information and privacy commission
new south wales

Enquiries: Sarah Wyatt
Telephone: 1800 472 679
Our reference: IPC19/A000292

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 Sir/Madam,

Mandatory notification of data breaches by NSW public sector agencies

The purpose of this correspondence is to provide a submission to the discussion paper prepared by the Department of Communities and Justice (the Department) entitled *Mandatory notification of data breaches by NSW public sector agencies* (July 2019) (Discussion Paper).The following comments are provided for consideration by the Department.

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

There is currently no obligation to report data breaches under the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) or otherwise in NSW. Currently agencies are encouraged to voluntarily report breaches to the Privacy Commissioner and develop robust processes to identify potential and actual breaches, as well as, identify steps to mitigate against the breaches. Agencies are also encouraged to voluntarily notify the aggrieved persons of the breach and their rights under the PPIP Act.

To support the voluntary data breach reporting scheme, the Information and Privacy Commission (IPC) has developed guidance and other resources to assist agencies, including a notification template.[1] We continue to support and encourage the robust reporting of voluntary breaches of privacy by public sector agencies under the current legislative arrangements.

The adoption of a scheme which facilitates greater reporting would be valuable and would support and promote responsible privacy practices. A mandatory data breach reporting scheme is supported in principle, subject to a proper consultation process.

The NSW Government is committed to using technology and data to better integrate government services and improve the quality and level of services available. The adoption of a mandatory data breach scheme would assist in supporting and promoting

[1] https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification

public confidence and trust in the Government's use of technology and data to improve outcomes and services for the public.

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?

With reference to [4.5] of the Discussion Paper we note that in order to be considered an eligible data breach (requiring notification under the Commonwealth Notifiable Data Breaches (NDB) Scheme), there needs to be unauthorised access to or disclosure of personal information. Examples of unauthorised access or disclosure include malicious action (by an external or insider party), human error, or a failure in information handling or security.

The NDB scheme does not require entities to report breaches of any Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth).

We consider that the requirements under a mandatory data breach scheme in NSW should operate independently from the requirements associated with the Information Protection Principles (IPPs) that are analogous to the APPs. This is because, like the APPs, the IPPs are directed to different, and at times broader, information governance principles concerning personal information. There are already operative complaint and review avenues for persons aggrieved to: the Privacy Commissioner, agencies and NSW Civil and Administrative Tribunal with respect to breaches of IPPs.

We consider that reporting under a NSW mandatory data breach scheme should be triggered in the same way that it is under the NDB Scheme by unauthorised access to or disclosure of personal information rather than by reference to a breach of an IPP.

Question 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?

With regard to the Office of the Australian Information Commissioner's report: *Notifiable Data Breaches Scheme 12-month Insights Report*[2] we note that there has been a 712% increase in notifications since the introduction of the NDB Scheme. This increased reporting under the NDB Scheme was the result of applying the 'serious harm' threshold (for which the Office of the Australian Information Commissioner has issued guidance). In that context, we are therefore supportive of applying the same threshold to a NSW scheme.

The IPC has published guidance on its website that assists agencies to identify the serious impacts of a data breach and how to determine that these have occurred.[3]

We support NSW legislation prescribing indicative factors that an agency must consider as a minimum when assessing whether a data breach meets the threshold of serious harm. The list is not to be considered exhaustive. With reference to the IPC's *Data Breach Guidance*, we suggest such factors may include:

---

[2] https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/ndb-scheme-12month-insights-report.pdf

[3] https://www.ipc.nsw.gov.au/data-breach-guidance

- The type and scope of data that has been breached – does it include financial, health or other sensitive categories of data, or a combination? Are there other characteristics of the data that could pose a high risk (e.g. commercial information that could pose a reputational risk to an agency or other organisation, or information that could result in the compromise of a person's identity)?

- The data context – does the breach affect data that would normally be publicly available, or is the data known to be very poor quality that if used could create risk to individuals?

- How easy would it be for individuals to be identified from this data?

- The circumstances of the breach – for example, was it a single incident (such as the loss of a USB or laptop) or a malicious attack that poses an ongoing risk, or was data altered in a way that it would pose a risk to the individuals to whom the data relates?

- The number of individuals/ entities affected by the data breach.

Inclusion of a threshold test would also enable better reporting and inform the regulatory response by the IPC. An effective definition may better support responses from both an operational and cultural perspective for agencies and citizens.

