



12 October 2026

Registry Data Consultation Team  
Australian Securities and Investments Commission  
GPO Box 9827  
Melbourne VIC 3001

Email: [consultation.registrydata@asic.gov.au](mailto:consultation.registrydata@asic.gov.au)

Dear Sir/Madam,

**SMSF ASSOCIATION SUBMISSION – ACCESS TO INFORMATION ON THE COMPANIES REGISTER**

The SMSF Association welcomes the opportunity to provide this submission in response to ASIC Consultation Paper 391, Access to information on the companies register (CP 391). We support ASIC's objective of maintaining transparency and confidence in the companies register while improving privacy, safety and security for individuals whose information appears on the register.

The SMSF sector has a particular interest in this consultation. Where an SMSF uses a corporate trustee, the fund's members are legally required to be the directors of that company. Many trustee companies are special purpose companies established solely to act as trustee of a regulated superannuation fund. The personal information of directors on the companies register therefore frequently relates to ordinary superannuation fund members rather than directors of operating businesses.

Our submission supports the overall direction of a tiered access model, the use of service addresses and the move to redacted lodged documents. However, we recommend stronger safeguards for enduring personal identifiers and residential information, together with clearer access pathways for professionals who need company information to undertake SMSF audit, administration, accounting, tax and financial advice functions.

In particular, the full director identification number should not be published through general access, residential addresses should not become publicly available merely because a service address has not been lodged, and access by company representatives should be based on the minimum information required for their role rather than automatically providing full access to data.

The Association also considers that the access settings should be tested against the anti-money laundering and counter-terrorism financing (AML/CTF) framework now applying to designated professional services. Where accountants, tax agents, financial advisers or other professionals provide a designated service, they have customer due diligence obligations requiring reliable and independent verification. AUSTRAC guidance specifically recognises ASIC register information as a source for verifying Australian companies and their ownership and control. CP 391 should therefore expressly accommodate verified professional users with a legitimate statutory compliance need.

We would be pleased to discuss these recommendations with ASIC as the access model and supporting legislative instrument are developed.



If you have any questions about our submission, please do not hesitate to contact Tracey Scotchbrook, Head of Policy and Advocacy via email [traceyscotchbrook@smsfassociation.com](mailto:traceyscotchbrook@smsfassociation.com)

Yours sincerely,

*Tracey Scotchbrook*

Tracey Scotchbrook  
Head of Policy and Advocacy

#### **ABOUT THE SMSF ASSOCIATION**

The SMSF Association is the peak body representing the self-managed superannuation fund (SMSF) sector which is comprised of over 1.2 million SMSF members and a diverse range of financial professionals. The SMSF Association continues to build integrity through professional and education standards for practitioners who service the SMSF sector. The SMSF Association consists of professional members, principally accountants, auditors, lawyers, financial advisers, tax professionals and actuaries. Additionally, the SMSF Association represents SMSF trustee members and provides them with access to independent education materials to assist them in the running of their SMSF.



## ASIC CP 391 – Access to Information on the Companies Register

### Table of Contents

|                                                                                                        |    |
|--------------------------------------------------------------------------------------------------------|----|
| <b>ASIC CP 391 – Access to Information on the Companies Register</b> .....                             | 3  |
| Executive Summary.....                                                                                 | 4  |
| Key Recommendations .....                                                                              | 5  |
| 1. SMSF context and the appropriate design principle.....                                              | 6  |
| 2. Protecting directors’ personal information .....                                                    | 6  |
| 2.1 Director ID numbers – Questions 1 and 4.....                                                       | 6  |
| 2.2 Residential address, locality and birth information – Questions 3, 5 and 6 .....                   | 7  |
| 2.3 Company access should not mean unrestricted representative access – Questions 11 and 15 .....      | 7  |
| 3. Access for SMSF professionals .....                                                                 | 8  |
| 3.1 Professional users that should be expressly recognised – Questions 11 and 12 .....                 | 8  |
| 3.2 Interaction with AML/CTF obligations for professional service providers – Questions 11 to 18 ..... | 9  |
| 3.3 Verification and safeguards – Questions 13 to 15 .....                                             | 10 |
| 4. Lodged documents, suppression and display flags.....                                                | 10 |
| 4.1 Redacted lodged documents – Question 7 .....                                                       | 10 |
| 4.2 Hidden information and suppression .....                                                           | 11 |
| 4.3 Display flags – Questions 8 to 10 .....                                                            | 11 |
| 5. Operational impacts, fees and transition – Questions 16 to 19 .....                                 | 11 |
| 6. Conclusion .....                                                                                    | 12 |
| Summary of responses to consultation questions.....                                                    | 13 |



