Australian Institute of Company Directors

Level 12, Tower 3, Darling Park,
201 Sussex Street,
Sydney NSW 2000

1300 739 119
contact@aicd.com.au
aicd.com.au

ABN 11 008 484 197

18 September 2026

Attorney General's Department

Via online form

Dear Attorney General's Department (the Department)

Privacy Reform – Consultation on Exposure Draft legislation

Thank you for the opportunity to provide a submission to the consultation paper and accompanying exposure draft *Privacy Amendment (Personal Data Protection) Bill 2026* (**Exposure Draft**) that would amend the *Privacy Act 1988* (**Privacy Act**).

The Australian Institute of Company Directors' (**AICD**) mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. The AICD's membership of more than 54,000 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.

The AICD has in recent years engaged extensively on proposed privacy and cyber security reforms as part of the Privacy Act Review, *Australia's 2023-2030 Cyber Security Strategy*, amendments to the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) and the *Privacy and Other Legislation Amendment Bill 2024*.

We have also supported directors to improve their knowledge of cyber security and data governance best practice through extensive guidance materials, including the *Cyber Security Governance Principles*, *Data Governance Foundations for Boards* and joint publications with the Australian Signals Directorate (**ASD**), including a 2026 resource on board oversight of frontier artificial intelligence (**AI**) threats.

Summary submission

*[This summary meets the request for 1,000 word submissions. **Attachment A** provides further detail on the key positions]*

The AICD supports reforms that would modernise the Privacy Act to ensure it reflects a digital economy where individuals and organisations are engaging, and providing personal information, in digital spaces and environments. We do not consider that the Exposure Draft proposals meet these objectives.

The AICD remains concerned[1] that there is no clear policy or public benefit case made for many of the reforms proposed. The benefits of many of the reforms, or the harm they are seeking to address, has not been demonstrated.

The proposed reforms will also impose very significant compliance costs on entities at a time of weak economic growth and stagnant productivity, which has been linked in part to federal regulatory accumulation.[2] The benefits of many of reforms, or the harm they are seeking to address, has not been demonstrated.

---

[1] AICD submission, Privacy Act Review Final Report, November 2023, available here.

[2] AICD Mandala Partners, $160 billion and counting: The cost of Commonwealth regulatory complexity, November 2025, available here.

We are disappointed that the Productivity Commission's 2025 recommendation for a outcomes-based privacy duty that would in time replace the Australian Privacy Principles (**APPs**) has not been progressed.[3] A duty of this nature would provide a flexible legislative framework that is better equipped to address rapid advances in how personal information is provided, collected, used and protected in digital environments. It would also avoid the complexity, prescription and high risk of unintended consequences that are present in the Exposure Draft.

The AICD recommends **that the Department pause progression** of the Exposure Draft and undertake further consultation before introducing legislation to Parliament. As highlighted in our submission, there are complex proposals in the Exposure Draft that will present significant uncertainty and compliance complexity for entities. The exceptionally short period to comment on the Exposure Draft does not allow for genuine consultation and creates a real risk that the Bill that is introduced into Parliament will be highly challenging for entities to implement.

Our other key points are:

- **Definitions**: The expanded definitions of personal information and consent will have significant operational implications. If advanced, a minimum 24-month implementation period supported by detailed Office of the Australian Information Commissioner (**OAIC**) guidance is required.

- **Fair and reasonable test**: While an outcomes-based approach is supported in principle, the proposed fair and reasonable test risks creating uncertainty, duplication and inconsistent compliance obligations and will be very challenging to implement.

- **Direct marketing and trading of information**: Direct marketing can deliver benefits to individuals and the broader economy including promoting competition, better tailored consumer offers and innovation. There is a risk that the proposals, in conjunction with other new obligations, will create substantial compliance costs and uncertainty, particularly for online advertising, acquisitions and intra-group information sharing.

- **Data security**: Reforms to the Notifiable Data Breaches scheme (**NDB scheme**) should avoid adding unnecessary complexity to cyber incident reporting and provide entities with greater flexibility when notifying regulators and affected individuals.

