Australian Institute of Company Directors

Level 5
No.1 Martin Place
Sydney NSW 2000

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

ABN 11 008 484 197

12 October 2026

Australian Securities and Investments Commission

Via email: consultation.registrydata@asic.gov.au

Dear Australian Securities and Investments Commission (**ASIC**)

Access to information on the companies register

Thank you for the opportunity to comment on the *Access to information on the companies register* Consultation Paper 391 (**Consultation Paper**).

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 includes directors and governance leaders across publicly listed entities, not-for-profits (**NFPs**), large and small businesses, and public sector bodies.

The AICD has engaged extensively over many years on the Government's Modernising Business Registers (**MBR**) program of work. We strongly supported the introduction of director identification numbers (**director IDs**) to help combat illegal phoenix activity and strengthen the integrity of registry information.

As a long-standing member of the MBR Business Advisory Group, the AICD advised on the design and implementation of the director ID regime and supported the onboarding of directors across Australia via a significant awareness raising campaign across our membership. More recently, the AICD is a member of ASIC's Registry Business Advisory Group (**RBAG**), advising on the stabilisation and uplift of ASIC's registers.

The AICD stands ready to assist ASIC in the implementation of the director ID linkage process to the companies register, recognising the significant communication and director awareness challenge ahead. Sustained engagement and targeted guidance will be critical to ensuring directors across all sectors understand the practical steps required to meet their obligations.

1. Executive Summary

The AICD supports linking director IDs to the companies register. This step is key to achieving the policy aims of the director ID regime and strengthening the integrity and utility of information on the companies register.

Critically, it also provides the opportunity to resolve the significant privacy and safety risks of director personal information being publicly available on the companies register. Reflecting the strong concerns of AICD members, we have long advocated for the removal of sensitive personal information of officeholders, including residential addresses and dates of birth, from public searches of the companies register.

The AICD has significant concerns with ASIC's proposal in the Consultation Paper to enable directors' residential addresses to be publicly available on the companies register where an alternative service

address is not provided. This proposal is inconsistent with the broader direction of Australian privacy law reforms and significant community concern with how personal information is collected, used, protected and disclosed.

The proposal would also be a regressive step from ASIC's decision in early 2026 to suppress directors' residential address information from company extracts available to the general public in response to heightened national security concerns. The AICD welcomed this decision and consider it an important and sensible precedent for the future registry reforms. The change and current operation of the register demonstrates that it can be effectively maintained and accessed by legitimate users for business and regulatory compliance purposes, while providing stronger privacy and safety protections for more than 3 million company directors in Australia.

Directors face significant privacy, cyber and personal safety risks arising from the public availability of personal information. These risks are not confined to large listed entities or high-profile directors. They extend across the director community, including directors of small and family-owned businesses, community and NFP organisations. Importantly, the impacts of publicly disclosing a residential address go beyond directors themselves, exposing their families to the same privacy and safety risks. We encourage engagement with the Department of Home Affairs and security agencies on the personal and national security considerations relevant to making officeholders' residential address information broadly available to the public, under any access model.

There is no legitimate public interest in continuing public access to directors' residential address information. Authenticated company, business (including media) and government users with legitimate needs will continue to have access to this information under the proposed tiered access settings.

Our submission focuses on ASIC's proposed approach to directors' personal information, with the following key points:

Tiered access

- The AICD strongly supports ASIC's proposed tiered access model. We consider it is appropriate that users of the companies register with legitimate administrative, business, professional (including journalistic) or regulatory purposes for accessing officeholder personal information continue to be given full access to this information.

- To the extent there are concerns that certain user groups are not currently contemplated within the proposed user categories, we would not be opposed to the expansion of these categories provided there is a legitimate use case for access and users are subject to appropriate verification by ASIC. We recommend ASIC develop and publish criteria for how it will verify users as well as conditions of access, including non-disclosure of personal information, to provide confidence in the rigour of the tiered access framework.

Residential addresses

- The AICD does not support ASIC's proposal for directors' residential addresses to be publicly available on the companies register where an alternative service address is not provided. Residential addresses should continue to be removed from public availability on a permanent basis.

- The linkage of director IDs to the companies register and their proposed public disclosure will mean that directors' residential addresses are no longer required as identifying information for the general public. The director ID number itself should provide sufficient confidence that an individual has been appropriately identified and verified by ASIC.