## Executive Summary

The SMSF Association supports a modernised companies register that preserves public access to core company information while restricting sensitive personal information to users who have a demonstrated and verifiable need. This approach is consistent with CP 391 and is particularly important for SMSF trustee companies, where directors are generally the fund members themselves.

The proposed model would materially improve privacy in several respects, including the use of service addresses, reduced disclosure of full birth information and redacted versions of lodged documents. We support those directions. There are, however, several areas where the balance should be adjusted.

- The full director ID number should not be made available through free or paid general access or broad business access. A public confirmation flag is sufficient for most identity-assurance purposes. The full number should remain within secure company-specific reporting and authorised workflows.
- Residential addresses should remain restricted even where an officeholder has not lodged a service address. A failure to complete an administrative step should not result in publication of a home address. ASIC should use reminders, enforcement and a non-personal flag or other service mechanism rather than disclosure.
- Company access should be role-based. A person being an authorised representative should not automatically provide access to every sensitive field, including full date of birth and residential address.
- ASIC should expressly recognise ASIC registered SMSF auditors, registered tax agents, financial advisers and SMSF administrators/accountants acting under client authority. The model should provide both verified professional access for legitimate professional purposes and company-authorized access for a specific client company.
- ASIC should align professional access with AML/CTF obligations. The regime is service-based — not every accountant, tax agent or financial adviser is automatically regulated — but where a professional provides a designated service, customer due diligence may require verification of a company's identity, beneficial ownership and control, representatives and related know your customer (KYC) information. AUSTRAC guidance contemplates ASIC registers for this purpose. A verified professional access pathway should support that work without widening general public access to sensitive personal information.
- Verification should use existing registers and credentials wherever possible, supported by strong authentication, audit logs, time-limited and revocable authority, controls on bulk harvesting and clear prohibitions on reuse or on-sale of restricted personal information.



## Key Recommendations

### 1. Do not publish full director ID numbers.

Remove the director ID number from general access and broad business access. Publish the director ID confirmation flag instead, with the full number confined to secure company-specific reporting and authorised regulatory workflows.

### 2. Keep residential addresses restricted.

Do not make a residential address generally available from 1 August 2028 merely because a service address has not been lodged. The existence of a service-address deficiency should be addressed without exposing the home address.

### 3. Apply least-privilege access to company representatives.

Different representatives should only receive access to the fields needed for their role. Full birth and residential information should not automatically be available to every authorised representative.

### 4. Expressly include SMSF professionals.

Recognise approved ASIC Registered SMSF auditors, registered tax agents, financial advisers and appropriately authorised SMSF administrators/accountants within the access framework, with access calibrated to professional need.

### 5. Provide two professional access pathways.

Use verified professional access for legitimate cross-company activities such as pre-engagement checks, and company-authorised access for client-specific administration, lodgement and advice functions.

### 6. Use strong verification and safeguards.

Leverage existing ASIC, Tax Practitioners Board and financial adviser registers where available, with multi-factor authentication, audit logging, expiry and revocation of authority, rate limits and anti-harvesting controls.

### 7. Enable recognised professionals to authorise staff.

Professionals included in item 6 above, should be able to nominate and authorise key staff to access data on their behalf. Responsibility and level of access authorisation to be determined by the professional. The Australian Taxation Office's Online Services for Agents provides an illustrative working model.

### 8. Support redaction and carefully designed flags.

Retain the proposed redaction of lodged documents and director ID confirmation flag. Any overdue annual review flag should include context, so it is not misread as evidence of insolvency or SMSF non-compliance.

## 9. Design a workable transition.

Provide targeted communications and scalable authorisation processes for special purpose trustee companies and their professional advisers and avoid per-search costs that impede statutory audit and compliance work.

