Australian Institute of Company Directors

18 Jamison Street,
Sydney NSW 2000

t: 1300 739 119
e: contact@aicd.com.au
aicd.com.au

ABN 11 008 484 197

14 July 2022

Data Security and Strategy
Technology Policy Branch
Digital and Technology Policy Division
Department of Home Affairs

via: datasecurityandstrategy@homeaffairs.gov.au

Dear Home Affairs Department

National Data Security Action Plan – Discussion Paper

Thank you for the opportunity to comment on the Discussion Paper (the **Discussion Paper**) concerning the National Data Security Action Plan (the **Action Plan**).

The Australian Institute of Company Directors' (**AICD**) mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. The AICD's membership of more than 49,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits (**NFPs**), large and small businesses and the government sector.

The AICD has over the past 12 months participated in a number of consultations on regulatory proposals to build cyber security resilience across the Australian economy. We also contributed to consultation by the Attorney General's Department on the Review of the *Privacy Act 1988* (Cth)(the **Privacy Act**). As reflected in the Discussion Paper, the cyber resilience of an organisation is essential to how it identifies, manages and protects the data that is collects and utilises in its business operations.

Our submission to the Home Affairs led consultation on strengthening Australia's cyber security regulations and incentives is available here, our submission to the second round of amendments to the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) is available here and the submission to the Privacy Act Review is here.

This submission draws upon the engagement we undertook with AICD members, industry experts and other industry bodies on the above submissions.

1. Executive Summary

The AICD welcomes the Home Affairs consultation on measures to modernise Australia's data security regulatory environment reflecting the rapid growth in data generation, storage and utilisation and its importance to a digital economy.

A growing focus of AICD's policy, practice and educational activities is the governance of cyber security, including protecting key organisational data, reflecting the prominence of this issue for directors. The AICD's Director Sentiment Index (**DSI**) results for 2021 and 2022 found that cyber security is the number one issue keeping directors awake at night.[1]

[1] AICD Director Sentiment Index (April 2022), available here.

The AICD's overarching view is that the Government's cyber and data reforms must be carried out in a coordinated manner that seeks to reduce existing regulatory complexity and helps to lift cyber security resilience. The AICD's strong view is that a partnership between Government and industry, including support for organisations of all sizes, has the best chance of improving Australia's cyber security and data management practices rather than focusing on layering additional regulatory obligations.

Our key points on the Discussion Paper are:

1. The AICD does not support the Action Plan proposing any new regulatory obligations or standalone legislation until the Privacy Act Review is completed.
2. There are existing accountability mechanisms, including director duties, that are effective in driving behaviour change in the management and oversight of cyber security and data security risks. Adding further duplicative regulatory accountabilities would exacerbate the existing complex regulatory framework for entities and regulators, and in the AICD's view could be counterproductive to the policy objectives of strengthening cyber resilience and data security practices.
3. The AICD supports steps to harmonise existing regulatory requirements and obligations as they relate to data management and cyber security.
4. The AICD considers that assessing opportunities for international alignment should wait until the completion of the Privacy Act Review, particularly the final position on adequacy with the General Data Protection Regulation (**GDPR**).
5. The AICD urges caution in proposing expanded data localisation requirements without further examination of the evidence base for such a change. We note the potential for such a move to not only impose undue costs and complexity on organisations but also weaken Australia's overall cyber security posture.
6. The AICD's considers that greater government guidance and support for small and medium enterprises (**SMEs**) and NFPs represents a more effective approach to protecting data and building cyber resilience than imposing new obligations.

The AICD has not commented on the questions where other stakeholders are best placed to assess the policy options and questions.

We look forward to consulting further with Home Affairs, and other Government agencies and departments, on data, cyber security and privacy reform options in the future.

2. Privacy Act Review

As noted in the Discussion Paper, the Privacy Act is currently the subject of an extensive review being conducted by the Attorney General's Department (**AGD**). We understand that there will be further updates from Government on the Review in the coming months.

Separately AGD has also consulted on an exposure draft *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (the **Online Privacy Bill**) that seeks to strengthen the Privacy Act obligations as it applies to social media companies and the data they collect.

The AICD is strongly of the view that the Government should not contemplate legislative change in respect of data management until the Privacy Act Review is completed and the status of the Online Privacy Bill is finalised. The Privacy Act is currently the primary legislative framework for the collection and

management of personal data and for captured entities sets key obligations and principles, including Australian Privacy Principle 11 – Security of personal information (**APP 11**).

We recognise that the Discussion Paper envisages 'data' as broader than the Privacy Act's focus on personal information. However, our view is that the data failures and mismanagement that the Action Plan is predominantly seeking to address, focuses on personal data and the harms that result to organisations and individuals from the loss or misuse of personal data. The AICD's position is that the Privacy Act represents an existing legislative framework that is best suited to address the policy issues identified in the Discussion Paper, and that the Action Plan should align and be coordinated with the Privacy Act Review.