- **Right to erasure on large digital platforms:** The narrowed right to erasure is preferable to a whole-of-economy approach, but further refinement is needed to ensure it does not inadvertently capture entities beyond the intended scope.

- **Commencement, guidance and a statutory review**: The reforms should be supported by a minimum 24-month commencement period, comprehensive OAIC guidance, and a statutory review three years after commencement.

We hope our submission will be of assistance.

If you would like to discuss any aspects of our submission further, please contact Simon Mitchell, Acting Head of Policy (smitchell@aicd.com.au) or Laura Bacon, Senior Policy Adviser (lbacon@aicd.com.au).

Yours sincerely,

Louise Petschler GAICD
GM, Education and Policy Leadership

[3] Productivity Commission, *Harnessing data and digital technology Inquiry report*, December 2025, available here.

Attachment A – Detailed submission

1. Policy development process and the case for a 'pause'

The AICD is deeply concerned with the policy process that has been undertaken by the Department. A two-and-a-half-week consultation is insufficient to comment on over 40 distinct proposals and draft legislation that would fundamentally transform the Privacy Act. Privacy law is complex and interacts with other state and federal legislation (e.g. *Spam Act 2003*). It is challenging for industry to assess the operational and governance implications of wide-ranging reforms in such a short period of time. It also creates a real risk that the legislation introduced into Parliament will be poorly drafted, contain inconsistencies and will be incoherent.

The Department's request for '1,000 word' submissions in the context of over 50 pages of draft legislation creates the impression that the consultation is not a genuine process seeking to improve the proposals or support effective and efficient implementation.

While the Privacy Act Review was the subject of multiple rounds of consultation, industry has not previously seen the proposed drafting. Critically a number of the key proposals are materially different to those previously canvassed under the Privacy Act Review.

This approach to consultation is inconsistent with the Office of Impact Analysis guidance that commits policy makers to consulting 'in a genuine and timely way' with impacted businesses and community organisations, and points to a minimum consultation period of 30–60 days on significant reforms.[4]

a) Interaction with other reforms

The proposed reforms are not occurring in isolation. Entities and industry stakeholders are trying to understand the connections and implications of a number of significant changes relevant to the Privacy Act, including:

- Implementing the new automated decision-making (**ADM**) transparency requirements by November in the absence of OAIC guidance;
- Responding to the OAIC's development of a Children's Privacy Code; and
- The Government's proposed Digital Duty of Care within the *Online Safety Act 2021*.

Stakeholders have been consistent in our engagement that given the short timeframe to comment it is exceptionally difficult to view these different strands in totality and identify where there are inconsistencies, duplication or new forms of uncertainty and ambiguity.

It is also important to consider the broader sphere of digital governance that boards and their organisations are currently grappling with how to respond to rapid advances in frontier AI models. Significant focus and resources are being dedicated to building cyber controls to account for the capability of these models, including strengthening the defence of personal information, and support for cross-sector and industry collaboration is required.

b) Pause progression of the Exposure Draft

The AICD recommends that the Department **pause progression** of the Exposure Draft and undertake further targeted consultation with business, community organisations and privacy experts before introducing legislation to Parliament.

The scale and complexity of the reforms, combined with implementation of other major digital, cyber security and data governance initiatives, warrants a more measured approach. This period should be used to directly engage with key stakeholders to resolve complexity and potential unintended consequences with the Exposure Draft.

[4] The Office of Impact Analysis, Best practice consultation, May 2023, available here.

This will enable direct consultation on the drafting of the Explanatory Memorandum, which will be a key source of guidance on how the reforms will be implemented and regulated by the OAIC.

AICD members have significant concerns with the trend of the Government continuing to add new forms of costly and disproportionate regulation on all Australian organisations. AICD research undertaken in 2025 highlighted how the weight of federal regulation is a key contributing factor in Australia's poor productivity and growth performance.[5] We urge the Department to consider this dynamic as it makes decisions on how quickly to progress the Exposure Draft and assess the appropriate implementation timelines.

c) Impact analysis

We note that the Department has yet to publish regulatory cost impact information and analysis that we understand was undertaken on the Privacy Act Review proposals in 2024 and 2025. Given the significant operational costs that will eventuate from the proposed legislation it is troubling that there is no assessment of the cost/benefit trade off and productivity implications.

