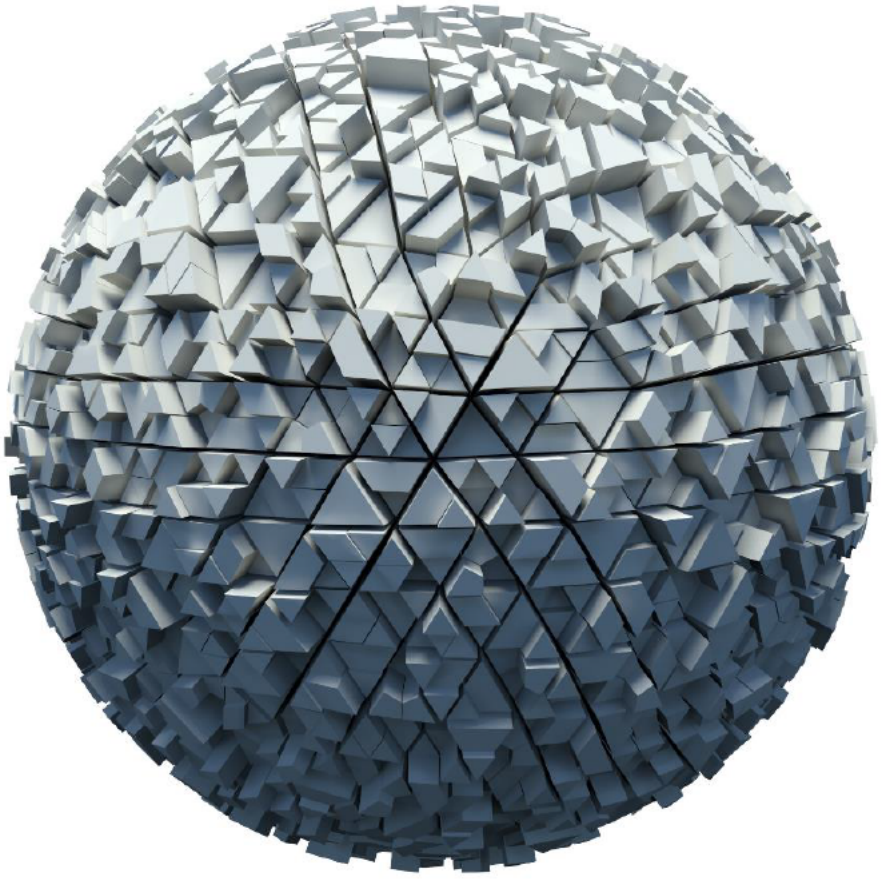
Deloitte.



Draft Privacy and Personal Information Protection Amendment Bill 2021

Deloitte Submission on the proposed changes to the Privacy and Personal Information Protection Act 1998

17 June 2021

Context

In July 2019, the NSW Department of Communities and Justice ('**DCJ**') released a discussion paper relating to the mandatory notification of data breaches by NSW public sector agencies ('**PSAs**') and which supported the introduction of a mandatory reporting scheme for NSW PSAs affected by data breaches. Submissions were invited from the public in response to the paper, to which Deloitte responded with its perspective.

On 7 May 2021, the DCJ published the Bill and has invited Deloitte to provide a submission in response to the proposed changes to amend the PPIP Act as contained in the Bill to:

- introduce a Mandatory Notification of Data Breach Scheme ('**MNDB Scheme**'); and
- extend the application of the PPIP Act's definition of public sector agencies to apply to all NSW State-Owned Corporations ('**SOCs**') not currently captured by the Privacy Act.

Note: There are other legislative changes proposed as part of the Bill (e.g. to repeal section 117C of the *Fines Act 1996*). Deloitte is only providing comments on the changes outlined in Divisions 1, 2, 3, 5 and 6 of the Bill.

