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

7 November 2022

Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Committee Secretary

**Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022**

Thank you for the opportunity to provide comment to the Senate Legal and Constitutional Affairs Committee (the **Committee**) regarding the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (**the Bill**).

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, large and small businesses and the government sector.

This Bill is being introduced at the same time as the Government considers the longstanding Review of the *Privacy Act 1988* (**Privacy Act**) (the **Review**). The AICD provided a submission to the Review in January 2022 that supported 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.[1] Separately, the AICD has over the past year participated in Department of Home Affairs led consultations on cyber security regulations and incentives, amendments to the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) and the National Data Security Action Plan.[2]

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

## 1. Executive Summary

The AICD welcomes the Committee's inquiry into these significant proposed amendments to the Privacy Act. The AICD supports a stronger Privacy Act, including enhanced powers and resources for the Office of the Australian Information Commissioner (**OAIC**), that drives Australian organisations to rigorously protect the sensitive personal data they collect.

The AICD recognises the significant public concern with recent large scale data breaches and the momentum this has provided for regulatory reform. We also agree that the current penalty regime for serious and repeated breaches of the Privacy Act is inadequate. However, AICD is concerned that without amendment, the proposed penalty regime has the potential to disproportionately punish

[1] AICD submission, Privacy Act Review Discussion Paper, January 2022, available here.

[2] AICD submission, Strengthening Australia's cyber security regulation and incentives, August 2021, available here; AICD submission, Amendments to the Security of Critical Infrastructure Act, January 2022, available here; AICD submission, National Data Security Action Plan, July 2022, available here.

Australian businesses that have experienced a crippling cyber security incident and broadly disincentivise the reporting of data breaches and cooperation with key regulators.

Our key recommendations to the Committee on the Bill are:

- consideration that the Bill be paused until the Privacy Act Review has made its recommendations and the Government has responded;
- the introduction of a defence or safe harbour based on 'reasonable steps' where unauthorised disclosures of personal information as a result of criminal activity would not necessarily give rise to a breach of the Privacy Act;
- 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;
- amendments to the penalty provisions of the Bill that are based on similar provisions in the *Competition and Consumer Act 2010*. The concept of 'benefits' and penalties linked to turnover is inappropriate in the context of the Privacy Act where the business in many cases also suffers significant financial loss and/or reputational impact;
- a reduction in the proposed maximum penalties, particularly the 30% of turnover maximum. This potential penalty is incredibly severe for a business that may also be the victim of crime, will drive less reporting and engagement with regulators, and is out of step with the penalty regime in the European Union;
- the introduction of a tiered model of penalties that reflects that privacy breaches, particularly those involving cyber security crime and data theft, run along a spectrum of liability or negligence where the business holding the data may also be a victim of a sophisticated attack;
- the OAIC support the reforms with comprehensive guidance for industry on how it intends to interpret and implement the proposed enhanced penalty provisions and enforcement powers; and
- the Committee signal to Government and regulators that more needs to be done to support Australian businesses in building cyber security resilience and data management practices.

## 2. General comments

AICD members are highly engaged regarding 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 the number one issue keeping directors awake at night in the AICD's biannual Director Sentiment Index (**DSI**).[3]

In addition, the AICD has recently published the Cyber Security Governance Principles (the **AICD CSCRC Principles**) in partnership with the Cyber Security Cooperative Research Centre (**CSCRC**).[4] The Principles are intended to fill an identified gap in practical guidance available to Australian directors of all sizes of

[3] DSI results (October 2022) available here.
[4] AICD CSCRC Cyber Security Governance Principles (October 2022) available here.

organisations to effectively oversee and engage with management on this rapidly evolving risk. Those Principles have also received explicit endorsement from the Minister for Home Affairs and Cyber Security.

In developing the AICD CSCRC Principles, and in engagement on earlier Government reforms, AICD members have consistently expressed concern with the often-uncoordinated Government approach to cyber security regulatory reforms. An example of this is the reporting or notification of cyber incidents and data breaches where, in addition to the Notifiable Data Breaches Scheme (**NDB Scheme**), there are separate Government reporting requirements that differ by industry and whether the organisation is subject to the SOCI Act. Senior directors have provided feedback that the complex and fragmented regulatory landscape, is often a barrier to an organisation effectively responding to significant cyber incidents and ensuring appropriate communication channels exist with government.

