Deloitte Risk Advisory Pty Ltd
ACN 611 748 184

Grosvenor Place
225 George Street
Sydney NSW 2000
PO Box N250 Grosvenor Place
Sydney NSW 1220 Australia

Tel: +61 2 9322 7000
Fax: +61 2 9322 7001
www.deloitte.com.au

23/08/2019

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

RE: Submission to the NSW Department of Communities and Justice on Mandatory Notification of Data Breaches by NSW Public Sector Agencies

This submission responds to the invitation from the Department of Communities and Justice to comment on whether a mandatory reporting scheme for data breaches should be adopted in NSW under the *Privacy and Personal Information Protection Act 1988* (PPIP Act).

Deloitte supports the introduction of a mandatory reporting scheme for NSW public sector agencies affected by data breaches and views this as a step towards bridging the gap between Commonwealth and state jurisdictions with regard to the reporting and management of data breaches. Deloitte suggests that the requirements set forth in the scheme largely align with those of the Commonwealth *Privacy Act 1988* to further support a harmonisation of privacy laws and regulations across Australia in the future.

Introduction

Our research over the years has demonstrated that Australians value transparency, and that transparency fosters trust between individuals and the organisations that they share their personal information with. Deloitte's own research in this space, as revealed in the Deloitte Australian Privacy Index 2019, found that transparency after a breach can and often does increase the chance that a consumer remains with a brand. In fact, 86% of consumers reported their trust in a brand would increase after a breach if timely and transparent notification was given.[1] We are confident that this finding would also apply to where NSW government agencies and departments are concerned.

There has been significant uplift of global privacy laws in recent years and the overwhelming themes and key focus areas of this uplift have been on transparency and on giving control over personal information back to individuals. The introduction of mandatory reporting would allow NSW public sector agencies to align themselves with this shift by being transparent about breaches when they occur, and in turn, empowering individuals to take action to minimise the chance of resulting harm to them.

The Asia Pacific Privacy Guide produced by Deloitte highlights that the rise of data breaches globally, in frequency and volume, has put pressure on governments to introduce mandatory data breach notification requirements.[2] It is clear that underreporting of data breaches has been the norm under the voluntary data breach reporting scheme that currently exists within NSW with only 45 voluntary notifications received by the Information Privacy Commission NSW (IPC) in the year 2017-18.[3] The introduction of the Commonwealth Notifiable Data Breaches (NDB) scheme saw a large increase in the number of data breaches reported to the Office of the Australian Information Commissioner (OAIC), over what had been

[1] Deloitte Australian Privacy Index 2019 – Trust: Is there an app for that? https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-150519.pdf

[2] Unity in Diversity, The Asia Pacific Privacy Guide, 2019, https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-unity-diversity-privacy-guide.pdf

[3] Discussion Paper, Mandatory notification of data breaches by NSW public sector agencies, 2019, https://www.justice.nsw.gov.au/justicepolicy/Documents/Mandatory%20data%20breach%20discussion%20paper.doc

reported under the preceding voluntary scheme. The recent Commonwealth NDB scheme 12-month insights report states that 1132 notifications were received by the OAIC in the first year of the scheme with 964 of them deemed "eligible data breaches".[4]

The introduction of the Commonwealth NDB scheme strengthened Australia's privacy framework and brought Australia in line with other jurisdictions, including the European Union (EU), the United Kingdom (UK) and the United States (US) with regard to mandatory reporting. The adoption of a mandatory reporting scheme at the state level will be a further step to potentially introducing a national standard for Australia and will address a key gap in privacy regulation in Australia caused by the multi-jurisdictional approach to privacy.

We have provided our response to the consultation questions below.

Consultation questions

Question 1: Should the NSW Government introduce a mandatory data breach notification scheme for NSW public sector agencies?
Deloitte supports the introduction of a mandatory data breach notification scheme for NSW public sector agencies and largely agrees with the reasons set forth by the NSW Government in the Discussion Paper. Mandatory data breach notification is an important transparency measure, which the IPC has already recognised through the existing voluntary scheme and through encouraging NSW public sector agencies to adopt breach reporting as a responsible business practice. Given the significant economic and reputational impacts that data breaches expose organisations and agencies to, introducing mandatory data breach notifications can be an effective instrument to require NSW government agencies to uplift their privacy practices.

Deloitte concurs that the primary rationale for mandatory data breach notification is to allow individuals whose personal information has been compromised in a data breach to take remedial steps to lessen the adverse impact that might arise from the breach, such as financial loss or identity theft. A key benefit of mandatory reporting is that it introduces a different lens to assessing breaches, one that puts individuals at the centre, through the assessment of the risk of serious harm to them.

The Deloitte Australian Privacy Index 2019 research found that government has 'had a significant drop in trust in privacy' over the years, ranking number two on the Privacy Index in 2016 and 2017, number three in 2018 and dropping to number eight in 2019.[5] The introduction of mandatory data breach notifications could enable government agencies to further build up trust with individuals.