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?

As noted at [4.14] of the Discussion Paper, the Commonwealth NDB scheme provides that a breach is not an eligible data breach if an entity acts quickly to remediate the breach, and as a result of this action, a reasonable person would conclude that the breach is not likely to result in serious harm. This is intended to provide entities with an incentive to take positive steps to address data breaches in a timely manner.

While we note the value of this objective we consider that the NSW scheme should not replicate this aspect of the NDB Scheme. This is because doing so may not adequately address and could in fact compound under-reporting of breaches and delayed reporting of breaches. We suggest that in reporting under a NSW scheme, remedial action, where it is taken on or around the time of reporting should be referred to and included in the notice to the Privacy Commissioner. However, the remedial action taken should not negate the reporting requirement.

Consistent with comments regarding data sharing and reporting contained within this submission the IPC would be in a position to report against action taken/advised by agencies and this provides a strong accountability measure and may positively impact public trust in government agencies. It is noted that not all remedial action taken occurs in a single occurrence. Some remedial action may form part of a broader remedial action plan. Importantly, the requirement to report should be at the point of assessment and not only in circumstances where the agency has determined that it is unable to prevent a likely risk of serious harm by remedial action.

Question 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?

The *IPC Data Breach Policy* provides guidance about what a notification to the Privacy Commissioner should contain.[4] We suggest the content of a notification should contain:

- information and a description about the breach, including when and how it happened
- details of the date that the Agency first became aware of the breach
- a description of what data has been disclosed
- assurances (as appropriate) about what data has not been disclosed
- what the agency is doing to control or reduce the harm
- what steps the person/organisation has taken to protect and negate further disclosure
- the number of persons affected (or potentially affected)
- whether the affected persons have been advised
- information about the agency's remedial action plan
- information as to whether any reports have been made to other relevant bodies (e.g. Cyber Security NSW, law enforcement agencies)

We support legislation prescribing the form and content of the notification. In this regard, a non-exhaustive approach may serve that objective. This will ensure consistent reporting across regulated entities. However we also recommend that consultation is conducted with agencies to ensure that operational experience informs the policy and legislative response by government.

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

With reference to [4.23] of the Discussion Paper, it is noted that the Commonwealth NDB scheme requires entities to take all reasonable steps to investigate within 30 working days of becoming aware that there may have been an eligible data breach.[5] Once the entity has reasonable grounds to believe there may have been such a breach, the Australian Information Commissioner and affected individuals must be notified as soon as practicable. We note the time frame for notification differs across jurisdictions referred to in the Discussion Paper. We suggest a suitable notification time frame in NSW of 10 working days. We suggest this time frame having regard to the immediacy of the impact of data breaches that generally require a swift response and remedial action.

Question 7 – (a) Does the NSW Privacy Commissioner require any additional powers to encourage compliance with a mandatory notification scheme? (b) Should monetary penalties apply where NSW public sector agencies fail to comply with the requirements of the scheme?

The Privacy Commissioner should be given the following additional powers in support of compliance with a NSW mandatory data breach scheme, some of which are commensurate with those of the Information Commissioner:

- The power to investigate agency systems, policies and practices and conduct audits: see, for example, Division 3 of Part 3 of the *Government Information (Information Commissioner) Act 2009* (NSW) (GIIC Act).

[4] <https://www.ipc.nsw.gov.au/sites/default/files/2018-12/IPC_Data_Breach_Policy_Nov2016.pdf>

[5] Section 26WH of the *Privacy Act 1988* (Cth).

- The power to accept enforceable undertakings, like the Australian Information Commissioner (AIC), which are enforceable in the Federal Court and Federal Circuit Court. The undertakings may be published on the OAIC website and require an entity to refrain from undertaking a specified action, comply with the *Privacy Act* and not interfere with the privacy of an individual.[6]

- The power to share information with other key regulators, such as Cyber Security NSW, State and federal law enforcement and the AIC. See for example Division 5 of Part 3 of the GIIC Act.

-The power to make recommendations to agencies, see for instance section 95 of the *Government Information (Public Access) Act 2009* (NSW) (GIPA Act).

