencies,* (submission to the Department of Communities and Justice, 30 August 2019) <https://www.lawsociety.com.au/sites/default/files/2020-03/Letter%20to%20Dept%20of%20Communities%20%26%20Justice%20-%20Mandatory%20notification%20of%20data%20breaches%20by%20NSW%20public%20sector%20agencies%20-%2030%20Aug%202019.pdf>.

Such notification enables the persons the subject of a data breach to take self-protective measures and potentially limit further adverse consequences associated with that breach, including by changing relevant usernames and passwords, or notifying financial institutions or other bodies of the breach. The ability to take precautionary self-protective measures is particularly important in circumstances involving family or domestic violence.

We note that the introduction of a MNDB scheme would formalise a practice that many NSW public sector agencies already voluntarily engage in, through the Information and Privacy Commission's (IPC) voluntary data breach reporting scheme, and would provide clarity in relation to the role and responsibilities of NSW public sector agencies.

However, as raised in our previous submission, the Law Society suggests that the NSW Government should also focus on developing mechanisms to require agencies to enhance data protection and implement strategies to identify, mitigate and manage residual risks of data breaches, for example, by encouraging a focus on a 'just culture' (shared accountability) approach to managing security of personal information.

The Law Society notes that the NSW Government has expressed an intention to be a leader in the adoption of data use and sharing to benefit citizens of NSW. The NSW Government's ability to implement initiatives to improve efficiency and convenience for citizens dealing with it largely depends on high levels of citizen trust in the Government's collection, handling and storage of data about them. However, the Auditor-General for NSW's December 2020 Report into Service NSW's handling of personal information, which focused on processes, technologies, and governance arrangements for how Service NSW handles customers' personal information, found clear deficiencies in that handling.[2]

In our view, there should be an obligation on agencies to encourage employees to report mistakes and for agencies to identify and improve processes that may lead to mistakes, rather than adopting a punitive approach to error-making. By requiring agencies to implement strategies to prevent data breaches, we consider a mandatory data breach regime could become an additional layer of protection, or a way for other agencies, the Privacy Commissioner or Government to better understand common issues and trends.

We set out our comments on specific provisions contained in the Draft Bill below.

1. Consistency with the Commonwealth Notifiable Data Breach Scheme

The Law Society broadly supports the proposed amendments to the *Privacy and Personal Information Protection Act 1998* (PPIPA) contained in the Draft Bill, noting they largely mirror the provisions in the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth), which amended the *Privacy Act 1998* (Cth) (Privacy Act) and established the Commonwealth Notifiable Data Breach Scheme (Commonwealth Scheme).

We note NSW public sector agencies may already be required to report breaches of certain information under the Commonwealth Scheme (for example, tax file number information) and in certain instances, under the European Union General Data Protection Regulation.

The Law Society recognises the value of nationally consistent notifiable data breach schemes, noting consistency will minimise the cost to agencies of obtaining appropriate advice and providing notifications. As far as we are aware, there have not yet been manifest errors or deficiencies identified in the Commonwealth Scheme and we therefore support the mirroring of that scheme so far as possible (subject to our specific comments below).

[2] Audit Office of NSW, *Service NSW's handling of personal information* (Special Report, 18 December 2020).

While supportive of measures to close the regulatory gap, we suggest that regulatory duplication should be avoided as far as possible. We note there is already overlap in coverage of the handling of health information by providers of the health services and their contractors under the Privacy Act and, in New South Wales, the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act). We suggest that where an entity is already regulated by the Commonwealth Scheme in relation to a particular notifiable data breach, and that entity complies with the requirements of the Commonwealth Scheme, that entity should not be required to make a separate notification to the NSW Privacy Commissioner under the NSW scheme. Instead, we suggest consideration be given to requiring agencies to simply provide a copy of the notification to the NSW Privacy Commissioner. In the alternative, we suggest an information sharing regime between the IPC and Office of the Australian Information Commissioner (if not otherwise permitted), be established to enable the easy flow of information concerning data breaches by NSW public sector agencies covered by the Commonwealth Scheme.

Reasonable suspicion that a breach has occurred before assessment of data breach

The Law Society notes the difference in language between section 59D of the Draft Bill and corresponding section 26WH of the Privacy Act (under the Commonwealth Scheme). We note, in particular, the varying requisite thresholds to enliven the public sector agency's obligation to assess whether a data breach is an 'eligible data breach'.

