Department of Customer Service response to Discussion Paper: Mandatory notification of data breaches by NSW public sector agencies

Question 1:

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

Yes, the *Privacy and Personal Information Protection Act 199*8 (PPIP Act) should be amended to include mandatory data breach notification. A mandatory data breach notification scheme for the NSW public sector agencies would:

- bring the NSW Government into alignment with the Commonwealth Notifiable Data Breach (NDB) scheme
- ensure that NSW public sector agencies are consistent in their data breach notifications
- clarify agency obligations and give the NSW public greater certainty about the safety and security of their personal information.

The scope of the scheme should be clearly defined, for example would this include local councils and universities as well as department and agencies?

Question 2:

Should legislation require NSW public sector agencies to report breaches:

(a) Where unauthorised access to or disclosure of personal information has occurred?

Yes. This should mirror the Commonwealth NDB scheme which represents a good balance between openness and accountability and protecting agencies from a significant reporting burden.

(b) Where any breach of an Information Protection Principle has occurred?

No, non-compliance with the Information Protection Principles does not necessarily represent a data breach because the scope of the principles is broader than data breaches.

Question 3:

(a) Is the threshold of 'likely to result in serious harm' appropriate, or should a different standard be applied?

Yes, this is an appropriate threshold.

(b) Should legislation define the term serious harm?

There should be a broad definition of serious harm: 'serious harm may include serious physical, emotional, financial or reputational harm'. However, this does not need to be prescribed in legislation. The broad definition should be supported with examples and guidance.

(c) Should legislation prescribe the factors an agency must consider when assessing whether a data breach meets the threshold of serious harm?

A set of assessable factors or a checklist would be a valuable resource for considering if serious harm could be caused by a data breach. Again, this does not need to be prescribed in legislation.

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?

Yes, the NDB scheme encourages quick and effective remedial action that effectively prevents the serious impacts of the data breach. Timeframes should be established within which action must be taken.

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?

NSW should follow the NDB Scheme whereby the entity must provide a notification statement that contains:

1. The identity and contact details of the notifying entity
2. A description of the data breach
3. The kind or kinds of information concerned
4. Recommendations to individuals about the steps that they should take to minimise the impact of the breach

The NSW Privacy Commissioner should provide an online form to help entities lodge notification statements and provide additional supporting information.

Any data breaches that are cyber related should also be reported to Cyber Security NSW. If there is a vulnerability, this could permeate multiple agencies. Cyber Security NSW needs to have as much information as possible in order to send intelligence products to the NSW Government.

Question 6:

What notification timeframe should be prescribed in the legislation?

The notification timeframe should align with the seriousness of the breach.

Tier 1 – compulsory notification within 24 hours for breaches where the serious harm threshold is met (noting the need for a clear definition of serious harm).

Tier 2 – compulsory notification within 10 days for all other eligible breaches.

Question 7:

a) Does the NSW Privacy Commissioner require any additional powers to encourage compliance with a mandatory notification scheme?

The NSW Privacy Commissioners powers should be aligned with those of the Commonwealth Commissioners, including Direction to notify and Declaration that notification need not be made, or that notification be delayed.

b) Should monetary penalties apply where NSW public sector agencies fail to comply with the requirements of the scheme?

Not to begin with, however this should be reviewed after 12 months.

Question 8:

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

The exceptions granted in the NDB scheme are reasonable and transferrable to a NSW State Government scheme.