

12 October 2026

Australian Securities and Investments Commission
GPO Box 9827
Melbourne VIC 3001

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

Re: Access to information on the companies register (CP 391)

To Whom It May Concern:

The Association of Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to provide feedback on the Australian Securities and Investments Commission's (ASIC) Consultation Paper 391, *Access to information on the companies register* (CP 391).

DSPANZ is the peak industry association for business software providers operating across Australia and Aotearoa New Zealand. Our members include tax, accounting, payroll, superannuation, invoicing and other software providers that support businesses with their day to day operations and meeting their compliance obligations.

DSPANZ supports ASIC's objective of modernising the companies register and developing access settings that appropriately balance transparency and access to company information with privacy, safety and security.

Through its RegistryConnect program, ASIC has an opportunity to make authoritative companies register information more accessible and useful within the software businesses and advisers already use.

To realise this opportunity, the proposed access settings and supporting Application Programming Interfaces (APIs) should be designed together. In particular, ASIC should clarify how information can be accessed through business software (e.g. taxation, accounting and superannuation products) on behalf of authorised users and ensure its services support business workflows beyond traditional company searches.

ASIC should also recognise that there are many different types of Digital Service Providers (DSPs) that exist across the Australian eco-system - the business and technical requirements to support the operations of an information broker will be substantially different to the requirements of business software providers.

Today, many business software providers do not currently interact directly with ASIC registry services, but the introduction of new APIs will create opportunities to validate information, support regulatory compliance and reduce manual processes.

Accordingly, throughout this submission “DSP” refers to the category of DSPs that access ASIC’s digital services and “business software providers” refers to accounting, payroll, practice management, company administration and similar software providers, who may or may not be ASIC DSPs today.

DSPANZ recommends that ASIC:

1. Enable authorised users to access register information through software, with clear rules for access tiers, verification, delegated authority and revocation.
2. Provide machine-readable validation, matching and status services that support legitimate business and compliance needs while minimising unnecessary disclosure of personal information, including consideration of verification-scoped access.
3. Recognise the different needs of information brokers and business software providers and engage both in designing commercially viable, technically ready API services, with DSPANZ supporting engagement with business software providers.
4. Provide clear transitional access and redaction rules and work with AUSTRAC to resolve how the proposed service-address arrangements interact with AML/CTF obligations.

DSPANZ welcomes the opportunity to work with ASIC and to facilitate further engagement with DSPs as the access settings and supporting digital services for the modernised company register are developed. Please contact Maggie Leese at maggie@dspanz.org for more information.

Regards,

Signed by:

E3E80D8A0D7A7097

Chris Denney,
Interim CEO & Executive Director
DSPANZ.

About DSPANZ

Digital Service Providers Australia New Zealand is the gateway for the government into the dynamic, world-class business software sector in Australia and Aotearoa New Zealand. [Our members](#) range from large, well-established companies to new and nimble innovators working at the cutting edge of business software and app development on both sides of the Tasman.



Design the access settings to work through software

DSPANZ supports access settings based on a user's role, authority and legitimate need for information. However, CP 391 does not clearly explain how these entitlements will operate when a company, director, accountant, company agent or other authorised representative accesses information through business software rather than directly through ASIC.

There are two distinct scenarios ASIC should accommodate:

1. Where a DSP accesses companies register information for its own purposes, for example to provide an information service.
2. Where software facilitates access on behalf of a customer who has an existing entitlement or authority. For example, an accountant or company agent may be entitled to access information about a client company and want to use that information with the practice or company administration software through which they manage that client.

Clarify how access tiers apply through software

CP 391 identifies information brokers and DSPs as stakeholders, but the proposed access categories do not explain how a software provider can facilitate access to information available to a verified end user.

ASIC should clarify:

- whether a software provider can retrieve and provide information to a customer based on that customer's verified access entitlement;
- whether the DSP, end user or both are responsible for establishing and maintaining that verification;
- how different access tiers will be represented through an API;
- whether DSPs facilitating access will be subject to additional accreditation or assurance requirements; and
- how commercial settings, including pricing and volume arrangements, will operate for API access.

The technical model should enable the appropriate access entitlement of the underlying user to operate securely through software.

