

Partnerships Directorate: Response to the Privacy and Personal Information Amendment Bill 2021

Context

The *Privacy and Personal Information Protection Act 1988* (PPIP) regulates how New South Wales public sector agencies manage personal information and sets out the functions of the NSW Privacy Commissioner. The proposed *Privacy and Personal Information Protection Act 1988* (Amendment Bill) seeks to strengthen the protection of privacy in NSW by creating a Mandatory Notification of Data Breach (MNDB) scheme.

A MNDB scheme will require public sector agencies bound by the PPIP Act to notify the Information and Privacy Commissioner (IPC) and affected individuals of data breaches of personal or health information likely to result in serious harm.

Consultation for the Amendment Bill is currently underway, and it is anticipated that the bill will be introduced into the NSW Parliament in 2021, and if passed the MNDB scheme will commence 12 months following the passage of legislation.

Non-Government Organisations (NGOs) key partners in DCJ service delivery

DCJ contracts with non-government organisations (NGOs) and providers to deliver services on behalf of Government our clients and communities. These contracts currently contain obligations to comply with legislation; this includes the PPIP.

By way of background, DCJ contracts with over 1400 NGOs and providers to deliver a range of human service programs to vulnerable people across NSW.

The types of service providers are diverse, ranging from small community organisations to large national NGOs. Smaller community organisations are often dependant on volunteers to function, and reliant on small grant funding. This contrasts with larger NGO's which have highly developed service delivery models, established corporate functions and various levels of funding through state and federal programs.

In addition, the Corrective Services Directorate delivers a small number of significant contracts across 3 locations for private prisons, as well as several smaller contracts for electronic monitoring and security services.

Implications of the scheme

To determine the implications of the proposed changes to the PPIP on contracted NGOs and providers, the Partnerships Directorate consulted with the following DCJ business areas.

- Open Government and Information and Privacy branch
- Commercial Law branch
- Corrective Services, Governance and Continuous Improvement.

The view of DCJ Commercial Legal team is:

On the basis that section 4(4)(b) of PPIP Act deems personal information held by an agent/contractor of public sector agency to be information held by the public sector agency, it would seem that any unauthorised access to, or unauthorised disclosure of, personal information held by an NGO to whom DCJ has outsourced services, has the potential to constitute an "eligible data breach" under s59C of the Privacy and Personal Information Protection Amendment Bill (Bill), and if the public sector agency reasonably suspects that an eligible data breach has occurred (which pre-supposes some knowledge by the public sector agency of the data breach), then responsibility for complying with the new mandatory notification scheme will lie solely with the public sector agency.

By virtue of the current contract provisions NGOs and providers are required to comply the PPIP Act. These existing contract obligations mean that NGOs or providers are required to report any breaches of personal or health information to DCJ. As part of our partnership we work closely with them to manage breaches, which may or may not involve reporting the breach to the Information and Privacy Commissioner (IPC).

Given the above advice, NGOs and providers are covered by the legislation and the proposed changes. However, the Amendment Bill needs to be more explicit about this and how best to manage the proposed changes - whether it is legislative or by contract obligation.

Ways to manage the proposed changes

On consideration of the proposed changes, we have explored two options to manage the change given the significance of NGO and provider services delivered on behalf of DCJ:

1. Propose an amendment to the Amendment Bill to make it an obligation that NGOs notify the public service agency of the data breach and require the appointment of an assessor to assess the breach and make the results of the assessment and action available to DCJ
2. In the absence of legislative provisions, DCJ strengthen our policy position by amending contract obligations to require NGOs to inform DCJ, appoint an assessor and make results of the assessment and action available to DCJ.

As the Amendment Bill currently reads, the MNDB scheme has several issues that will need to be addressed before we implement the scheme for contracted NGOs or providers:

- The role of the public sector agency or the NGOs/providers in the assessment and reporting of any eligible data breach as part of the scheme. There is some confusion about whether the NGO/provider or the public sector agency has the responsibility to report to IPC.
- The administrative and reporting burden for NGOs to meet the requirements of the scheme. There is an argument that this additional reporting requirement will increase the burden of reporting on NGOs/providers. NGOs are not-for-profit organisations that have a significant reliance on government funding or funds raised through donations or philanthropy. NGOs are likely to seek additional funds to compensate them for these additional obligations to ensure compliance. In the case of Corrective Service contracts, providers could consider a change in mandatory policy a case for entitlement to request costs from the State. Given DCJ does not have additional funds it is possible that providers would then be required to draw upon existing funds. This impact may then have a flow on effect to the level of program outputs achieved for vulnerable clients and communities, and then outcomes reported to the NSW Treasury.
- Additional administrative requirements on DCJ contract and legal teams to work with providers to assess and manage the scheme obligations. This will add to the administrative burden on teams administering the contracts at a time of increasing efficiency and with limited resources.
- The proposed legislative changes require that the Information Privacy Commissioner draft guidelines on breaches that are deemed to cause significant harm. This may necessitate DCJ preparing further guidance material and providing additional support to providers during the implementation phase of the change.
- Finally, DCJ has in excess of 2,000 contracts with NGOs or providers that may need to be amended if a change to the Bill is not considered an option. The introduction of the scheme requires providers to report all serious harm breaches, however current contracts have differing provisions on information and privacy. These DCJ contracts have different cycles of review and timing of the introduction would need to support a staggered implementation for contracted service providers to be compliant with the scheme under the PPIP Act.

Proposed actions/changes

In summary, please consider the following information and input as part of the consultation process for the draft legislative changes.

1. Amend the *Privacy and Personal Information Protection Act 1988* (Amendment Bill) to impose a legislative obligation on NGOs or providers to inform the public service agency of the information privacy breach and to work with the agency in the assessment and notification of the breach.
2. If this is not available, DCJ would need to amend existing contract obligations to reflect similar action, with implementation and compliance to occur after the legislation comes into effect for new contracts and contract renewals.
 - DCJ would need to strength our policy position by amending contract obligations that require NGOs to inform DCJ, appoint an assessor and make results available for contract obligations.
 - Given the significant number of contracts, this would be a time-consuming process to vary agreements, or alternatively align the changes to planned reviews of agreements over the next 2 years. In the case of the Human Services Agreement, it is a contract common to several NSW Government agencies (DCJ, NSW Health and NSW Education). Other contracts may have different review cycles and a phase implementation of the obligations may need to be considered.
3. The Information and Privacy Commissioner should provide clear guidance on the criteria and decision-making process for determination of serious harm to guide NGO's in advice to DCJ as the appropriate reporting authority.

Approval

Role	Electronic approval by	Date
[Redacted]		