



OVER 100 YEARS OF SERVING
THE REAL ESTATE INDUSTRY

Submission on the Privacy Reform Exposure Draft Legislation

September 2026

Submitted to:
Attorney-General's Department

Contents

About REIA.....	2
Executive summary	2
Recommendations.....	4
1. Consultation process	7
2. Small-business exemption and cumulative regulation	7
3. Trading in personal information	8
4. Expanded definition of personal information.....	11
5. Fair and reasonable handling	13
6. Rental applications	14
7. Digital ID and Consumer Data Right solutions.....	16
8. Controller and processor framework.....	17
9. Collection notices	18
10. Consent.....	19
11. De-identification and aggregated property information.....	20
12. Existing records and transitional arrangements	21
13. Access, erasure, and platform-held information.....	22
14. Direct marketing	22
15. Data breaches and the 72-hour notification period	23
16. Implementation and regulatory guidance.....	25
Conclusion.....	25

About REIA

The Real Estate Institute of Australia (REIA) is the national peak body for the real estate profession. Its members comprise the real estate institutes in each state and territory, which collectively represent real estate agencies, property professionals, and their clients across Australia.

Real estate businesses handle personal information as an essential part of property sales, leasing, property management, identity verification, client due diligence, and regulatory compliance.

The industry is predominantly made up of small businesses operating under extensive state and territory regulatory frameworks. Agencies also rely increasingly on large property technology, forms, customer relationship management, identity verification, and rental application platforms.

REIA convened a Privacy Working Group comprising representatives of its state and territory members to inform this submission.

For the purposes of this submission:

Real estate transaction or tenancy process means an activity reasonably connected with the proposed or actual appraisal, listing, marketing, sale, purchase, leasing, or management of real property. It includes responding to enquiries, conducting inspections, assessing applications or offers, verifying identity, undertaking due diligence, preparing agreements, maintaining required records, and facilitating customer-requested professional services.

Executive summary

REIA supports strong and proportionate privacy protections that maintain consumer confidence. These protections must also reflect the practical circumstances in which real estate businesses operate.

REIA welcomes the Government's decision to retain the small-business exemption. It is an important protection for agencies already dealing with substantial federal, state, and territory regulation, including new Commonwealth anti-money laundering and counter-terrorism financing obligations.

Several proposals would, however, significantly dilute that exemption.

REIA does not support the proposed trading-in-personal-information provisions in their current form. The provisions could expose a small real estate agency to Privacy Act obligations because of consent or disclosure processes designed and controlled by a third-party supplier.

If the provisions proceed, the legislation should place the primary evidentiary obligation on businesses whose primary business activity is trading in personal information. A commercial data supplier should be responsible for obtaining, retaining, substantiating, and providing evidence of the consent or other authority relied upon for a disclosure.

A small-business purchaser should be able to rely on that evidence unless it knows, or could reasonably be expected to know, that the evidence is false or the disclosure is unlawful. An ordinary agency should not be required to conduct a separate legal audit of a larger supplier's collection and consent processes.

The provisions must also avoid capturing ordinary real estate activities. A small agency may share information through a customer-requested referral, franchise arrangement, inter-agency relationship, or another activity reasonably connected with a real estate transaction or tenancy process. This should not cause the agency to be characterised as a commercial data supplier where trading in personal information is not its primary business activity.

REIA also has concerns about:

- the open-ended operation of the proposed fair and reasonable test;
- the interaction between federal privacy law and state and territory property laws;
- the application of the reforms to rental applications;
- the allocation of responsibility between small agencies and large technology platforms;
- the treatment of small businesses that have activity-specific Privacy Act obligations under the AML/CTF regime;
- unnecessary legal complexity in the proposed consent requirements;
- the application of the expanded definitions of personal information and collection, particularly for property information and information generated by technology platforms;
- the practical operation of a fixed 72-hour data breach notification period where agencies depend on third-party platforms and service providers;
- the treatment of existing records and legacy databases; and
- the absence of an explanatory memorandum.

Privacy responsibility should follow actual conduct, control, and commercial benefit. Large data suppliers and technology platforms should not be permitted to transfer privacy risks to agencies through standard-form contracts or product design.

