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

31 March 2023

Attorney General's Department

privacyactreview@ag.gov.au

Dear Attorney General's Department

Review of the *Privacy Act 2008* – Report

Thank you for the opportunity to comment on the *Privacy Act 2008* Review (**Privacy Act**) Report (**Report**) and the proposals contained within the Report.

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 50,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits (**NFPs**), large and small and medium enterprises (**SMEs**) and the government sector.

Enclosed at **Attachment A** are our high-level policy positions on a number of the key proposals contained in the Report. **Attachment B** provides our detailed responses to each of these proposals. The AICD's policy positions have been informed by engagement with privacy and legal experts, entities, industry bodies and AICD members.

1. Executive Summary

The AICD commends the work of the Attorney General's Department in undertaking the Review and consulting on proposals to amend the Privacy Act to ensure it remains fit for purpose. As reflected in our submission to the Discussion Paper, the AICD supports the Review as an important opportunity to modernise the Privacy Act to ensure it reflects a digital economy where individuals and businesses are engaging, and providing personal information, in innovative ways.[1]

However, we urge the Government to consider the Report's recommendations holistically with other potential reforms in adjacent policy areas, including the development of the *2023-2030 Cyber Strategy*. A coordinated approach across portfolios must be taken to ensure policy settings and reforms are consistent and do not unnecessarily add to the existing complexity of cyber security and data management obligations.

In devising privacy reforms, AICD considers that the Government must appropriately balance strengthening how Australians' personal information is collected, stored and protected, with not unduly stifling the innovative use of data or imposing a counterproductive regulatory burden.

Our view is that it has not been demonstrated that the policy benefits of a number of the proposals will outweigh the costs on entities, and a clear evidence base must be presented for such a major reform.

[1] AICD submission, *Review of the Privacy Act 2008 – Discussion Paper*, January 2022, available here.

We recommend the Government undertake a cost benefit analysis of the proposals in their totality. Our key points on the proposals outlined in the Report are as follows:

1. The AICD does not support the removal of the small business exemption for all currently exempt businesses or NFPs. We consider that a targeted approach for industries with high privacy risks, or a proportionate application of the Privacy Act obligations to small businesses, would be a more effective policy response.

2. The AICD supports measures to harmonise, and more importantly clarify, existing data retention laws and reporting obligations, including establishing a single portal for data breach and cyber incident reporting. In particular, we consider that the harmonisation of data retention laws across the Commonwealth, States and Territories should be a priority reform. Absent such work, it would be very challenging for entities to implement a number of the proposals, including the right to erasure.

3. The AICD in-principle supports a direct right of action for individuals to seek compensation in circumstances where they have suffered loss or damage as a result of an interference of their privacy. We recommend however that a direct right of action be limited only to 'serious' interferences of privacy involving significant fault on the part of an entity, and that application in the cyber security context be suitably constrained. We are concerned that without an appropriate harm threshold there is a risk of unintended consequences, including circumvention of the proposed gateway model, a proliferation of class action activity, entities being subject to multiple claims for redress –particularly if a tort of invasion of privacy is legislated.

4. The AICD in-principle supports the introduction of a statutory tort for serious invasions of privacy, provided it is the model recommended by the Australian Law Reform Commission (**ALRC**), requiring a fault threshold of 'intentionality or recklessness'**.** We do not however support an outcome where it would be open to claimants to seek compensation for the same actionable conduct under multiple heads of claim. To avoid this risk, we encourage legislative clarity that only one form of action can be pursued or separately a statutory tort is reserved only for actions against entities, individuals or matters *not* covered by the Privacy Act.

5. The AICD considers a number of the key proposals to the Privacy Act require additional work to demonstrate the policy case for change. We in-principle support changes to the definition of 'personal information' and amendments to Australian Privacy Principle 11 Security of Personal Information (**APP 11**). However, we are concerned that other key proposals, including the objective test of 'fair and reasonable' information handling, may unnecessarily add a layer of complexity to the Privacy Act with very limited benefit.

6. The AICD recommends that proposals for a privacy impact assessment and a senior officer with responsibility for privacy obligations should be limited to larger businesses. Disproportionally imposing entity level requirements of this nature on SMEs and NFPs could be a counterproductive compliance requirement, creating unnecessary costs.

7. The AICD does not support the OAIC being able to make delegated legislation in the form of privacy codes. Our view is that this power would be inconsistent with the intent of delegated legislation and in time would add complexity for entities seeking to interpret and comply with the Privacy Act, particularly those with limited resources. The focus should be on consolidating the various legislative frameworks that govern privacy obligations, data management and cyber security rather than providing the OAIC with additional regulation making-powers.

8. The AICD in-principle supports the introduction of mid and lower tier penalty provisions and the OAIC being able to issue penalty notices for administrative breaches of the Privacy Act. We recommend the Government provide legislative clarification in primary legislation and/or the Explanatory Memorandum on what nature or severity of a breach would give rise to serious, mid and lower tier penalties.

2. Next Steps

We hope our submission will be of assistance and stand ready to support the Government in this important area of policy reform. If you would like to discuss any issues further, please contact Simon Mitchell, Senior Policy Adviser at smitchell@aicd.com.au or Laura Bacon, Senior Policy Adviser at lbacon@aicd.com.au.

Yours sincerely,

Christian Gergis GAICD
Head of Policy

Attachment A: Summary of AICD policy positions

#	Proposal	AICD Policy Position	Detail - page
4.1 – 4.2	Definition of personal information	In-principle support	18
5.1	Provide the OAIC with new powers to make privacy codes	Do not support	22
6.1	The removal of the small business exemption	Do not support for all currently exempt entities. Recommend the Government consider removal of the exemption for high privacy risk small businesses or the proportionate application of Privacy Act obligations between small and large businesses	9
12.1 – 12.3	Fair and reasonable personal information handling test	Do not support	18
13.1	Privacy impact assessments for activities with high privacy risks	Support, subject to the obligation being limited to large businesses	21
15.2	Entities required to designate a senior employee with responsibility for privacy	Support, subject to the obligation being limited to large businesses	21
18.3	Introduction of a right to erasure	In-principle support subject to data retention obligations being harmonised and an assessment of existing rights under APPs	18
21.1 – 21.4	Amendments to APP 11	Support other than proposal 21.4. Recommend further analysis of the policy case for proposal 21.4 (and proposal 4.6)	18
21.6 – 21.8	Data retention practices	Support 21.6 Support 21.7 and 21.8 subject to extensive work to harmonise and simplify data retention obligations across the Commonwealth and states and territories	12
22.1	Introduce the concepts of APP entity controllers and processors	Further analysis required	20
25.1	New mid-tier and lower-tier penalty provisions	In-principle support subject to clarification on what severity of breach would give rise to a serious, mid and lower tier penalties	23