## 10. Align professional access with AML/CTF obligations.

Provide a verified pathway for AUSTRAC reporting entities undertaking customer due diligence, including relevant accountants, tax agents and financial advisers. Permit proportionate pre-engagement and cross-company verification, with sensitive information protected through purpose-limited access or match/no-match verification.

---

### 1. SMSF context and the appropriate design principle

CP 391 proposes four access categories – general, company, business and government – and seeks to make core company information broadly available while limiting more sensitive personal information to users with a clear need whose role or authority can be verified. The Association supports that underlying principle.

In the context of SMSFs the need for a purpose-based approach is reinforced. Under section 17A of the *Superannuation Industry (Supervision) Act 1993* (Cth), members of an SMSF with a corporate trustee are generally directors of that company, subject to limited exceptions. ASIC also recognises superannuation trustee companies as a class of special purpose company established to act solely as trustee of a regulated superannuation fund. The presence of a director on the register can therefore reflect participation in a private retirement savings vehicle rather than involvement in a trading or operating business.

For this cohort, the key policy objective should be to disclose enough information to identify the company, verify its status and officeholders, support lawful service and enable professional compliance work, without publishing personal identifiers or home-related information that is not necessary for those purposes. The statutory balancing tests referred to in CP 391, including privacy and safety impacts under sections 1274AB and 1274AC of the Corporations Act 2001, support this approach.

### 2. Protecting directors' personal information

#### 2.1 Director ID numbers – Questions 1 and 4

The Association does not support the proposal to make the full director ID number available through free and paid general access and across business access categories. A director ID is a unique, lifelong identifier, similar to our personal tax file numbers (TFN). TFNs are protected under statute and its use and handling strictly regulated. Director IDs must be similarly protected.

Australian Business Registry Services currently instructs directors to keep the number secure and store it with company records. Making the full identifier freely searchable would cut across that security message and could facilitate data matching, impersonation, social-engineering and fraudulent activity.

For most users, the proposed “director ID confirmed” flag provides the relevant assurance. It confirms that identity verification has occurred without disclosing the identifier itself. Where a reliable public cross-reference is needed to distinguish people with similar names or trace directorships, ASIC should consider a registry-generated public reference that is distinct from the director ID.

The full director ID should be accessible only where it is necessary for a company-specific regulatory reporting function, and then only to the director, the company and a specifically authorised representative within an authenticated workflow. It should not appear on downloadable extracts or be exposed to broad business users.

### *2.2 Residential address, locality and birth information – Questions 3, 5 and 6*

The Association supports replacing full date of birth and full residential address with less intrusive subsets where some identifying information is genuinely needed. A year of birth and state/country are preferable to a full date and street address. However, even these data points can contribute to re-identification when combined with other public information and should remain subject to proportionate access controls.

We strongly oppose the proposal to make a residential address available through general access from 1 August 2028 simply because a service address has not been lodged. ASIC removed residential addresses from purchased company extracts in February 2026 following longstanding privacy and safety concerns. Reintroducing public access as a consequence of an administrative omission would undermine that policy direction and create a disproportionate privacy outcome.

Instead, ASIC should retain the restriction on residential addresses and address a missing service address through targeted reminders, enforcement, a non-personal “service address not lodged” indicator, or another legally available service mechanism. The register should not use disclosure of a home address as the consequence for non-lodgement.

The same principle should apply to business access. Once a reliable service address exists, legal practitioners should generally be able to use that address for service and journalists should not receive a residential address as a class entitlement. Access to a residential address should require an exceptional, purpose-specific basis that cannot reasonably be met using the service address or other information.

### *2.3 Company access should not mean unrestricted representative access – Questions 11 and 15*

CP 391 proposes that company access is available to the company, officeholders, associated roles and authorised representatives, with access to all listed company and person details, including birth information and residential addresses. We support no-fee company access but recommend a more granular model for representatives.

An officeholder accessing their own company information is different from a third-party representative accessing information on the company’s behalf. A nominated agent, accountant, adviser, administrator or community advocate should only receive the information reasonably required for the authorised function. For example, an SMSF administrator may require officeholder status, appointment dates, service address and company electronic address, but not the director’s full date of birth or residential address.



ASIC should therefore allow the company or officeholder to grant role-based permissions, with access capable of being limited by information type, duration and function. This would better align company access with the “clear need” principle underpinning CP 391.