Service address

- The AICD recommends that a company's registered office be disclosed as the publicly available service address by default, unless a director elects to provide an alternative service address. This would ensure ongoing protection and mitigate the risk of directors not taking the step of nominating a service address, recognising the significant awareness raising challenge for over 3 million Australian directors - including directors of small family-owned businesses, community organisations and NFPs.

Date of birth information

- The AICD strongly supports ASIC's proposal to restrict public access to directors' full dates of birth and instead provide access to a year of birth only. Full dates of birth are sensitive personal information and public disclosure, both on their own and together with residential address information, creates unnecessary and elevated privacy, fraud and cyber security risks. The removal of full dates of birth from the public-facing companies register is consistent with international practice and will no longer be required as a key identifier following the linkage of director IDs to the companies register.

Director ID numbers:

- The AICD supports the publication of director IDs, *provided residential address information is not made publicly available*. Director IDs are key to improving the integrity and reliability of Australia's companies register and provide a more targeted mechanism for identifying directors than reliance on residential addresses or full dates of birth.

- However, if ASIC proceeds with allowing residential addresses to become publicly available by default where a service address is not provided, the AICD would not support the public disclosure of the full director ID. In these circumstances, we recommend that director IDs be only partially disclosed for general public users – for example, where the first six digits are displayed and the last six digits are de-identified.

- We do not consider that the partial display of the director ID would undermine the objects of the regime. General public users would still have confidence that a director's identity has been verified by ASIC, while authenticated users would still have access to the director ID number in full under the proposed tiered access settings along with other director personal information.

2. Next Steps

We hope our submission will be of assistance. If you would like to discuss any aspects further, please contact Laura Bacon, Senior Policy Adviser, at lbacon@aicd.com.au.

Yours sincerely,



Simon Mitchell GAICD
Acting Head of Policy

Australian Institute of Company Directors

Level 5
No.1 Martin Place
Sydney NSW 2000

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

ABN 11 008 484 197

Attachment A – Detailed submission

3. Inconsistency of ASIC proposals with privacy reforms

The Government has been consulting on a very significant package of reforms to the *Privacy Act 1988* (**Privacy Act**).[1] This follows significant new protections in the first tranche of reforms legislation in 2024, including a statutory tort for privacy. This multi-year effort to modernise the Privacy Act is based on the recommendations of the Privacy Act Review.[2]

The privacy reforms are focused on strengthening individuals' control over their personal information, including through stronger consent requirements, expanded individual rights, greater transparency and protections against unfair or unreasonable collection, use and disclosure of personal data. They also seek to reduce the risk of harm from the misuse or loss of personal information, through stronger security and data-breach obligations and protections designed for emerging digital technologies, including AI. The foundation of these reforms reflects significant community unease and concern with how personal information is collected, used and protected in digital environments or spheres. Members of the Australian community see this in the proliferation of scam and fraud activity that results from the loss of personal information in data breaches. The privacy risks are clearly magnified with the capability of agentic AI models to potentially harvest and assess vast amounts of data, including from secure environments.

The Government through its privacy changes is responding to a community expectation that personal information should only be collected and disclosed where there is a clear and justified need, and that individuals should be robustly protected from unnecessary privacy and security risks.

Against this backdrop, the AICD is very concerned that ASIC's proposal to maintain public access to directors' residential address where an alternative service address is not provided is inconsistent with the direction of Government privacy policy and most importantly community expectations for the protection of personal information.

As noted in Professor Pamela Hanrahan's advice for the AICD in respect of the *Treasury Laws Amendment (Business Registries Stabilisation and Uplift) Bill 2026*:[3]

> *"Protecting an individual's personal information from public dissemination is recognised as key to combatting real – and growing – physical and cyber safety and security risks in the community."*(page 1)

> *"Personal information is defined in s 6 of the Privacy Act 1988 (Cth); OAIC unequivocally treats a person's home address, email address, telephone number, and date of birth as personal information."*(page 2)

The potential continued public availability of residential address information exposes directors to risks including identity theft, fraud, harassment and threats to personal safety. In addition to being inconsistent with the direction of Privacy Act reform, it is troubling that ASIC's proposed approach to disclosing personal information is not grounded in a 'privacy by design' principle. Privacy by design is advocated

[1] Attorney-General's Department, Privacy Act Review Report 2022, available here.
[2] Government response to the Privacy Act Review Report, September 2023, available here.
[3] Professor Hanrahan advice for the AICD, June 2026, available here.

for by the Office of the Australian Information Commissioner (**OAIC**) as it is more 'effective and efficient to manage privacy risks proactively, rather than to retrospectively alter a product or service to address privacy issues that come to light'.[4]

It is difficult to reconcile the broad direction of privacy reform that will strengthen individual privacy protections across the economy while retaining public access to personal residential address information for potentially more than 3 million directors. In the AICD's view, the policy settings governing access to companies register information should reflect the same modern privacy principles that apply to the collection, use and disclosure of personal information under the Privacy Act.