#	Proposal	AICD Policy Position	Detail - page
25.7	OAIC resources	Support additional OAIC resources. Do not support an industry funding model	8
26.1	Introduction of an individual direct right of action	In-principle support subject to the direct right of action being limited only to serious interferences with privacy involving significant fault on the part of an entity	12
27.1	Introduction of a statutory tort for privacy	In-principle support subject to the tort being limited to a fault threshold of 'intentionality or recklessness' and a statutory tort is reserved only for actions against entities, individuals or matters not covered by the Privacy Act	12
28.1 – 28.2	Changes to the Notifiable Data Breaches Scheme	Support 28.1 In-principle support 28.2 subject to the 30-day window to undertake an assessment of a suspected eligible data breach being retained	11
29.3	Commonwealth, state and territory working group to harmonise privacy laws	Support	12

Attachment B: Responses to key proposals

1. General comments

The AICD strongly support steps to modernise the Privacy Act. Since the introduction of the Privacy Act in 1988 there have been profound changes in how Australians and Australian businesses interact, transact and share information. The Privacy Act, as the central legislative data framework, should reflect this digital paradigm and instil confidence in Australians that their information is being appropriately collected, stored and secured.

However, we are concerned that there is not currently an analysis of the costs and benefits of the proposals were they to be implemented in totality or in part. In addition, the AICD considers that, given the scale of proposed reforms, a phased multi-year implementation of the proposals and appropriate OAIC resourcing will be key to ensuring the reforms achieve their intended objectives in the coming years.

Clear understanding of the costs and benefits

The scope of the proposals contemplated under the Report is considerable and were they to be implemented fully, or in part, they would fundamentally transform the privacy law framework in Australia. With 116 separate proposals it is very challenging for informed stakeholders to fully understand the potential impact of the changes, including assessing whether the benefits from a particular proposal will result in an uplift in data management practices that outweighs the costs to entities and the economy more broadly.

Consistent with our submission to the Discussion Paper, we are concerned that the policy case for many of the changes has not been made, including a clear analysis of the costs and benefits. The AICD considers the objective of the reforms should be to modernise the Privacy Act in a manner that is responsive to the Australian community's expectations on data management and privacy while ensuring entities can efficiently and safely use personal information to the benefit of the Australian economy.

However, we are concerned that a number of the proposals are motivated by the objective of bringing Australia's privacy regime into alignment with international jurisdictions, primarily 'adequacy' with the General Data Protection Regulation (**GDPR**), rather than a focus on improving data practices in Australia. It is not clear, at least from the Report, that any benefits from improved data flows or international trade from adequacy with the GDPR, by way of example, would outweigh the costs of these new obligations.

Stakeholders' feedback is clear that the proposals will result in a significant increase in the compliance costs in meeting the Privacy Act obligations and for many entities it will be very resource intensive and complex to implement the new requirements to meet them in an ongoing manner. Across the economy, the changes may in aggregate impose unnecessary barriers to the dynamic and creative use of data in a way that impedes innovation by Australian businesses. The proposals need to both enhance the protection of personal information without unnecessarily stifling innovation, and a comprehensive cost benefit analysis will assist that assessment. We note the Productivity Commission, as a component of its five yearly productivity inquiry, found that the Government should adopt a risk-based approach to imposing new cyber and data regulations:

> *An overly legalistic focus on the need for privacy safeguards that is not coupled with a consideration of their costs in limiting data use, competition and technological innovation risks regulation swinging too far in the direction of restriction. The costs of overly restrictive privacy*

regulations are not just felt by businesses, but also by individuals. Consumers value their privacy; however, they also place a high value on the products and services that are made available by data sharing.[2]

As discussed below in respect of the small business exemption, many of the proposals are disproportionate or regressive in nature, in that the compliance costs will be far higher for SMEs and NFPs relative to large businesses and the data risk profile of these entities. Our strong view is that reforms should be designed in a proportionate and graduated manner, such that SMEs or small NFPs do not incur the same compliance obligations as larger entities with a higher data risk profile.

We also strongly encourage the Government to undertake a comprehensive Regulation Impact Statement (**RIS**) of the reforms in their totality prior to bringing any legislation to Parliament. A comprehensive cost benefit analysis of the proposals is an important policy making step that will provide visibility on how the Government has assessed the trade-offs between improved data management practices, and any other policy objectives, as well as the costs on entities from the changes.

Director focus on cyber security and data governance

AICD members are highly engaged on the governance of cyber security and data protection and are motivated to build the cyber resilience of their organisations. Cyber-crime and data security is consistently cited as the number one issue keeping directors awake at night in the AICD's biannual Director Sentiment Index.[3]

To support AICD members in governing cyber risk we published the Cyber Security Governance Principles (**the Cyber Principles**) in partnership with the Cyber Security Cooperative Research Centre (**CSCRC**), in October 2022.[4] The Cyber Principles have filled an identified gap in practical guidance available to Australian directors of all sizes of organisations to effectively oversee and engage with management on this rapidly evolving risk. Notably, the Cyber Principles have received the endorsement from the Minister for Home Affairs and Cyber Security, the Hon Clare O'Neil MP. To date, the Cyber Principles and supporting resources have received over 16,000 unique downloads reflecting the appetite of directors to improve their knowledge of cyber security risk and build organisational-wide cyber resilience.

In developing the Cyber Principles, and through engagement on earlier Government reform proposals, AICD members have consistently expressed concern with the often-uncoordinated Government approach to cyber security regulatory reforms. An example that is raised by members is that the Government is separately pursuing the development of a *2023-230 Cyber Strategy* while at the same time contemplating fundamental changes to the Privacy Act. Directors are concerned that these two important reform initiatives are both focused on strengthening Australia cyber security and data management practices, but are not aligned and run the real risk of layering new regulatory obligations on top of an already highly complex privacy and cyber security landscape.

The success of the Cyber Principles reflects the opportunities that exist for industry to be a genuine partner with Government in driving a 'team Australia' agenda to building data governance practices and cyber resilience. The speed at which the threat landscape has been evolving, consistent with changes in technology and personal behaviour with digital products, makes a policy focus solely on strengthening the 'stick', or compliance elements of regulatory regimes, counterproductive.

---

[2] Productivity Commission, Advancing Prosperity 5-year Productivity Inquiry Report, Volume 4: Australia's data and digital dividend, page 88.
[3] AICD Director Sentiment Index, Second Half 2022, available here.
[4] AICD CSCRC Cyber Security Governance Principles, October 2022, available here.

Phased implementation

The AICD recommends the Government adopt a multi-year and phased approach to any implementation of the reforms outlined under the Report. Indeed, given the complexity of some of the proposals dedicated consultation processes would be warranted.