Design agent authority for digital workflows

Similar issues arise where access depends on an agent's appointment or authority.

DSPANZ supports ASIC's proposal that access based on an appointment should cease when that authority ends. However, this needs to be capable of operating efficiently at scale.

Where an adviser manages multiple client companies through software, ASIC should enable the adviser's identity and professional status to be verified once, with authority for each client separately established and maintained. For example, DSPANZ member experience

with ATO digital services (for example, super stapling processes) demonstrates that requiring businesses to separately nominate software providers through a government portal can reduce adoption and increase support costs.

ASIC should therefore consider enabling authority to be established within software workflows, subject to appropriate assurance, rather than requiring separate portal nominations for each company.

The supporting digital services should also enable changes in authority to flow through to software promptly, including automated revocation where an appointment ends.

ASIC should provide clear rules for information already obtained through a valid authority when that authority subsequently ceases. Software providers need to understand whether that information can continue to be held where required for legitimate business or record-keeping purposes and when access or retention should cease.

Recommendation 1: ASIC should enable authorised users to access register information through software, with clear rules for access tiers, verification, delegated authority and revocation.

Enable authoritative register information to support validation and compliance

The modernisation of the companies register is an opportunity to improve how authoritative company information is used across the broader digital business ecosystem.

Business software providers may not need to reproduce an ASIC search or extract within their products. Their use case may instead be to establish that information supplied by a customer is correct or that a particular status or relationship exists.

This distinction should inform the design of ASIC's APIs.

Entity validation and ongoing verification

Business software providers increasingly use authoritative information to verify that customers are legitimate businesses, confirm officeholder relationships and monitor changes that may affect compliance.

For example, the [ATO's DSP Operational Security Framework](#) requires DSPs accessing its digital services to undertake entity validation. Similar verification needs arise in customer onboarding, payments and AML/CTF processes.

These use cases may require ASIC to provide more than traditional register extracts. Potential services include:

- company and officeholder status validation;
- notifications of changes such as deregistration, external administration or officeholder appointments;
- narrowly scoped identity or attribute matching, including where date of birth is no longer available through general extracts; and
- alignment with Australian Business Register identifiers and services where relevant.

ASIC should consider whether verified businesses undertaking legitimate compliance activities require a distinct form of verification-scoped access.

Verification without unnecessary disclosure

Not every validation requires access to the underlying information.

For example, where the relevant business purpose is to establish whether a Director ID has been confirmed, software may only require an authoritative confirmation rather than access to the Director ID itself.

This principle could be applied more broadly through structured, machine-readable attribute and status services.

Any such services would require appropriate authority, security and purpose controls. However, designing around a specific validation question can provide a more privacy-preserving approach than requiring users to obtain and retain larger amounts of register information.

Ensure flags can be relied upon

DSPANZ supports ASIC's proposal to use flags to make relevant company and officeholder statuses more readily identifiable.

These flags may also be valuable through APIs. However, where software, financial institutions or other businesses use a flag to inform a process or decision, the accuracy and meaning of that flag becomes important.

ASIC should clearly specify:

- what each flag means;
- when and how it is updated;
- the date or currency of the underlying information;
- how errors can be disputed and corrected; and
- whether and to what extent the flag can be relied upon.

DSPANZ considers that an appropriate correction process should be established before status flags are used more broadly.

Protect personal information by design

The proposed access settings also raise broader privacy considerations.

DSPANZ supports limiting the information that needs to be transferred or retained where a business purpose can be achieved through a verification response.

The same principle should inform the treatment of historical names and other personal information made available through general access. Member feedback has identified a potential safety risk where former names become freely available, particularly for individuals who have changed their name (e.g. for safety reasons).

ASIC should consider an appropriate suppression process and system controls such as authentication or proportionate rate limiting where these can reduce bulk harvesting or misuse of public personal information without unduly limiting legitimate access.

Recommendation 2: ASIC should provide machine-readable validation, matching and status services that support legitimate business and compliance needs while minimising unnecessary disclosure of personal information, including consideration of verification-scoped access.

Recognise the different needs of ASIC's DSP stakeholders

ASIC should recognise that information brokers and business software providers will consume companies register information for different purposes.