### 3. Access for SMSF professionals

#### *3.1 Professional users that should be expressly recognised – Questions 11 and 12*

The proposed business access category expressly identifies registered liquidators, legal practitioners and journalists. The Association recommends that ASIC also expressly provide for key SMSF professional users. CP 391 refers to auditors within company access, but it should be clear that this includes SMSF auditors registered with ASIC when acting in relation to the fund, not only auditors recorded in relation to the trustee company itself.

The following access pathways would reflect how SMSFs are administered in practice:

| Professional / role                            | Routine need                                                                                                                                                                   | Recommended access                                                                                                                                                                                                       |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registered SMSF auditor                        | Independent verification of trustee company status, officeholders, appointment/cessation dates and other information relevant to the annual SMSF audit; pre-engagement checks. | Verified professional access to core and detailed company information, service addresses and director ID confirmation status. No routine access to full residential address, full birth details or director ID.          |
| Registered tax agent / accountant              | Preparation and lodgement work, maintenance of company and fund records, assisting with change of details, and client administration.                                          | Company authorised access for the specific trustee company. Where a regulatory lodgement requires the raw director ID, access should occur only inside the secure authorised lodgement workflow.                         |
| SMSF administrator                             | Ongoing administration across multiple client funds, often on behalf of trustees and accounting practices.                                                                     | Company-authorised, practice-level access with delegated staff permissions, audit logs and revocation. No broad access to sensitive personal fields unless specifically required.                                        |
| Financial adviser / AFS licence representative | Verification of trustee structure and officeholders when providing or implementing advice involving an SMSF.                                                                   | Verified access to core company details, officeholder names/status, appointment dates, service address and confirmation flags; company-authorised access to additional non-sensitive contact information where required. |



For accountants and administrators who do not hold a government-issued professional registration, the appropriate basis for access should generally be explicit authority from the company or officeholder rather than unrestricted access across the register. This preserves a clear chain of authority while allowing the professionals who perform the work to access the information they need.

### *3.2 Interaction with AML/CTF obligations for professional service providers – Questions 11 to 18*

From 1 July 2026, the expanded AML/CTF regime applies to accountants and other professional service providers who provide designated services. Financial advisers will also be subject to AML/CTF obligations if they provide designated services. Importantly, the regime is service based. Professional title alone does not determine whether the obligations apply.

Before a designated service can be provided, the professional will need to undertake customer due diligence which includes establishing on reasonable grounds the identity of the customer, persons on whose behalf the service is received, persons acting for the customer and their authority, and — for non-individual customers — beneficial owners. AUSTRAC guidance for bodies corporate also contemplates collection of information about those responsible for governance and executive decisions, including a director identification number where applicable. The guidance expressly identifies ASIC registers as reliable and independent sources for verifying Australian company information and for cross-checking ownership and control. Ongoing customer due diligence can also require KYC information to be reviewed, updated and, where appropriate, reverified.

This creates a potential regulatory mismatch in CP 391. The proposed business access category expressly identifies registered liquidators, legal practitioners and journalists, but does not expressly include accountants, tax agents or financial advisers. Some members of those professions may nevertheless have a statutory AML/CTF purpose for accessing authoritative registry information. General access may be sufficient for many routine enquiries, but in higher-risk or more complex matters the absence of an appropriate professional pathway could require regulated professionals to rely on less direct sources, commercial intermediaries or additional client-supplied documents, increasing cost and friction.

Company access does not fully resolve the issue. Initial customer due diligence will generally need to be completed before the designated service begins, so a professional may need to undertake independent checks before a client appointment or company authority has been fully established. In addition, beneficial ownership and control enquiries may require tracing related companies beyond the particular company that has appointed the professional. Requiring an existing company-specific authority for every such enquiry risks creating a circular onboarding process.

We do not consider this to be a direct legal inconsistency. The AML/CTF framework permits the use of other reliable and independent data and does not prescribe the ASIC register as the only verification source. It is, however, an important regulatory-alignment issue. ASIC should provide a verified professional access pathway for users who can demonstrate a legitimate statutory or professional purpose, with access limited to the information reasonably required for that purpose and subject to the safeguards recommended below.