The scope and complexity of the proposals necessitates that impacted entities be provided with sufficient time to educate themselves and prepare for the commencement of the obligations. The number of changes and the challenges in developing and implementing legislation means that this reform process cannot be rushed. Rather, a detailed and sequential approach to implementing the proposals will provide entities with sufficient time to prepare to make changes to internal resources, systems and processes. A further fundamental component will be ensuring the OAIC has sufficient resources to ensure that the other proposals are implemented with enough support and guidance for industry.

At a high level, we consider that the core phases should be:

a. Phase 1: Resourcing of the OAIC and Attorney General's Department to support the changes;

b. Phase 2: OAIC regulatory, enforcement and penalty powers;

c. Phase 3a: Harmonisation of existing obligations (e.g. Data retention laws, NDB scheme);

d. Phase 3b: Structural changes to the Privacy Act (e.g. definition of personal information);

e. Phase 4: Entity level obligations (e.g. Privacy Impact Assessment);

f. Phase 5: Direct right of action and statutory tort;

g. Phase 6: Consideration of the small business exemption.

The AICD would welcome the Government, when making its formal response to the Review, to clearly state the timeline for the development of legislation, consultation and proposed implementation.

Proposal 25.7: OAIC resources

As outlined in our submission to the Discussion Paper, the AICD supports additional resources for the OAIC recognising its importance and expanding role in Australia's digital economy. Given the scope and number of proposals in the Report will require significant OAIC support, it is not possible to see how meaningful reform of the Privacy Act can be progressed without a substantial increase in OAIC funding.

Consistent with our submission to the Discussion Paper, we remain of the view that an industry funding model is inappropriate for an economy wide regulator. Identifying entities that operate in high-risk privacy environment as being subject to a particular statutory or industry levy would be highly complex and subjective. Further, a cost recovery approach that charges entities for guidance or assistance would disincentivise engagement with the regulator and be counterproductive to the broader objectives of improving information handling practices and cyber resilience

We recommend that the Government provide any increase in resources and funding for the OAIC 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.

2. Small business exemption

This section responds to:

a. Proposal 6.1: The removal of the small business exemption

Privacy risk profile of SMEs and NFPs

The AICD does not support the removal of the small business exemption as proposed under 6.1. While we support the elements of the proposal covering an 'impact analysis' and support for small business, our current view is that the costs and significant regulatory challenges associated with removing the exemption for all currently exempt entities outweigh the potential privacy benefits. As set out below, we encourage the Government to assess whether a policy response focused on small businesses with high privacy risks, or a proportionate application of the Privacy Act obligations, would be a more effective approach to lifting data management practices of SMEs and NFPs.

The AICD acknowledges that in an ideal regulatory environment, all Australian entities would be required to meet consistent privacy obligations regardless of size or business complexity. We are also of the view that SMEs and small NFPs should be proactively building their cyber resilience and data management practices, with strong support from Government and industry bodies. We note that the Cyber Principles contained guidance targeted at the SME and NFP directors, including a standalone Snapshot, to assist directors of smaller entities identify practical steps to build cyber resilience.[5]

The AICD however considers that applying the Privacy Act to all entities regardless of size would ignore the reality of the very limited resources and staffing of small businesses and NFPs, and the often lower privacy risk profile of these organisations. Faced with increased compliance costs and the complexity of the Privacy Act obligations, many smaller organisations may consequently adopt a 'tick a box' compliance approach, as opposed to making genuine efforts to build cyber resilience and improve data management practices. We note the Productivity Commission has cited research that the introduction of the GDPR in Europe has resulted in increased compliance costs and reduced profits that have predominantly impacted small businesses.[6] In aggregate, we do see risks that extending the Privacy Act to small business and NFPs will, in time, limit the growth prospects of these entities with resulting impacts on employment, or the pursuit of their charitable purposes.

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 undertaking a Privacy Impact Assessment, appointing a privacy officer or understanding the distinction between a "processor" and "controller". Our view is that it would be very likely that a high proportion of small businesses and NFPs would simply not be aware that the Privacy Act applies to them, resulting in a large degree of inadvertent non-compliance, thereby undermining the intent of removing the exemption.

The AICD strongly recommends that the Government consider whether a more targeted approach focused on industries or sectors where there are elevated privacy risks will result in greater benefit than a blanket application to all entities. Our view is that prescribing further acts and practices under section 6E of the Privacy Act is an appropriate mechanism to target small entities with higher privacy risks.

---

[5] AICD CSCRC Cyber Security Governance Principles, October 2022, available here.

[6] Productivity Commission, Advancing Prosperity 5-year Productivity Inquiry Report, Volume 4: Australia's data and digital dividend, page 88.

A common example that has been shared with us, and noted in the Report, is that real estate agents collect significant amounts of personal information and represents high privacy risks. Our view is that the Privacy Act obligations should extend to sectors of this nature. This targeted policy making approach would seek to maximise the privacy benefits to the broader community while limiting regulatory compliance costs to those businesses with elevated privacy risks.

Proportionate response

The AICD recommends that absent a focus on high-risk industries and practices, as set out above, the Government could explore imposing the obligations under the Privacy Act in a proportionate and graduated manner based on the size of the entity. This approach would appropriately exempt small entities from meeting the more prescriptive elements of the Privacy Act, thereby limiting the potential regulatory burden.

The AICD notes that a proportionate approach to regulation is utilised in other Commonwealth policy areas, for example modern slavery reporting or the application of certain Australian Prudential Regulation Authority (**APRA**) prudential standards. We also note that the United Kingdom is currently undertaking reforms to its data protection laws and is expressly examining whether to exempt small business from elements of the regime.[7]

We strongly encourage the proposed 'impact analysis' to examine how a proportionate model could be designed in a manner that limits the burden on small business. Key existing or proposed elements of the Privacy Act that may be appropriate for a proportionate approach include privacy impact assessments, senior employees with responsibility for privacy and exemptions from all or components of certain APPs, for example APP 2 Anonymity and Pseudonymity and APP 12 Access to Personal Information

Ultimately, our view is that the road to enhanced small business cyber resilience and data management practices is via constructive support and guidance, rather than a focus on imposing regulatory requirements. We strongly support additional support for small business of the nature that is outlined in section 6.5 of the Report, including the OAIC establishing a small business hub and e-learning tools. Considering many SMEs should already be meeting the Privacy Act obligations by virtue of having annual turnover greater than $3 million, our strong view is that these support measures should be implemented regardless of whether the small business exemption is retained or not.

As discussed above, we support greater resources for the OAIC and consider this in part could be directed at a collaborative and support focused approach to improving information protection practices across SMEs.