Information brokers typically provide information products and services, while business software providers may incorporate ASIC information into accounting, practice management, company administration or compliance workflows.

These differences affect the information required, frequency and volume of access, authority arrangements and commercial viability of integration.

ASIC's existing engagement with information brokers provides an important perspective but will not reflect the needs of business software providers that do not currently interact with ASIC. New API services may create business cases for these providers that are not reflected in current usage. ASIC should therefore test proposed API services with both existing consumers of register information and potential business software users.

DSPANZ notes that ASIC is not currently accepting new DSP applications to access the existing companies register and with applications to access the new APIs expects to reopen in 2027. We are aware that this approach has impacted a number of DSPs that are seeking access to companies register information to support their product operations.

To provide business software providers with certainty to plan integrations, ASIC is encouraged to publish the reopening timeline, eligibility criteria and access terms, to support 1 July 2027 commencement.

Design commercial settings for different use cases

The commercial model is also relevant to business software participation.

Pricing designed around individual searches or extracts may not be suitable for software performing high-volume, narrowly scoped validation. This includes bulk validation of existing customer records and ongoing monitoring.

ASIC should consider transaction pricing, volume arrangements and accreditation requirements alongside API design to ensure legitimate software use cases remain commercially viable.

Engage business software providers throughout design

DSPANZ would welcome the opportunity to assist ASIC in engaging business software providers as these services are designed.

This engagement should occur before technical and commercial settings are finalised. It can help ASIC test whether proposed APIs, authority arrangements, data services and pricing models support real software workflows.

DSPs will also need the normal foundations required to implement government digital services successfully, including:

- stable API specifications and data definitions;
- clear authentication, authorisation and access rules;
- consistent identifiers;
- predictable error responses;
- versioning and change-management processes;
- appropriate service levels and rate limits;
- production-quality test environments and representative test data;
- technical support; and
- sufficient time to build, test and deploy integrations after these dependencies are stable.

Software development time should also be considered separately from ASIC's own development timeframe. DSPs cannot fully build and test integrations until policy settings, specifications, services, test environments and commercial arrangements are sufficiently stable.

Recommendation 3: ASIC should recognise the different needs of information brokers and business software providers and engage both in designing commercially viable,

technically ready API services, with DSPANZ supporting engagement with business software providers.

Address transition and cross-regulatory dependencies

The proposed access settings will not operate in isolation. DSPANZ encourages ASIC to consider both the transition from existing register arrangements and interactions with obligations administered by other regulators.

Provide a clear transition between access settings

ASIC proposes new registry services and access settings from 1 July 2027, with full implementation of the new information requirements from 1 August 2028.

This creates a period in which software and users may encounter information subject to different rules depending on when it was lodged or updated.

For example, CP 391 proposes transitional arrangements for residential addresses and redaction of lodged documents. Software providers consuming this information need to be able to determine what information is available, what rules apply to it and whether differences reflect the transition rather than an error or incomplete record.

ASIC should provide clear guidance and machine-readable definitions identifying what information is available or redacted for each access tier during the transition, including how historical and newly lodged information should be treated.

Resolve the interaction between service addresses and AML/CTF obligations

DSPANZ also encourages ASIC to consider the interaction between its proposed service address model and the expanded AML/CTF regime. We believe the relationship between the AML/CTF obligations and the proposed use of service addresses for individual officeholders is not clear. In short, ASIC is making residential addresses less visible at the same time AUSTRAC is requiring more entities, including those who would provide service addresses, to identify and verify people.

We would encourage ASIC to engage with AUSTRAC to clarify this interaction before the new service address arrangements commence.

ASIC should also consider the practical alternatives available where an officeholder does not want their residential address made public but their accountant or adviser is unwilling to provide a service address. This may warrant consideration of other approved service address models.

Finally, where an agent manages ASIC obligations for a company or officeholder, ASIC should consider whether electronic notices can also be provided to the authorised agent. This could help ensure important communications are incorporated into the existing company administration workflow.

Recommendation 4: ASIC should provide clear transitional access and redaction rules and work with AUSTRAC to resolve how the proposed service-address arrangements interact with AML/CTF obligations.