Our ref: LS19/07120

3 September 2019

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

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

Dear Policy, Reform and Legislation

Submission on the Discussion Paper: Mandatory notification of data breaches by NSW public sector agencies

Transport for NSW (**TfNSW**) appreciates the opportunity to make a submission to the Department of Communities and Justice on the *Discussion Paper: Mandatory notification of data breaches by NSW public sector agencies.*

The submission has been prepared by TfNSW as a coordinated Transport Cluster response.

The Transport Cluster supports the introduction of a mandatory data breach notification scheme in New South Wales. Such a scheme:

- provides for transparency of agencies' collection, handling, use and disclosure of personal information,
- helps to prevent future breaches by strengthening data breach and privacy processes; and
- increases public confidence and trust in government.

The first section of the attached submission discusses three issues arising out of the Discussion Paper in some detail. The second section responds to the specific questions raised in the Discussion Paper.

TfNSW thanks the Department of Communities and Justice for the opportunity to make this submission. TfNSW would be happy to engage in further discussion on any of the matters raised in this submission.

If you have any further questions please contact [redacted]

Yours sincerely

[redacted]

Anne Hayes
Deputy Secretary Corporate Services

Transport for NSW
18 Lee Street, Chippendale NSW 2008 | PO Box K659, Haymarket NSW 1240
T 02 8202 2200 | **F** 02 8202 2209 | **W** transport.nsw.gov.au | ABN 18 804 239 602

Transport Cluster Submission on Mandatory notification of data breaches by NSW public sector agencies

August 2019

Introduction of a mandatory data breach notification scheme in NSW

Transport for NSW (**TfNSW**) appreciates the opportunity to make a submission to the Department of Communities and Justice on the *Discussion Paper: Mandatory notification of data breaches by NSW public sector agencies* (**Discussion Paper**).

TfNSW supports the introduction of a mandatory data breach notification scheme in New South Wales. Such a scheme:

- provides for transparency of agencies' collection, handling, use and disclosure of personal information,
- helps to prevent future breaches by strengthening data breach and privacy processes;
- increases public confidence and trust in government.

The first section of this paper discusses three issues arising out of the Discussion Paper in some detail. The second section responds to the specific questions raised in the Discussion Paper.

Detailed discussion

Reporting threshold

TfNSW supports the development and implementation of a reporting threshold. Without a reporting threshold, agencies may take an inconsistent approach to notification, leading to over and under- reporting outcomes. Neither outcome is good regulation. In particular, over-notification carries similar risks as under-notification if it leads to complacency or 'notification fatigue' amongst agencies and the public. The mandatory reporting of serious breaches is best practice, strengthens public trust in government, and gives government (through the Privacy Commissioner) insight into data management risks and practices within agencies.

The Commonwealth experience of the mandatory data breach scheme has been that the OIAC does not 'name and shame' corporations involved in breaches, but does publish statistics around the causes of breaches, industries most affected, and methods of preventing and managing breaches. This guidance is critical to the development of a mature privacy regulatory regime.

For a mandatory notification scheme to be beneficial for both agencies and the public the reporting threshold should be set at a level which:

- provides certainty as to when reportable breaches of sufficient significance occur, and
- captures significant breaches so that government and the public can benefit from learnings associated with an analysis of breach trends.

The Discussion Paper seeks views on whether the Commonwealth reporting threshold of a breach being 'likely to result in serious harm' is appropriate in the NSW context. TfNSW's view is that the 'likely to result in serious harm' test may need review in the NSW context.

In the Transport cluster context, there are principally three main categories of data breaches: breaches due to a cyber-attack, unauthorised disclosure by an agency to another State or Commonwealth agency, and unlawful disclosure by an agency to a member of the public or private entity. In order to satisfy the aims of a mandatory data breach scheme applicable to agencies, the reporting threshold should operate in all three contexts.

The type of harm that may result to a member of the public if their personal information is disclosed by one agency to another is likely to be different to and less than the harm suffered if

personal information is disclosed to a non-government party. However, if such breaches are not reported to the Privacy Commissioner then the aims of the mandatory reporting scheme may not be met.

One alternative is for a reporting threshold to be developed based on a notion of a 'serious breach' rather than 'serious harm'. Parameters as to what constitutes a 'serious breach' can be based around factors which include subjective notions of 'serious harm' but which also pick up more objective reporting thresholds, such as the number of individuals whose personal information has been breached. Reporting of a 'serious breach' could be more nuanced than is the case with the Commonwealth approach, in that while the Privacy Commissioner should always be notified of a serious breach, there may be no need for individuals to be notified if they are unlikely to suffer serious harm arising from the breach. Notification in those circumstances adds regulatory burden to agencies and potentially causes distress to individuals without sufficient corresponding benefit.

