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

10 January 2022

Attorney General's Department

via: PrivacyActReview@ag.gov.au

Dear Attorney General's Department

Review of the Privacy Act 1988 – Discussion Paper

Thank you for the opportunity to comment on the Discussion Paper (the **Discussion Paper**) concerning the review of the *Privacy Act 1988* (**Privacy Act**).

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 47,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits, large and small businesses and the government sector.

The AICD's policy positions on the Discussion Paper have been informed by engagement with privacy experts, industry bodies and AICD members.

1. Executive Summary

The AICD supports reforms that modernise the Privacy Act to ensure it reflects a modern digital economy where individuals and businesses are engaging, and providing personal information, in new and innovative ways. However, we consider that a number of the proposals in the Discussion Paper require additional detail to enable an informed assessment. Without such material it is difficult to assess the case for change and discern whether any increase in regulatory obligations on entities is outweighed by the public benefit.

A growing focus of AICD's policy and educational activities is the governance of cybersecurity, reflecting the prominence of this issue for directors. The AICD's latest Director Sentiment Index (**DSI**) for the second half of 2021 found that cybersecurity is the number one issue keeping directors awake at night.[1] The AICD's overarching view is that the Government's cyber reforms, including amendments to the Privacy Act, must be carried out in a coordinated manner that seeks to reduce existing regulatory complexity and helps to lift organisational resilience.

Our key points are as follows:

1. The AICD strongly supports greater cooperation amongst regulators and the harmonisation of privacy and related cyber security laws across the Commonwealth and states and territories. Currently, obligations can span a range of pieces of legislation, hampering their overall efficacy.

2. The AICD supports amendments to Australian Privacy Principle 11 – Security of personal information (**APP 11**) to clarify the meaning of 'reasonable steps' however we do not support changes being accompanied by a mandatory privacy code. A mandatory code would be inconsistent with the

[1] AICD Director Sentiment Index (December 2021), available here.

principles-based nature of APP 11, add to the existing complex patchwork of cybersecurity related obligations faced by entities and boards, and could be counterproductive to the objective of improving cyber resilience across the economy.

3. While supportive of a consumer direct right of action in principle, the AICD is concerned that the proposal, if not properly contained, could result in class actions where an entity experiences a sophisticated cybersecurity attack and has suffered a loss of information. The AICD's preliminary position is that a direct right of action should be reserved for serious breaches of the Privacy Act, rather than those involving cybersecurity attacks on entities. Further detailed consultation is required on this proposal, including its interaction with the proposed statutory tort and enhanced Office of the Australian Information Commissioner (**OAIC**) enforcement powers.

4. The AICD does not support, based on the detail in the Discussion Paper, any changes to the small business exemption. Additional support for small businesses through education, guidance and assistance would be more effective at building cyber resilience than applying the resource-intensive and complex Privacy Act obligations.

5. The AICD does not consider that an industry-based funding model for the OAIC, whether a cost recovery model and/or statutory levy, is the most appropriate or efficient mechanism to provide additional OAIC resources. We would recommend that additional funding be sourced from consolidated revenue.

The AICD has not commented on proposals where other stakeholders are better placed to offer an informed view.

2. The case for change

The Discussion Paper is extensive in its length, the policy areas that it covers and the proposals, options and questions that are canvassed. In many of the chapters there is insufficient detail on what is being contemplated by the Attorney General's Department to enable an informed comment. This has made it challenging for stakeholders, including the AICD, to assess and provide a definitive position on the policy proposals.

In future consultation rounds, the AICD would welcome a narrowing of the policy proposals. Policy options should be supported by a more detailed case for change or evidence base and what is envisaged in terms of specific amendments to the Privacy Act and/or other legislation. Further, consultation rounds on specific areas would allow proposals to be considered in context, such as enforcement proposals outlined in Chapters 25-27 of the Discussion Paper.

A policy area the AICD would welcome further detail and analysis on is aligning the Privacy Act and other regulatory settings with international regimes, including the General Data Protection Regulation (**GDPR**). The AICD supports reforms to Privacy Act that seek to lower the cost of Australian businesses doing business overseas, including with customers in the European Union.

However, based on the information contained in the Discussion Paper it is difficult to assess whether seeking GDPR "adequacy" will result in benefits that outweigh any increase in regulatory burden applying to all Australian businesses, including small businesses that are currently exempt from the Privacy Act. The Discussion Paper notes that GDPR adequacy would likely require changes to a range of Australian laws. Without further detail on what these amendments would be, and to what legislation, it is difficult for the AICD to comment on the proposal to seek GDPR adequacy.