While not directly related to the Bill and our submission, it is noted that the Australian Federal government is also reviewing the *Privacy Act 1988* (Cth) (**'Privacy Act'**). On 30 October 2020, the Attorney-General's department published an issues paper relating to this review and invited submissions in response to the review matters for consideration.[1] This issues paper considered whether the current scope of the Privacy Act and its enforcement mechanisms are fit for purpose. The impact and effectiveness of the Commonwealth Notifiable Data Breach Scheme ('**NDB Scheme**') was an area of focus to be considered to better ensure the NDB Scheme:

- Promotes the protection of the privacy of individuals and raises awareness about the importance of data security while balancing the interests of entities governed by the Privacy Act as part of carrying out their legitimate functions and activities[2].
- Improves the data security practices of entities governed by the Privacy Act[3].
- Allows individuals to take actions to protect themselves from a likely risk of serious harm as a result of a data breach that involves their personal information.[4]

A discussion paper is now anticipated to be released later in 2021 to seek more specific feedback on the preliminary outcomes of this issues paper and the submissions received in response to it. This includes possible options of legal reform to address the privacy issues identified.

As the Information Privacy Commissioner (**'IPC'**) is continuing to uplift the *Privacy and Personal Information Protection Act 1998* (NSW) ('**PPIP Act**'), in particular the data breach reporting requirements through the draft *Privacy and Personal Information Protection Amendment Bill 2021* (NSW) ('**Bill**'), Deloitte encourages the DCJ to follow the progression of the Privacy Act review and the changes anticipated to be made at the Commonwealth level.

Introduction

This submission provides comments, insights and considerations informed by Deloitte's practical privacy advisory experience, our previous submission provided in 2019, [5] and our consumer and industry research.

Deloitte continues to support the creation of an MNDB Scheme for NSW PSAs. We reassert our support for the PPIP Act to apply to all NSW SOCs not currently captured by the Federal Privacy Act.[6] The proposed changes present significant benefits and opportunities to:

1. Give new powers to the IPC to facilitate the monitoring of data breach management.
2. Instil public trust in the ability of NSW PSAs to protect and manage personal information.
3. Provide greater clarity to NSW PSAs about which breaches need to be reported to affected individuals.

[1] Attorney-General's Department, *Privacy Act Review Issues Paper,* October 2020, p18.
[2] Attorney-General's Department, *Privacy Amendment (Notifiable Data Breaches) Bill 2016 Regulation Impact Statement* (Regulation Impact Statement, 11 January 2017), p15.
[3] Attorney-General's Department, *Privacy Act Review Issues Paper,* October 2020, p81.
[4] Ibid p75.
[5] Ibid.
[6] Deloitte, *Deloitte Submission to the NSW Department of Communities and Justice on Mandatory Notification of Data Breaches by NSW Public Sector Agencies,* August 2019, p2.

4. Provide individuals with an opportunity to mitigate the harm that is, or could be, caused to them by a breach.
5. Create a consistent reporting process for NSW PSAs to reduce under-reporting in some agencies and alleviate the compliance burden where PSAs are required to notify other regulatory bodies in addition to the OAIC and IPC.

We have provided our comments based on these benefits and opportunities below.

Proposed privacy changes, benefits, and opportunities

1. **The MNDB Scheme gives new powers to the IPC that will facilitate the monitoring of data breach management. However, Deloitte considers that these powers are still not sufficient to allow the IPC to effectively enforce compliance with the Scheme.**

Deloitte welcomes the introduction of section 59Y of Division 5 in the Bill, which will give the IPC the power to investigate, monitor, audit and report on agencies for compliance with the MNDB Scheme. This power allows the IPC to identify systemic issues that may result in data breaches and monitor responses to these issues. However, the IPC is not provided with the ability to compel agencies to implement specific measures to remedy these issues. Giving the IPC the power to compel agencies to implement specific measures will likely reduce the risk of future breaches and should be in place to ensure that the proposed Scheme is effective at improving NSW PSAs privacy and data management practices, and at reducing the occurrence of data breaches that are likely to result in serious harm.[7] This power should take the form of an order or determination made by the IPC and Deloitte recommends that orders or determinations of this nature should be made enforceable by NSW Courts.