3. Harmonisation of existing obligations and regulatory frameworks

This section responds to:

a. Proposals 28.1 – 28.2: Changes to the Notifiable Data Breaches Scheme

b. Proposals 21.6 – 21.8; 29.3: Data retention practices and Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues

[7] UK Department for Digital Culture, Media & Sport, Data: a new direction – government response to consultation, June 2022

28.1 – 28.2 Notifiable Data Breaches scheme (NDB scheme)

AICD members have consistently raised concerns with the complexity of existing regulatory frameworks that apply to data and cyber security management practices. This complexity produces significant compliance costs, creates challenges when responding to a cyber-attack or data breach, and generates significant uncertainty on what data an entity is required to hold and for how long.

In this context, the AICD strongly supports Proposal 28.1 to undertake further work to examine opportunities for alignment between multiple reporting processes. The AICD appreciates that different reporting and notification regimes are established for different purposes by distinct regulators or legislative regimes, and there are inherent challenges in harmonising these obligations. However, for an entity that is responding to a significant cyber incident and resulting data breach, it can be complex and unhelpful to meet separate notification obligations for distinct Commonwealth regulators.

The AICD considers that, at a minimum, the additional work under Proposal 28.1 should explore opportunities for a notification under the NDB scheme, and its accompanying detail, to be shared with other regulators at the permission and direction of the entity. We note that the Productivity Commission recently expressly recommended this model (Recommendation 4.5) under its Productivity Inquiry, finding:

> *A business may face multiple reporting requirements for a single cyber security incident, depending on its operations and the nature of the breach. This can place unnecessary burdens on businesses that are focused on recovering from the cyber incident. More coordination between government agencies and streamlining of reporting requirements (such as via a single online interface) would assist in reducing reporting burdens on businesses.*[8]

A platform approach would allow for future reporting or notification obligations, such as ransomware reporting as is contemplated under the *2023-2030 Cyber Strategy* Discussion Paper, to be readily incorporated.

The AICD in-principle supports Proposal 28.2 to specify that an entity has 72 hours to notify the OAIC when it has reasonable grounds to believe there has been an eligible data breach. This change would be an improvement over the existing 'soon as practicable' terminology and broadly consistent with obligations under the *Security of Critical Infrastructure Act 2018* and GDPR. More fundamentally, having a clearly defined regulatory obligation is preferable to an ambiguous one.

For the avoidance of doubt, we would not support any amendment to section 26HW and the 30-day window to undertake an assessment of a suspected eligible data breach. Cyber-attacks and accompanying data losses can be very complex, opaque and dynamic events where it is challenging for entities to determine in the early stages the extent of data that has been lost or compromised, from where and the impacted individuals. The 30-day period appropriately reflects this dynamic and gives an entity sufficient time to understand the data breach and notify the OAIC with appropriate details.

The AICD also supports changes to section 26WL(3) to clarify the obligations on informing impacted individuals and separately having a requirement under the NDB provisions for an entity to have a plan for responding to an eligible data breach. We note that the AICD recommends a comprehensive response plan as a matter of better practice under the Cyber Principles.[9]

---

[8] Productivity Commission, *Advancing Prosperity 5-year Productivity Inquiry Report*, Volume 4: Australia's data and digital dividend, page 82.

[9] AICD CSCRC Cyber Security Governance Principles, October 2022, available here.

21.6 – 21.8; 29.3 Data retention practices and Commonwealth, state and territory working group

The AICD strongly supports proposals 21.6 and 29.3 to examine data retention laws as a component of Commonwealth, state and territory work to harmonise existing privacy laws.

We have received feedback from both AICD members and industry experts on the current challenges with interpreting, navigating and complying with Commonwealth, state and industry specific data retention laws. Members have shared with us instances of an entity having to grapple with inconsistent data retention obligations and requiring costly legal advice on how to navigate the conflicting requirements. Recent Gilbert + Tobin analysis indicates that there approximately 100 laws, standards and enforceable guidelines applying to the retention and management of customer and business data in the financial services sector alone.[10]

Directors have reflected that the result of the maze of data retention laws is that organisations will hold personal information for extended periods out of an abundance of caution to ensure they are meeting any applicable obligations. The AICD's view is that this regulatory complexity is a key contributing factor to entities holding personal information for longer than is necessary, which in turn increases the extent of data loss and potential damage from a significant cyber incident or data breach.

Our view is that harmonisation and the repeal of outdated or unnecessary data retention obligations is a necessary precondition to pursuing proposals 21.5 and 21.7. The AICD in-principle supports amending APP 11 as is outlined under proposals 21.5 and 21.7. In particular, the flexibility provided to entities to set minimum and maximum retention periods under proposal 21.7 is welcomed and is consistent with other jurisdictions. However, it will not be possible to meet these obligations consistent with the policy intent until the broader set of data retention requirements is consolidated and simplified.

Further, these issues directly impact upon the following discussion on potential new causes of action, as the lack of clarity on data retention obligations can then mean that organisations are exposed to higher litigation risk.

4. Direct right of action and statutory tort

This section responds to:

a. Proposal 26.1: Introduction of an individual direct right of action

b. Proposal 27.1: Introduction of a statutory tort for privacy

26.1 Direct right of action

The AICD in-principle supports a direct right of action for individuals to seek compensation in circumstances where they have suffered loss or damage as a result of a serious interference of their privacy.

The proposed gateway model, requiring individuals to make a complaint first to the OAIC to assess for conciliation before a claim may proceed to the Federal Court, is also supported by the AICD. We understand that this requirement is intended to ensure effective use of court resources and mitigate the risk of unmeritorious or vexatious claims from proceeding to the Federal Court.

[10] Australian Financial Review, *Business navigates a maze of data obligations, law firm warns*, 20 March 2023.

However, to avoid unintended consequences, the AICD strongly encourages that the right of action be limited to 'serious' interferences with privacy, that requires significant fault on the part of an APP entity, resulting in serious loss or damage.

We outline the following concerns with a direct right of action being introduced without such conditions being met.

Gateway model may be circumvented

Our interpretation of the proposed gateway model is that a complainant may still seek leave to the Federal Court instead of pursuing conciliation (at a complainant's election), or even in circumstances where the OAIC has determined that there has been no breach of the Privacy Act and has terminated the matter.[11] Our concerns with this are two-fold. Firstly, a claimant may seek to circumvent the gateway model by electing not to participate in a conciliation process via the OAIC. This risk is even more pronounced in the case of class actions initiated on behalf of claimants by plaintiff law firms and litigation funders with commercial imperatives that drive a preference for litigation. Secondly, without a harm threshold that requires a *serious* interference of privacy, there is a risk that a direct right of action will be pursued in court even where the OAIC has established that an entity has taken reasonable steps under APP11 to protect personal information.

