THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL:JvdPsl010622

1 June 2022

Ms Margery Nicoll
Acting Chief Executive Officer
Law Council of Australia
DX 5719 Canberra

By email: nathan.mcdonald@lawcouncil.asn.au

Dear Ms Nicoll,

Consultation on Australia's National Data Security Action Plan

Thank you for the opportunity to contribute to a Law Council submission in relation to the Department of Home Affairs' Discussion Paper on a proposed National Data Security Action Plan (NDSAP). The Privacy and Data Law Committee of the Law Society contributed to this submission.

General Comments

We refer to our submission to the Law Council dated 26 August 2021 relating to the Department of Home Affairs Discussion Paper titled 'Strengthening Australia's cyber security regulations and incentives', and reiterate two concerns raised in that submission that, in our view, should be front of mind when considering cyber security risk management.

(1) An impending need for cyber security agility

As cyber-attacks become increasingly sophisticated, there is an impending need to ensure cyber security practices can be regularly adapted and improved. To facilitate the adoption of new technologies, and to promote Australia's growth as a modern digital economy and a leader in AI (the ambition set out in the Australian Digital Economy Strategy and the AI Action Plan), regulatory settings should provide incentives for Australian organisations to adopt a dynamic and iterative approach to assessment, mitigation and management of cyber security risks, that tracks and responds to emerging threats and vulnerabilities.

(2) Defining the different roles of actors when managing cyber security risks across the supply chain

Often security issues arise because points of vulnerability emerge over time through a combination of devices and services, or changes to particular devices or services as used in combination or interaction with other services.

Mitigation and management of cyber security risks therefore often requires organisations to understand whether and how other entities are addressing security risks that arise within a multiparty data handling and processing ecosystem. Cybersecurity settings of each entity within this multiparty ecosystem may lead to vulnerabilities arising elsewhere in the

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000, DX 362 Sydney
ACN 000 000 699 ABN 98 696 304 966
lawsociety.com.au
T +61 2 9926 0333 F +61 2 9231 5809
E lawsociety@lawsociety.com.au

ecosystem. Security of a particular internet accessible device or service is often dependent upon configurations and other settings made by others in relation to different but interacting devices or services and over time. "Security" of a particular internet accessible device or service must therefore be assessed over time, and having regard to factors that are often outside the control of the supplier or user of a particular device or service.

Given the diversity of actors, increased complexity of supply chains for internet accessible devices and services, and the variety of contexts and scenarios of deployment and use, a 'one size fits all' regulatory requirement that a device or service must be "secure" is unlikely to provide appropriate incentives for entities across a multiparty data handling and processing ecosystem to assess and address evolving cybersecurity risks.

Consultation Question 2

How can Australian Government guidance best align with international data protection and security frameworks? Are there any existing frameworks that you think would be applicable to Australia's practices (e.g. the European Union's General Data Protection Regulation)?

The Law Society is generally supportive of the provision of Australian guidance based on the European Union's General Data Protection Regulation (EU's GDPR),[1] as it is cited as a best practice example by experts in the field, noting, however, the need for further analysis and consultation as to whether there are particular domestic contexts where generalised adoption of the GDPR could have unintended consequences.

Privacy compliance can be challenging for Australian businesses needing to navigate the requirements of overseas jurisdictions, most notably, the EU's GDPR, in order to be considered a trustworthy recipient of personal information. Without Australia, as a whole, being regarded as providing 'adequate' privacy compliance, businesses must rely on their own capabilities and resources to navigate these complex laws. Achieving GDPR adequacy would bring significant benefits to some Australian businesses in the form of reduced compliance costs associated with negotiating contractual provisions and streamlined interactions with businesses trading in the EU.

Consultation Question 6

How can data security policy be better harmonised across all jurisdictions?

The Law Society agrees with the statement in the Discussion Paper, that "the harmonisation and enhancement of data security standards across all jurisdictions will ensure public trust in the handling of personal and sensitive information is maintained to enable the growth in digital government services" (p 22).