Recommendations

REIA recommends that the Australian Government:

1. Retain a meaningful small-business exemption, including for agency activities unrelated to an activity that is already specifically subject to the Privacy Act.
2. Not proceed with the proposed trading-in-personal-information provisions in their current form, as they would disproportionately dilute the small-business exemption and expose agencies to liability for processes controlled by third parties.
3. If the provisions proceed, introduce a statutory obligation requiring an entity whose primary business activity is trading in personal information to obtain, retain, substantiate, and provide the purchaser with evidence of the valid consent or other legal authority relied upon for the disclosure.
4. Provide a statutory safe harbour allowing a small-business purchaser to rely on the supplier's evidence where the supplier is an APP entity and the purchaser does not know, and could not reasonably be expected to know, that the evidence is false or the disclosure is unlawful.
5. Limit any loss of the small-business exemption to the particular data-handling activity concerned, unless the conduct is knowing, reckless, repeated, or systemic.
6. Clarify that trading in personal information does not include:
 - genuine customer-requested referrals;
 - ordinary intra-agency, franchise, or inter-agency cooperation reasonably connected with a proposed or actual real estate sale, purchase, leasing, or property management process;
 - the incidental sharing of an enquiry to respond to a person's expressed property needs; or
 - access to property listings, comparable sales, market information, and ordinary property analytics.
7. Modernise the definitions of personal information and collection subject to clear statutory and property-sector guidance on the connection required between information and an individual, the treatment of property information, and responsibility for generated or inferred information. Do not apply the expanded definitions to information acquired or created before commencement solely because it continues to be held or, at a minimum, provide a substantial transition period and a risk-based remediation safe harbour.

8. Redraft the fair and reasonable test to provide objective statutory criteria, recognise compliance with state and territory property laws, and allow the assessment to be conducted at the level of the overall process and purpose.
9. Provide statutory protection, or at a minimum a rebuttable presumption, that information handling is reasonably necessary for a real estate transaction or tenancy process, and that is undertaken consistently with applicable state or territory law, is fair and reasonable.
10. Require the privacy regulator to develop specific rental application guidance, in consultation with REIA, state and territory regulators, our member Institutes, and relevant technology providers.
11. Establish a funded national implementation pathway for Digital ID and Consumer Data Right solutions in rental applications, including affordable and interoperable access for agencies.
12. Allocate controller and processor responsibility according to actual control, conduct, and commercial benefit, rather than contractual labels.
13. Expressly provide that an otherwise exempt small business does not become an APP entity or controller for unrelated activities merely because the Privacy Act applies to information handled in connection with its AML/CTF obligations.
14. Support clear collection notices and meaningful consent while avoiding requirements for separate consent for every data point or closely related step in a real estate transaction or tenancy process.
15. Adopt a contextual and risk-based de-identification standard, supported by practical guidance and appropriate transitional protection.
16. Ensure the reforms do not impose retrospective liability, require businesses to obtain fresh consent for existing records solely because the statutory definition of consent has changed, or otherwise impose new liability for pre-commencement information handling that was lawful when undertaken.
17. Retain a practical access exception where access is technically impossible or infeasible, while requiring platforms to assist agencies to respond to access requests.
18. Do not proceed with the proposed fixed 72-hour data breach notification period and retain the requirement to notify as soon as practicable after an entity has reasonable grounds to believe that an eligible data breach has occurred. If a fixed period proceeds, provide extensions for complex and third-party incidents, protect good-faith preliminary notifications, require rapid platform-to-agency cooperation, and facilitate coordinated notification where multiple entities are affected by the same incident.

19. Provide:

- at least 24 months between passage and substantive commencement;
- final regulator and sector-specific guidance at least 12 months before commencement; and
- further consultation on a complete bill, explanatory memorandum, transitional provisions, regulatory impact analysis, and complaint and enforcement framework.

1. Consultation process

The exposure draft was released on 31 August 2026, with submissions due on 18 September 2026. The Government has encouraged submissions of approximately 1,000 words.

The exposure draft is 58 pages long and contains approximately 40 proposals affecting consent, data trading, rental applications, direct marketing, security, breach reporting, technology providers, access, erasure, complaints, and enforcement.

An 18-day consultation period is not adequate for reform of this scale.

The Government has relied on consultations conducted over several years. However, those consultations largely considered broad policy propositions rather than the detailed legislative provisions now proposed.

There has been no meaningful recent, sector-specific opportunity to test the provisions against real estate operations, technology systems, or state and territory property laws.