The AICD recognises the significant public concern with recent large scale data breaches and the momentum this has provided for regulatory reform. However, we are concerned that the Bill has been introduced to Parliament before the Privacy Act Review has made its recommendations and the Government has responded. Our view is that it would be appropriate to consider stronger penalty provisions and regulator powers in the context of the broader, more holistic changes to the Privacy Act. As discussed below, stronger penalty provisions in isolation will not set the appropriate incentives or provide the regulatory tools to drive improvements in data practices.

Rushing to pass and implement the Bill will exacerbate the existing complexity and piecemeal manner of cyber regulatory reforms and increase the challenges for organisations of all sizes in building cyber resilience and data protection practices.

## 3. Increased penalties

This section responds to section 14 of the Bill concerning increased penalty provisions under section 13G of the Privacy Act.

### Reasonable steps defence or safe harbour

The AICD recognises that the current penalty regime for serious and repeated breaches of the Privacy Act is inadequate given the potential impact on individuals from large scale data breaches. However, the AICD is concerned that the proposed penalty regime may disproportionality penalise a business that experiences a significant data incident despite taking all reasonable steps to protect the data consistent with the Privacy Act, notably Australian Privacy Principle (**APP**) 11 – Security of Personal Information.

The AICD further considers the proposed penalty regime is inconsistent with the Explanatory Memorandum's statement that they are a '*reasonable and proportionate response to the behaviours the penalties are intended to deter and penalise*'.[5] The AICD notes that the Bill was not accompanied by a Regulatory Impact Statement that would assess this claim, assess alternatives, and quantify the likely net benefit of increased penalties.

A number of senior Australian directors have discussed with AICD several significant cyber incidents where customer, employee and supplier data were stolen or accessed. In almost all cases, the business in question had taken what it considered to be reasonable steps to protect this data from misuse, including extensive investment in cyber security processes and infrastructure and meeting relevant industry cyber security obligations. These examples demonstrate that in many instances an organisation

[5] Explanatory Memorandum, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, page 7.

may not have been 'reckless' or 'negligent' in its data controls, but still fallen victim to very sophisticated threat actors that can penetrate the most apparently secure organisations, including Government agencies.

As discussed further below, the core obligations under the Privacy Act are currently principles-based with the threshold for the new penalties to be 'serious or repeated interference' under section 13G. This means that businesses do not have a clear understanding on what actions or failings may result in the OAIC pursuing a civil penalty under section 13G. This context makes it very challenging for businesses to be clear on what steps they should take to meet the core obligations of the Privacy Act.

The AICD recommends the Committee consider whether a defence or 'safe harbour' based around the threshold of reasonable steps is appropriate in the context of the enhanced penalties. APP 11 already has the concept of 'reasonable steps' as central to its obligations. Expanding the concept of reasonable steps to the liability thresholds would appropriately allow for instances where unauthorised disclosures of personal information as a result of criminal activity would not necessarily give rise to a breach of the Privacy Act. It would also reflect that currently the Privacy Act currently does not have a clear link between failing to meet the core obligations and a potential civil penalty.

Importantly such a defence or safe harbour would generate two clear policy benefits:

- incentivise continuing compliance with the NDB Scheme and engagement with the OAIC and other regulators in the event of significant data breaches; and
- strongly incentivise all Australian businesses to build cyber security resilience and improving data management practices in order to meet the reasonable steps defence. The OAIC could support such a defence with comprehensive best practice guidance about what constitutes 'reasonable steps', including expectations for key cyber security standards or frameworks.

A defence or safe harbour of this nature would also signal to businesses of all sizes that the key legislative architecture for protecting the personal information – the Privacy Act – is designed to promote cyber security resilience rather than a narrow focus on solely punitive deterrents.

In addition, the AICD recommends the Committee support clarification of the existing substantive obligations under the Privacy Act, so that organisations are clear on their responsibilities, and therefore when penalties may be applicable to any breach.

**Competition and Consumer Act drafting**

We note the new maximum penalties for major or repeated breaches of the Privacy Act are framed to mirror recent amendments to the *Competition and Consumer Act 2010* (Cth) (**CCA**) in the *Treasury Laws Amendment (More Competition, Better Prices) Bill 2022*.

Whilst the Attorney-General's Department Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers (the **Guide**) notes the consideration of relevant penalty benchmarks for consistency across legislation, the CCA and the Privacy Act vary in purpose, scope and regulatory enforcement activity. Separately, the Guide also notes in the context of penalties based on turnover:

> *A penalty as a percentage of turnover should generally be avoided because of a lack of connection between an organisation's total turnover and the contravening conduct.*[6]

Linking penalty amounts to turnover or 'benefits' may be suitable in the context of a CCA breach where a company, or group of companies, often derive a quantifiable benefit that can be seen in turnover or other financial benefits (e.g. profit margin) from the conduct, such as misuse of market power or cartel behaviour. However, this assessment framework is not appropriate in the context of the Privacy Act.