In addition to this power, we also suggest introducing a specific power to enable the IPC to compel agencies to conduct independent security reviews. This power, combined with the ability to request NSW PSAs to report to the IPC on their security compliance with the MNDB Scheme, would alleviate the regulatory burden placed on the IPC as the Commission could then exercise its audit powers on such agencies as the IPC selects, without being required to audit every agency. Deloitte agrees that the exercise of these regulatory powers should be based on an escalated model of engagement.[8] To help ensure that the selection of NSW PSAs is objective and appropriate, we suggest the Privacy Commissioner exercises his/her power to conduct an audit on a NSW PSA only where:

- specific privacy complaints have been lodged or otherwise made known to the IPC; and/or
- findings are produced from an independent security review against the specific PSA, as relating to the PSA's compliance with the MNDB Scheme.

2. **The proposed MNDB Scheme is a crucial transparency measure that will instil public trust in NSW PSAs and their ability to protect and manage personal information.**

Deloitte's privacy research has highlighted a steady increase in the privacy awareness of Australian consumers over several years, particularly in relation to the personal information that they share and the transparency expected from the organisations that they interact with. Through our annual Australian Privacy Index, we have tracked consumer trust across multiple industries (including in the government and public sector) from 2015-2021. We found that trust remains the primary driver affecting a person's interactions with any organisation, public or private.[9]

MNDB schemes are considered best practice globally to promote transparency and accountability in the way that entities handle personal information. This is reflected by the quick spread of mandatory breach reporting laws in numerous jurisdictions across the globe. For example, the introduction of the Commonwealth Notifiable Data Breach scheme in 2018 brought Australia in line with several US states, the European Union, the United Kingdom, South Korea, the Philippines, China, Indonesia, Taiwan and Canada. Our research over the years consistently demonstrates that Australians also value transparency when it comes to how their personal information is processed and that transparency builds trust between individuals and the organisations they share their personal information with. In particular, the 2018 Deloitte Australian Privacy Index found that transparency after a breach can and often does increase the chance that a consumer remains with a brand, with consumers reporting that their trust in a brand would increase after a

[7] Deloitte, *Deloitte Submission to the NSW Department of Communities and Justice on Mandatory Notification of Data Breaches by NSW Public Sector Agencies,* August 2019, p3.
[8] NSW Department of Communities and Justice, *Privacy and Personal Information Protection Amendment Bill 2021 – Factsheet*, 2021, p6.
[9] Deloitte, *Deloitte Australian Privacy Index 2021 – Seeing beyond the surface: The future of privacy in Australia,* 2021, https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index.html.

breach if timely and transparent notification was given.[10] We are confident that this finding would equally apply to the reputation of, and trust held for, NSW PSAs as part of introducing the MNDB Scheme.

The IPC already recognises the importance of data breach notification through the existing voluntary data breach reporting scheme and by encouraging NSW PSAs to adopt notification as a responsible business practice.[11] The IPC also publishes several fact sheets and guidelines to encourage timely and transparent notification and appropriate data breach management, such as the 'Data Breach Guidance for NSW Agencies'[12] and the 'Data breach prevention checklist'.[13] Although this regulatory guidance is made available to the public and NSW PSAs via the IPC's website, data breach notification is still not mandated at the NSW level. As a result, it is unlikely that all NSW PSAs have a documented data breach procedure or policy in place, nor other mechanisms to effectively manage data breaches from the identification of a breach to its assessment, mitigation, reporting and post incident review.

Deloitte agrees that:

- The existing voluntary data breach reporting scheme needs to be replaced by an MNDB Scheme.
- Current regulatory guidance needs to be supported by the introduction of minimum organisational mechanisms to guide effective management of data breaches by NSW PSAs, as proposed by Division 6 of the Bill, in addition to establishing assessment, notification and reporting requirements.

Given the significant economic and reputational impacts that data breaches expose organisations to, and their potential to disrupt trust in government processing of citizen information, introducing the MNDB Scheme can be an effective instrument to require NSW PSAs to uplift their data breach management practices. Deloitte considers that uplift is particularly required for privacy practices related to developing and embedding a data breach policy, and maintaining a data breach register to facilitate incident review procedures that consider process improvements for prevention and response. As a result, Deloitte agrees with the introduction of sections 59ZC, 59ZD and 59ZE in Division 6 of the Bill, requiring NSW PSAs to each publish a data breach policy, keep a public notification register, and maintain an internal register of data breaches. The existence and continuous maintenance of these mechanisms for data breach management demonstrates to individuals that NSW PSAs take their responsibility to protect personal information seriously, which is integral to building and maintaining trust in NSW PSAs and their ability to appropriately collect, store, use, secure and disclose personal information.

