GPO Box 4052,
Sydney, NSW 2001

icare.nsw.gov.au

Consultation Paper on Mandatory Notification of Data Breaches by NSW Public Sector Agencies

Questions

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

   If mandatory notification of privacy breaches is implemented, icare's view is that it should be limited to serious breaches and that the scope and implementation are appropriate in the light of the potential administrative burden. In this regard, the setting of realistic time-frames, clear and concise definitions and manageable obligations are essential.

2. Should legislation require NSW public sector agencies to report breaches:

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

      To the extent that mandatory notification of breaches is introduced, icare is of that view is that it should be limited to breaches resulting from unauthorised access to or disclosure of personal information, provided that such breaches are likely to result in serious harm and are not able to be/have not been mitigated.

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

      icare considers that making a breach of the Information Protection Principles subject to mandatory notification would impose an unacceptable administrative burden on agencies such as icare and on the NSW Privacy Commissioner.
      The principles are replete with concepts such as 'such steps as are reasonable in the circumstances', 'not excessive' and 'an unreasonable extent'. Reasonable minds may differ as to the interpretation of these concepts.
      Additionally, little interpretive assistance is provided by cases considering the principles as many of them are tribunal decisions that rely on specific facts.

3.

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

      See answer 2(a) above.

b) Should legislation define the term 'serious harm'?

Yes, the clarity and certainty of legislative guidance is desirable. Consistency with the Commonwealth NDB scheme would likewise be desirable.

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

Yes, provided that such factors are clear and unambiguous and that the list is inclusive. Icare sees some benefit in these factors aligning with those in the Commonwealth NDB scheme.

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, this approach would minimise unnecessary distress to the relevant individual. It would also reduce the administrative burden on agencies such as icare and align with the Commonwealth NDB scheme.

5.

a) What information should be notified to the NSW Privacy Commissioner and affected individuals in relation to data breaches?

The legislation should create a distinction between notification of the NSW Privacy Commissioner and the individual. The former should receive information as per cl 4.18 of the consultation paper, with an exemption for information that is not readily available in the light of an agency's limited resources. The latter should receive similar information, but in plain English, and with a focus on remedial action that the individual may take and that the agency is taking.
Additionally, the legislation should permit the agency to consider the safety of any individual when framing the content of a notification.

b) Should the legislation prescribe the form and content of the notification?

In relation to form:
Yes, provided that it admits different methods resulting from technological advances.
In relation to content:
Yes, provided that the legislation aligns with answer 5(a) above, does not impose an excessive administrative burden and is clear and unambiguous.

6. What notification timeframe should be prescribed in the legislation?

   A distinction should be made between breaches that may lead to possible harm to an individual and/or involve potentially criminal conduct and those of a less serious nature. The former should be notified as soon as is practicable, or not later than 30 days (in line with the Commonwealth NDB scheme).

   All other breaches should be notified within 60 days (unless there are extenuating circumstances), in line with notification requirements of internal reviews. icare submits that this is a realistic time-frame, given the quantity of information and complexity of the storage systems that such agencies use.

   In particular:
   icare estimates it currently manages (88, 000) claims on behalf of the Nominal Insurer, the NSW Self-Insurance Corporation and a number of other schemes.

   It is worth noting that icare has been voluntarily notifying the NSW Privacy Commissioner of serious data breaches in relation to these claims since January 2016.

   icare is concerned that, if there is insufficient time allowed for the provision of a notice, the resultant hasty decisions may lead to undesirable consequences.

7.

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

      The Privacy Commissioner already has expansive powers under s36 of the *Privacy and Personal Information Protection Act 1998.*

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

      No response.

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

   No response.