Significant new legislation introduced by the Government should be subject to a transparent view on the likely benefits and costs of new regulatory requirements. The lack of reliable impact analysis deprives stakeholders of a balanced debate on the merits of new regulation, and the trade-offs that may come from greater compliance costs.

We strongly recommend that a comprehensive impact analysis covering all 41 proposals is published prior to the introduction of the legislation to Parliament. We expect that such an impact analysis would be rigorous and verifiable, including that cost estimates are based on genuine data collected from entities.

2. Definitions

This section responds to Schedule 1 of the Exposure Draft.

We in-principle support amending the definitions of 'personal information' and 'consent' to reflect how individuals provide different forms of information in digital environments and separately to allow for a more robust understanding of consent consistent with community expectations.

The proposed changes are very significant and will vastly expand the scope of data and information that is captured under the Privacy Act. Our interpretation from the Exposure Draft and consultation paper is that fragmentary and time limited pieces of digital data, such as pixel or cookie data, that in isolation cannot be used to identify an individual, may be now captured. This change will cascade through an entity's privacy compliance controls and data storage practices and have very material consequences for how entities meet other Privacy Act obligations, including consent and transparency.

The impact of the changes in definitions should not be underestimated. We expect the costs of making these system changes and how definitional changes then cascade through other Privacy Act requirements will be significant. As detailed below, we strongly recommend that a commencement period **of at least 24 months from Royal Assent** is provided to allow sufficient time for entities to make the necessary process and system adjustments.

An appropriate implementation timeline must be supported by comprehensive guidance from the OAIC. As an example, the inclusion of 'geolocation data' in the definition of personal information is proposed. Directors and industry stakeholders have raised with the AICD the complexity and uncertainty of the Privacy Act now applying to common geolocation and telematic data. We understand that it is common for businesses in transport and logistic industries to use fleet monitoring software as a key workplace health and safety control and it is unclear if this use would be caught under the employee records exemption. How geolocation data is treated will become increasingly important as smart vehicles are connected to digital systems, such as autonomous driving software.

[5] AICD Mandala Partners, *$160 billion and counting: The cost of Commonwealth regulatory complexity,* November 2025, available here.

This one example demonstrates that passage of this legislation cannot occur in a vacuum of guidance from the OAIC. All entities will need guidance well in advance of a start date to effectively and efficiently meet the requirements from day one.

3. Fair and reasonable test

This section responds to Schedule 2, Part 1 of the Exposure Draft.

In isolation we consider that a 'fair and reasonable' test represents a welcome shift towards an outcomes-based approach to privacy regulation in Australia. However, as currently drafted the new test in APP 3 will only add to the complexity, uncertainty and ambiguity that entities will face when complying with Privacy Act requirements. We remain of the view that the Productivity Commission's proposal for an overarching outcomes-based test that would replace the APP framework is far more appropriate than the new test that will sit alongside other obligations that are duplicative (e.g. consent).

As proposed, the new test will be challenging to implement given the significant subjectivity inherent in the key factors listed in subsection 3.2 and exceptions in subsection 3.3. By way of example, it is unclear how an entity will balance or reconcile considering whether the individual has 'genuine choice' with the new definition of consent being 'voluntary, informed, current'. Further, the test has a principle of data minimisation contained within it despite the enhanced consent and collection of information requirements. This may result in a perverse outcome of an entity meeting key arms of the Privacy Act on consent, collection and protection and then being found to breach the new test in APP 3.

Separately, key stakeholders have raised with us uncertainty about how the exceptions under subsection 3.3 will work in practice. This uncertainty is particularly focused on 'permitted general situations'. For example, it is unclear whether personal information collected by financial institutions and used to identify fraud threats or potential financial abuse will be considered under this exception. The test is drafted in a manner that is orientated towards the interests of the individual to the exclusion of how an entity may lawfully use information to support broader business operations and have product features/services that benefit an individual. It is key that the OAIC reflects this dynamic in how it regulates this test and develops guidance.

