CITY OF SYDNEY

City of Sydney
Town Hall House
456 Kent Street
Sydney NSW 2000

+61 2 9265 9333
council@cityofsydney.nsw.gov.au
GPO Box 1591 Sydney NSW 2001
cityofsydney.nsw.gov.au

23 August 2019

Our Ref: S077041
File No: 2019/410005

[redacted]
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 [redacted]

**City of Sydney submission on Mandatory Notification of Data Breaches by NSW Public Sector Agencies**

The City of Sydney (the City) welcomes the opportunity to provide constructive feedback on the mandatory notification of data breaches by NSW public sector agencies discussion paper July 2019.

We have provided responses to your questions below:

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

Yes, the NSW Government should introduce a mandatory data breach notification scheme for serious data breaches for NSW public agencies in the interests of consistency, transparency and openness. It is recommended for reporting purposes, that statistics for types of organisations (e.g. Councils) are grouped together (rather than reporting individually), which will encourage reporting.

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

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

Yes, legislation should require NSW public sector agencies to report breaches to the Information and Privacy Commission where unauthorised access to or disclosure of personal information has occurred.

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

No, because it would be unworkable. The internal processes and complaint mechanisms of an organisation should identify if there has been a breach of the Information Protection Principles and education should prevent this from occurring. Additionally, it would be a higher threshold than required by the Commonwealth NDB scheme.

**Question 3:**

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

Yes, as long as it is defined clearly and guidelines are provided on how this would work in practice.

**(b) Should legislation define the term serious harm?**

No, we suggest that this is defined in a guideline.

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

No, we suggest guidelines (which should be a mandatory consideration) are introduced because they can be updated more readily than legislation and are a best practice approach. The guidelines would need to outline the factors to consider, and could be similar to GIPA OPIAD considerations.

**Question 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?**

Yes, this is a pragmatic approach. The City does not see any value to be gained by the reporting of 'near misses' or other breaches of information protection principles that do not have a potential direct impact on those affected. The City suggests the focus for reporting be limited to those that are "likely to cause serious harm".

***Question 5:***

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

We recommend that the following is notified to the NSW Privacy Commissioner in relation to data breaches:

1. Information about the breach, including when it happened.
2. Description of the data that has been disclosed.
3. What the agency is doing to control or reduce the harm.

We recommend that the following is notified to affected individuals in relation to data breaches:

1. Information about the breach, including when it happened.
2. Description of their data that has been disclosed.
3. What the agency is doing to control or reduce the harm of their data being disclosed.
4. Information about the individual's right to lodge a privacy complaint with the NSW Privacy Commissioner and contact details for the IPC.

It is beyond the City's remit to include what steps the person can take to further protect themselves so we do not recommend including it as required information.

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

No, guidelines would be sufficient.

**Question 6: What notification timeframe should be prescribed in the legislation?**

There should be two timeframes:

1. Initial notification to NSW Privacy Commissioner and affected individuals – as soon as practicable after becoming aware that a reportable breach has occurred (but within 5 days).
2. Completion of investigation and steps taken to resolve it to NSW Privacy Commissioner – 30-60 days from becoming aware that a reportable breach has occurred.

**Question 7**:

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

No, because the NSW Privacy Commissioner can already impose orders under section 55 of the Privacy and Personal Information Protection Act.

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

No, the City agrees with the 'preferred approach of the Commissioner to work with entities to encourage and facilitate compliance with the obligations of the scheme'. Additionally, section 55 (2)(a) of the Privacy and Personal Information Protection Act has provision for requiring the public sector agency to pay to the applicant damages up to $40,000 compensation for any loss or damage suffered because of its conduct.

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

The exemptions in the current Privacy and Personal Information Protection Act are sufficient.

Should you wish to speak with a Council officer about this submission, please contact [redacted]

Yours sincerely

[redacted]

**Monica Barone**
Chief Executive Officer