With reference to [3.13] of the Discussion Paper, we note that the Australian Community Attitudes to Privacy Survey 2017 found that 94 per cent of respondents agreed that they should be told if a business loses their personal information.[7] Ninety-five per cent of respondents agreed that they should be told if a government agency loses their personal information.[8] In our view, the community attitude is that data breaches are a significant issue and the community expects that their sensitive information and data will be held and stored by government securely. Monetary penalties would signify to the community that non-compliance in data management is a serious matter that warrants serious consequences via monetary penalty. There are analogous regulatory schemes, such as that administered by the Australian Securities and Investments Commission that utilise monetary penalty powers to great effect.

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

We note the exceptions from the requirement to notify under the Commonwealth NDB scheme set at [4.32] of the Discussion Paper. Such exceptions would be suitable for a NSW scheme and as the Discussion Paper notes, in NSW, law enforcement and investigative agencies are already exempted from certain requirements under the PPIP Act.

Other relevant comments

Dual reporting obligations

There are currently a small number of NSW public sector agencies (that collect tax file number information) with reporting obligations under the NDB Scheme. Consideration should be given to the impact on agencies that fall within the scope of both the NDB Scheme and the proposed NSW scheme. Reporting obligations will become particularly onerous if the two schemes operate under different definitions or different thresholds for determining an eligible breach.

Jurisdictional overlap and dual obligations are also apparent in another context. Currently the *Health Records and Information Privacy Act* 2002 (NSW) (HRIP Act) provides a legislative and jurisdictional overlap in relation to complaints about private health service providers. This arises because of the definition of 'health service

[6] Section 80V, Privacy Act; Gabriella Rubagotti, 'Social Media and Privacy' in Patrick George, (ed), *Social Media and the Law* (Lexis Nexis Butterworths, 2nd ed, 2016) 136.

[7] Office of the Australian Information Commissioner, Australian Community Attitudes to Privacy Survey, 2017, p. 16.

[8] Ibid.

provider'. Complainants may be asked to decide if they wish to make their complaint under either the NSW legislation or under the Commonwealth *Privacy Act 1998*. Once the complainant chooses the jurisdiction they would like the complaint to be dealt under, they cannot seek further assistance from the other jurisdiction if they are later dissatisfied with the outcome of the complaint (see HRIP Act section 43(2)(f)). Consideration will need to be given to how private health providers would be covered where a mandatory data breach scheme is introduced in NSW and they are likely covered by the NDB Scheme.

Resource Impacts

Consideration will need to be given to the resource impacts for the IPC from the introduction of a mandatory data breach scheme. The Discussion Paper does not address this issue.

Introduction of a mandatory scheme in NSW is likely to result in an increase of reports to the IPC requiring review and investigation. Although not directly comparable due to its differing jurisdictional remit, it is noted that the Office of the Australian Information Commissioner experienced a 712% increase in notifications during the first 12 months of operation of the NDB Scheme compared with the previous 12 months under the previous voluntary scheme. The OAIC's *Notifiable Data Breaches Scheme 12-month Insights Report* noted, at page 9:

> Growth in the number of data breaches after the introduction of mandatory reporting is consistent with trends overseas. In the Netherlands, Germany and United Kingdom, approximately 15,400, 12,600 and 10,600 breaches were notified to supervisory authorities respectively in the first eight months after the GDPR took effect. It should be noted that notification thresholds under each country's respective schemes and population sizes differ substantially compared with Australia.

The IPC would also need to direct resources into the development of new information guidance for both the public sector and citizens and develop educational resources for agencies, possibly in the form of an e-learning module. Other resources, such as the privacy self-assessment tool[9] would need to be updated to reflect the introduction of a mandatory notification scheme.

Additionally, the IPC would need to undertake a review of its existing case management system to accommodate and reflect the requirements of any new legislative scheme. The IPC's case management system would support the operation of the scheme and enable reporting to the Privacy Commissioner.

Introduction of investigative and other powers for the Privacy Commissioner to appropriately support the scheme would necessitate a review of IPC resources. Currently the IPC adopts a risk-based proportionate approach to the exercise of regulatory functions. This approach would be applied to additional functions within the remit of the IPC. However, the introduction of a mandatory notification scheme must be accompanied by an appropriate regulatory response to the notification. If the scheme is to operate according to a 'serious harm' threshold public expectation would legitimately foresee that the regulator would take a regulatory response commensurate to that 'serious harm'. The regulatory response is inextricably linked to the availability of

[9] <https://www.ipc.nsw.gov.au/information-governance-agency-self-assessment-tools-information>

regulatory resources. There is a risk to the integrity of any notification system that does not adequately consider the resultant resource implications.