If the Government does not accept the strong advice of the AICD and other stakeholders to amend the Exposure Draft, the AICD recommends additional action. As a minimum, the OAIC will need to develop comprehensive guidance, informed by consultation, to support implementation. This guidance must in place well in advance of commencement. It will be extremely challenging for entities to implement the new test and reconcile it with other existing and new obligations in the Privacy Act.

4. Direct marketing and trading of information

This section responds to Schedule 2, Part 3 of the Exposure Draft.

a) Direct marketing

The AICD supports the objective of improving transparency and individual control over direct marketing practices, particularly in digital environments where consumers may be unaware of how their personal information is used for targeted advertising. However, the AICD also notes that direct marketing delivers benefits to consumers and the broader economy by enabling individuals to receive information about products, services and opportunities that are relevant to their interests and circumstances. For many businesses, particularly small and medium-sized enterprises, direct marketing is an important means of reaching customers, competing with larger incumbents and promoting innovation.

We are concerned that the cumulative impact of the proposed direct marketing reforms, when combined with the expanded definition of personal information, strengthened consent requirements, the concept of individuation and the new fair and reasonable test, will create considerable regulatory uncertainty and significant compliance costs. The introduction of new concepts such as 'genuine choice' may have unintended consequences for digital advertising models and customer engagement practices. There is a risk that consumers will be swamped by

consent notices that only serve to frustrate and create significant friction in navigating the internet and digital environments. Restricting access to tailored offers that better meet the needs of consumers (including in comparison to current products or services from their existing suppliers) would not be a net public benefit.

Greater clarity and guidance is required on the practical operation of the proposed direct marketing provisions, particularly in relation to ad-supported services and online advertising. Businesses will need to review consent mechanisms, customer communications, digital advertising practices and online interfaces to comply. In light of these significant operational impacts, comprehensive and practical guidance through the OAIC will be critical.

b) Trading of information – Intra-group arrangements and acquisitions

There is significant ambiguity in how the proposed prohibition on the trading of personal information will work with common business transactions, including acquisitions.

The exception in section 6FC on the meaning of 'trade' implies that consent will not be required from customers when there is an acquisition of a business and that customer information is 'incidental' or not the 'substantial purpose' of the purpose. In many acquisitions the customer base and the corresponding customer information can be a core intangible asset that is central to the acquisition. This dynamic is not just linked to digital businesses or platforms but many service businesses where the acquirer is seeking to reach a new or expanded customer base

We strongly recommend clarity on the operation of this provision, including how it applies to the movement of personal information between related companies within a group structure. As currently drafted, a narrow or conservative reading could be that consent may be required from customers as a component of a standard business acquisition process.

5. Data security

This section responds to Schedule 3 of the Exposure Draft.

a) NDB scheme changes

We in-principle support the modernisation of the NDB scheme contemplated under the Exposure Draft. However, we do have concerns that elements of the amendments are overly prescriptive and will impose an unreasonably high burden on entities as they respond to complex cyber and data incidents with often incomplete information.

We recognise that the proposed 72-hour window is consistent with similar timeframes under the *Security of Critical Infrastructure Act 2018* and the *Cyber Security Act 2024*.

The AICD has a long-standing position that there must be a concerted effort by government and regulators to harmonise, where possible, existing data and cyber security and reporting notifications. AICD members have consistently raised concerns with the complexity of existing notification obligations. This complexity produces significant compliance costs and creates challenges when responding to a cyber-attack or data breach. In this context we strongly supported Proposal 28.1 under the Privacy Act Review to address this issue, which was subsequently supported by the Government and has separately been listed as a priority under the *2023-30 Australian Cyber Security Strategy*.

Directors are frustrated that despite these commitments there has been no progress made to address this issue. While the portal on cyber.gov.au is an important step in providing visibility to businesses in meeting multiple reporting obligations, it does not address the underlying issue that a business in many cases has to report the same incident to multiple regulators via multiple different mechanisms.