For particularly sensitive identifiers, ASIC should also consider verification without disclosure. For example, a verified professional could submit a date of birth, residential address or director ID



supplied by the client and receive a match/no-match response rather than being shown the underlying registry data. This would support independent AML/CTF verification while remaining consistent with the Association's position that raw director IDs and residential addresses should not be made generally available.

### *3.3 Verification and safeguards – Questions 13 to 15*

ASIC should use existing credentials wherever practical rather than create duplicative verification requirements:

- ASIC registered SMSF auditors can be verified against ASIC's professional registers;
- registered tax agents can be verified through the Tax Practitioners Board public register;
- financial advisers and relevant AFS representatives can be verified against existing ASIC professional registers; and
- company agents and other authorised representatives can be linked through a company-specific authority.

We recommend the following safeguards for restricted and professional access:

- multi-factor authentication and verification of the individual user and, where relevant, their professional credential;
- company-specific authority that can be granted, reviewed, limited, delegated within a practice and revoked;
- automatic expiry when a professional appointment, engagement or authority ends;
- audit logs visible to ASIC and, where appropriate, to the company or officeholder;
- rate limits and technical controls to prevent bulk harvesting of personal data;
- clear terms prohibiting the reuse, on-sale or aggregation of restricted information beyond the authorised purpose; and
- a higher threshold for any exceptional access to residential addresses, full birth details or the raw director ID.

For general access, ASIC should not require authentication merely to view core company information. However, where paid general access includes data such as year of birth or residential locality, an authenticated account, rate limiting and anti-scraping controls would be reasonable safeguards.

## **4. Lodged documents, suppression and display flags**

### *4.1 Redacted lodged documents – Question 7*

We support the proposal to provide redacted versions of lodged documents to general and business users where the document contains information that the user is not otherwise entitled to access. This is a sensible way to preserve access to corporate records without allowing a lodged document to defeat the access restrictions applied to the structured register data.

The same access rules should apply consistently across extracts, document images, APIs and any bulk or machine-readable services. Restricted information should not be recoverable through historical copies, metadata or alternative search pathways merely because it appears in a lodged document.

#### *4.2 Hidden information and suppression*

The Association supports a separate process for hidden or suppressed information where there are heightened privacy or safety risks. The process should be clear, accessible and capable of urgent action, particularly where there is a risk of family and domestic violence, stalking, identity misuse or other personal safety concerns. Suppression should be capable of extending to former names, locality information and service-address information where disclosure of those fields would create the relevant risk.

#### *4.3 Display flags – Questions 8 to 10*

We support the proposed director ID confirmation flag. It provides useful assurance without requiring disclosure of the identifier itself. We also see merit in an overdue annual review flag, provided its meaning is carefully explained.

A late annual review payment or administrative delay should not be interpreted as evidence that the company is insolvent, that the SMSF is non-compliant or that the trustees have breached superannuation law. The flag should therefore use neutral wording, appear only after any appropriate processing or grace period, and be accompanied by a short explanation of what it does and does not indicate.

### **5. Operational impacts, fees and transition – Questions 16 to 19**

The proposed model can reduce compliance friction if professional access is designed around existing SMSF workflows. Conversely, repeated manual authorisations, per-user setup for every staff member or per-search charges could materially increase costs that are ultimately borne by SMSF trustees.

These impacts may be more pronounced where AML/CTF customer due diligence applies. If a reporting entity cannot efficiently verify information directly from ASIC, it may need to purchase third-party verification services or duplicate document collection for information that is already held on the register. A controlled professional pathway can reduce those costs while improving data quality and preserving privacy safeguards.

ASIC should provide a scalable authority model that allows a trustee company to authorise a professional practice, with that practice then able to assign appropriately controlled access to individual staff. The company should be able to see and revoke the authority, and the practice should remain accountable for its users. This is particularly important for SMSF administrators and accounting firms that service large numbers of trustee companies.

Company authorised access should remain free, as CP 391 proposes. ASIC should also consider fee-free or low-cost verified professional access where the information is required to perform a statutory or regulatory function, including annual SMSF audit work. A subscription or practice-level model may be more efficient than repeated transaction fees and should be offered as an option.