The Discussion Paper seeks feedback in a number of policy areas that are also being directly contemplated under the Privacy Act Review, such as adequacy with the GDPR. Further, the Privacy Act Review is examining amendments to APP 11, the status of the small business exemption and harmonisation of privacy requirements across jurisdictions amongst a raft of other measures. Were these changes to the Privacy Act to occur, even in part, it would represent a profound shift in the obligations organisations face in the collection and protection of personal information.

The AICD would be very concerned were the Action Plan to pre-empt the Privacy Act Review through proposed data focused amendments to other key legislation, such as the *Corporations Act 2001* (Cth)(**Corporations Act**), or the creation of new standalone legislation. This policy approach would create significant industry uncertainty and confusion and also exacerbate the existing complexity in data regulatory obligations that organisations of all sizes face – an issue identified by the Discussion Paper.

3. Accountability mechanisms

This section responds to question 15.

The Discussion Paper provides limited detail on what may be entailed by new accountability mechanisms on organisations, including government bodies. Further, it does not demonstrate or make the policy case that there are deficiencies in existing accountability mechanisms that are resulting in weak data management practices.

Organisations and boards currently face a wide range of obligations that a relevant to the management of data. These obligations can apply across the economy (e.g. Privacy Act), a subsection of key organisations (e.g. SOCI Act) or be industry specific (e.g. APRA prudential requirements).

Significantly, the overlay of director duties under the Corporations Act provides an overarching set of personal governance obligations on directors that ensure they have appropriate oversight of key risks, including cyber security and the management of data. Notably, section 180 of the Corporations Act imposes a civil obligation in relation to care and diligence which requires directors to guard against key business risks. There is no 'one-size-fits-all' approach to compliance with section 180. This requires directors to stay informed and apply an enquiring mind about the organisation's activities, monitor its affairs and policies, test information put before them by management and proactively consider what other information they require. These obligations apply to a wide range of business risks, including having appropriate systems to prevent and respond to cyber security and data incidents.

As noted above, our view is that the Privacy Act is the most appropriate framework to strengthen data management obligations in Australia. The Privacy Act already contains accountability mechanisms, including the Notifiable Data Breaches Scheme (**NDB Scheme**) and the enforcement powers of the Office of the Australian Information Commissioner (**OAIC**). The Privacy Act Review is assessing

strengthening accountability mechanisms, including boosting the enforcement powers of the OAIC and introducing a consumer direct right of action. The AICD's submission to the Privacy Act review supported additional resourcing for the OAIC recognising its importance and expanding role in Australia's digital economy.[2]

As set out in detail in our submission to the Home Affairs led consultation on *Strengthening Australia's cyber security regulations and incentives*, the AICD's position is that existing directors' duties provides clear accountability mechanisms both against entities and their directors for any failure to effectively address cyber security and data management risks.[3]

The AICD strongly rejects any view that Australia's corporations laws and directors' duties are limited in clarity and coverage in effectively addressing cyber security and data management threats, or are solely focused on protecting the interests of shareholders. In our view, protecting key organisation data and ensuring cyber security resilience forms part of many existing obligations applicable to directors.

We would be happy to facilitate engagement with senior AICD members on how they oversee the management and protection of key data at their organisations to help inform Home Affairs' approach.

4. Harmonisation

This section responds to question 8.

The AICD supports the focus of the Discussion Paper in examining Australia's complex and overlapping regulatory and policy settings as they relate to data and explore opportunities to set a coordinated set of obligations and expectations across the economy. The Discussion Paper presents a table at Figure 3 that highlighted the key regulatory bodies, and corresponding legislation, that is relevant in Australia's data security landscape. We note this summary does not include industry or sector specific requirements, for instance APRA prudential requirements or the *My Health Records Act 2012* (**MHR Act**), that also are relevant in assessing the current data management regulatory obligations.

AICD members have consistently provided feedback that the existing complexity and patchwork nature of regulatory obligations that are relevant to cyber security and data management are a barrier to building cyber resilience. This complexity will only increase with the commencement of expanded obligations under the SOCI Act and the proposed ransomware reporting requirements under the Ransomware Action Plan.

Consistent with our submission to the Privacy Act Review, we would welcome any steps by Government to harmonise existing obligations as they relate to data management. Reporting and notification requirements is one area where we would encourage close examination of the opportunity for harmonisation. The Privacy Act Review flags the potential for harmonisation of the NDB Scheme with other reporting and notification frameworks, including the MHR Act, the SOCI Act and various state schemes.[4] While there would be complexity in harmonising reporting regimes such a move would provide clarity to industry on where and how to report data incidents and reduce compliance costs with meeting different reporting obligations.