Separate from GDPR adequacy, the Discussion Paper also raises a series of questions on a proposed Cross-Border Privacy Rules (**CBPR**) certification framework. From the information contained in the Discussion Paper, both the CBPR certification proposal and with GDPR adequacy may result in a significant increase in regulatory complexity and costs with potentially limited benefit for most businesses subject to the Privacy Act. However, it is again challenging for the AICD to provide an informed policy position on the CBPR certification proposal without additional detail on what would be contemplated in a certification system, including the role of Accountability Agents.

The AICD supports the Privacy Act continuing to reflect the unique legal, economic and social circumstances of Australia while also seeking to lower the barriers for businesses with overseas customers and partners. The AICD encourages the Attorney General's Department to undertake future specific consultation on international alignment proposals, including a detailed analysis of regulatory changes and potential costs.

The AICD would welcome involvement in future consultation rounds on amendments to the Privacy Act, including facilitating engagement with AICD members.

3. Regulatory complexity and Notifiable Data Breaches scheme

This section responds to proposals 28.2 and 28.3 in respect of the Privacy Act's interactions with other regulatory schemes and Chapter 27 on the Notifiable Data Breaches scheme (**NDB scheme**).

The AICD strongly supports proposals 28.2 and 28.3 on greater cooperation amongst regulators and the establishment of a working group to harmonise privacy laws across the Commonwealth and states and territories. The Discussion Paper demonstrates the existing complexity of current privacy regulatory settings with the case-study illuminating the costs and inefficiencies inherent in existing regulatory and legislative settings.[2]

The AICD in its submission to the Treasury/Home Affairs consultation on 'Strengthening Australia's cyber security regulations and incentives' cited regulatory complexity, including the Privacy Act, as a barrier to directors and organisations understanding existing obligations and building cyber resilience.[3] We noted that new and proposed reforms, for instance the expansion of the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**), will add to the current complex patchwork of obligations that are relevant to cyber security and the protection of personal information.

The AICD encourages the Attorney General's Department to closely consider whether any of the proposals and policy options outlined in the Discussion Paper (for instance changes to APP 11) would contribute, to the challenges entities and boards face in understanding cybersecurity and privacy obligations. While proposals 28.2 and 28.3 are an important recognition of the complexity that exists in privacy regulation we would be concerned if other amendments to the Privacy Act contributed to complexity and uncertainty in the broader cybersecurity regulatory landscape. The AICD considers that a coordinated approach to reforms across privacy and cybersecurity regulatory frameworks is necessary to avoid exacerbating the current patchwork approach and ideally identify opportunities for harmonisation.

---

[2] Attorney General's Department, Privacy Act Review – Discussion Paper, 25 October 2021, page 216.

[3] AICD submission, Strengthening Australia's cyber security regulation and incentives, 27 August 2021, available here.

The Discussion Paper raises the potential for harmonisation of the NDB Scheme with other reporting and notification frameworks, including the *My Health Records Act 2012,* the SOCI Act and various state schemes.[4] In addition to existing reporting frameworks, the Government has also announced its intention to develop a ransomware reporting regime as a component of the Ransomware Action Plan.[5] While more detail is required, the AICD supports in-principle any steps to align or harmonise existing and proposed reporting regimes with the NBD Scheme.

We consider harmonisation in reporting could be a significant opportunity to make progress in reducing current complexity and serve as an example of how the regulatory burden on entities may be reduced in a coordinated and targeted manner.

4. Australian Privacy Principle 11

This section responds to proposals 19.1 and 19.2 in respect of APP 11.

APP 11 through its focus on the management, protection and destruction of personal information is one of the central regulatory obligations that is directly relevant to an entity's management of cybersecurity risk. For many entities, information collected from customers and partners is their most valuable asset and how this information is secured is a key focus of cybersecurity arrangements and is a significant focus for directors. As noted above, in a recent survey, AICD members advised that cybersecurity is the issue that is most likely to keep them awake at night.

The AICD supports proposals 19.1 and 19.2 to include further detail on what is entailed by 'reasonable steps' that would provide a degree of certainty to entities in securing information and managing this risk. Additional detail would go beyond simply adding 'both technical and organisational measures' while maintaining the principles-based approach to APP 11. The option in the Discussion Paper to elevate existing guidance from APP Guidelines into APP 11.1 on what factors or characteristics an entity should consider when determining reasonable steps appears to be a sensible approach to provide clarity and clearer baseline for entities. Ideally any amendments to APP 11.1 would provide additional clarity while preserving flexibility and a technology-neutral approach.

We consider that amendments to APP 11, including detail on reasonable steps, present an opportunity to align with existing cybersecurity obligations. For instance, we would encourage consideration of whether an entity that meets other cybersecurity requirements, such as APRA *Prudential Standard CPS 234 Information Security* or Article 32 of GDPR, is by default taken to have met the obligations under APP 11, including demonstrating reasonable steps.