The transition from 1 July 2027 should include targeted communications to special purpose superannuation trustee companies and the professionals who service them. ASIC should provide bulk or agent-assisted mechanisms for lodging service addresses and establishing authorities, sufficient testing time for software providers and intermediaries, and clear guidance about how existing company agents and professional representatives will migrate to the new access settings.



Importantly, residential addresses should remain restricted throughout the transition and after 1 August 2028. A trustee company that has not yet lodged a service address should receive escalating reminders and compliance action rather than having directors' residential addresses exposed.

## 6. Conclusion

The Association supports ASIC's objective of a modern, secure and useful companies register. The proposed tiered model provides a sound foundation, but the final settings should more clearly distinguish between information needed for corporate transparency and information that creates avoidable privacy and security risk.

For SMSF trustee companies, the appropriate balance is to keep core company and officeholder information readily available, protect enduring identifiers and home-related information, and provide secure, efficient access to verified professionals and authorised service providers. This will preserve the integrity and utility of the register without imposing unnecessary privacy costs on SMSF members or unnecessary compliance costs on the professionals who support them.

Aligning verified professional access with AML/CTF obligations would strengthen this balance by supporting financial-crime prevention and statutory compliance without using those obligations as a basis for broader public disclosure of directors' personal information.



## Summary of responses to consultation questions

| No.                                          | ASIC Consultation question                                                                                                                                                              | Summary response                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Information types and access settings</b> |                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                             |
| 1                                            | Do you agree with our proposed access settings for each information type in our proposed access model? Which settings do you support or not support, and why?                           | Broadly support the tiered model, but not all proposed settings. The full director ID should not be available through general or broad business access; residential addresses should remain restricted; and representative access should be limited to the information reasonably required for the role.                                    |
| 2                                            | Are there any information types that should be added, removed, combined or described differently?                                                                                       | Yes. Remove the full director ID from general and broad business access and rely on the director ID confirmation flag, or a separate public registry reference, for identity assurance. ASIC should also consider a non-personal “service address not lodged” indicator and verification-without-disclosure for sensitive data.             |
| 3                                            | Do you agree with the proposal to provide subsets of personal information (i.e. year of birth instead of full date of birth and state and country instead of full residential address)? | Yes, where some identifying information is genuinely required. Year of birth and state/country are preferable to full birth and residential details, but they can still contribute to re-identification and should remain subject to proportionate access controls.                                                                         |
| 4                                            | Do you agree with the information we propose to make available through free and paid general access? Is there any information that should be restricted?                                | Core company and officeholder information should remain readily available, but the full director ID should be removed from general access. Residential addresses should remain restricted. Where paid general access includes more identifying information, authenticated accounts, rate limits and anti-scraping controls are appropriate. |
| 5                                            | Do you agree with the proposed approach to making residential addresses available for general access from 1 August 2028 if a service address has not been lodged with ASIC?             | No. A failure to lodge a service address should not result in publication of a home address. ASIC should instead use reminders, enforcement, a non-personal indicator or another lawful service mechanism while continuing to protect the residential address.                                                                              |
| 6                                            | Are there any practical recurring issues for registry users or other stakeholders if access to residential addresses is restricted?                                                     | Not sufficient to justify routine disclosure. A service address should generally meet service and contact needs. Exceptional access to a residential address should require a purpose-specific basis where the need cannot reasonably be met using a service address or other information.                                                  |
| 7                                            | Will redacted copies of documents that have been lodged with ASIC be sufficient for the needs of general and business users?                                                            | Yes, in principle. Redaction is a sensible way to preserve access to corporate records without defeating restrictions on sensitive data. The same rules should apply consistently across extracts, document images, APIs and bulk or machine-readable services.                                                                             |



