Law Council
OF AUSTRALIA

National Data Security Action Plan Discussion Paper

Department of Home Affairs

17 June 2022

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world. The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 90,000[1] lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2022 Executive as at 1 January 2022 are:

- Mr Tass Liveris, President
- Mr Luke Murphy, President-elect
- Mr Greg McIntyre SC, Treasurer
- Ms Juliana Warner, Executive Member
- Ms Elizabeth Carroll, Executive Member
- Ms Elizabeth Shearer, Executive Member

The Acting Chief Executive Officer of the Law Council is Ms Margery Nicoll. The Secretariat serves the Law Council nationally and is based in Canberra.

1 Law Council of Australia, *The Lawyer Project Report*, (pg. 9,10, September 2021).

Acknowledgement

The Law Council gratefully acknowledges the input of the Law Society of New South Wales to this submission, in addition to contributions from the Privacy Law Committee of the Law Council's Business Law Section.

Introduction

1. The Law Council of Australia (**Law Council**) welcomes the opportunity to respond to the Department of Home Affairs' Discussion Paper in relation to the proposed National Data Security Action Plan (**Action Plan**).

2. The Law Council commends the Department of Home Affairs for seeking to constructively engage with stakeholders to inform the development of the Action Plan, and the Law Council welcomes the opportunity to continue to engage with the Department as work on the Action Plan progresses.

3. The Law Council recognises that data and privacy concerns have been the focus of several recent consultations to address prominent vulnerabilities, including:

   - the Department of Home Affairs' Discussion Paper released in July 2021 ('Strengthening Australia's Cyber Security Regulations and Incentives');
   - the Department of Home Affairs' consultation on the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022;[2]
   - the Attorney-General's Department's consultation on the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021;[3] and
   - the Attorney-General's Department's ongoing review of the *Privacy Act 1988* (Cth) (**Privacy Act**).[4]

4. While these consultations focus on different aspects of privacy, data and security in the Australian context, the Law Council is of the strong view that a complementary and holistic approach is important to avoid fragmentation in the reform process and to improve transparency for consumers and regulatory consistency for organisations. This is particularly the case in relation to the review of the Privacy Act where there will be significant policy benefits to aligning respective efforts and ensuring there is a coherent approach to data management and regulation.

5. The Law Council agrees that as Australia's economy and society continues to digitise, facilitating a proliferation of data and information, it is increasingly critical to ensure that Australian governments, businesses and individuals know how their data is managed, stored and secured.[5] The Law Council accordingly supports the development of the Action Plan and welcomes its stated intent of simplifying, educating and improving national data security.[6]

6. This submission predominately draws upon positions previously provided by the Law Council in the course of the above consultations, supplemented by recent contributions from its membership to respond to Discussion Paper Questions 2, 6, 8 and 12.

---

[2] Department of Home Affairs, 'Engagement on critical infrastructure reforms' (Web Page, 2022) <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-our-critical-infrastructure-reforms-engagement>.
[3] Attorney-General's Department, 'Online Privacy Bill Exposure Draft' (Web Page, 2021) <https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/>.
[4] Attorney-General's Department, 'Review of the Privacy Act 1988' (Web Page, 2022) <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.
[5] Department of Home Affairs, *National Data Security Action Plan* (Discussion Paper, April 2022) 5.
[6] Ibid.

General comments

7. Prior to specifically addressing the abovementioned questions in the Discussion Paper, the Law Council seeks to reiterate two considerations which should be front of mind to encourage stronger cyber and data security risk management:[7]

   (a) 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 artificial intelligence (**AI**) (the ambition set out in the Australian Digital Economy Strategy[8] and the AI Action Plan[9]), 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.

   (b) 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 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 with 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 end-to-end 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 cyber security risks.

[7] Law Council of Australia, *Submission to the Department of Home Affairs: Strengthening Australia's cyber security regulations and incentives* (8 September 2021), 7 <https://www.lawcouncil.asn.au/publicassets/ea4a4407-0615-ec11-9440-005056be13b5/4089%20-%20Strengthening%20cyber%20security.pdf>.
[8] See Australian Government, 'Australia's Digital Economy' (Web Page, 2022) <https://digitaleconomy.pmc.gov.au/>.
[9] See Department of Industry, Science, Energy and Resources, 'Australia's Artificial Intelligence Action Plan' (Web Page, June 2021) <https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-action-plan>.

Responses to specific consultation questions

Building a common understanding

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?

8. The Law Council is of the view that data sharing, data security and data privacy in Australia will significantly benefit from a harmonisation approach, similar to the one adopted in the European Union through the General Data Protection Regulation (**GDPR**).[10]

9. The Law Council is generally supportive of the provision of Australian guidance based on the GDPR.[11] However, it is noted that there is a need for further analysis and consultation as to whether there are particular domestic contexts where generalised adoption of the GDPR could have unintended consequences.

10. Privacy compliance can be challenging for Australian businesses who need to navigate the requirements of overseas jurisdictions, most notably, the European Union's GDPR, in order to be considered a trustworthy recipient of personal information. Without Australia being broadly regarded as providing 'adequate' privacy compliance, businesses must rely on their own capabilities and resources to navigate these complex laws.