We understand that jurisdictions such as New Zealand and Singapore have a similar direct right of action mechanism to compensate individuals for loss or damage arising out of an interference with their privacy, which is not limited to a seriousness threshold.[12] However, we note that direct right of action mechanisms in these jurisdictions operate differently to that being contemplated by the Report and do not give rise to the same risk of unintended consequences as outlined above, for example:

- New Zealand's privacy legislation requires privacy complaints to be made first to its Office of the Privacy Commissioner (**OPC**) for investigation. If settlement cannot be reached, then proceedings can be brought in the Human Rights Review Tribunal and damages sought. If an aggrieved individual disagrees with the Tribunal's decision, only then can an action be appealed to the High Court.[13]

- The gateway model in Singapore operates in a similar way. Singapore's privacy and data protection legislation requires privacy complaints to be made first to its Personal Data Protection Commission (**PDPC**). A direct right of action by way of civil proceeding in court is then only exercisable after a decision issued by the PDPC has become final, after all avenues of appeal have been exhausted.[14] Even then, appeal to the High Court or Court of Appeal in Singapore may only be made on limited grounds, such as on a point of law or regarding the amount of a financial penalty.[15]

In other words, under each of these models the prospects of a speculative class action being commenced in court are more remote and subject to a greater degree of scrutiny before progressing. The AICD strongly recommends that the gateway model for a direct right of action in Australia apply a stricter requirement for claimants to participate in conciliation if the OAIC determines that a claim is

[11] Final Report, p. 275.
[12] However we note in respect of injury to a person's feelings, loss of dignity or humiliation, the New Zealand legislation applies a threshold of "significant": *Privacy Act 2020 (NZ)*, s 69.
[13] *Privacy Act 2020 (NZ)*, s 98.
[14] *Personal Data Protection Act 2021* (Singapore), s 480.
[15] Advisory Guidelines on Enforcement of the Data Protection Provisions, Personal Data Protection Commission Singapore,(available here).

suitable for this process and remove any ability for claimants to elect not to participate. This, in our view, together with a harm threshold of 'seriousness' and significant fault threshold on the part of the APP entity, would help ensure claimants and in particular, class actions, do not seek to circumvent the gateway.

In the AICD's view, remediation of affected individuals of major data breaches is a critical component of an incident's response and recovery process. The Cyber Principles recommend that where a major cyber incident occurs and individuals have been significantly exposed by a data breach, an organisation should offer to pay compensation (financial or in-kind) and/or provide reimbursement for any out-of-pocket expenses incurred in seeking to mitigate their actual or potential loss.[16] In our view, the proposed gateway model should ensure that Federal Court consideration of a claim is a last resort measure, and that genuine efforts by all parties are made to remediate consequential loss and damage in the aftermath of a breach, or through the OAIC's existing conciliation process in the first instance.

Significant class action risks

A direct right of action with a low harm threshold could open the flood gates to speculative or opportunistic class actions in respect of data breaches – particularly where "loss or damage" under the Privacy Act extends to humiliation and injury to a person's feelings. Indeed, a claim involving hundreds of thousands, or even millions of customers, could have a major financial impact on entities if a court were to determine that the appropriate economic loss and/or non-economic loss (in the case of humiliation or injury to a person's feelings) was even a small sum such as a few hundred dollars.

Further, as highlighted in our submission to the Discussion Paper, the AICD has been extensively involved in recent reforms to the regulatory settings and commercial incentives driving Australia's attractiveness for securities class actions and litigation funding. We have received market feedback that those pre-reform settings resulted in adverse economic and legal consequences, including a D&O insurance market that has until recently been in crisis.[17] We consider that any proposals to provide new avenues for class actions should be carefully considered and proportionate to the harm suffered by complainants.

Cumulative impact of multiple redress mechanisms

We have concerns with the interaction and cumulative effect of the multiple redress mechanisms – both existing and proposed. For example, as outlined in the illustrative example below, an entity that breaches the Privacy Act may not only face the imposition of penalties by the OAIC, but also the prospect of a direct right of action claim for compensation and a separate statutory tort action.

Moreover, directors and officers of an entity in breach of the Privacy Act may also face individual director liability under what is known as the 'stepping stone' approach to liability - a unique feature of Australian law.[18] Stepping stone liability arises where a company is found to have breached the law and its directors may be pursued for failing to exercise reasonable care and diligence under section 180 of the *Corporations Act 2001* (Cth) (**Corporations Act**) in causing or failing to prevent the company from breaching the law (for example, APP 11 of the Privacy Act).

Special considerations for data breaches stemming from cyber attacks

[16] AICD-CSCRC Cyber Governance Principles, p. 46.
[17] AICD submission, Treasury Laws Amendment (2021 Measures No.1) Bill 2021, 28 May 2021, available here.
[18] See advice from law firm, Allens (available here).

In many cases, data breaches are the direct result of third-party cyber-attacks which continue to regularly impact Australian entities, large and small, in a dynamic and high threat operating environment. Even organisations with the most rigorous cyber security practices, that take all reasonable steps to protect their data, can fall victim to sophisticated, sometimes state-sponsored, cyber-attacks. Indeed, certain organisations may face heightened exposure given their critical role in the Australian economy (e.g. critical infrastructure providers), and the unsettled state of geo-politics currently.

It would be unjust in our view to have entities and their directors subject to multiple claims for the same actionable conduct without a requirement of complainants to establish a serious element of harm and significant fault on the part of the entity. In the aftermath of a data breach, policy settings should incentivise organisations to focus on response and recovery, as well as appropriate remediation of affected individuals, rather than encouraging responses with litigation risk front of mind.

Further, as noted earlier, were the relevant harm and fault thresholds set at too low a level, private actions might be brought against organisations that suffered a data breach, despite having robust cyber controls in place. This would be especially likely where organisations have millions of customers, making the prospect of a class action potentially very lucrative for litigation funders and plaintiff lawyers, even should individual claims be relatively modest. In our view, unless a 'serious' interference with privacy can be shown involving significant fault on the part of a penetrated organisation, and absent appropriate remediation, enforcement of privacy obligations should be left to the relevant regulators.

Illustrative example – a significant data breach at a large Australian financial institution

To highlight our concerns, the following hypothetical example illustrates the impact that multiple enforcement and redress mechanisms, including a direct right of action and statutory tort without a 'serious' harm and significant fault threshold, could have in practice.