Section 59D of the Draft Bill provides that the section is engaged if a public sector agency 'reasonably suspects that an eligible data breach *has* occurred'. Meanwhile, under the Commonwealth Scheme, section 26WH of the Privacy Act only requires the agency to be 'aware that there are reasonable grounds to suspect that there *may* have been an eligible data breach', even if it is '*not aware* that there are reasonable grounds to *believe* that the relevant circumstances amount to an eligible data breach'. (emphasis added)

On our reading, there is a lower threshold for engagement of the assessment requirements under the Privacy Act, where the mere awareness of reasonable grounds to suspect that an eligible breach *may* have occurred is sufficient to oblige an agency to make an assessment (noting there are separate requirements to prepare a statement about a breach when an agency has reasonable grounds to *believe* a breach has occurred, per section 26WK of the Privacy Act). The Draft Bill on the other hand would require an agency to reasonably suspect an eligible data breach *has* occurred for the assessment requirements to be enlivened, which necessitates the formation of a view that there are grounds potentially amounting to an eligible data breach.

We query whether the language of the Draft Bill is intended to create a disparity in assessment thresholds. If this was not the intention, then we suggest the Draft Bill be amended to mirror the relevant provisions of the Privacy Act under the Commonwealth Scheme.

If there was an intention to create a disparity, then we query whether such an approach is consistent with the Department's stated objectives for developing such a scheme, which include to 'improve agency data management, reduce underreporting and reduce the occurrence of data breaches that cause serious harm'.[3] We consider that, as currently drafted, section 59D may result in underreporting of data breaches.

[3] Department of Communities and Justice, 'Privacy and Personal Information Protection Amendment Bill 2021 Factsheet', May 2021, p 2 <https://www.justice.nsw.gov.au/justicepolicy/Documents/proposed-changes-to-NSW-privacy-laws/privacy-and-personal-information-protection-amendment-bill-2021-factsheet.pdf>.

Health information as personal information

The Law Society supports the inclusion of health information within the definition of 'personal information' for the purposes of proposed new Part 6A of the PPIPA (under section 59B of the Draft Bill). We note that the HRIP Act does not impose an obligation on agencies to notify affected individuals about breaches of health information held by NSW public sector agencies. Conversely, health information held by Commonwealth public sector agencies is covered under the Commonwealth Scheme.

We consider the inclusion of health information under the NSW MNDB scheme would be a welcome step toward closing the regulatory gap. However, as outlined above, we suggest that where the breach of that information is already subject to notification under the Commonwealth Scheme, then a separate notification to the IPC should not be required.

Notification requirements to affected individuals

We note that under the Commonwealth Scheme, an agency is required to prepare a statement for the Information Commissioner, containing the identity and contact details of the breaching agency, a description of the potential breach, the kinds of information that may have been breached, and recommendations to the affected individual on next steps in response to the breach.

In addition to the Commonwealth Scheme requirements, the NSW Scheme would require agencies to inform affected individuals of the date and type of breach, how the breach occurred, the actual information breached (rather than merely the kinds of breached information), the amount of time the information was disclosed for, planned or current remedial actions, and the complaints and internal review mechanisms available to the individual.

The Law Society supports the expanded requirements on the content of notifications to affected individuals about eligible data breaches (contained in subsections 59N(a)-(l) of the Draft Bill). Although more extensive than the requirements of the Commonwealth Scheme, in our view, this expanded list would be better at informing and supporting affected individuals in the event of a data breach, and would enhance agency transparency and accountability.

2. 'Serious harm' threshold

The Law Society notes the comments we made in our 2019 submission regarding issues with the 'serious harm' threshold. At that time, we suggested that a threshold of 'serious breach', rather than 'serious harm' may be more appropriate in the NSW privacy context. We suggested that, from an accountability and transparency perspective, it is important that agencies be required to report data breaches that occur internally within the NSW Government, but that agencies would be unlikely to consider unauthorised disclosures of data within their own agency, or to another public sector agency, as reaching the requisite level of 'serious harm'. We suggested such reporting would help preserve public trust and confidence in the public sector and would provide the NSW Privacy Commissioner with the enhanced ability to collate, track and report on any need to, and strategies for, addressing this type of breach.

We also considered a 'serious breach' threshold would be better able to adapt to different circumstances, taking account of both subjective criteria, including the likelihood of serious harm, and objective criteria such as the number of individuals affected by the breach. In our view, this would not only encourage an open culture of reporting and shared accountability in

public sector agencies, but would also ensure that large-scale data breaches are addressed, even if the harm falls short of the requisite 'seriousness' threshold.

