Office of the Information Commissioner
Queensland

18 June 2021

Level 7
133 Mary Street
Brisbane Q 4000

PO Box 10143
Adelaide Street
Brisbane Q 4000

Phone (07) 3234 7373
www.oic.qld.gov.au

ABN: 70 810 284 665

Department of Communities and Justice
Locked Bag 10
STRAWBERRY HILLS NSW 2012

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

Consultation draft of the Privacy and Personal Information Protection Amendment Bill 2021

The Queensland Office of the Information Commissioner (OIC) welcomes the opportunity to provide a brief submission in response to the Department of Communities and Justice's consultation draft of the Privacy and Personal Protection Amendment Bill (the Bill).

About the OIC

The OIC is an independent statutory body that reports to the Queensland Parliament. We have a statutory role under the *Right to Information Act 2009* (RTI Act) and the *Information Privacy Act 2009* (IP Act) to facilitate greater and easier access to information held by government agencies. We also assist agencies to understand their obligations under the IP Act to safeguard the personal information they hold.

OIC's statutory functions include mediating privacy complaints against Queensland government agencies, issuing guidelines on privacy best practice, initiating privacy education and training, and conducting audits and reviews to monitor agency performance and compliance with the RTI Act and the IP Act. Our office reviews decisions of agencies and Ministers about access to, and amendment of, information under the RTI and IP Act.

OIC's Submission

OIC supports the aims of the Bill to strengthen privacy protections in NSW by establishing a mandatory data breach (MNDB) scheme to require public sector agencies bound by the *Privacy and Personal Information Protection Act 1998* (PPIP Act) to notify affected individuals and the NSW Privacy Commissioner of data breaches relating involving personal or health information likely to result in serious harm. OIC notes the proposal to extend the application to state-owned corporations not regulated by the Commonwealth *Privacy Act 1988* (Privacy Act).

As noted by the OAIC, 'the requirement to notify individuals of eligible data breaches goes to the core of what should underpin good privacy practice for any entity—transparency and accountability. Being ready to assess and, if appropriate, notify of a data breach provides an opportunity for entities to understand where privacy risks lie within their operations, to address the human and cyber elements that contribute to data breaches and to prevent or minimise harm to individuals and the community….The requirements under the NDB

scheme incentivise entities to ensure they have reasonable steps in place to secure personal information'.[1]

The Notifiable Data Breaches Scheme (NDB) under the Commonwealth Privacy Act appears to be functioning well and is a critical element in managing data breaches and mitigating privacy risks for individuals. It also is a necessary element for Australia to achieving adequacy under the GDPR.

As states and territories look to adopt this requirement in their jurisdictions, it is important that there is national consistency, to the greatest extent practicable, to ensure the efficacy of the system and reduce any unnecessary duplication or regulatory burden on government agencies.

Public sector agencies may already have obligations to comply with mandatory reporting obligations under the NDB scheme, for example where the breach relates to tax file numbers. OIC notes the proposed MNDB has been designed to adopt, as far as possible, key features of the Commonwealth NDB scheme to reduce interjurisdictional consistencies, limiting the impact of this overlap and reducing regulatory burden.

OIC supports alignment of notification thresholds in the proposed MNDB scheme with the Commonwealth NDB scheme. OIC notes that 'serious harm' is not defined in the Bill. What constitutes serious harm will depend on the circumstances of each breach. OIC further notes that the Bill prescribes a number of factors to consider when assessing whether an eligible breach is likely to cause serious harm. As outlined in the fact sheet,[2] it is intended that judicial and academic consideration of the Commonwealth NDB scheme threshold will be used, aiding consistency of interpretation and application. Different thresholds can cause community uncertainty and unnecessary anxiety as demonstrated by the PAGE UP world-wide data breach.

OIC also supports the proposal to confer additional regulatory powers on the NSW Privacy Commissioner, including powers of entry and inspection, conducting audits and furnishing reports to the head of agency and responsible minister, to aid enforcement and compliance with the proposed MNDB scheme.

OIC will continue to support the introduction of a mandatory data breach scheme in Queensland, recommended as part of legislative reform to Queensland's privacy legislation,[3] and seek alignment with the requirements of the Commonwealth NDB scheme, to the greatest extent possible.

Your sincerely

[redacted]

[redacted]

[redacted]

[1] https://oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

[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

[3] Recommendation 12, Crime and Corruption Commission Queensland, *Operation Impala – Report on misuse of confidential information in the Queensland Public Sector*, February 2020; Recommendation 13, Report on the review of the *Right to Information Act 2009* and *Information Privacy Act 2009* (Review report), October 2017. Recommendation 13 of the Review report states 'conduct further research and consultation to establish whether there is a justification for moving towards a single set of privacy principles in Queensland, and whether a mandatory data breach notification scheme should be introduced'.