Penalties for data breaches

Question 7(b) of the Discussion Paper asks whether monetary penalties should apply where a NSW public sector agency has failed to comply with the scheme requirements. A penalty regime sends a public message regarding the importance of pro-actively ensuring compliance with the scheme. The availability of penalties would demonstrate to the NSW public that there are consequences to privacy breaches even where the individuals affected by the breach do not bring proceedings seeking compensation. The introduction of a penalty scheme would also be consistent with overseas jurisdictions.

TfNSW's view is that the value of a penalty scheme which would result in one government agency paying government funds to the government regulator is unclear, particularly since at this stage there is insufficient information to determine whether or not a penalty scheme is needed. In addition, the OAIC reports on data breaches indicate that some two thirds of breaches occur as a result of cyber security attacks by third parties. Although agencies should be encouraged to ensure that their personal information holdings are secure from attacks, in some cases it may not be reasonable to penalise an agency for a cyber security attack by a sophisticated and well-resourced third party.

TfNSW suggests that the introduction of a penalty scheme be reconsidered once the results of the mandatory data breach scheme (if introduced) are known. For example, the mandatory data breach scheme might indicate that agency data breaches are relatively rare or that the introduction of the scheme is sufficient to drive changes in agency compliance.

'Just culture'

Although outside the scope of the specific questions in the Discussion Paper, the Discussion Paper raises a broader question of whether the agency based NSW privacy regime should be updated to encourage a focus on a 'just culture' approach to managing personal information. The 'just culture' approach recognises that staff will make errors, but that risks of error are more likely to be reduced if there is a non-punitive reporting of genuine mistakes with a focus on identifying and improving the organisational factors that impact on compliance.

The 'just culture' approach has been successful in complex industries such as aviation and health where preventing errors is more important than attributing blame for an individual lapse. Given the many factors that can be at work in a privacy breach and the harm resulting from that breach, a 'just culture' approach may be an appropriate model to adopt and may encourage agencies to consider management of privacy issues at a more global level. For example, a 'just

culture' approach to privacy might require agencies to:

- identify their personal information holdings and attach a level of significance to each 'holding';
- develop a data management plan for each personal information holding, which must be audited and updated as appropriate; and
- ensure that learnings from a breach notice are reflected in changes to the agency's privacy practices.

Transport Cluster responses to the discussion paper questions

1. Should the NSW Government introduce a mandatory data breach notification scheme for NSW public sector agencies?

TfNSW supports the introduction of a mandatory data breach notification scheme for NSW public sector agencies by the NSW Government. Data breaches pose a significant risk to individuals who have placed their trust and confidence in government to not only appropriately manage and use their personal information but to keep it protected. The consequences for individuals and public sector agencies can be significant, far-reaching and serious. The essential service nature of government service delivery means that in some cases individuals cannot opt out of providing their personal information to public sector agencies. In return individuals have an expectation that agencies will safeguard all personal information they collect and report to individuals when a data breach occurs.

The introduction of a mandatory data breach notification scheme would go some way in ensuring agencies are consistent and transparent in their approach to the reporting and handling of data breaches. It would also allow individuals to take remedial steps to avoid potential adverse consequences of their personal information having been compromised in a data breach. Mandatory breach notification requirements not only help mitigate harm (or the risk of it) but they make agencies more accountable for privacy breaches, and allow the Privacy Commissioner to address systemic issues before they cause any further harm.

2. Should legislation require NSW public sector agencies to report breaches:

a) Where unauthorised access to or disclosure of personal information has occurred?

b) Where any breach of an Information Protection Principle has occurred?

TfNSW supports legislation which requires agencies to report breaches in the event of unauthorised access to or disclosure of personal information on the basis that:

- agencies are not 'named and shamed' as a result, but
- the Privacy Commissioner uses the reporting information she receives to publish an annual report identifying systemic issues and trends so that agencies and government can benefit from a holistic understanding of privacy issues.

TfNSW does not support the suggestion that agencies report breaches of any Information Protection Principle (**IPP**). Not all breaches are of sufficient seriousness to warrant the additional reporting burden that could result, and this would also mean that NSW was out of step with the Commonwealth regime. TfNSW considers that breaches of the IPPs should continue to be handled through the internal review process in section 53 of the *Privacy and Personal Information Protection Act 1998*.

3. a) Is the threshold of 'likely to result in serious harm' appropriate, or should a different standard be applied?

b) Should legislation define the term serious harm?

c) Should legislation prescribe the factors an agency must consider when assessing whether a data breach meets the threshold of serious harm?

