18 June 2021

Project Team
Policy, Reform and Legislation Branch
Department of Communities and Justice
Via email: Policy@justice.nsw.gov.au

Reference:

Submission to the Privacy and Personal Information Protection Amendment Bill 2021

Dear Policy Team,

Thank you for the opportunity to provide feedback on the *Privacy and Personal Information Protection Amendment Bill 2021* (**PPIPA Bill**). Sydney Water has been consulted on the proposed privacy framework for State-owned Corporations (SOCs) back in late 2019 and early 2020 and we broadly welcome the announcement with this Bill that SOCs will be subject to the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**).

We would like to submit the following comments based on our review of the PPIPA Bill.

Commencement timing:

We note that within the consultation factsheet that public sector agencies will have 12 months from the time the legislation is enacted to commence operating under the changes. We consider that this timeframe is sufficient for the introduction of the mandatory notification of data breach (MNDB) scheme for public sector agencies, however as a State-owned Corporation (SOC), we would recommend that:

- SOCs are given 12 months to be compliant with the PPIP Act, and
- A further 3-6 months to introduce measures to support the MNDB scheme

We feel that this is a reasonable request and timeframe that would allow a SOC with no previous formal compliance obligations with respect to the personal information it manages, to introduce a compliance program to sufficiently cover its practices.

Our concern, if we were to have the same commencement date apply to our compliance with the PPIP Act and with the MNDB scheme, is it will potentially expose us to the risk of inadvertent noncompliance given the likely compounding of compliance measures that will be required under each of the PPIP Act and the MNDB scheme. Should anything occur, we are concerned that this could lead to potential unfavourable attention of those affected, the regulator and the community.

Further, if we were to have the same commencement date apply to our compliance with the PPIP Act and with the MNDB scheme, this would require us to significantly increase our resourcing

requirements to support the changes needed internally for compliance with the PPIP Act and with the MNDB scheme. This was previously raised in a meeting with members of the Policy Team in March 2021.

Therefore, we recommend that a staggered approach to compliance be introduced for SOCs to initially:

- Comply with the PPIP Act, followed by
- Compliance with the MNDB scheme

Retrospectivity:

We had raised and it was confirmed verbally by the Policy teams that retrospective compliance is not considered as part of object of the Bill. However, we reiterate that we do not expect that the Bill introduces retrospective requirements for SOCs to be covered by the requirements of the PPIP Act.

Privacy Management Plan (PMP):

We note that within Sect 33 of the PPIP Act, public sector agencies have a 12 month period to prepare and implement a privacy management plan (PMP). Does the same 12 month period apply to SOCs, or is the intention that SOCs will have a PMP prepared and implemented by the time the amendments come into effect?

We see the development of a PMP essential for us to provide our customers, staff and other members of the community with relevant information about our privacy practices. Therefore, we seek to have this clarified.

Section 59ZH – Privacy Commissioner may make guidelines:

With the introduction of the MNDB scheme, it is our desire to see a suite of guidelines from the Privacy Commissioner with respect to the scheme. The capability shift that is required within the sector may vary from public sector agencies, however it is crucial to the success of the MNDB scheme that the sector receives decisive guidance and leadership from the Privacy Commissioner. This section leaves the issuing of guidance as an option to our reading.

To have a successful introduction of such a scheme, we recommend that the Privacy Commissioner be required to make guidelines, therefore the term ‘may make’ be replaced with ‘will issue’.

Further, within the draft bill, sub-section (2)(c) I would replace ‘given’ with ‘give’.

We thank you once again for the opportunity to provide feedback on the proposed changes, and welcome the opportunity to discuss our feedback in further detail, should it be required.

Yours sincerely