In many cases the business itself also suffers financial loss and/or reputational impact in the instance of a cyber security crime or data theft. Where a company has misused personal information for gain (e.g. marketing activities not related to the purpose of collection) it would be very challenging to determine a quantifiable benefit. We expect that there would only be very rare instances where there is a clear financial gain from a serious breach of the Privacy Act.

The AICD recommends that this arm of the penalty provisions, sub-section 13G(3), be deleted or amended. In particular, we recommend the removal of the concept of 'benefits' and amendment of the 30% turnover maximum. As discussed below, such a significant turnover linked penalty would be disproportionate to the spectrum of breaches, has the potential to financially cripple many businesses covered by the Privacy Act, and separately will disincentive reporting via the NDB Scheme.

**Turnover maximum**

The AICD is concerned that the proposed penalty regime under the Bill, particularly the turnover linked maximum, is so severe and disproportionate that it will disincentivise businesses from reporting via the NDB Scheme and proactively engaging with the OAIC, and other regulators.

The structure of the penalty regime that enables a maximum penalty of up 30% of adjusted turnover in Australia during the breach period is incredibly severe and has the potential to financially cripple a business. While recent high-profile data incidents have been from large corporations, the Privacy Act applies to many small and medium sized enterprises (**SMEs**) and not-for-profits (**NFPs**) with turnover greater than $3 million. It is difficult to envisage how these smaller organisations would be able to meet the proposed maximum penalties, notwithstanding judicial discretion, and worryingly from a transparency and individual remediation perspective, it may disincentivise reporting to the OAIC via the NDB Scheme. Often a business that has experienced a data breach is also a victim of crime (e.g. ransomware attack) and can face significant financial, operation and reputational impacts as they seek to limit the attack and recover. The proposed penalties under the Bill may give these businesses pause to consider whether they should report via the NDB Scheme and inform impacted individuals.

While the AICD strongly believes that there needs to be appropriate penalties for severe instances of negligence this needs to be balanced by a structure that promotes compliance with the NDB Scheme and cooperation with regulators. The Privacy Act Review cites statistics and research that indicates there may already be a degree of underreporting in Australia compared to similar overseas jurisdictions.[7] It would be a poor public policy outcome if the Bill ultimately led to greater underreporting, less Government visibility of the extent of data breaches in Australia, and ultimately large numbers of individuals who are not aware their data has been lost or stolen (denying them the opportunity to take remedial action).

---

[6] Attorney-General's Department, Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers, 2013, page 41.
[7] Privacy Act Review Discussion Paper, page 199.

Further, AICD's analysis of the tiered penalty framework under the General Data Protection Regulation (**GDPR**) indicates that what is proposed under the Bill is more significant than the maximum penalties under GDPR, particularly the link to 30% of turnover.[8] As discussed below, the AICD recommends that the Bill be amended to adopt a tiered model consistent with the GDPR. However, were the Committee to not pursue a tiered model, then at least close consideration should be given to the reducing the current maximum amounts, particularly the 30% of turnover maximum.

**Tiered penalties**

The AICD recommends the proposed penalty framework under the Bill be tiered to cap maximum penalties in a manner that is proportionate to the seriousness of any breach and the level of negligence. A tiered model would reflect the privacy breaches, particularly those involving cyber-crime and data theft, run along a spectrum of liability or negligence where the business holding the data may also be a victim of a sophisticated attack where its ability to defend or prevent the data breach may be limited. This is particularly the case with very sophistic threat actors, often state sponsored.

A tiered model would enable courts to consider whether an organisation can show they were not negligent or reckless. This could be demonstrated through, for example, early disclosure of breaches, engagement with the OAIC and impacted individuals and compliance with industry cyber security obligations (e.g. SOCI Act) or international standards frameworks.

We note that the OAIC has only once applied for a civil penalty for contraventions of the Privacy Act, a matter which is still before the courts.[9] As currently drafted, the core provisions of Privacy Act, notably the Australian Privacy Principles, are principles-based. This provides businesses with flexibility and discretion with how they meet these obligations however it also results in challenges for the OAIC, and the court, in determining whether a breach has occurred Similarly, the principles-based approach can make it difficult for entities to assess whether they have met their obligations. From a rule of law perspective, it is also important that persons subject to a particular piece of legislation are clear on what conduct is prohibited.