The absence of an explanatory memorandum is a particular concern. The consultation paper provides broader policy narrative, but it cannot provide an authoritative explanation of the legislative intention, operation, or interaction of individual provisions.

The suggestion that affected organisations confine their submissions to approximately 1,000 words is also inconsistent with the breadth and significance of the reforms.

REIA recommends that the Government undertake further consultation on:

- a complete bill;
- a detailed explanatory memorandum;
- transitional and commencement provisions;
- sector-specific regulator guidance;
- the interaction with state and territory laws; and
- a regulatory impact analysis addressing the cumulative impact on businesses.

2. Small-business exemption and cumulative regulation

REIA welcomes the retention of the small-business exemption. The exemption must remain meaningful in practice and should not be progressively displaced through broadly framed exceptions.

Many real estate agencies are small businesses. They operate in a heavily regulated environment that includes state and territory licensing, trust accounting, residential tenancy, property sales, auction, consumer protection, record-keeping, anti-discrimination, and professional conduct obligations.

From 1 July 2026, real estate agents have been brought within the AML/CTF regime as reporting entities, creating significant additional regulatory obligations, including AML/CTF programs, risk assessments, and customer due diligence. Small businesses that are reporting entities will be subject to the Privacy Act in relation to personal information handled in connection with their AML/CTF obligations, even where their other activities remain exempt.¹

This activity-specific coverage demonstrates that privacy obligations can apply to particular higher-risk conduct without removing the exemption across an entire small business.

The likely cost and complexity of implementation should be assessed against this broader regulatory environment.

3. Trading in personal information

REIA's overarching position

REIA does not support the proposed trading-in-personal-information provisions in their current form.

The provisions could substantially erode the small-business exemption and disproportionately affect real estate agencies. An agency may acquire prospective vendor, landlord, buyer, or investor information without visibility of how the supplier collected the information or presented its consent process.

A small agency may have no practical ability to determine whether the supplier's consent was voluntary, informed, current, specific, and unambiguous.

Under the proposed framework, the agency could face significant legal consequences because of a defect in a process designed and controlled entirely by the supplier.

This is particularly concerning where the supplier is a large APP entity with substantially greater resources, information, negotiating power, and control over the relevant collection process.

The entity that collects and commercially trades personal information should bear primary responsibility for establishing the legal authority to supply it.

¹ Section 6E, *Privacy Act 1988*.

Statutory obligation for commercial data suppliers

If the data-trading provisions proceed, an entity whose primary business activity is trading in personal information should be required to:

- obtain any consent or other legal authority necessary for the disclosure;
- retain adequate records demonstrating that authority;
- substantiate that the consent satisfies the applicable statutory requirements; and
- provide appropriate evidence to the purchaser.

This obligation should focus on businesses that operate commercially as data suppliers.

It should not apply merely because a small real estate agency incidentally supplies or shares information during an activity reasonably connected with a real estate transaction or tenancy process, referral, franchise arrangement, or inter-agency relationship.

A real estate agency may, for example:

- refer a prospective seller or buyer to another office servicing the relevant area;
- transfer an enquiry to an office with a suitable property;
- share information within a franchise network to respond to a customer request;
- refer a client to a conveyancer, utility provider, finance broker, insurer, removalist, or building professional; or
- facilitate another customer-requested service reasonably connected with a proposed or actual real estate sale, purchase, leasing, or property management process.

These activities should not cause an agency to be characterised as a commercial data supplier where trading in personal information is not its primary business activity.

The distinction should turn on the nature and primary purpose of the business activity, rather than whether an incidental commercial benefit may arise from an ordinary real estate service.

Protecting small-business purchasers

The proposed framework should not require an ordinary real estate agency to independently reconstruct or legally audit a supplier's consent process.

In most cases, the agency did not:

- design the supplier's collection process;
- communicate with the individual at the time of collection;
- determine the wording or presentation of the consent;
- control the supplier's records; or
- decide how the supplier originally commercialised the information.

Where a supplier is an APP entity whose primary business activity is trading in personal information, a small-business purchaser should be entitled to rely on evidence provided under the supplier's statutory obligation proposed above.

This protection should apply unless the purchaser knows, or could reasonably be expected to know, that the evidence is false or the disclosure is unlawful.

A commercial warranty may support this protection, but it should not replace it. Small agencies frequently have limited ability to negotiate the terms offered by a large supplier.