The AICD is concerned that the changes in timeframes and notification requirements under the NDB scheme will only exacerbate existing complexity in how any entity reports a cyber and data incident. By way of an example, an insurer that experiences a cyber and resulting data breach incident will have to make separate reports to the ASD/Home Affairs under SOCI Act obligations, the OAIC, APRA and various state-based insurance regulators. At the same time, of course, entities will be focused on protecting consumer interests and effective consumer communication, market disclosures and substantive cyber responses. Overlapping and complex regulatory

notification obligations divert resources and management and board attention from responding to an incident to the ultimate detriment of impacted individuals and the organisation.

We recommend that in developing guidance to support this change that the OAIC work with other regulators on how advice to industry and reporting portals can be designed to minimise inconsistency and duplication across the suite of federal cyber and data incident reporting requirements.

Incomplete statements and notifying individuals

We do not support the obligation on an entity to still provide an incomplete statement on a potential eligible data breach, even though it does not have full visibility of the incident and its impact (i.e. it is not entirely clear what has occurred and whether an eligible data breach has occurred).

This requirement is overly prescriptive and contorted and puts entities in a highly difficult situation where it is still required to notify – even if the nature and severity of the incident is unclear, and information is changing rapidly.

Compounding this concern is that requirement to notify impacted individuals at the same time as the OAIC, including where there is incomplete information, and then to subsequently notify impacted individuals at every material notice provided to the OAIC. These provisions do not reflect the realities of data breaches, where critical facts are complex, unclear and evolving rapidly in the days and weeks following an incident. The 'facts' of the incident can change as the technical investigation is undertaken making the likelihood of an entity making multiple notices to the OAIC, and by extension to individuals, particularly high.

Our strong view is that the drafting of sections 26WK - 26WL should provide greater discretion to an entity to appropriately manage how it notifies impacted individuals. This discretion could be framed within an overriding principle that informing individuals must occur within a reasonable period once a full statement has been made and the entity has confidence on the nature and impact of the incident. As drafted, there is a real risk that individuals will be inundated with unhelpful, technical notifications in a way that may create unnecessary anxiety and fear.

As above, we consider the focus in the immediate period following a significant cyber and data incident should be triaging the incident, obtaining necessary support and establishing the nature and impact of the incident, including the degree to which personal information has been compromised or lost[6]. This should be supported by coordination amongst regulators of notifications, with the aim of supporting an effective, timely response and focus.

Implementation

We expect that this new set of requirements will have significant awareness raising challenges across the entity population.

It is difficult to understand from current OAIC published data the degree to which small and medium sized entities make notifications under existing NDB scheme settings. Our view is that to the extent there is currently material inadvertent non-compliance amongst smaller entities with NDB scheme requirements this will only increase with the proposed reforms. For instance, for entities with limited resources and employees there will be threshold challenges in communicating the distinction between a 'data breach' and 'eligible data breach' and the fact both are required to be reported.

We strongly support that reforms to the NDB scheme are coordinated with the work of Home Affairs on Horizon 2 of the Cyber Strategy. Given the interdependencies between cyber security resilience and strong data controls we encourage the OAIC to utilise the CyberSmart initiative to raise awareness of the proposed reforms, including where an entity can gain assistance in the event of a data breach.

We also strongly support the OAIC taking a facilitative approach to regulating the changes to the NDB scheme and provide latitude for inadvertent non-compliance.

---

[6] See AICD resources including *Governing Through a Cyber Crisis* and *Cyber Security Governance Principles* for principles and guidance provided to support Australian boards and directors.

A regulatory and enforcement approach that focuses on imposing penalties for non-compliance may ultimately disincentivise entities from reporting under the scheme to the detriment of impacted individuals and visibility of the extent of data breaches across the Australian economy.

b) Security and destruction of personal information

We support the amendments to APP 11 to require entities to consider whether to destroy personal information it holds and to regularly assess its security and destruction practices. This is consistent with mature data governance practices. AICD guidance to Australian directors and boards promotes a focus by the board on overseeing how an organisation is identifying and retiring or destroying legacy systems and data[7].