As drafted, section 13G of the Privacy Act, to which the proposed penalties will apply, sets the threshold at 'serious or repeated interference'. The fact that the OAIC has taken very limited public enforcement activity under this provision indicates the threshold may be difficult to prove. Seeking to introduce a tiered model may assist the OAIC in undertaking enforcement activity and be consistent with current settings under the GDPR where there are two tiers of breaches (serious and less severe breaches).[10]

As noted above in the General Comments section, the AICD considers these structural challenges in the current drafting of the Privacy Act, such as the liability provisions, should be addressed after the Privacy Act Review has been completed. Considering proposed amendments in totality will allow stakeholders to comment in an informed manner, including whether changes in liability and penalty provisions will work together to achieve the desired policy outcome.

Pursuing reform of the penalty elements of the Privacy Act in isolation may drive some improvement in data management practices however there will still be challenges in the OAIC undertaking enforcement activity due to construction of the key provisions and, as set out above, will disincentivise businesses from

[8] Serious infringements: Up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. Less severe infringements: up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.
[9] OAIC media release (March 2020), available here.
[10] Detail on the GDPR penalty framework is available here.

reporting and engaging with the OAIC. However, were the Committee to recommend the Bill proceed, the AICD strongly supports a tiered model for the penalty regime.

## 4. Enhanced enforcement and information sharing powers and OAIC guidance

The AICD in-principle supports the proposed enhanced enforcement and information sharing powers. In particular, we support mechanisms to enable information sharing between regulators in a manner that limits or removes the need for a business to report multiple times and engage with different regulators on the same privacy incident or breach. Consistent with our submission to the Privacy Act Review, any increase in regulatory powers should be mirrored through greater resourcing for the OAIC.

While the AICD supports greater powers for the OAIC connected to the Privacy Act, we encourage the Committee to consider whether a review of existing overlapping data and cyber security investigation and enforcement powers needs to be undertaken. The AICD understands that depending on the entity, and the nature of the breach, that investigation and enforcement action could be undertaken by the OAIC, Australian Competition and Consumer Commission, Australian Communications and Media Authority, Australian Securities and Investments Commission or the Department of Home Affairs. This environment presents significant complexity for a business experiencing a data or cyber incident, including which agencies it should coordinate with, and distracts from the key tasks of recovering from the incident and notifying and remediating impacted individuals.

Lastly, we strongly recommend that the OAIC support these reforms with comprehensive guidance for industry on how it intends to interpret and implement the proposed enhanced penalty provisions and enforcement powers. Imposing increased penalties without appropriate education, guidance, and assistance for business is likely to impact awareness and ultimately compliance, especially with SMEs and NFPs. In respect of enforcement activity, we would expect to see detail on how the OAIC will assess breaches, including consideration of mitigating factors. We note that the European Union has guidance in respect of the GDPR on how to assess penalties for data breaches which outlines 10 criteria, including gravity and nature of the breach, precautionary measures, and history of previous infringements.[11]

## 5. Greater guidance and support for business

The Bill focuses on strengthening the 'stick' or deterrent elements of the Privacy Act. What is absent from these reforms are measures to support Australian businesses in building cyber security resilience and data management practices. As discussed above, a legislative component that we recommend be considered as a part of this Bill is a form of defence or safe harbour under the Privacy Act.

While outside the strict scope of this Bill, the AICD also encourages the Committee to consider signalling to Government and regulators an expectation that more needs be done to provide support to Australian businesses to manage their privacy obligations effectively. We recommend the Committee note the following areas where greater guidance and support would be welcomed by businesses of all sizes:

- greater coordination across relevant agencies on future cyber security reforms, including aligning the Privacy Act Review outcomes with other future regulatory proposals, such as the changes to the Cyber Security Strategy 2020;

[11] Detail on the 10 criteria to determine a GDPR fine is available here.

- clarity on regulator responsibilities when undertaking investigations and enforcement activity on cyber security and data breaches;
- consideration of how existing reporting and notification obligations can be harmonised or streamlined with the goal that a business only needs to report or notify to the Government once;
- targeted support for SMEs and NFPs to build cyber security resilience and improve data management practices, including that support would entail education, training and assistance in the event of experiencing a cyber security incident;
- addressing urgent skills shortages in technology and cyber security specialties, including support via Australia's immigration programs; and
- proactive threat and intelligence sharing by key Government agencies (e.g. Australian Cyber Security Centre, OAIC) with industry.

## 6. Next Steps

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

Yours sincerely,

**Christian Gergis GAICD**

Head of Policy, Governance & Policy Leadership