11. The Law Council considers that achieving GDPR adequacy would bring significant benefits to many Australian businesses in the form of reduced compliance costs associated with negotiating contractual provisions and streamlined interactions with businesses trading in the European Union. Once successful, the benefits of adequacy are:[12]

    - economy-wide, in that it applies to each Australian Privacy Principle (**APP**) within minimum steps that the APP entity needs to take at the entity level, which will help reduce complexity and eliminate 'red tape';
    - consistent with other transborder requirements be they regional (such as Asia-Pacific Economic Cooperation) or industry-specific as an outcome of any given code of binding scheme;
    - preserving the application of existing measures adopted by many APP entities, including standard contractual clauses, binding corporate rules or similar frameworks under Articles 46 and 47 of the GDPR; and
    - enabling Australian law to develop:
        - without the need to copy or artificially supplant aspects of the GDPR, while still building on some of the more universal aspects of the GDPR; and
        - in a manner that supports harmonisation and interoperability.

[10] *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.
[11] See, James Walsh, 'The EU General Data Protection Regulation' (2018) 21(4) *Internet Law Bulletin Online* 63; Veronic Scott and Ashley Fehrenbach, 'GDPR: The Final Countdown: What it Means for Australia' (May 2018) 37(2) *Communications Law Bulletin* 15.
[12] Law Council of Australia, *Submission to the Attorney-General's Department: Privacy Act Review Discussion Paper* (27 January 2022) 18, <https://www.lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf>.

Government's role – Federal, State and Territory and municipal government uplift

Question 6: How can data security policy be better harmonised across all jurisdictions?

12. The Law Council 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.*[13]

13. To this end, the Law Council welcomes the recent announcement there will be a dedicated Minister for Cybersecurity and notes that this is the first occasion that cybersecurity has had its own portfolio in the Australian Cabinet. It is hoped that this role will provide a greater opportunity to promote a multidisciplinary approach to data security and achieve greater harmonisation and coherency across the various arms of data security policy.

14. The Law Council considers that there is a need for greater government oversight of security policy at Local, State, Territory and Commonwealth levels, and would support appropriately targeted and balanced regulation of uses of new and emerging technologies by the public and private sectors.

15. In the Law Council's view, a key element of a harmonised data security policy should be the protection and promotion of the fundamental rights of individuals, especially vulnerable and disadvantaged groups, as this is critical to building enduring trust in those technologies.

16. 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**), 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 breaches of privacy, to protect against incursions of privacy enabled by new technologies.

17. The Law Council considers that 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. Further, consistency in regulation would almost certainly support transparency for consumers and reduce compliance burdens on organisations.

18. While the Law Council supports the ongoing role of the Digital Transformation Agency (**DTA**), it is important that the DTA acquire expertise in public law and human rights, which can act as an intermediary between both digital technology specialists and policymakers, including the legal profession.

[13] Department of Home Affairs, *National Data Security Action Plan* (Discussion Paper, April 2022) 22.

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?

19. A key challenge faced by industry is the current 'patchwork' quality of data security regulation. Australians are currently subject to fragmented data privacy, data security and data sharing regimes and complex legislative instruments and international human rights obligations in relation to data security requirements. For instance, under APP 7, the Privacy Act currently regulates an organisation's use and disclosure of personal information for the purpose of direct marketing. However, APP 7 does not apply to the extent that the *Spam Act 2003* (Cth) (**Spam Act**) or *Do Not Call Register Act 2006* (Cth) (**DNCR Act**) applies.[14]

20. The Law Council considers that any reform at the Commonwealth level should ensure that the collection, use and protection of privacy utilises consistent terminology and coverage across the Privacy Act, the Spam Act and the DNCR Act. This would ensure that the processes and protections are more transparent and accessible for consumers and end-users.[15]

Clarity and empowerment for business

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?

21. As a general principle, data protection regulation should enable a balance between an individual's right to control their private information and the general public's commercial interest in data subject to appropriate controls and restrictions. This approach will ensure that Australia is able to develop as a central hub for innovation and industry, as well as decrease regulatory barriers for small businesses.[16]

22. The Law Council acknowledges 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, although these entities may be bound by the APPs in certain circumstances.[17] Small businesses and not-for-profit organisations that would otherwise not be covered by the Privacy Act may choose to be treated as an organisation for the purposes of the Privacy Act, by publicly committing to good privacy practices and adhering to the APPs.[18]

23. Where handling of personal information is a core business activity, the carve-in from the small business exemption will generally mean that the Privacy Act already operates, such as for businesses sharing such data for commercial purposes as a business activity.

24. The current exemption for many small businesses in Australia's privacy regime recognises the resourcing constraints of the small business sector, and the potentially onerous nature of ongoing monitoring and compliance. Consistent with this approach, it is preferable for any guidance under the Action Plan to have regard to a company's

[14] *Privacy Act 1988* (Cth) sch 1, APP 7.8.
[15] Law Council of Australia, *Submission to the Attorney-General's Department: Privacy Act Review Discussion Paper* (27 January 2022) 23, <www.lawcouncil.asn.au/publicassets/eda682c2-6388-ec11-9449-005056be13b5/4161%20-%20Privacy%20Act%20review%20discussion%20paper.pdf>.
[16] Ibid 6 [10].
[17] *Privacy Act 1988* (Cth) ss 6C, 6D.
[18] See, Office of the Australian Privacy Commission, 'Opting in to the Privacy Act' (Web Page, 2022) <https://www.oaic.gov.au/privacy/privacy-registers/privacy-opt-in-register/opting-in-to-the-privacy-act>.

size rather than a ‘one size fits all approach’. This guidance should underpin the broader principles-informed approach to data security outlined in the Discussion Paper, and provide businesses with practical and clear direction that is tailored to their respective size.