A breach is also likely to result in a near-vertical spike in demand on an organisation's internal operations, so one challenge will be having enough resources to continue business-as-usual operations alongside setting up an effective breach response operation.[14] Having a data breach policy in place would allow PSAs to prepare for such an occurrence and plan how resources should be allocated. Introducing a requirement to maintain an internal data breach register is also beneficial because a register gives organisations the ability to track common themes and address root causes of similar breaches by providing an overarching view of all data breaches encountered. It also requires NSW PSAs to keep appropriate records and will support the expeditious assessment of data breaches.

Research from the 2020 Deloitte Australian Privacy Index found that government has 'had a significant drop in trust in privacy' since our first index in 2015.[15] Each year we ask 1,000 consumers which brands they trust the most and the least with their privacy. Those results are aggregated across industry sectors, returning a net negative or positive trust in privacy score. In 2020 and 2021, government returned a near-zero result, meaning there were as many consumers saying they trusted government brands as there were that distrusted them.[16] Although this drop in trust is not specific to NSW PSAs only, it is notable that across the same period (2020-2021) a number of NSW PSAs encountered high-profile and wide-reaching data breaches. The introduction of an MNDB Scheme that guides and mandates NSW PSAs to provide individuals with timely and transparent notification could enable the ability of NSW PSAs to rebuild trust with individuals.

---

[10] Deloitte, *Deloitte Australian Privacy Index 2018 – The Symbiotic Relationship: Getting the balance right,* 2018, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-privacy-index-2018.pdf.
[11] Information Privacy Commissioner, 'Voluntary Data Breach Notification', https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification, accessed June 10, 2021.
[12] Information Privacy Commissioner, *Data Breach Guidance for NSW Agencies,* September 2020, https://www.ipc.nsw.gov.au/media/816.
[13] Information Privacy Commissioner, *IPC Data Breach Prevention Checklist*, https://www.ipc.nsw.gov.au/media/822
[14] Deloitte, *Deloitte Canada Insights 2018 – Taking a customer-centric approach to a data breach: Insights from crisis response*, 2018, https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-Data-Breach-Customer-Centric-POV-EN-AODA.pdf.
[15] Deloitte, *Deloitte Australian Privacy Index 2020 – Opting-in to meaningful consent,* 2020, https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-australian-privacy-index-2020.pdf.
[16] Deloitte, *Deloitte Australian Privacy Index 2021 – Seeing beyond the surface: The future of privacy in Australia,* 2021, https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index.html.

3. **Introducing an MNDB Scheme will allow NSW PSAs to have greater clarity about which breaches need to be reported to affected individuals.**

Deloitte understands that notification is not always an appropriate response to a breach, and a key challenge for NSW PSAs will be to determine if and when individuals should be notified. The proposed MNDB Scheme will help bring clarity to this. Deloitte agrees with the introduction of Division 2 of the Bill, which would clarify what sort of data breach is an 'eligible data breach' and help agencies assess whether they have experienced an 'eligible data breach' that would require them to notify affected individuals.

As suggested in our previous submission, Deloitte considers that additional guidance supporting the legislation (for example, in the form of a fact sheet) would be beneficial to help ensure consistency, minimise confusion and subjectivity around what serious harm means and how to assess it when evaluating the eligibility of a data breach.[17] In Deloitte's experience, organisations often find such guidelines or fact sheets particularly useful for training purposes and for providing their staff with further clarity around the rights and obligations contained in the law.

Introducing an MNDB Scheme would also cut down on unnecessary over-reporting by providing certainty for NSW PSAs and their staff regarding what actions should be taken if a privacy breach occurs. The reporting of data breaches that are ineligible could result in undue alarm and distress to individuals and lead to notification fatigue where affected individuals become less likely to proactively protect themselves because they are notified about an influx of security incidents which may not necessarily be likely to result in serious harm to them.[18] The reporting of ineligible data breaches could also cause reputational damage to agencies, even if they have taken the necessary steps to contain the breach so that the breach is no longer likely to result in serious harm to individuals. As a result, Deloitte agrees with the introduction of s59T of Division 4 in the Bill, which exempts NSW PSAs from notifying affected individuals if action has been taken to mitigate the harm so that the data breach would no longer likely cause serious harm.