GIPA Act considerations

A consequence of a data breach is that information is 'revealed' to the world at large. Many of the public interest considerations against disclosure listed in the Table in section 14 of the GIPA Act refer to something being 'revealed' by disclosure of the information in question. Clause 1 of Schedule 4 of the GIPA Act defines 'reveal' information as meaning to 'disclose information that has not already been publicly disclosed (otherwise than by unlawful disclosure).' Where something is publicly disclosed it is difficult to resist disclosure with reference to an overriding public interest consideration against disclosure. It is arguable that disclosure by data breach may amount to unlawful disclosure. In *McInnes v NSW Department of Education and Communities* [2013] NSWADT 219 at [43] the Tribunal stated that '[o]nce information is known by an applicant, it cannot then be revealed or disclosed, unless it was originally revealed by unlawful means.' The Tribunal's analysis draws at [42] on the authority that 'it is not possible, according to the ordinary use of language, to 'disclose' to a person a fact of which he is, to the knowledge of the person making a statement as to the fact, already aware': *Foster v Federal Commissioner of Taxation* (1951) 82 CLR 606.

Consideration should be given to the relationship and effect of a NSW mandatory data breach scheme with other information governance legislation, such as the GIPA Act.

Under Schedule 2 of the GIPA Act, information that relates to complaint handling and investigative functions of an agency is excluded information. This means that an application for access to government information that seeks excluded information of an agency is an invalid access application. An access application cannot be made to an agency for access to excluded information of the agency.

Information about the Privacy Commissioner's review, complaint handling, investigative and reporting functions is excluded information under the GIPA Act. Consideration should be given to whether the Privacy Commissioner's functions under the mandatory data breach scheme in NSW would fall within the functions identified in the GIPA Act as excluded. We consider that there should not be a mechanism to access information via the GIPA Act about information derived from the exercise of the Privacy Commissioner's functions under a mandatory data breach scheme in NSW. That said, we support publication of statistics about the operation of a mandatory data breach scheme and the IPC already publishes quarterly statistics about the voluntary scheme in NSW.[10]

Consideration should also be given to the information sharing provisions under both the PPIP Act and the GIIC Act because in exercising regulatory functions either Commissioner may be assisted by the power to share information relevant to data breaches by affected agencies and/or agencies more broadly. This power may also better assist the functions of the Privacy Commissioner in particular who may seek to undertake preliminary enquiries with other agencies regarding data breaches, and disclosure of some relevant information may be necessary in conducting those enquiries.

Finally, the Information Commissioner released in May 2019 a statutory guideline: *Guideline 7 – Open Data and Opening Government Data*.[11] A mandatory data breach scheme in NSW should make clear that there are types of data that should be open and

[10] <https://www.ipc.nsw.gov.au/privacy/voluntary-data-breach-notification>

[11] <https://www.ipc.nsw.gov.au/sites/default/files/2019-05/GIPA_Guideline_7_Open_Data_May_2019.pdf>

that public sector agencies have dual obligations to both protect and open data as required.

Additionally, consideration of a mandatory data breach notification scheme may need to explore the operation of extant legislation in NSW and the digital environment. For example, government is increasingly applying data to conduct impact analysis in public policy decision-making (including gender impact analysis given its clear relationship to faster economic growth). Impact analysis is reliant upon appropriate information sharing. Currently, information sharing between agencies is not expressly authorised under legislation; rather exemptions or legislation-specific authorisations may be introduced to permit such sharing. In such cases there is the potential for concerns regarding unauthorised access to or disclosure of personal information even in controlled environments.

There may be opportunities presented in considering the introduction of a mandatory data breach notification scheme to recognise appropriate classification of breach types or indeed information/data classifications and in doing so identify mechanisms to facilitate appropriate information sharing between agencies within the jurisdiction of the scheme. Tests including acting in 'good faith' or for 'a proper purpose' provide established legal tests that may have application in facilitate sharing of appropriate information under controlled environments.

I hope these comments will be of assistance. Please do not hesitate to contact us if you have any queries. Alternatively, your officers may contact Sarah Wyatt, Director, Legal Counsel and Regulatory Advice on 1800 472 679 or by email at [redacted]

Yours sincerely

[redacted]

Elizabeth Tydd
Information Commissioner
19/8/19

[redacted]

Samantha Gavel
Privacy Commissioner
19/8/19