The AICD strongly encourages ASIC to ensure that future access settings for the companies register are aligned with contemporary privacy expectations and appropriately balance public interest considerations against the legitimate privacy and security interests of directors.

4. Tiered access

The AICD strongly supports ASIC's proposed tiered access model. This includes different layers of access for different user groups across four main categories: general, company, business and government.

A tiered access model has long been contemplated as part of the future state of the companies register, including through the Australian Business Registry Services' (**ABRS**) MBR program. We welcome ASIC's efforts to build on and progress this design as part of the registry uplift program.

The AICD supports ASIC's proposed user groups and verification process for company, business and government users. This will help ensure that those being given access to personal officeholder information have legitimate administrative, business, professional or regulatory need for that information.

We recommend that ASIC detail criteria for how it will 'verify' a user in the specific groups, including the information that the prospective user will be required to provide and steps ASIC will take to validate this information. We would be concerned if meeting a particular business use case category was based on subjective or broad criteria and contained an element of self-attestation. By way of example, we consider ASIC's current definition of a 'journalist' for the purposes of determining access to the companies register is appropriate.[5]

As noted by Professor Hanrahan's advice:[6]

> *"The categories of authenticated persons should, in my view, be restricted to specified occupations that are subject to licensing or other regulatory oversight and that have a legitimate need to access an individual's personal information in performing their functions."*

We consider that users within the tiered access framework should be subject to conditions of access. That is, ASIC should only grant access to sensitive personal information to users on the condition that the information is used for a proper purpose, is not misused and cannot be published or disclosed. For example, while journalists investigating public interest stories will have access to directors' residential address information, we consider that conditions should apply such as not publishing the home address or identifying imagery. This would provide an appropriate safeguard to protect the privacy of directors

[4] OAIC, Privacy by design guidance, available here.
[5] ASIC, Journalist access to ASIC business register.
[6] Professor Hanrahan advice for the AICD, June 2026, available here.

and their families, given the personal safety risks that may arise from the publication or broadcasting of this information.

ASIC should also have a process by which verified users are periodically reviewed with accompanying administrative steps where a user is removed from the tiered access if they no longer meet the criteria.

The AICD understands that there may be use cases for access to certain director personal information (for example, residential address or date of birth) by additional user groups within these categories. For clarity, we do not object to the expansion of the 'business' user category to accommodate additional user groups. However, the AICD cautions against providing greater access to directors' personal information to general public users as the solution.

In our view, a targeted expansion of the 'business' user group subject to appropriate verification by ASIC and access controls should address any legitimate access requirements. This would ensure that genuine business needs are met without undermining privacy and safety protections for directors.

However, for the reasons detailed in sections 5 and 7 below, we consider it is an unacceptable privacy and personal safety risk in 2026 that directors' personal information (such as residential addresses and date of birth) could be made available to anyone for a nominal $10 fee.

A tiered access model, together with the linking of the director ID to the companies register, is the appropriate solution to balance transparency and integrity of officeholder information against privacy, safety and security risks.

5. Residential address information

The AICD does not support ASIC's proposed approach to make officeholders' residential addresses available by default for general public access if a service address has not been lodged with ASIC. We have significant concerns with this approach.

Directors' residential address information is not currently available on the companies registers after appropriate steps were taken by ASIC earlier in 2026 to suppress this information in response to privacy and safety concerns. As ASIC itself recognises:[7]

> *"This change is a sensible precaution that balances the need to reduce easily accessible personal information while maintaining effective and transparent registers.*
>
> *This action does not remove residential address information entirely but introduces a barrier at the most widely available access point.*
>
> *Law enforcement agencies, government departments, and those who require address details for regulatory compliance and business purposes will still have access to this information."*

This is a sound policy rationale and the AICD strongly welcomed ASIC's measures.

We see no strong policy case why these important protections are proposed to be reversed where a director does not provide an alternative service address. In our view, there is no legitimate use case for

[7] ASIC media release, ASIC updates information available through purchased extracts, available here.

the public to access the residential address of directors, and we consider this information should continue to be removed from public availability on a permanent basis.