This approach places responsibility on the entity controlling the original collection and commercialisation of the information. It avoids imposing a separate and potentially unworkable compliance regime on small-business purchasers.

Limit the consequences to the relevant activity

Any loss of the small-business exemption should be confined to the relevant data-handling activity. It should not automatically extend to the purchaser's entire business.

Whole-of-business Privacy Act coverage would be disproportionate where an agency has engaged in an isolated acquisition of data or reasonably relied on evidence supplied by a larger APP entity.

Broader consequences should be reserved for conduct that is knowing, reckless, repeated, or systemic.

Genuine referrals and ordinary industry arrangements

The reforms should preserve genuine customer-requested referrals. REIA welcomes that this matter has been contemplated as part of the consultation.

Real estate clients frequently ask agents to recommend conveyancers, utility providers, finance brokers, insurers, removalists, building inspectors, and other professional services.

Where the customer requests the referral and understands that relevant contact details will be provided for that purpose, the arrangement should not constitute trading in personal information.

The exclusion should also cover ordinary intra-agency, franchise, and inter-agency arrangements where information is shared to respond to a person's expressed property needs.

For example, an agent may refer a prospective seller to another office that services the relevant area or refer a prospective buyer to an office with a suitable listing.

These activities should not be captured merely because they may lead to a future commercial opportunity. They should be recognised as ordinary activities reasonably connected with a real estate transaction or tenancy process.

Property data products and incidental access

The legislation should distinguish between:

- purchasing an identified list for marketing or lead generation;
- subscribing to a broader property data or analytics product;
- accessing listings, comparable sales, ownership, or market information;
- exchanging information reasonably connected with a current or proposed real estate sale, purchase, leasing, or property management process; and
- commercially trading personal information as a product in its own right.

If incidental access to personal information through an ordinary property information product constitutes trading, a substantial portion of the real estate industry could be captured unintentionally.

The legislation should therefore clarify that ordinary access to property listings, sales history, market analytics, valuation information, and comparable transactions is not necessarily trading in personal information.

Clear statutory boundaries are required. Guidance alone will not provide sufficient certainty where the consequence may be the loss of the small-business exemption.

4. Expanded definition of personal information

REIA supports modernising the definition of personal information to reflect contemporary technologies and information-handling practices. Information should not fall outside appropriate privacy protections merely because it is generated, inferred, or does not include an individual's name.

The exposure draft would replace information "about" an individual with information that "relates to" an identified or reasonably identifiable individual. A person may be identifiable where information allows them to be recognised, singled out, or treated as a distinct individual, including through an identifier, location information, behaviour, preferences, or patterns of activity.

The revised definition of collection would also clarify that personal information may be collected when an entity generates or derives it and includes it in a record. In a real estate context, this could include applicant rankings, tenant suitability assessments, prospective-seller classifications, enquiry and inspection histories, and profiles derived from CRM or platform activity.

REIA's concern is not with protecting genuinely personal information. It is with ensuring that businesses can determine, with reasonable certainty, when information crosses the threshold into personal information and which entity is responsible for it.

This is particularly important for information that principally concerns a property. An address, sale price, rental amount, valuation, listing history, or property characteristic should not automatically become personal information merely because it may be possible to connect the property with an individual. Consistent with the consultation paper, there should be a sufficient and non-trivial connection between the information and the individual.

The position may differ where property information is deliberately combined with other information to profile an individual, influence a decision about them, or infer their circumstances or likely behaviour. Clear property-sector guidance is needed to distinguish these situations.

Responsibility for generated or inferred information should follow the entity that creates, records, and uses the relevant inference. A technology platform that independently generates an applicant score, behavioural profile, or prospective-seller classification should remain responsible for that information and should not transfer responsibility to an agency that does not control or understand how the output was produced.

The exposure draft would apply the expanded definitions to all information held after commencement, including information acquired or created before commencement. This could require agencies, institutes, and technology providers to review and potentially reclassify historical CRM records, forms data, archived information, and existing analytical datasets against standards that did not apply when the information was collected.

REIA recommends that the expanded definitions not apply to information acquired or created before commencement solely because that information continues to be held. Appropriate security obligations may continue to apply to legacy information, but businesses should not face immediate liability or remediation requirements arising solely from a subsequent change in statutory definition.