| No.                                 | ASIC Consultation question                                                                                                                    | Summary response                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Display flags</b>                |                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                          |
| <b>8</b>                            | Do you agree with our proposal to publish new display flags or indicators, such as director ID confirmation and overdue annual review status? | Yes, subject to careful design. The director ID confirmation flag is strongly supported because it provides assurance without disclosing the identifier. An overdue annual review flag may also be useful if its meaning is clearly explained.                                                                                                           |
| <b>9</b>                            | Are the proposed flags useful for people dealing with companies? Are there any risks or unintended consequences?                              | Yes, but there is a risk of misinterpretation. An overdue annual review should not be read as evidence of insolvency, SMSF non-compliance or trustee misconduct. Neutral wording, appropriate timing and explanatory context are required.                                                                                                               |
| <b>10</b>                           | Are there other flags or indicators that would help users understand company register information?                                            | Yes. ASIC should consider a non-personal “service address not lodged” indicator rather than disclosing a residential address. Any additional flags should communicate a specific registry fact and avoid implying broader compliance conclusions.                                                                                                        |
| <b>User groups and verification</b> |                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                          |
| <b>11</b>                           | Do you agree with the proposed access settings for each user group – namely, general, company, business and government?                       | Support the four-category structure, but the settings need refinement. Company access should be role-based rather than automatically exposing all sensitive fields to representatives, and business access should expressly accommodate verified SMSF professionals and AML/CTF-regulated professional users where there is a legitimate need.           |
| <b>12</b>                           | Are there other business users that should have access to more companies register information? Why does that group need access?               | Yes. Registered SMSF auditors, registered tax agents, financial advisers and appropriately authorised SMSF administrators/accountants should be recognised. They need reliable registry information for audit, administration, advice, tax and, where applicable, AML/CTF customer due diligence, including pre-engagement and ownership/control checks. |
| <b>13</b>                           | What verification should we require before giving a user access within a restricted user group?                                               | Use existing professional registers and credentials wherever possible, together with strong identity verification and multi-factor authentication. Access should be linked to the relevant professional credential, appointment or company authority and should expire or be revoked when that basis ends.                                               |

| No.                                | ASIC Consultation question                                                                                                                                                                                                 | Summary response                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 14                                 | Should we authenticate general users or introduce other access controls for general access? If yes, what controls would be appropriate?                                                                                    | Authentication should not be required merely to view core public company information. However, where paid general access includes more identifying information, authenticated accounts, rate limits, anti-scraping measures and controls against bulk harvesting would be reasonable.                                                                                |
| 15                                 | What safeguards should we put in place for access to company data by company representatives, including company agents, legal representatives, community legal centres, auditors, liquidators and external administrators? | Apply least-privilege access, multi-factor authentication, auditable and revocable authority, automatic expiry, access logs, rate limits and anti-harvesting controls, and prohibitions on reuse or on-sale. Particularly sensitive fields should require a higher, purpose-specific threshold.                                                                      |
| <b>Impacts, costs and benefits</b> |                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                      |
| 16                                 | What costs, benefits or operational impacts would the proposed access model create for you or your organisation?                                                                                                           | A well-designed professional access model can reduce compliance friction and improve data quality. Conversely, repeated manual authorisations, per-user setup and per-search fees would increase costs for SMSF practices and trustees. The impact is greater where AML/CTF customer due diligence requires independent verification.                                |
| 17                                 | Would the proposal affect competition, compliance costs, fraud prevention, credit risk assessment, due diligence, enforcement, journalism, research or other activities?                                                   | Yes. Properly calibrated access can support audit, due diligence, AML/CTF compliance and fraud prevention. If regulated professionals cannot efficiently access registry information, they may need commercial intermediaries or duplicate client documentation, increasing compliance costs without materially improving privacy.                                   |
| 18                                 | Are there changes we could make to reduce costs or impacts while still protecting personal information?                                                                                                                    | Yes. Provide verified professional and company-authorized access pathways, allow practice-level delegated permissions, keep company-authorized access free and consider low-cost professional access for statutory functions. For sensitive identifiers, use match/no-match verification rather than disclosure wherever feasible.                                   |
| 19                                 | Are there any transitional issues we should consider before the proposed access settings start on 1 July 2027?                                                                                                             | Yes. Provide targeted communications to special purpose SMSF trustee companies and their advisers, scalable mechanisms to lodge service addresses and establish authorities, sufficient testing time for software providers and clear migration guidance. Residential addresses should remain protected throughout the transition.                                   |
| 20                                 | Do you have any other comments on the proposed access model?                                                                                                                                                               | The tiered model is a sound foundation, but it should more clearly distinguish public transparency from legitimate professional need. For SMSF trustee companies, core company information should remain accessible while enduring identifiers and home-related information are protected and verified professionals have secure, efficient, purpose-limited access. |