TfNSW suggests that a different standard should be applied than the threshold 'likely to result in serious harm'. As noted above, TfNSW considers a more appropriate threshold could be a 'serious breach' which can incorporate objective and subjective factors. Although this would mean that the NSW and Commonwealth approaches would be different, this is appropriate given the different entities to which the legislation applies, and the purpose of a reporting scheme.

Agencies would benefit from a definition of 'serious breach' being included in legislation.

TfNSW also supports the inclusion of prescribed factors in the legislation which an agency must consider when assessing whether a data breach meets the threshold of serious harm. A list of prescribed factors (such as the effectiveness of remediation) would give certainty to agencies and an incentive to address data breaches.

4. Should legislation require NSW public sector agencies to report data breaches only where the agency has been unable to prevent likely risk of serious harm with remedial action?

TfNSW supports the introduction of legislation which requires public sector agencies to report data breaches only where the data was obtained or potentially could have been obtained by a member of the public or private entity, and the agency has been unable to prevent likely risk of serious harm with remedial action.

However, as noted above, the NSW reporting scheme should also recognise that a data breach should be reported to the Commissioner even if 'serious harm' is unlikely if the breach also rises to a threshold of a 'serious breach'. This is because a government to government breach is unlikely to result in a risk of serious harm, but it is important to identify these breaches in order to meet the aims of a mandatory reporting scheme, and to preserve public trust and confidence in the public sector. However such breaches should not be reported to the individuals affected by the breach if those individuals are unlikely to suffer serious harm, since notification in those circumstances will add unnecessary burden to agencies without sufficient corresponding benefit to the individuals involved.

5. a) What information should be notified to the NSW Privacy Commissioner and affected individuals in relation to data breaches?

b) Should the legislation prescribe the form and content of the notification?

TfNSW suggests that the form of notification to the NSW Privacy Commissioner and affected individuals should have sufficient information to understand the circumstances of the breach, the possible impacts of the breach and the agency's response efforts. An example of best practice are the IPC's and OAIC's guidance and notification forms which provides a good prompt for assessing the data breach and considering the steps the agency and affected individuals should take in response to a breach. The ACCC's guidelines regarding product recall notification and reporting are also a good model for how an organisation can track and report on its remediation process.

However, the form and content of the notification should not be prescribed in legislation. Many

breaches are not alike, and the main aim of notification should be to communicate key information about the breach, rather than compliance with a particular reporting format.

6. What notification timeframe should be prescribed in the legislation?

One of the main objectives of the introduction of a mandatory data breach notification scheme is to equip affected individuals with the power to mitigate harm caused to them. However, this should be balanced alongside an agency's ability to quickly investigate and assess a breach, particularly given the resourcing of smaller agencies.

TfNSW supports adoption of the timing under the Commonwealth NDB scheme in sections 26WH & 26WK of the *Privacy Act 1988* (Cth). Accordingly, NSW public sector agencies would have to take all reasonable steps to investigate within 30 days of becoming aware that there may have been an eligible data breach. Then once the agency has reasonable grounds to believe there may have been such a breach, they must notify as soon as practicable the NSW Privacy Commissioner and affected individuals.

7. a) Does the NSW Privacy Commissioner require any additional powers to encourage compliance with a mandatory notification scheme?

b) Should the monetary penalties apply where NSW public sector agencies fail to comply with the requirements of the scheme?

The NSW Privacy Commissioner should have additional or enhanced powers consistent with the introduction of a mandatory scheme and the Commissioner's other powers set out in the *Privacy and Personal Information Protection Act 1998* that are aimed at addressing serious interferences with the privacy of an individual.

With the introduction of the Commonwealth NDB scheme the Australian Privacy Commissioner gained a number of enforcement powers to ensure entities meet their obligations under the scheme. For instance, the Australian Privacy Commissioner has the power to direct an entity to notify them of an eligible data breach under section 26WK of the *Privacy Act 1988*. The NSW Privacy Commissioner should have similar powers.

However, TfNSW does not support the introduction of monetary penalties at this stage. The need for penalties is unclear, and should be reassessed once more evidence is available about the extent of privacy breaches by government agencies and the causes of those breaches.

8. What exemptions from the requirement to notify individuals and the NSW Privacy Commissioner of eligible data breaches should apply?

TfNSW suggests that similar exceptions as are included in the Commonwealth NDB scheme should be introduced as part of the broader introduction of a mandatory notification scheme in NSW. In particular however, agencies should be exempt from the requirement to notify individuals (but not the NSW Privacy Commissioner) where such notification would not be in the public interest. For example, this might occur where a law enforcement investigation is being undertaken into the breach and notification would impede that investigation. However, on the basis that the Privacy Commissioner will not make individual privacy breaches public, notification of the Commissioner should occur.