Under the proposed tiered access arrangements, which the AICD supports, authenticated users across the company, business and government user categories that have legitimate needs for directors' residential addresses will continue to have access to this information. As such, there will be no avenue for a director to hide or obscure their identity or 'go dark' as some stakeholders have suggested. This approach strikes an appropriate balance between preserving access to director information where there is a genuine need, while safeguarding against unnecessary public exposure that compromises directors' privacy and personal safety.

For all other general public users, access to an individual director's name, service address (discussed further below) and the director ID number itself should provide sufficient confidence that the individual has been appropriately identified and verified by ASIC.

Public interest test under section 1274AC - Privacy and safety concerns

ASIC has the statutory discretion to determine whether to restrict access to prescribed information on the companies register. In doing so, ASIC must have regard to a range of factors under section 1274AC of the *Corporations Act 2001* (Cth) (**Corporations Act**) to assess whether the benefits of restricting access outweigh the risks of disclosure. In particular, the statutory test requires ASIC to consider privacy and safety impacts, including any harms that could result from having, or not having, restrictions.

In the AICD's view, the substantial privacy, cyber security, identity fraud and personal safety risks associated with the disclosure of residential address information strongly support the exercise of ASIC's power to restrict access under section 1274AC. In particular, paragraph 1274AC(2)(c), concerning harm to persons from not having the restriction, strongly supports restricting public access. Further, we do not consider that any broader public interest, including protecting consumers from wrongdoing factor at 1274AC 2(a), would outweigh the significant identified privacy risks.

We also note that the Explanatory Memorandum to the *Treasury Laws Amendment (Business Registries Stabilisation and Uplift) Bill 2026* specifically highlights that ASIC has a particularly important power to:

> *"[…] take positive measures to protect privacy, for example by redacting or restricting public access to personal information such as residential address. This power is underpinned by considerations of protecting personal safety, public order and security, and has been designed to promote a reasonable and proportionate approach."*

The AICD has been advised by the national identity and cyber incident support service, ID Care, that the compromise of individual names, residential addresses and dates of birth has led to $155m in losses from their exploitation in the past 18 months, with an average loss per person of $33,000.

We have also been made aware of the lengths cyber criminals will go to exploit information on the companies register. This includes sharing detailed guidance on the dark web on how director and company information can be accessed through ASIC company extracts to facilitate identity fraud, establish impersonation websites designed to harvest personal credentials, offer fraudulent products and services, and run sophisticated phishing attempts and investment scams.

Directors also face significant personal safety risks as a result of the public availability of personal information. The AICD has heard first-hand accounts of directors being subjected to stalking, harassment,

threatening correspondence and protests at their homes. In some instances, these threats have extended beyond directors themselves to their spouses and children.

Importantly, these safety risks are not limited to directors of large or high-profile organisations. Any director who transacts, makes decisions or represents an organisation within the community may become the subject of grievances, disputes or unwanted attention. For example, directors across the economy, including those serving in small or family-run businesses, charities and community organisations, will regularly engage with employees, customers, shareholders, unions and other stakeholders, exposing them to personal safety risks. The AICD is aware, for example, of concerns of directors governing organisations operating in particularly sensitive areas. This includes domestic and family violence support services, community legal centres, religious organisations and child protection organisations that can be exposed to heightened personal safety risks due to the nature of the organisation's activities and stakeholders.

6. Service address

The AICD is concerned with ASIC's current proposal that directors must actively nominate an alternative service address in order to have their residential address removed from the public-facing companies register.

With over 3 million directors in Australia, it is highly unrealistic to expect that ASIC communication of these requirements will reach the full director population or that a majority of directors will act on these communications. Further, this approach is silent on the administrative challenge and likely cost a director will face in establishing an alternative address. It is critical that ASIC recognises that most directors are one by virtue of contributing to community organisations or being involved in a small or family-owned business. This proposal appears to be from the perspective of assuming most directors sit on the boards of a listed company and have ready or existing access to a service address via a law or accounting firm. This is not the case for the vast majority of directors.

We highlight Professor Hanrahan's advice that:[8]

> *"For a range of practical reasons, it is likely that the majority of directors will not nominate an alternative address. This might be because they are not aware they are able to do so, or because they do not have access to a ready alternative."*

It is our strong view that the level of privacy protection afforded to directors should not depend on whether they are aware of administrative requirements and/or have the means to establish a service address. The default setting should favour protection rather than publication, consistent with the public interest test safeguards set out in the Corporations Act and broader 'privacy by design' principles.