We acknowledge that the meaning of 'eligible data breach' in the Draft Bill has been developed to explicitly capture both intra-agency and inter-agency data breaches (per subsection 59C(3) of the Draft Bill). We support this development.

However, we retain concerns about the concept of 'serious harm' as the threshold for enlivening an agency's assessment obligations under the proposed scheme. From our members' experience with the Commonwealth Scheme, we consider that, in practice, this ambiguous concept results in confusion and inconsistent application, in large part due to insufficient articulation of what a privacy harm is, and how to tell a 'serious harm' from a harm that is not serious. Further, as an objective test, the 'serious harm' threshold fails to take into account the specific situation of each individual citizen affected (for example, issues may arise in the context of an affected individual who fears violence by a former partner). It also fails to contemplate issues of an immediate serious harm versus a delayed serious harm, which is often the case with identity theft (as information may be on-sold for several months or even years before a person tries to use such information for nefarious purposes).

In our view, the 'serious harm' threshold is overly focused on the likely consequences of a data breach, rather than on facilitating a preventative and holistic approach to data breach regulation generally. Such a threshold may also not reflect community expectations that any breach of their privacy (regardless of whether or not 'serious harm' could result) should be reported.

We note the Department's suggestion that the 'judicial and academic consideration' of the Commonwealth Scheme threshold will be used in developing agencies' understanding of what constitutes 'serious harm' for the purpose of the NSW scheme.[4] We draw the Department's attention to Danielle Keats Citron and Daniel J. Solove's recent research paper, 'Privacy Harms'[5] for a more detailed analysis of the issues associated with the concept of privacy 'harms' from both a judicial interpretation and academic perspective.

Despite our ongoing concerns with this concept, we recognise (as outlined above) the benefits of consistency with the Commonwealth Scheme. If the 'serious harm' threshold is adopted in NSW, then we suggest that, at the least, consideration be given to better articulating (whether in the legislation or elsewhere) that 'serious' means sufficiently substantial (including distress) to not be trivial, and that the standard be applied to any of the affected cohort.

3. Commissioner's reports and recommendations to the Minister

The Law Society broadly supports section 59ZB of the Draft Bill, which would give the Privacy Commissioner the power to make written reports. We also support the procedural requirements set out in that provision, in the case that the report contains adverse comments about a person or public agency and when such a report is sought to be published.

While this provision may serve as a deterrent to intentional unauthorised disclosure and carelessness, given the Privacy Commissioner's potential ability to make comments that

[4] Department of Communities and Justice, *Privacy and Personal Information Protection Amendment Bill 2021 Factsheet* (May 2021) p 2 <https://www.justice.nsw.gov.au/justicepolicy/Documents/proposed-changes-to-NSW-privacy-laws/privacy-and-personal-information-protection-amendment-bill-2021-factsheet.pdf>.

[5] Danielle Keats Citron and Daniel J. Solove, 'Privacy Harms' (Legal Studies Research Paper 11/2021, The George Washington University Law School, February 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222>.

adversely affect a person (including a public sector employee) or public sector agency, we suggest this power should be carefully deployed to ensure it does not have the effect of inhibiting candid reporting to both agency heads and the Privacy Commissioner.

We suggest that the effects of this provision will need to be closely monitored to ensure it does not have an impact on the development of a 'just culture' and the promotion of open reporting of potential breaches.

4. Record-keeping and publication provisions

The Law Society supports the introduction of the Division 6 requirements for public sector agencies to publish a data breach policy (section 59ZC), keep a public notification register (section 59ZD), and maintain an eligible data breach incident register (section 59ZE). These requirements align with our recommendations in our 2019 submission. In our view, the provisions would promote transparency of agency processes in managing, assessing, and reporting data breaches, and would enhance government accountability. These requirements would also allow public sector agencies to collate and analyse common trends, which could support initiatives to target those issues and reduce the future occurrence of data breaches.

We suggest consideration be given to requiring agencies, under proposed section 59ZC, to review their data breach policies on a regular basis to ensure they are fit for purpose, and for a statement or summary of this review to be included in any annual report it might be required to prepare. One further addition to the section 59ZE requirement to maintain a register of eligible data breaches is the inclusion of details of actions taken to remediate the data breach, and not only details of actions taken to prevent future breaches (per paragraph 59ZE(2)(d)).

Thank you again for this opportunity to comment on the Draft Bill. Should you have any questions in relation to this submission, please contact [redacted], Policy Lawyer, on (02) [redacted] or email [redacted].

Yours faithfully,

[redacted]