A large listed Australian financial institution (**Organisation**), which is regulated by APRA and Australian Securities & Investments Commission (**ASIC**), suffers a significant data breach as a result of a cyber-attack by a sophisticated, malicious third party actor. Millions of Australian customer records, including names, dates of birth, residential and email addresses, phone numbers, credit card and Medicare numbers, as well as passport and driver's license information (**Customer Data**), are accessed by the malicious actor and leaked on the dark web. Following market disclosure of the attack, the Organisation's share price falls by 10%.

Regulatory enforcement action

An investigation into the personal information handling practices of the Organisation is initiated by the OAIC to determine whether reasonable steps to protect personal information in compliance with APP 11 was taken by the Organisation. The OAIC through its investigation finds that the data breach was caused by a malware infection instigated by the malicious actor. This particular occurrence was preventable, although such attacks are not completely preventable by organisations. A determination is made by the Federal Court that the Organisation did not take all reasonable steps to protect the personal information of its customers and was negligent (although not grossly negligent) in its exercise of personal information handling practices. The Federal Court imposes civil penalties, the greater of: A$50million; three times the value of benefits obtained or attributable to the breach; or 30% of the corporation's 'adjusted turnover' during the 'breach turnover period'.

Separately the Organisation faces regulatory enforcement action by APRA and ASIC. APRA examines whether the Organisation has breached its prudential requirements, including under Prudential Standard CPS 234 Information Security. ASIC also investigates the organisation for whether it has breached its Australian Financial Services License (**AFSL**) risk management obligations.

Compensation claims

In parallel, 5 million affected customers of the data breach join a class action led by an Australian plaintiff law firm via the direct right of action mechanism. The plaintiffs lodge a complaint with the OAIC, citing loss and damage (including hurt feelings and anxiety caused by the compromised data) on behalf of millions of affected customers. Instead of pursuing conciliation via the OAIC, the class action elects to seek leave to have the direct right of action claim heard in the Federal Court.

Separately, the same plaintiffs initiate a claim in the Federal Court via the statutory tort for invasions of privacy citing misuse of private information. Establishing the tort claim does not however require the affected customers to demonstrate actual damage or loss, and damages may be awarded for emotional distress.

Each of these claims proceed to the Federal Court without the need for the class action to establish data breach was due to significant fault on the part of the Organisation.

A second plaintiff law firm seeks to bring a securities class action on behalf of shareholders, alleging that the Organisation breached its continuous disclosure obligations by failing to adequately disclose their privacy risks and vulnerabilities. The plaintiffs allege that the breach of continuous disclosure obligations was as a result of recklessness or negligence on behalf of the company.

Directors' duty enforcement

Finally, in addition to investigating the Organisation for a breach of its AFS licence obligations, ASIC also initiates civil proceedings against the directors and executives of the Organisation for a breach of their statutory duty of care and diligence under section 180 of the Corporations Act. ASIC alleges that the directors and senior executives of the Organisation failed to give sufficient focus to the risk of a major data breach and take reasonable steps to ensure appropriate policies, procedures and systems were in place to protect the personal information of its customers.

This example highlights that where a direct right of action is able to be initiated by a claimant without a serious harm threshold and a requirement for significant fault on the part of an entity, a claimant (or in this case, a class action) is able to progress the claim to the Federal Court in parallel with other regulatory enforcement measures. However, should the direct right of action require a serious interference with privacy and a requirement for significant fault on the part of an entity, this claim may not have met the threshold to be actionable under a direct right of action (i.e. a standard of 'intentionality or recklessness' on the part of the Organisation). Rather, the OAIC's imposition of penalties for failing to take reasonable steps to protect personal information (i.e. negligence on the part of the Organisation) would have been adequate punitive action in these circumstances.

27.1 Statutory tort

The AICD in-principle supports the introduction of a statutory tort for serious invasions of privacy provided it adopts the model recommended by the ALRC Report 123. We recognise that a statutory tort would provide a means of redress for claimants in respect of serious invasions of privacy not currently covered by the Privacy Act (for example, against non-APP entities such as individuals and small businesses).

The AICD agrees with the ALRC's reflections that a statutory tort of invasion should require a fault threshold of 'intentionality or recklessness', and mere negligence is not sufficient – particularly where it is proposed that the tort of invasion be actionable even without proof of actual damage. As noted by the ALRC:[19]

> *Adopting a fault element of intention and recklessness would allow an action in tort without proof of damage in line with the torts of assault and false imprisonment. Extending the fault element to negligence would undermine an important justification for making the tort actionable without proof of damage. Proof of damage is an essential element of the tort of negligence.*

A statutory tort with a fault threshold of intentionality or recklessness would also be consistent with comparable jurisdictions such as the UK, New Zealand and the US.[20]

That said, as noted above, we have some concerns with the interaction between, and cumulative impact of, the proposed direct right of action and a statutory tort. Our interpretation of the operation of the two mechanisms is that it would be open to claimants to seek compensation under both a direct right of action and statutory tort for an invasion of privacy – potentially on different evidentiary grounds, and in different forums. For example, a direct right of action would require proof of loss or damage, while a statutory tort as recommended by the ALRC would not. Moreover, while a direct right of action would be limited to civil proceedings in the Federal Court following lodgement of a complaint with the OAIC, a statutory tort claim could be actionable in the Federal Court as well as state and territory courts.[21]

Although the AICD is supportive of both a direct right of action and statutory tort for invasions of privacy, we do not support an outcome where it would be open to claimants to seek compensation for the same actionable conduct under multiple heads of claim. We note again the potential for these actions to run concurrently (including by way of class action) in addition to any penalties imposed independently by the OAIC.

[19] ALRC Report 123, p. 117-118.
[20] ALRC Report 123, p. 94.
[21] ALRC Report 123, p. 165.

To avoid this risk, we encourage claims under a statutory tort to be available only for actions against entities, individuals or matters not covered by the Privacy Act (or in other words, where a direct right of action is not able to be pursued). Alternatively, clarification could be provided that claimants may only elect to seek compensation via one form of action.

5. Structural changes to the Privacy Act

This section responds to:

a. Proposals 4.1 – 4.2: Definition of personal information

b. Proposals 12.1 – 12.3: Fair and reasonable personal information handling

c. Proposal 18.3: Introduction of a right to erasure

d. Proposals 21.1 – 21.4: Amendments to APP 11

e. Proposal 22.1: Introduce the concepts of APP entity controllers and processors

4.1 – 4.2: Definition of personal information

The AICD in-principle supports the broadening of the definition of 'personal information' and a supporting list of the types of information that fall within the definition.

The AICD considers this definitional change will clarify that the Privacy Act obligations apply to information that is increasingly collected when individuals are interacting in a digital environment, for instance metadata. The change will in practice expand the volume and nature of information subject to relevant Privacy Act obligations. This is likely to be a significant change for many entities and will require amendments to existing information systems and processes. As set out above, our strong view is that a multi-year phased implementation is necessary to ensure that entities are prepared to implement significant structural changes to the Privacy Act, such as an expanded definition of personal information. Comprehensive OAIC guidance, co-designed with industry, will also be key to successful implementation of this change.