4. **The requirement to notify affected individuals of an eligible data breach under the proposed MNDB Scheme provides individuals with an opportunity to mitigate the harm caused by a breach.**

Informing affected individuals of when privacy breaches have occurred provides those individuals with an opportunity to take remedial actions to lessen the adverse impact that might arise from the breach. These adverse impacts include identity theft or fraud, which can cause financial loss to those individuals or lead to broader cybercrime.[19] As a result, Deloitte agrees that a critical benefit of introducing an MNDB Scheme is to offer consumer protection. Deloitte considers that the proposed MNDB Scheme is an opportunity to prescribe NSW PSAs to evaluate breaches through the lens of the consumer by requiring agencies to assess a breach according to the likelihood of serious harm to the individual.

Deloitte welcomes the introduction of s59C of Division 1 in the Bill, which mandates the reporting threshold as being a data breach that "would be likely to result in serious harm to an affected individual".[20] As a result, where serious harm is likely to result from a breach and meets the reporting threshold, mandated notification allows an individual to take steps to remediate this harm. For example, notification in this way might allow an individual to change passwords where those passwords have been hacked or to cancel credit cards if details have been stolen.[21]

5. **By mandating when notification is required, the proposed MNDB Scheme creates a consistent reporting process for NSW PSAs, which will capture those data breaches not currently captured by the existing voluntary scheme.**

Although some NSW PSAs are currently reporting breaches to the IPC under the existing voluntary scheme, it is likely that not all data breaches, including those that could result in serious harm, are being reported. Deloitte's Asia Pacific Privacy Guide highlights the rise, both in frequency and volume, of data breaches globally;[22] however, under the voluntary data breach reporting scheme in NSW, only 79 voluntary

[17] Deloitte, *Deloitte Submission to the NSW Department of Communities and Justice on Mandatory Notification of Data Breaches by NSW Public Sector Agencies,* August 2019, p3.
[18] Ibid, p4.
[19] Ibid, p3.
[20] *Privacy and Personal Information Protection Amendment Bill 2021 (NSW*), s59C.
[21] Department of Communities & Justice, *Mandatory Notification of Data Breaches by NSW Public Sector Agencies Discussion Paper*, July 2019, p 9.
[22] Deloitte, *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.

notifications were received by the Information Privacy Commission in the 2019-2020 financial year.[23] The Commonwealth experience also suggests that voluntary data breach notification schemes are not well utilised as the introduction of the NDB Scheme resulted in a large increase in reported data breaches.[24] For example, the Office of the Australian Information Commissioner (OAIC) reported that notifications increased by 712 per cent during the first year of the Commonwealth NDB Scheme from 2018–2019.[25] The NDB Scheme's 12-month insights report states that 964 notifications of eligible data breaches were received by the OAIC in the first year of the scheme from the 2018-2019 period.[26] In 2020, this number increased but remained relatively steady, with the OAIC receiving 1,051 notifications.[27] Without a clear and consistent mandated legislative framework, agencies will likely continue to adopt different approaches to manage and report data breaches. Some agencies may report all data breaches, some may report serious breaches only, while others may not report at all.

Deloitte also agrees with the introduction of section 59D of Division 2 in the Bill, which specifies that an agency must assess a data breach within 30 days and promptly notify individuals as soon as practicable if eligible. Deloitte concurs with this proposed timeframe as it is consistent with that set by the Commonwealth NDB Scheme, which also requires organisations to assess data breaches within 30 days. In Deloitte's experience as part of assisting organisations to prepare for and respond to data breaches under the Commonwealth NDB scheme, the timeframe set by the NDB Scheme provides organisations with a reasonable amount of time to investigate data breaches and perform a thorough assessment, whilst still ensuring reporting is conducted expeditiously.