We recommend the OAIC provide specific guidance on 'regularly evaluate', including expectations for frequency of any evaluation and how this should be aligned. We also recommend that the guidance developed on APP 11 is harmonised and is consistent with broader cyber security and data protection guidance that has been developed by other arms of government, including the ASD and the Department of Home Affairs. Notably, the development of a CyberSmart Hub for SME and NFP guidance represents an opportunity for key material from regulators across the federal government to be located and updated in one location.

6. Right to erasure on large digital platforms

This section responds to Schedule 4, Part 2 of the Exposure Draft.

We welcome that the proposed right of erasure has been modified from the proposal under the Privacy Act Review that would have applied to all entities. As highlighted by the Productivity Commission there was not a strong policy case for this change applying to all entities. Given this, it is appropriate that is reform is restricted to a particular set of entities with the resources and technical capacity to meet requests. It is also consistent with the concern some members of the community have with how personal information is utilised by large digital platforms.

Industry stakeholders have shared with us concerns that the obligation will potentially apply to a far broader range of entities than is implied by the consultation paper or the common use understanding of 'large digital platforms'. For example, it has been shared with us that large retailers and financial entities, such as banks, may be caught under the obligations through the definition of designated internet service as defined in the *Online Safety Act 2021*.

From engagement with the Department and our reading of the consultation paper we understand that it is not the intent of the proposal to capture these types of entities. This isolated issue within the current drafting is indicative of the broader issue that the Exposure Draft contains significant complexity and the potential for unintended consequences and industry has not had sufficient time to consider the implications of the proposals. As detailed above we strongly recommend that more time is taken to directly consult with key stakeholders. A 'pause' will allow a more thorough consideration of the drafting that will ultimately benefit the Bill that is introduced to Parliament.

7. Commencement, guidance and a statutory review

a) Commencement

We recommend that at a minimum there is a **24-month commencement period** from Royal Assent. This period is consistent with the ADM reforms and will provide a bare minimum of time for entities to undertake the significant exercise of updating processes, policies and investing in expertise and system design changes necessary to give effect to the changes. As stressed above,

24 months provides the OAIC with sufficient time to develop the guidance necessary to support implementation in a manner that is consistent across entities and supports the objectives of the reforms. Following passage of the legislation we recommend that the OAIC and Department release a regulatory roadmap that details the sequencing by which it proposes to support implementation, including developing the necessary guidance. A roadmap will provide a degree of certainty to industry and allow for the planning of system and process changes.

[7] See, for example, AICD resource Data Governance Foundations for Boards

We urge the Department to consider how commencement of the reforms could be amended or delayed if the necessary guidance is not finalised with a sufficient buffer prior to commencement.

We understand that a one-year period is being contemplated by the Department. Such a short duration would not only be inappropriate from an entity burden perspective but also run the real risk that the reforms would start with significant inadvertent non-compliance and uncertainty about interpretation of the requirements. We are also highly sceptical that the OAIC has the capacity to develop and consult on the necessary guidance in such a short timeframe.

b) Critical importance of guidance

As noted at various points in this submission the development of OAIC guidance will be fundamental to implementation of the reforms.

Industry stakeholders have shared significant concerns with the development of guidance to support ADM commencement. Guidance on ADM is still not finalised despite the obligations commencing in November of this year. The OAIC has had a two-year period to develop this guidance. The result is that entities and advisors are still unsure on critical issues and how to update key policies and processes. This example raises legitimate concerns about the capability of the OAIC to genuinely support these significant reforms.

An approach that may assist the OAIC meet the extensive expectations for guidance on these reforms is a genuine industry codesign process. Working with industry and drawing on the talent and expertise within entities may be a method by which the development of guidance can be expedited.

We also recommend consideration by Government of how the OAIC can be provided with appropriate resources to support implementation.

c) Statutory review

We recommend the legislation introduced to Parliament contains provisions for a **three-year statutory review** from the date of commencement. A statutory review is critical feature of significant legislation and allows a comprehensive assessment of whether the reform is achieving its intended objectives, whether there are unintended consequences and opportunities for improvement.

Given the complexity of Exposure Draft and the real risk of significant compliance costs and unintended consequences a statutory review should be a component of the Bill that is introduced to Parliament.