I·C·A·C
INDEPENDENT COMMISSION
AGAINST CORRUPTION
NEW SOUTH WALES

Policy, Reform and Legislation Branch
NSW Department of Communities and Justice
By email: policy@justice.nsw.gov.au

2 September 2019

Our Ref: AD19/0115

Dear Sir or Madam,

**SUBJECT: Mandatory notification of data breaches by NSW public sector agencies**

The NSW Independent Commission Against Corruption (the Commission) has received the discussion paper *Mandatory notification of data breaches by NSW public sector agencies* (the discussion paper) and submits the following comments for consideration.

*A mandatory notification scheme*

The Commission agrees that there should be a scheme for the mandatory notification of privacy breaches.

The Commission agrees the scheme should include some form of seriousness test such as the "likely to result in serious harm" threshold described in the discussion paper. This will assist agencies and the Information and Privacy Commission (IPC) to focus limited resources on the matters that are most damaging. However, the Commission does not have a firm view about how to specify the required test.

*Overlap with the Commission's jurisdiction*

The definition of corrupt conduct is set out in ss 7-9 of the *Independent Commission Against Corruption Act 1988* (ICAC Act). Among other things, corrupt conduct can include:

> "*any conduct of a public official or former public official that involves the **misuse of information or material** that he or she has acquired in the course of his or her official functions, whether or not for his or her benefit or for the benefit of any other person*" (s8(1)(d), emphasis added).

Self-evidently, this could include the misuse of personal information.

The ICAC Act also has a mandatory reporting provision, set out in section 11. This requires the principal officer of each public sector agency to report any "*matter that the person suspects on reasonable grounds concerns or may concern corrupt conduct*".



Level 7, 255 Elizabeth Street, Sydney NSW 2000 | GPO Box 500 Sydney NSW 2001 | ABN 17 934 402 440
T 02 8281 5999 | F 02 9264 5364 | E icac@icac.nsw.gov.au | www.icac.nsw.gov.au

Consequently, there exists the potential for overlap between the Commission's jurisdiction and the matters reported under the proposed mandatory notification scheme. This overlap exists with or without a mandatory notification scheme. However, it is likely that a mandatory notification scheme will require agencies to report certain matters to both the Commission and the IPC. Where a privacy breach relates to a cyber security event, additional reporting may be required under the NSW Cyber Security Policy. This overlap could create confusion and a level of 'reporting fatigue' among agencies.

As it has done with a number of other agencies, the Commission would be open to discussing a memorandum of understanding (MOU) with the IPC which could deal with matters that are reported to both agencies and matters that need to be referred between agencies. Subject to agreement, the terms of such a MOU might assist in limiting dual reporting by agencies.

*Form of reporting*

The ICAC Act does not prescribe the form that s11 reports must take. However, pursuant to s11(3) of the Act, the Commission issues reporting guidelines, which appear adequate. Commission staff would be happy to discuss the detail of its guidelines if requested.

*Observations about mandatory reporting*

Based on its own mandatory reporting scheme, the Commission's experience is that:

- allowing certain agencies to report by a regular schedule (e.g. quarterly) may reduce the administrative burden of reporting matters individually
- agencies should be encouraged to report urgent or time-critical matters immediately by telephone
- agencies value the ability to speak with a senior officer who can provide advice about reporting and the status of particular matters
- the requirement to report and the time taken to assess reports should not unreasonably prevent an agency from taking necessary remedial action
- administrative arrangements need to be in place to generate prompt acknowledgement letters, identify any reports that are covered by the *Public Interest Disclosures Act 1994* and properly triage incoming matters
- from time to time, agencies need to be reminded of their reporting obligations, which can be done in writing or face-to-face.

*Exemptions*

As noted in the discussion paper, law enforcement agencies such as the Commission are exempt from aspects of the *Privacy and Personal Information Protection Act 1998*. The Commission's position is that these exemptions should also extend to any mandatory notification scheme. It would not be appropriate for the Commission to report under a mandatory scheme because doing so might:

- diminish the independence of the Commission; and
- hinder the confidential and covert nature of the Commission's work, which often involves obtaining and using personal information.

As noted above, the Commission would be open to establishing a MOU with the IPC which would facilitate the exchange of information by agreement.

Thank you for the opportunity to respond to the discussion paper. Should you require any further information, please contact me [redacted].

Yours sincerely,

[redacted]

Philip Reed
Chief Executive Officer
2/9/19

Please note, ICAC is an investigative agency & the proposed
of the PPIP Act 1998 (s 24) /

[redacted]
2/9/19