Deloitte recommends that a mandatory data breach scheme for NSW public sector agencies be aligned with the current Commonwealth NDB scheme. This will ensure consistency across both state and Commonwealth laws and begin to set a national standard on Data Breach Notifications.

To avoid doubt when we use the term 'agencies', we believe that a NSW mandatory data breach notification scheme should apply to all NSW departments, executive agencies, state-owned corporations, universities established under state legislation and other state agencies.

Question 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?
Deloitte agrees that legislation should require NSW public sector agencies to report breaches where unauthorised access to or disclosure of personal information has occurred. Implementing a legislative requirement to report all data breaches may not be practicable for agencies to comply with and could in

[4] Office of the Australian Information Commissioner, Notifiable Data Breaches scheme 12-month insights report 2019 https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

[5] Deloitte Australian Privacy Index 2019 – Trust: Is there an app for that? https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-150519.pdf

some cases create more harm than good, particularly where reporting would not lessen the impact of the breach. The complaints mechanisms available to individuals under both Commonwealth and NSW privacy regulations already provide avenues to individuals to seek resolve for breaches to other privacy requirements which may affect them.

Question 3:

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

Deloitte suggests that the current threshold of 'likely to result in serious harm' is appropriate and that there is a benefit with aligning the reporting threshold with that of the Commonwealth NDB scheme. Deloitte suggests that there should be additional guidance provided in support of the legislation to assist agencies to understand and interpret this threshold.

(b) Should legislation define the term serious harm?

Deloitte agrees with the point made in the Discussion Paper that the term serious harm is not required to be defined, while noting that providing additional guidance in support of the legislation would be beneficial. This could minimise confusion around the meaning of the term, the subjectivity of the assessment made and provide a clear and common direction for all agencies by setting the minimum expectations.

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

As mentioned above, Deloitte believes that additional guidance supporting the legislation would be beneficial to ensure consistency and minimise confusion and subjectivity around what serious harm means and how to assess it.

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?

Deloitte suggests that legislation should require NSW public sector agencies to report only those data breaches where the agency has been unable to prevent the likely risk of serious harm with remedial action. Reporting of data breaches which are not serious could result in undue alarm and distress to individuals, lead to notification fatigue and expose organisations to reputational damage, even if they have taken the necessary steps to contain the breach and to prevent harm to individuals.

Question 5:

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

Deloitte suggests that the IPC should align the suggested content of the notification with the content required under the Commonwealth NDB scheme. Streamlining the terminology and content and aligning the method of notification with that of the Commonwealth NDB scheme requirements will achieve consistency, begin to set a national standard and will streamline reporting for those agencies who may have obligations to report to under both schemes, such as state government agencies that hold tax file number information (TFN), that are prescribed NSW state owned corporations under section 8 of the Commonwealth Privacy Regulation (2013)(such as Essential Energy, Ausgrid and Endeavour Energy) or who are otherwise required to report due to contractual obligations to the Commonwealth.

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

Deloitte suggests that the legislation should prescribe the form and content of the notification through the use of templates as this will further streamline the scheme and set the standard for agencies to ensure that all agencies are clear on what is expected of them when reporting a data breach. This will also ensure that the IPC has accurate and consistent records for record keeping.

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

Deloitte recommends that the notification timeframe that should be prescribed within the legislation should be consistent with the timeframe set by the Commonwealth NDB scheme. In Deloitte's experience of assisting organisations to prepare for and respond to data breaches under the Commonwealth NDB scheme, the timeframe set by the scheme gives organisations a reasonable amount of time to investigate

Deloitte.

data breaches and perform a thorough assessment, whilst still requiring reporting where reasonable grounds to believe an eligible data breach has occurred have already been established, in an expeditious manner.

Question 7:

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

Deloitte believes that the existing powers of the NSW Privacy Commissioner are not sufficient to allow it to effectively enforce compliance. Specific powers to compel agencies to conduct independent security reviews and implement specific measures to reduce the risk of future breaches should be in place to ensure that this scheme is effective. Further, orders or determinations of the Commissioner of this nature should be enforceable by the NSW Courts.

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

Deloitte does not consider monetary fines to be the correct deterrent for non-compliance with the proposed scheme for public sector agencies, on the condition that orders and determinations made to enforce compliance with the scheme and underlying information security standards are enforceable by the IPC.

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

Deloitte suggests that any exemptions from the requirements to notify individuals and the IPC of eligible data breaches should align with the exemptions under the Commonwealth NDB scheme.

Final comment

Deloitte welcomes the introduction of mandatory notification of data beaches by NSW public sector agencies. We thank you for the opportunity to comment on the Discussion Paper.

[redacted]

[redacted]