We consider that there is a need for greater government oversight of security policy at both state/territory and Commonwealth level, and would support appropriately targeted and balanced regulation of uses of new and emerging technologies by both the public and private sectors.

In our view, a key element of a harmonised data security policy should be the protection and promotion of the human rights of all people, and especially vulnerable and disadvantaged groups, as this is critical to building enduring public trust in those technologies. The right to privacy is recognised as a fundamental human right in Article 12 of the *Universal Declaration of Human Rights*, Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR),

[1] *Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) [2016] OJ L 119/1.

Article 16 of the *Convention on the Rights of the Child* (CRC) and other instruments and treaties. Australia's obligations under the ICCPR and CRC – which Australia ratified in 1980 and 1990 respectively – require enhanced protections against breach of privacy, to protect against incursions of privacy enabled by new technologies.

Another key element of a harmonised data security policy should be a whole-of-government approach to data security. Such an approach is important to ensure that a consistent and principled approach is taken across government agencies, and that data security practices are not dependent upon the department or portfolio in which the project is housed. In this regard, while the ongoing role of the Digital Transformation Agency (DTA) is supported, it is important that the DTA include a branch with expertise in public law and human rights, which is able to intermediate between both digital technology specialists and policymakers, including the legal profession.

Consultation Question 8

> *What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of Government, including municipal governments?*

Our members observe that the main challenge faced by industry is the patchwork quality of data security regulation. Australians are subject to a patchwork of legislation and international human rights obligations in relation to data security requirements.

Consultation Question 12

> *Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a 'size' threshold).*

We acknowledge the need to maintain an appropriate balance between privacy considerations and business efficacy. Under the current framework, small businesses with an annual turnover of $3 million or less are exempt from the obligations under the *Privacy Act 1988* (Cth) (Privacy Act). There are a range of considerations at play in considering an equitable regulatory regime for small businesses, one which balances privacy risk and the avoidance of an overly burdensome compliance regime.

We note that many small businesses that are required to interact with larger businesses (such as payment terminal providers, insurance companies, or other suppliers) may be familiar with privacy concepts and have systems in place which are capable of facilitating good privacy practices. For small businesses in this situation, processes and practices for compliance with the Privacy Act may now be quite well understood, and therefore no longer considered a significant regulatory burden.

On one view, there is limited justification for small businesses not to comply with basic privacy protections, and that therefore the minimum threshold could be removed in its entirety. 93% of Australian businesses have an annual turnover of $2 million or less.[2] This means that less than 7% of Australian businesses are likely subject to the obligations under the Privacy Act. However, nearly all Australian businesses (by virtue of payment methods and e-commerce) will collect, use and may even disclose personal information.

That said, there are arguments that support the continuation of a small business exemption. We note that the definition of 'small business' in the Privacy Act differs from that used by the

[2] *Australian Bureau of Statistics, Counts of Australian businesses, including entries and exits*, accessed 20 November 2020, < https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/latest-release>.

Australian Taxation Office ($10 million turnover test) and by the Australian Competition and Consumer Commission (ACCC) under the Australian Consumer Law Unfair Contract terms legislation (20 employee test – whether full-time, part-time or casual).[3]

The Law Society notes that many businesses, especially small ones, are struggling with the ongoing economic impact of COVID-19. Given current economic conditions, it may not be appropriate to remove the exemption for small business at this time, given the additional compliance cost that doing so would add to those businesses.

If the exemption were to be removed, acknowledging that new compliance requirements may be an impost on business, it may be worth considering a transition period to removing the exemption, and that any legislative amendments be accompanied by Government-issued guidance, training and other assistance to support business compliance. The Commissioner should also be authorised to make class exemptions from particular requirements of the Privacy Act if, in practice, compliance with specific obligations proves unduly burdensome for certain small businesses as a class.

Thank you for the opportunity to contribute to the Law Council's submission. Questions at first instance may be directed to Stephanie Lee, at 9926 0275 or stephanie.lee@lawsociety.com.au.

Yours sincerely,

Joanne van der Plaat
President

[3] *Competition and Consumer Act 2010* (Cth) sch 2 s 23 (definition of 'small business contract').