The AICD encourages comprehensive consultation on draft legislation and OAIC guidance to implement this change. We expect there may technical challenges with the drafting and the potential for unintended consequences, particularly in the context of the vast number of other proposals, that will need to be considered by stakeholders.

12.1 – 12.3: Fair and reasonable personal information handling

The AICD considers that introducing an overarching 'fair and reasonable' test may result in considerable legal complexity and unnecessarily complicate the existing APPs framework. While we understand the broad policy intent behind the proposal, our view is that targeted amendments to key APPs to enhance the concepts of fairness and reasonableness would be more effective than a broad test.

The proposed test combines two distinct legal concepts or thresholds in 'fairness' and 'reasonableness' and taken together it may be very challenging for an entity, the OAIC or a court to form a view of whether the test has been breached. We note that the Report cites the UK/European Union, Singapore and Canada as examples of jurisdictions that have similar tests. However, in each of these jurisdictions there is only one limb of the proposed test. For example, in the UK/GDPR it is 'fairness', while in Canada and Singapore it is 'reasonableness'. Further, the Australian Consumer Law is limited to 'fairness'. We are

not aware of any comparable jurisdiction or domestic legislative framework that has both 'fairness' and 'reasonableness' as components of the one test.

While Proposal 12.2 covers a list of matters that would be considered by an entity in considering the test, we do consider it will ultimately be very difficult to determine what an objective reasonable person would have considered as a fair and reasonable collection and use of the personal information. In addition, the matters under Proposal 12.2 are from the perspective of the individual and the Report is silent on whether there should a corresponding test that would enable entities to use personal information in situations where it is fair and reasonable to do so. Further, it is unclear how the proposed test will interact with other proposed reforms, including more stringent consent obligations, or mandatory data collection and retention obligations outside of the Privacy Act.

The Privacy Act already has 'reasonableness' and 'fairness' as concepts through a number of the APPs (e.g. APP 3). The AICD's view is that rather than an overarching test, targeted amendments to particular APPs to elevate the prominence of the fair and reasonable use of personal information may be a more effective, and less complex regulatory approach that would still elevate the concepts of reasonableness and fairness in the Privacy Act.

18.3: Introduction of a right to erasure

The AICD in-principle supports the right to erasure reflecting that an individual should have appropriate access to, and control of, their personal information as held by entities. However, we consider that prior to implementing this proposed right that data retention obligations should be harmonised and clarified.

We note the Privacy Act already has mechanisms or protections for an individual to access their information, including a right to make a correction (APP 13), the right to interact anonymously and pseudonymously (APP 2) and the obligation to destroy or de-identify the information (APP 11). Further, the Report has a number of proposals that strengthen rights and provide enhanced protections, notably changes to APP 11, changes to the definition of consent and new objective test on information handling. We recommend the Government consider the necessity of a right to erasure in the context of existing, and proposed, elements of the Privacy Act.

As discussed above in respect of data retention practices, our strong view is that proposal 18.3 cannot be progressed until there is harmonisation and clarity on data retention obligations across the Commonwealth, states and territories. An entity cannot be expected to implement a right to erasure process without a clear understanding of whether the request is consistent with data retention obligations they may have to hold certain information for certain periods - for instance a bank holding records under the Corporations Act and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* .

The AICD considers that ultimately any right of erasure should be balanced with appropriate exceptions where an entity is not able to fulfil the request due to other legal obligations. The AICD also expects that implementing a right to erasure will be a challenge for many entities from a process perspective and may be very resource intensive. We strongly recommend that, as this would represent a significant structural change to the Privacy Act, it be implemented with sufficient lead time for entities and accompanying OAIC guidance and support.

21.1 – 21.4: Amendments to APP 11

The AICD supports proposal 21.1 to amend APP 11 to state that 'reasonable steps' includes technical and organisational measures.

The AICD in-principle supports proposal 22.2 to include a set of baseline privacy outcomes under APP 11. We strongly consider that the outcomes are drafted in a manner that provides discretion to the entity to meet these outcomes taking into account the entity's operating environment, information holdings and the types of privacy risks.

As reflected in the Report, the Government is currently developing a *2023-2030 Australian Cyber Security Strategy* that is contemplating broad regulatory reform, including the establishment of a standalone Cyber Security Act. It is crucial that any outcomes attached to APP 11 are harmonised with existing and future cyber security regulatory obligations. AICD members consistently cite complexity with current cyber and data related regulatory frameworks, and the uncoordinated manner in which regulatory reform occurs in these policy areas. We would be very concerned if amendments to APP 11 were inconsistent with broader cyber security reforms and encourage any amendments to cross-reference relevant legislation or frameworks where possible to simplify interpretation for users.

The AICD supports proposal 22.3 for the OAIC to enhance guidance on 'reasonable steps' under APP 11. Consistent with proposal 21.2, the AICD recommends this guidance aligns with relevant cyber security regulatory frameworks and guidance, including that developed by the Australian Cyber Security Centre (**ACSC**) and APRA**.** We encourage the OAIC to consult extensively, including across Government and relevant regulators, on the development of APP 11 guidance.

We consider that further detail is required on proposal 21.4 (and proposal 4.6) to require entities to take 'reasonable steps to protect de-identified information'. Stakeholders have expressed confusion about this proposed amendment noting that 'de-identified information' by its nature has gone through steps or a process that protects the data by stripping out identifying characteristics. We have received feedback that the risks from disclosure of de-identified information are low and that the policy case for applying APP 11 to this information is not strong. We recommend that the Government undertake further analysis on this proposal, including whether the additional compliance burden from extending APP 11 to de-identified information will be outweighed by what appears to be minimal privacy benefits.

22.1: Introduce the concepts of APP entity controllers and processors

We have received mixed feedback on the appropriateness of introducing the processor and controller distinction in the Privacy Act. For large companies that offer technology or digital products and services there is an attraction to this differentiation as it aligns with current business models and is a concept that is utilised in other jurisdictions, including under the GDPR. However, others consider it is an unnecessary change that will increase complexity for very limited benefit.

On balance, the AICD considers that the policy case as set out in the Report for introducing the entity controller and processor distinction is not strong. Our current view is that this distinction may add a layer of unnecessary complexity to interpreting and meeting the Privacy Act obligations, particularly where it may be difficult to determine which category an entity falls into. The example provided in the Report presents a relatively straightforward case of determining which entity is a processor or a controller, however our view is that for many entities it may be blurred or not apparent and will likely differ based on the personal information in question. This dynamic will also present challenges for the OAIC in investigating breaches and attributing responsibility. For SMEs, this change will add further complexity to an already significant uplift in compliance obligations that is contemplated under the Report, particularly if the small business exemption is removed.