The AICD also sees opportunity in the Action Plan exploring whether a single regulator should be chiefly responsible for data security across the economy. Currently the OAIC has responsibility as it relates to

[2] AICD submission, *Review of the Privacy Act 1988 – Discussion Paper*, 10 January 2022, available here.
[3] AICD submission, *Strengthening Australia's cyber security regulation and incentives*, 27 August 2021, available here.
[4] Attorney General's Department, Privacy Act Review – Discussion Paper, 25 October 2021, page 202.

personal information, with other regulators, such as the ACCC and APRA, having responsibility as it relates to particular industries or regulatory obligations. A regulator with primary responsibility would assist in harmonisation, promote greater coordination in policy development and allow for an educative mandate that includes lifting data security practices across the economy.

As discussed above, the AICD would caution against policy development or legislative change that pre-empts the Privacy Act Review. This would run the real risk of exacerbating the existing complexity across jurisdictions and different regulatory regimes.

5. International alignment and data localisation

This section responds to questions 2, 4 and 5 on international alignment and data localisation.

The AICD is supportive of measures that lower the cost of Australian organisations doing business overseas, including maximising the opportunities of cross-border data flows. Unreasonable protectionist barries to the flow of data across countries will ultimately impose costs on organisations and individuals, including through detrimental impacts on innovation.

One of the central issues of the Privacy Act Review is whether Australia should seek adequacy with the GDPR and the implications of such a move, including removing the small business exemption. The AICD's view is international alignment is a very complex policy debate where there may be real costs in moving to GDPR adequacy that would need to be clearly outweighed by the benefits, including lower business costs and improved data security practices. As with the above issues, we would urge the Action Plan to not reach a definitive position on international alignment until the Privacy Act Review is completed.

The AICD's view is that caution should be taken in proposing any widespread data localisation requirements for specific types of data. We recognise that it is appropriate for certain data collected by the Government, such as health records, to be stored in Australia. However, it is not apparent, at this stage, that there is a strong public policy rationale for imposing data localisation obligations more broadly. Our key concerns with expanded data localisation requirements are:

- The risks of a cyber security breach and loss or misuse of data may increase under localisation obligations with Australian organisations unable to utilise more cyber secure providers overseas.
- Australian organisations utilise large international providers of information systems and infrastructure, such as cloud or data centre providers, to secure key data reflecting the porous and interconnected nature with which businesses and customers interact digitally. Requiring Australian organisations to find domestic alternatives is likely to be highly complex and costly and may deprive organisations of cost effective and innovative data management solutions.
- There would be significant legislative complexity in designing and drafting data localisation requirements in a clear manner, including what types of data is captured under any obligations.
- It is not apparent there are currently significant management or misuse issues with Australia data being stored overseas, or that regulators or law enforcement agencies are unable to access this data in a timely manner. If there is such evidence, it should be presented.

The AICD would welcome involvement in future consultation rounds on international alignment and data localisation, including facilitating engagement with AICD members.

6. Support for SMEs and NFPs

This section responds to questions 3 and 9-12.

The AICD welcomes the focus of the Discussion Paper on what support and guidance the government may be able to provide Australia organisations to uplift data management practices. The AICD is currently working to expand guidance for members in the key area of cyber security.[5] While industry and membership bodies can support better practice in cyber security and data management, the Government should play a key role in supporting higher standards across the economy.

The AICD's observation, based on feedback from directors and industry experts, is that there are significant challenges for SMEs and NFPs in addressing cyber security and data management risks. It is these organisations, rather than larger well-resourced companies, where there are likely to be weaknesses in data management practices and data breaches or failings can go unobserved. Directors have noted that not only do SMEs and NFPs face resource and time constraints in managing cyber security risks, they also do not have support from government in responding to cyber incidents.

Consistent with our previous submissions, the AICD's view is that greater government support for SMEs and NFPs represents a more effective approach to protecting data and building cyber resilience than imposing new obligations. This support would entail education, better practice guidance, training and assistance in the event of experiencing a cybersecurity incident.

The ACSC currently has excellent guidance resources available to SMEs on implementing practical cyber security controls.[6] However, our sense is that awareness of these resources is currently low and that coordinated approach to promoting and consolidating existing guidance across government may assist in educating SMEs and NFPs of best practice in data management.

The AICD welcomed the Government's funding commitment in the May 2022 budget to provide advisory services to SMEs to help them build digital capabilities. A wider program that offers support to a larger population of SMEs and NFPs, similar to the Help to Grow program in the United Kingdom, could represent an effective policy intervention to uplift data management practices amongst SMEs and NFPs.[7]

7. Next Steps

We hope our submission will be of assistance. If you would like to discuss any aspects further, please contact Simon Mitchell, Senior Policy Adviser (smitchell@aicd.com.au) or Christian Gergis, Head of Policy (cgergis@aicd.com.au).

Yours sincerely,

Louise Petschler GAICD
General Manager, Governance & Policy Leadership

[5] The AICD plans to release additional guidance on governing cyber security risks and building cyber resilience in the second half of 2022.

[6] See ACSC Small Business Cyber Security Guide (October 2021), available here.

[7] Detail on Help to Grow can be found here.