As discussed above, a significant concern of AICD members is the existing complexity of cybersecurity obligations and the AICD would welcome any changes to APP 11 that recognise other frameworks and seek to remove any unnecessary or duplicative requirements.

Cyber security code

The Discussion Paper notes the Government is considering legislative changes and other measures to improve cyber resilience, including the recent consultation on a proposal for a cyber security code for

[4] Attorney General's Department, Privacy Act Review – Discussion Paper, 25 October 2021, page 202

[5] Ransomware Action Plan, 13 October 2021, available here.

personal information (the **Code**) that would sit under the Privacy Act.[6] The Discussion Paper raises the potential of complementary changes to APP 11 through the proposed Code.

The AICD provided a submission to the separate Treasury/Home Affairs consultation that strongly encouraged a partnership approach from Government to managing cybersecurity risks that avoids costly prescription and adding to the complexity of existing requirements.[7] While we did not comment directly on the Code proposal we did argue strongly in respect of the governance standard proposal that any mandatory approach would be counterproductive. Our strong view is that the same principle applies in respect of assessing the policy rationale for a Code under the Privacy Act.

The AICD urges caution with assessing the evidence base for a Code that may undermine the principles-based nature of APP 11 and the flexibility afforded to entities to meet the obligations. We would see the development of a code that set minimum obligations as adding to the existing patchwork of complex obligations that entities and directors face. In addition, it is not apparent there is a strong policy rationale for a Code when the Government is pursuing other avenues for improving cyber resilience across the economy. The AICD encourages alignment within Government noting the various parallel initiatives currently in train including the ongoing cybersecurity governance consultation.

5. Direct right of action

This section responds to proposal 25.1 that individuals be given a direct right to bring actions and class actions against entities to seek damages for the financial and non-financial harm suffered as a result of an interference with their privacy under the Privacy Act.

The AICD in-principle supports the right of individuals to have a direct right of action in circumstances where there is significant negligence or wilful breaches of the Privacy Act. However, based on the limited detail in the Discussion Paper, we are concerned that the current proposal could result in a proliferation of class actions for privacy incidents, even when an entity has itself been the victim of a cybersecurity attack.

Cybersecurity attacks, including ransomware activity, have been increasing rapidly in Australia and are often the result of well-resourced and malicious criminal or state actor activity. [8] Even commercial entities and government organisations that have rigorous cybersecurity practices can find themselves the victim of a cyber-attack. In these circumstances, an entity may meet respective Privacy Act obligations, such as taking reasonable steps under APP 11, and still suffer from a loss of customer, employee or stakeholder information with significant financial and reputational consequences. In our view, it would be unjust to have entities further penalised by being subject to the risk of a class action claim in such circumstances.

The AICD acknowledges the proposed gateway model - with the OAIC the first forum for a complaint - is intended to minimise vexatious or opportunistic litigation. However, our reading of this model is that a complainant could still seek leave to the Federal Court in circumstances where the OAIC has determined that there is not a breach of the Privacy Act, or where the OAIC has terminated the matter. Our view is this could result in entities facing class actions even where the OAIC has established they have taken all steps, and met the obligations under the Privacy Act, to protect personal information. Given the evolving nature of cybersecurity risk and the principles-based nature of APP 11, there would likely be several

---

[6] Attorney General's Department, Privacy Act Review – Discussion Paper, 25 October 2021, page 146.

[7] AICD submission, Strengthening Australia's cyber security regulation and incentives, 27 August 2021, available here.

[8] ACSC Annual Cyber Threat Report 2020-21, September 2021, available here.

avenues for a claimant to argue that an entity has failed to meet its obligations in a cyber-attack, absent an appropriate threshold to a direct right of action.

The AICD has been extensively involved in the Government's reforms on the regulatory settings and commercial incentives driving Australia's attractiveness for securities class actions. The AICD's position in sperate submissions on reforms to disclosure laws and litigation funding arrangements reflects strong feedback from directors that existing settings have driven a highly risk averse culture at the board level.[9] This has resulted in adverse economic and legal consequences, including a D&O insurance market that has been in crisis.[10] Enabling increased class action activity, particularly speculative or opportunistic class actions, would risk heightening these negative impacts and be inconsistent with the objectives of these recent Government reforms.

The proposals in Chapters 25-27 would, if implemented together, represent a significant expansion of the risk of liability under the Privacy Act. For instance, this strengthening of the enforcement tools available to the OAIC under proposals in Chapter 25 will be a key mechanism to incentivise compliance with Privacy Act obligations.