As discussed in the General Comments section above, this is one of the proposals where we are concerned the policy objective is primarily associated with seeking adequacy with the GDPR, rather than

improving data practices or individuals' privacy outcomes. In the context of the vast suite of other proposed enhancements in the Report, it has not been demonstrated how this proposal will result in a material improvement in privacy outcomes for individuals or data practices by entities. The AICD recommends that this proposal undergoes further extensive analysis, including an understanding of its costs and benefits.

6. New entity level obligations

This section responds to:

a. Proposal 13.1: Privacy impact assessments for activities with high privacy risks

b. Proposal 15.2: Entities required to designate a senior employee with responsibility for privacy

13.1 Privacy impact assessments for activities with high privacy risks

The AICD supports large entities being required to undertake a privacy impact assessment (**PIA**) for activities with high privacy risks. Feedback from members indicates that this process is already being undertaken by large companies that have products and services or business operations that may have high privacy risks associated with them.

As with Proposal 15.2, discussed below, the AICD does not support this obligation being extended to SMEs should the small business exemption be removed. This is an example of a proposed obligation where it would be appropriate for there to be a proportionate and graduated application between large and small entities. This approach would reflect the resourcing of smaller entities and the potential limited benefit in data practice improvements that would result from requiring SMEs to undertake PIAs. In particular, our view is that there would be challenges in the OAIC raising awareness of a PIA obligation amongst the SME population and further ensuring that SMEs undertake PIAs consistent with the objective of the requirement. Our concern is that should PIAs be required of SMEs, there would be significant inadvertent non-compliance and to the extent it was undertaken, it would be in a limited compliance/tick-a-box manner with very little benefit in data management practices.

The AICD agrees with the Report that the OAIC should support any PIA obligation with extensive guidance, including comprehensive detail and worked examples of what is envisaged by high privacy risk activities.

15.2 Senior employee with responsibility for privacy

The AICD in-principle is supportive of large entities being required to nominate an individual with responsibility for privacy. The AICD understands that in practice many large complex entities already allocate responsibility for privacy and data oversight to an individual or group of individuals. We consider that clear guidance on this obligation from the OAIC will be key to meeting this new requirement, including the expectations for the seniority of the role, where it may sit in the organisation and reporting or engagement with the board of the entity.

As set out in section 2 above, the AICD does not support this obligation being imposed on SMEs and small NFPs with a low privacy risk profile. We consider this would be a disproportionate to the privacy risk of these entities and would not reflect the very limited resources these entities have to meet all the compliance requirements they may face. Further, it is hard to envisage how this obligation would work in practice if the entity has a small number of employees, or is predominantly a casual or volunteer based workforce which would be the case for many NFP.

Consistent with our broader points on the small business exemption, we consider disproportionally imposing a requirement of this nature on small entities would be a counterproductive compliance requirement that would create confusion and costs with very limited benefit in terms of data management practices.

7. OAIC powers and penalty provisions

This section responds to

a. Proposal 5.1: Provide the OAIC with new powers to make privacy codes

b. Proposal 25.1: New mid-tier and lower-tier penalty provisions

5.1 OAIC to make privacy codes

The AICD does not support proposal 5.1 to provide the OAIC with the ability to develop privacy codes where there is public interest and with the approval of the Attorney General. Our view is that the existing industry-led code development process under the Act is sufficient, and the Report does not demonstrate that a regulator code making power is necessary.

Providing a regulator with delegated legislation capacity should be approached with considerable caution. The ALRC noted in Report 129 that the making of delegated legislation can limit public scrutiny and accountability. Further, the ALRC cited the Legislation Handbook as listing what are appropriate matters for primary legislation, this includes:

> *(b) significant questions of policy including significant new policy or fundamental changes to existing policy;*
>
> *(c) rules which have a significant impact on individual rights and liberties; and*
>
> *(d) provisions imposing obligations on citizens or organisations to undertake certain activities (for example, to provide information or submit documentation, noting that the detail of the information or documents required should be included in subordinate legislation) or desist from activities (for example, to prohibit an activity and impose penalties or sanctions for engaging in an activity)*.

Our understanding of the code making proposal from the Report and the Discussion Paper is that it will cover significant new policy and impose new obligations on entities. For example, in respect of cyber security settings for an entity to implement in order to meet APP 11. This approach could undermine the legitimate role of the legislature and would be inconsistent with guidance in the Legislation Handbook, thereby risking regulator over-reach.

We are also concerned that given the broad concept of 'public benefit', that were the OAIC to have the power to make codes, it would eventually result in a significant volume of delegated legislation (on top of the current patchwork of existing regulation). Noting that the Report contemplates that in time the Privacy Act will apply to all businesses, we do not consider it appropriate for key regulatory obligations to be contained outside of the primary legislation. This will only add to the complexity and challenges for entities seeking to comply with the obligations, particularly those with limited resources.

25.1 New mid-tier and lower-tier penalty provisions

The AICD in-principle supports the introduction of mid and lower tier penalty provisions and the OAIC being able to issue penalty notices for administrative breaches of the Privacy Act. A well-designed tiered model has the potential to reflect that privacy breaches, particularly those involving cyber-crime and data theft, run along a spectrum of culpability where the entity holding the data may also be a victim of a sophisticated attack and have limited ability to defend or prevent the data breach from occurring.

Our submission to the Senate Legal and Constitutional Affairs Committee on the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* in November 2022 raised significant concerns with the substantial increases in the penalty amounts for serious and repeated breaches of privacy under section 13G.[22] In that brief consultation, we considered that there should be clarification of the substantive underlying obligations that would lead to a civil penalty under section 13G of the Privacy Act, so that organisations are clear on the steps they should take to comply with the Privacy Act requirements. This policy principle extends to the proposed mid and lower tier penalty provisions. The Report provides very limited detail of what breaches or entity failings would be covered.

We strongly recommend the Government provide legislative clarity in primary legislation or the Explanatory Memorandum on the nature or types of breaches which would give rise to a serious, mid and lower tier penalty actions by the OAIC. Only with this clarity will entities understand the potential liability but also importantly the steps they should take to avoid serious or mid-tier breaches. By way of example, compliance with APP 11 and cooperation with the OAIC in a breach event could be listed as a relevant factor for the OAIC, and ultimately the Court, in assessing the breach and associated penalty. This approach would also be consistent with other proposed amendments to the Privacy Act, for instance APP 11, where additional detail is being provided on key provisions and obligations on entities.

[22] AICD submission, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, November 2022, available here.