THE LAW SOCIETY
OF NEW SOUTH WALES

Our Ref: PDL: EEap1776231

30 August 2019

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 breaches by NSW public sector agencies

The Law Society of New South Wales (NSW) appreciates the opportunity to comment on the Discussion Paper, 'Mandatory notification of data breaches by NSW public sector agencies'. The Law Society's Privacy and Data Law Committee has contributed to this submission.

Our general observations of the issues raised in the Discussion Paper are outlined below.

A mandatory notification scheme

The Law Society supports the introduction in NSW of a mandatory reporting regime of data breaches for NSW public sector agencies. Breaches of data held by public sector agencies have the potential for serious negative impact on both individual members of the community and government agencies. 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 their information to be appropriately protected, used and stored. There should also be an obligation for agencies to notify individuals when their personal information has been compromised, so that remedial steps to avoid potential adverse consequences may be taken. We consider a mandatory data breach notification scheme would enhance transparency around agencies' collection, handling, use and disclosure of relevant information, and would better ensure government accountability in identifying and managing data breaches.

Avoiding regulatory duplication

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

We support measures to close the regulatory gap, while also noting the need to avoid regulatory duplication. There is already overlap in coverage of handling of health information by providers of the health services and their contractors under the

Privacy Act 1988 (Cth) and, in New South Wales, the *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act). We recommend that where an entity is regulated by the Commonwealth Notifiable Data Breach 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 notification to the NSW Privacy Commissioner under a new NSW scheme. For clarity, we note compliance may mean following the requirements of the Commonwealth Notifiable Data Breach scheme and making a decision that notification is not required.

Where a NSW public sector agency is not regulated by the Commonwealth Notifiable Data Breach scheme (as commonly will be the case), we recommend the assessment criteria and forms of notification required under the Commonwealth scheme be mirrored as far as is reasonably practicable in the NSW scheme. We consider this 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 Notifiable Data Breach scheme. Accordingly, and to enhance privacy officers' ability to comply with the various reporting requirements, we recommend a NSW scheme mirror the Commonwealth Notifiable Data Breach scheme so far as possible, subject to our specific comments on the proposed breach threshold (below) and any additional alterations necessary to ensure the scheme is workable in the NSW privacy context.

Under mirroring provisions, notification of data breaches under relevant NSW legislation, including the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIPA) and HRIP Act, would be to the NSW Privacy Commissioner.

Other mechanisms for enhancing data protection and preventing breaches

While we are supportive of the introduction of a mandatory data breach notification system in NSW, we recommend the Government also consider focusing on 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.

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.

'Serious harm' threshold

We note there are three main categories of data breaches in the Government context:

1. breaches caused by malicious acts, including cyber-attacks,
2. unlawful disclosure of information by an agency to another agency, and
3. unlawful disclosure by an agency to a member of the public or private entity.

To be effective, we consider the relevant reporting threshold should apply in all three contexts. We note however, obligations under the PPIPA are largely agency-focused, and we query whether an agency will be likely to regard an inadvertent or otherwise not permitted disclosure of data to another Government agency as likely to lead to

'serious harm'. We consider a Government-wide, rather than inter-agency, 'serious harm' threshold may lead to underreporting of data breaches that should be brought to the attention of the NSW Privacy Commissioner.

From an accountability and transparency perspective, we consider it important that agencies be required to report data breaches that occur inter-agency within NSW Government. 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 therefore recommend the Government consider whether a threshold of 'serious breach', rather than 'serious harm' may be more appropriate in the NSW privacy context. We consider such a definition could be developed to capture both subjective and objective elements. Subjective criteria could focus on notions including the potential for 'serious harm' while objective factors could consider the number of individuals whose personal information has been breached.

While we recommend the Privacy Commissioner be notified of all breaches that meet a proposed 'serious breach' threshold, consideration could be given to requiring agencies to notify concerned individuals only if such a breach would result in serious harm to that person.

Enhanced record-keeping and publishing requirements

Regardless of the threshold and reporting obligations to the Privacy Commissioner and / or individuals, we consider stringent record keeping obligations in relation to data breaches is critical to ensuring transparency of Government agencies' privacy compliance. While the specific details of persons affected by a suspected data breach should be confidential, there appears to be no in principle impediment to requiring agencies to document and publish both:

1. their processes to manage, assess and report data breaches involving their customers' personal information; and
2. an ongoing and public record of such data breaches identified and how those breaches were managed.

While we note Government agencies may be subject to general record keeping obligations, so that such matters may be recorded in agency files, we are not aware of any obligations on agencies to publicise information about their privacy compliance in relation to their customers' personal information. We consider requiring agencies to have a public record of such matters is appropriate to assure agency customers that the trust they place in such agencies is being reflected in appropriate agency actions to protect personal information.

Thank you again for the opportunity to comment on this Discussion Paper. Should you have any questions in relation to this submission, please contact Adi Prigan, Policy Lawyer, on (02) 9926 0285 or email Adi.Prigan@lawsociety.com.au.

Yours sincerely,

Elizabeth Espinosa
President