At a minimum, the legislation should provide a substantial transition period during which entities can identify and assess legacy information, supported by practical sector guidance and a documented, risk-based remediation safe harbour.

REIA supports the modernisation of the definition of personal information, subject to clear statutory and sector-specific guidance on the connection required between information and an individual, the treatment of property information, and responsibility for generated or inferred information. Amend the application provision so that the expanded definitions do not apply to information acquired or created before commencement solely because it continues to be held.

5. Fair and reasonable handling

REIA understands the policy intent behind requiring the collection, use, and disclosure of personal information to be fair and reasonable. However, REIA does not support the proposed test in its current form.

The test would introduce an open-ended and potentially subjective assessment above the requirement that conduct be lawful.

Businesses could be required to determine separately whether each type of information, collection method, use, and disclosure is fair and reasonable. This would create substantial uncertainty and compliance costs.

The consultation paper indicates that the assessment would consider matters such as:

- reasonable expectations;
- the kind and sensitivity of the information;
- the organisation's functions and activities;
- whether the impact is proportionate;
- the use of online choice architecture; and
- reasonably foreseeable risks of harm.

These factors remain broad and may produce different conclusions depending on the regulator, court, industry, and factual context.

If the test is retained, the legislation should:

- provide clearer and more objective statutory criteria;
- recognise the operation of state and territory property laws;
- allow the assessment to be undertaken at the level of an overall process and purpose;
- avoid requiring a separate assessment for every data point and every process;

- recognise information reasonably necessary for a real estate transaction or tenancy process;
- provide a rebuttable presumption that conduct expressly required or permitted by applicable property legislation is fair and reasonable; and
- distinguish information handling necessary to provide the requested real estate, leasing, or property management service from optional secondary commercial uses.

An agency following a lawful process prescribed or expressly permitted by state or territory property law should not be exposed to federal liability without clear evidence that its conduct was disproportionate or otherwise harmful.

6. Rental applications

Rental applications occupy a unique position. They are principally governed by state and territory tenancy legislation, prescribed forms, anti-discrimination requirements, agency obligations, and duties owed to property owners.

An agency must be able to collect sufficient information to:

- verify identity;
- assess an applicant's capacity to meet rental payments;
- check relevant tenancy history;
- understand proposed occupancy;
- detect fraud or inconsistencies;
- comply with applicable state and territory requirements; and
- assist the property owner to select a suitable tenant.

The fair and reasonable test should not require agencies to undertake repeated legal assessments at every stage of a rental application. Nor should it mandate a rigid staged process that prevents an agency from gathering the core information needed to assess applicants consistently.

Waiting until the tenancy agreement stage to obtain essential information may be too late. By that point, the agency may already have selected a preferred applicant and recommended that person to the owner.

Overly restrictive collection can also produce counterproductive outcomes. If an agency is limited to considering income, the property may effectively default to the highest-income applicant.

That outcome may prevent an agency from considering other relevant indicators of reliability and suitability. It may also disadvantage applicants who can meet the tenancy obligations but do not have the highest income.

Applicants should remain able to volunteer supporting information where they believe it strengthens their application, provided they are not pressured to disclose unnecessary or sensitive information.

Interaction with the 2Apply determination

The privacy regulator's determination concerning 2Apply illustrates the complexity of applying broad privacy principles to rental application platforms.² We note that this decision is subject to review before the Administrative Reviews Tribunal.

The determination found that the platform had direct privacy responsibilities and was more than a passive intermediary. It considered:

- whether the platform collected information in its own right;
- information reasonably necessary to assess identity, ability to pay, and likely care of the property;
- the relevance of state and territory tenancy laws;
- staged collection;
- the power imbalance experienced by applicants;
- limited practical choice;
- online choice architecture; and
- the fairness of requiring particular information.³

The decision provides useful direction but also highlights the absence of coordinated, prospective guidance for agencies and technology providers.

If the reforms proceed, the regulator should issue detailed rental application guidance explaining:

- what information may reasonably be collected at each stage;
- how federal privacy requirements interact with each jurisdiction's tenancy laws;
- how voluntary supporting information should be handled;
- the respective responsibilities of the agency and platform;

² Office of the Australian Information Commissioner, Commissioner Initiated Investigation into IRE Pty Ltd (Privacy) [2026] AICmr 24 (1 April 2026), available at https://www.oaic.gov.au/__data/assets/pdf_file/0022/263254/IRE-Pty-Ltd-Privacy-2026-AICmr-24.pdf.

