23 August 2019

NSW Department of Communities and Justice

Contact: [redacted]
Our Ref: DOC2019/084172

Via email only:
policy@justice.nsw.gov.au

To Whom it May Concern

CONSULTATION ON MANDATORY DATA BREACH NOTIFICATION SCHEME

Cessnock City Council (**Council**) welcomes the opportunity to lodge a submission regarding the above noted scheme and supports the objectives of openness and transparency the Department of Communities and Justice (**the Department**) is attempting to achieve outlined in the *Mandatory Notification of Data Breaches by NSW Public Sector Agencies Discussion Paper* (**Discussion Paper**).

Council agrees with the observations in the Discussion Paper that a privacy breach can occur "*due to a technical problem, failure to take reasonable steps to manage risk of human error, inadequate policies and training, or a misunderstanding of the law and that common privacy breaches include:*

- *Sending emails to unintended recipients;*
- *Accidental loss of paper records, laptops or USB flash drives;*
- *Unauthorised access to information (for example, an employee looking up restricted information for personal reasons)".* [1]

Council also agrees with the observations that privacy breaches can occur as a result of malicious or criminal attacks which are "*deliberately crafted to exploit known vulnerabilities for financial or other gain such as phishing, malware, ransom ware, bruteforce attacks or hacks*" or deliberate acts committed by employees such as theft of paperwork or storage devices. Unsurprisingly, sixty present of notifications received by the Office of Australian Information Commissioner in the period 1 April 2018 to 31 March 2019 involved malicious or criminal attacks when compared to 35 percent of notification involving human error.[2]

Council takes privacy and protection of personal information very seriously. Hence, Council is in agreement that a mandatory data breach notification scheme for NSW public sector agencies should be introduced. Having noted this, bringing the desire to provide the public with the expected assurance into realisation needs to be realistic and proportional. Unsurprisingly and as rightfully noted by the Australian Law Reform Commission, such an

[1] NSW Department of Communities and Justice, *Mandatory Notification of Data Breaches by NSW Public Sector Agencies Discussion Paper,* July 2019, pages 5-6.
[2] Ibid, page 6.

t: 02 4993 4100 **f**: 02 4993 2500
p: PO Box 152 Cessnock NSW 2325 or DX 21502 Cessnock
e: council@cessnock.nsw.gov.au **w**: www.cessnock.nsw.gov.au
ABN 60 919 148 928

exercise comes at a cost that most likely exceeds the expected damage as a result of the privacy breach and its consequences, especially in circumstances which Council cannot control.[3]

As a local government organisation, Council collects, holds, uses and stores a vast variety of personal information and exercises its best endeavours, with the resources available, to protect this information. A lot of this personal information is unsolicited. Internal and external audits, random internal data reviews, data security software, Information Breach Security protocol and guideline, and a Cyber Security Breach Response procedure are some of the methods used to identify, monitor and protect personal information. Any non-conformances are immediately escalated to senior management and dealt with appropriately, in accordance with the Information and Privacy Commission factsheets and guidelines. Staff are trained to identify and report privacy breaches, and in instances of intentional or malicious mishandling of personal information, Council follows internal guidelines and prescribed practices in accordance with the relevant Award/Enterprise Bargaining Agreement.

Council is of the view that if a mandatory reporting scheme was introduced, NSW public sector agencies should only report where unauthorised access to, or disclosure of, personal information has occurred and not where a breach of an Information Protection Principle (**IPP**) has occurred. The reasons behind such a suggestion are:

- The IPPs place far broader obligations upon entities to the point that the burdens of such a scheme would defeat the purpose and benefits of it;

- Local councils already operate on limited resources and imposing such burdens on them would contribute to either diverting scarce resources from higher priority projects or intentional non-compliance simply because the 'numbers do not add';

- Such burdens are not imposed on federal entities under the Privacy Act, so why should council carry that load?

- It is not unreasonable to argue that even where councils can take proactive actions to remedy privacy breaches and report as required under the proposed scheme, often the public is not cooperative in providing their updated information or refusing to follow the right process to correct their personal information. This in turn can result in the whole exercise being turned into an unsuccessful fishing expedition by councils, or the public escalating matters unnecessarily which can only mean more scarce council resources being wasted away, in particular when the personal information in question was unsolicited by councils. The scheme should be structured in a way that is fair and acknowledges these burdens that can be placed on local government entities, and require individuals to be more diligent with their own personal information.

One of the concerns Council has with determining what serious breaches look like is that often, staff within roles assessing and determining whether a 'serious harm is more probable to occur than not as opposed to possible' do not have legal background to adequately interpret the intention of legislation or common law, especially in rural councils. As pointed out in the Discussion Paper, the term 'serious harm' is not defined and any supplemental guidance will always leave an opportunity for error or inconsistency in application of the law. This can prove very costly for entities as there is a risk of litigation proceedings by affected individuals which will most certainly result in negative media publicity and hence reputational damage, or even worse, loss of confidence in Council operations and functions. Should such

[3] Ibid, page 7.

consequences eventuate, it is not unreasonable to expect that councils' risk appetite portfolio would increase and result in higher insurance premiums.

The best approach the Government should take is to define the term serious harm and prescribe the factors an agency must consider when assessing whether a data breach meets the threshold of serious harm in a manner that is definitive. Legislation should also be drafted to prescribe the manner, form and content of the notification necessary and to 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. This way, councils will have an opportunity to demonstrate their commitment to protecting personal information and if they do not, they should be facing the risk of legal action, consequential costs and public condemnation by individuals involved.

Council considers the timeframe prescribed by the Commonwealth National Data Breaches Scheme reasonable – entities to take all reasonable steps to investigate within 30 days of becoming aware that there may have been an eligible data breach and as soon as the entity has reasonable grounds to believe there may have been such a breach, they are to report to the Australian Information Commissioner and affected individuals as soon as practicable. Council also considers that the imposition of penalties where privacy breaches continue to occur, in spite of the NSW Privacy Commissioner's encouragement for compliance, is reasonable. With respect to exemptions to the proposed scheme, Council is of the opinion that the only way to exercise its law enforcement and investigative functions is if such functions remain exempt from the restrictions of the IPPs under the *Privacy and Personal Protection Information Act 1998* (NSW).

Yours faithfully

[redacted]

[redacted]

Governance Officer