Registered office address

The AICD strongly recommends that any service address that is made publicly available by default is the company's registered office address (and not the director's residential address) unless the director provides ASIC with an alternative service address. This would ensure ongoing protection and mitigate the risks associated with directors not taking the step of nominating a service address.

We are concerned that, in the absence of a registered office address being used as a service address, directors of small family-owned businesses, community organisations and NFPs may not have the

[8] Professor Hanrahan advice for the AICD, June 2026, available here.

resources to establish and maintain a separate service address (which we understand can range in cost between $200-$600 per year).

The registered office already exists as the principal address for service and communication with the company. As a result, the public interest in ensuring directors and companies can be contacted and served documents can continue to be met without requiring disclosure of residential address information.

7. Date of birth information

The AICD strongly supports ASIC's proposal to restrict general public access to directors' full date of birth information and provide access to a year of birth instead. It is appropriate, in our view, that only authenticated company, business and government users have access to full date of birth information.

Full dates of birth are widely recognised as sensitive personal data. As noted above, the public availability of directors' full date of birth together with residential address information exposes directors to heightened risks of privacy and cyber risks.

With the linking of director IDs to the companies register, we consider there is less justification for continuing to publicly disclose a full date of birth as a means of verifying identity. A year of birth should provide sufficient differentiation between individuals with similar names for general public users of the companies register.

Australia has also been an outlier internationally for some time in providing public access to directors' date of birth information. The AICD has compared Australia's position to six other jurisdictions, including New Zealand, the United Kingdom, the United States of America, Canada, Hong Kong and Singapore. Notably, no other jurisdiction in this list discloses the full date of birth of directors to the public.

8. Director ID numbers

The AICD supports ASIC's proposal to provide public access to directors' unique director ID numbers on the companies register, *subject to residential address information being removed from public availability on a permanent basis*. That is, consistent with our recommendations above that a director's residential address is not disclosed in public searches and a service address that is made publicly available by default is the company's registered office.

The AICD has consistently supported the linking of director IDs to strengthen the integrity and reliability of information on the companies register. The display of the director ID for all users is a key step in achieving this aim. We also support ASIC's proposal to publish new display flags to indicate that a director ID has been verified by ASIC and confirmed by the director.

Critically, the publication of director IDs to the companies register reduces the need to rely on more sensitive personal information such as residential addresses and full dates of birth as a means of distinguishing between individuals. A unique, verified identifier provides a targeted mechanism for confirming identity, while avoiding the privacy and safety risks associated with the public availability of residential address and date of birth information.

Partial display of director ID if residential addresses remain publicly available

In circumstances where directors' residential addresses are made publicly available as the default where a service address is not provided, despite our significant concerns with ASIC's proposal, the AICD would not support the publication of the director ID in full on the companies register.

Publishing a director ID number in full publicly together with a director's name and a residential address (where an alternative service address has not been provided) will increase the potential for misappropriation online by cyber criminals, including the risk of identity theft, fraud or impersonation attempts. While the public disclosure of residential address or director ID each present risks in isolation, disclosure of these data points together creates a more comprehensive director profile that may be exploited.

The AICD has previously been advised by ID Care that director IDs, once publicly accessible, are likely to become 'trust markers', and it is anticipated that cyber criminals will use director IDs to deceive their targets. The use of trust markers (for example, ABN, ACN and TFN numbers, logos and telephone numbers) together with other personal identifying information can heavily influence a victim's decision to engage with cyber criminals. The very nature of the director ID being "valid for life" and unable to be changed will increase its attractiveness as a target.

In circumstances where ASIC elects to proceed with its current proposal for residential addresses to be made publicly available where a service address is not actively provided, the AICD recommends that director IDs be partially displayed on the companies register for general public users. For example, a partially disclosed director ID number could be limited to six digits '123 456 *** ***'. How many digits are displayed should be determined based on consultation with cyber security experts.

We do not consider that the partial display of the director ID would undermine the objectives of the regime. General public users could still have confidence that a director's identity has been verified by ASIC, while authenticated users would still have access to the director ID number in full on the companies register along with other director personal information.

In our view, this measure is an important precaution. The full disclosure of the director ID is very difficult to unwind back at a future point. Registry information is routinely scraped, copied and stored by third parties, meaning that once the information enters the public domain it may continue to be accessed and reused even if access settings are modified in the future.