The AICD would welcome further detail and targeted consultation on the proposals contained in Chapters 25-27. To allow for more comprehensive comment by stakeholders this would expand the current outline of the direct right of action model covered on pages 188-190 of the Discussion Paper. This detail would also include an analysis of how the direct right of action would interact with the proposed statutory tort and separately existing options for redress, such as via the common law and the OAIC conciliation process. The AICD stands ready to work with the Attorney General's Department on this topic, including facilitating targeted engagement with experienced AICD members.

6. Support for SMEs and the small business exemption

This section responds to Chapter 4 on the small business exemption and support for small businesses in meeting Privacy Act requirements.

The observations in the Discussion Paper on the challenges faced by small businesses in addressing cybersecurity risk align with previous feedback from directors of small and medium sized enterprises (**SMEs**), including not-for-profits (**NFPs**). Directors have observed that not only do SMEs face resource challenges in managing cybersecurity risk they also do not have support from government in addressing and responding to cyber incidents.

The AICD is not persuaded that applying the Privacy Act obligations, including the NDB scheme, will mitigate the cybersecurity challenges faced by small businesses and NFPs or result in improved management and protection of personal information. Most small businesses and NFPs have very limited resources and/or skills to understand and implement the Privacy Act requirements in a comprehensive manner. Faced with increased compliance costs and the complexity of the Privacy Act obligations, many smaller organisations may seek to meet the obligations in a minimal, narrow or incomplete way.

There may also be considerable challenges for the OAIC in building awareness and education amongst small businesses and NFPs on the application of the Privacy Act and how to meet the requirements, such as the NDB scheme. It is likely that there will be a large proportion of small businesses that would simply

---

[9] AICD submission, Treasury Laws Amendment (2021 Measures No.1) Bill 2021, 1 March 2021, available here.

[10] AICD submission, Exposure Draft Treasury Laws Amendment (Measures for Consultation) Bill 2021: Litigation funders, 6 October 2021, available here.

not be aware that the Privacy Act now applies to them. The result would be a large degree of inadvertent non-compliance, undermining the intent of removing the exemption.

Finally, while we agree with the Discussion Paper's reflection on the growing use of technology by small businesses, including the importance of an online presence, our view is that this alone does not justify reducing or removing the $3 million annual turnover exemption. Our strong view is that greater Government support for these businesses, and the broader SME population, represents a more effective approach to protecting information and building cyber resilience than imposing new obligations. This support would entail education, training and assistance in the event of experiencing a cybersecurity incident. As discussed below, we support greater resources for the OAIC and consider this in part could be directed at a collaborative approach to improving information protection practices across businesses of all sizes.

The AICD appreciates that continuing to exempt small business may impact Australia obtaining GDPR adequacy. However, our view at this stage is that the policy case for making this change has not been made. We are not satisfied that applying the significant obligations of the Privacy Act is a proportionate response to cybersecurity challenges faced by small businesses. Further, as discussed above, the resourcing and awareness building challenges would likely result in narrow and patchy compliance with a limited improvement in the protection on information across small businesses.

7. Funding of the OAIC

This section responds to proposal 24.7 in respect of an industry funding model for the OAIC.

The AICD supports additional resources for the OAIC recognising its importance and expanding role in Australia's digital economy. As discussed above, we see the OAIC as playing a key role in supporting and educating entities on best practice in protecting information, particularly SMEs.

However, the AICD does not consider that an industry funding model for the OAIC, whether a cost recovery model and/or statutory levy, is the most appropriate or efficient mechanism. The OAIC is distinct from industry specific regulators, such as the Australian Securities and Investment Commission, in that it regulates a framework that applies across the economy and is relevant to every Australian.

Based on the limited detail in the Discussion Paper on the design of an industry funding model, our preliminary concerns are:

- An industry-based model would be very difficult to design and administer in a cost-effective manner due to the large number of entities in different sectors that the OAIC regulates across the economy;
- A cost recovery approach that charges entities for seeking OAIC guidance or assistance would disincentivise engagement with the regulator and be counterproductive to the broader objectives of improving information handling practices and cyber resilience; and
- Identifying entities that operate in high-risk privacy environments as being subject to a particular statutory levy would be highly complex and subjective. Such an approach would potentially stifle innovation by businesses seeking new ways of utilising information in a digital economy.

The AICD recommends that any increase in funding for the OAIC should come from consolidated revenue. This would be the most efficient way of resourcing the OAIC and appropriately reflects the OAIC's role in regulating obligations that apply across the economy.

8. 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 at smitchell@aicd.com.au.

Yours sincerely,

Christian Gergis GAICD
Head of Policy