Deloitte welcomes the fact that provisions in the Bill concerning notification timeframes, the reporting threshold and assessment requirements are closely consistent with those in the NDB Scheme. This consistency will alleviate some of the compliance burden on NSW PSAs who have reporting obligations under both the state and the federal frameworks (e.g. an agency that collects Tax File Numbers); however, the compliance burden will not be completely addressed. The issues paper for the review of the Commonwealth Privacy Act identified that the emergence of other notification schemes can increase entities' compliance burdens because of the requirement to notify other regulatory bodies in addition to the OAIC, and that notification frameworks could be streamlined to avoid duplication.[28] The issues paper also identified that an area impacting the effectiveness of the NDB Scheme is the effective navigation of multi-party breaches.[29] The proposed section 59R of Division 4 in the Bill is the same as its parallel provision in the NDB Scheme; it mandates that only one agency is required to carry out notification if a multi-agency breach occurs. If that agency takes the steps required under the MNDB Scheme, this constitutes compliance for all agencies that hold the information; though if no agency takes the necessary steps, all affected agencies have breached their obligations.

In reviewing the Commonwealth NDB Scheme, the OAIC identified this provision as an area for improvement.[30] For example, despite the fact that under the NDB Scheme only one entity is required to carry out notification in a multi-party breach (in the same way as under the proposed MNDB Scheme), between April to June 2018 the OAIC received more than 50 notifications from a single supplier entity and its clients in relation to a single incident.[31] It was reported that individual consumers also received multiple notifications relating to the data breach, creating the potential for confusion.[32] The OAIC recommends that entities with the most direct relationship with individuals affected by a data breach carry out the notification.[33] The OAIC also recommends that confusion and duplication can also be pre-empted by addressing accountabilities for notification and the assessment of harm in data breach response plans and supplier contracts.[34]

---

[23] Information Privacy Commission, *IPC Voluntary Breaches Quarterly Statistics: FY2019/20 Q1 & Q2*, https://www.ipc.nsw.gov.au/sites/default/files/2020-03/IPC_Voluntary_Breaches_Quarterly_Statistics_FY2019-2020_Q1%262.pdf; Information Privacy Commission, *IPC Voluntary Breaches Quarterly Statistics: FY2019/20 Q3 & Q4*, https://www.ipc.nsw.gov.au/sites/default/files/2021-02/IPC_Voluntary_Breaches_Quarterly_Statistics_FY2019-2020_Q3_Q4_.pdf.
[24] Department of Communities & Justice, *Mandatory Notification of Data Breaches by NSW Public Sector Agencies Discussion Paper*, July 2019, p8.
[25] Office of the Australian Information Commissioner, *Notifiable Data Breaches Scheme 12-month Insights Report*, 13 May 2019, https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/ndb-scheme-12month-insights-report.pdf, p3.
[26] Ibid.
[27] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report July to December 2020,* 28 January 2021, https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/2020-2/Notifiable-Data-Breaches-Report-July-Dec-2020.pdf.
[28] Attorney-General's Department, *Privacy Act Review Issues Paper*, October 2020, p18.
[29] Ibid, p79-80.
[30] Office of the Information Commissioner, *Notifiable Data Breaches Scheme 12-month Insights Report*, 13 May 2019, https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/ndb-scheme-12month-insights-report.pdf, p16.
[31] Ibid, p17.
[32] Ibid.
[33] Ibid.
[34] Ibid.

Final comment

Deloitte welcomes the proposed changes to the PPIP Act outlined by the Bill to strengthen privacy obligations placed on NSW PSAs. We also recognise benefits and opportunities to further enhance aspects of the Bill to:

- Encourage and improve efficient and proactive data management practices for NSW PSAs.
- Hold NSW PSAs accountable to notify and report eligible data breaches.
- Improve the current interoperability of New South Wales privacy law with the Privacy Act and in doing so, address a key gap caused by the Federated approach to privacy by better aligning NSW privacy obligations to Commonwealth privacy obligations, as well as international trends in privacy regulation.
- Potentially introduce a uniform scheme across Australia.
- Better meet public expectations on protecting the personal information of individuals residing in New South Wales.

We thank the NSW Department of Communities and Justice for the opportunity to comment on the Bill and look forward to providing support as part of future consultations required to progress the Bill.

Contact us

[redacted]

Acknowledgements

[redacted]

Deloitte.