³ Ibid.

- appropriate retention and deletion periods;
- consent requirements for optional services and secondary uses;
- how existing customer records should be treated; and
- how agencies should respond where a platform controls the relevant fields and workflow.

That guidance should be developed in consultation with state and territory tenancy regulators, REIA, our member Institutes, and technology providers.

7. Digital ID and Consumer Data Right solutions

REIA supports privacy-preserving technology that reduces the unnecessary collection and retention of rental applicants' personal information.

The Australian Government's Digital ID and Consumer Data Right rental pilot demonstrated that Digital ID can verify relevant identity attributes without requiring applicants to provide copies of identity documents.

Consumer Data Right information can also help demonstrate an applicant's financial capacity without requiring the applicant to upload complete bank statements or payslips.⁴

The Department of Finance has reported on the completion and outcomes of the pilot.

These solutions offer a practical way to improve privacy while still providing agencies with reliable information needed to assess applications.

The Government should develop and fund a national implementation pathway that:

- gives agencies affordable and interoperable access to Digital ID and Consumer Data Right services;
- does not require every agency to become a fully accredited Consumer Data Right data recipient;
- enables participation through accredited intermediaries and existing property technology systems;
- produces verified results rather than unnecessary copies of source documents;

⁴ Australian Government Digital ID System, "Digital ID Renters' Pilot: Reducing the Excessive Collection of Renters' Personal Information" (26 June 2026), <https://www.digitalidsystem.gov.au/news/digital-id-renters-pilot-reducing-the-excessive-collection-of-renters-personal-information>.

- remains voluntary for applicants;
- provides a workable non-digital alternative; and
- complements other information lawfully required to assess suitability.

If the Government is serious about reducing unnecessary information collection in the rental market, implementation of these technologies should accompany the proposed legislative reforms.

8. Controller and processor framework

REIA is concerned that the proposed controller and processor framework could place disproportionate liability on small agencies using large rental application and property technology platforms.

The exposure draft would generally attribute a processor's handling of personal information to the controller where the processor acts under the controller's documented instructions. Both parties must be APP entities for the proposed processor exception to apply.

Contractual terminology should not determine responsibility.

A large platform should not be able to describe itself as a processor where it independently controls matters such as:

- the default application form;
- the information fields available;
- mandatory and optional questions;
- the user interface;
- consent architecture;
- applicant accounts and profiles;
- retention settings;
- secondary marketing;
- analytics;
- data commercialisation; or
- product development.

Responsibility should follow actual control, conduct, and commercial benefit.

Where both the agency and platform determine relevant purposes or processes, the legislation should provide for shared or functionally allocated responsibility.

A platform should remain directly responsible for conduct undertaken for its own purposes, including profiling, analytics, marketing, product development, and retention beyond the agency's instructions.

Businesses built around collecting and handling personal information should not be permitted to shift responsibility for that information to small agencies through standard-form contracts.

Interaction with AML/CTF coverage

The controller and processor framework must recognise the activity-specific nature of the small-business exemption.

An otherwise exempt agency may become subject to the Privacy Act for personal information handled in connection with its AML/CTF obligations. That should not make the agency an APP entity or controller for every unrelated activity.

The legislation should expressly provide that:

- APP-entity status arising from AML/CTF obligations is limited to the relevant AML/CTF activity;
- unrelated rental, sales, marketing, and platform activities remain subject to the ordinary small-business exemption;
- the parties to an unrelated platform arrangement cannot rely on the processor exception merely because the agency has activity-specific AML/CTF coverage; and
- an APP-entity platform remains directly responsible for its handling where the agency is not an APP entity for the relevant activity.

Where information processed through a platform is unrelated to an agency's AML/CTF activities and there is no other basis for treating the agency as an APP entity, the agency should not be treated as a controller for the purpose of the proposed framework.

Specific guidance will also be required for mixed-purpose systems that process both AML/CTF information and ordinary information associated with a real estate transaction or tenancy process.

9. Collection notices

REIA supports clearer, shorter, and more accessible collection notices.

Under the existing *Privacy Act*, APP 5 requires an APP entity to take reasonable steps to notify an individual of specified matters at or before collection, or as soon as practicable afterwards.

The proposed reforms would simplify the required content and focus notices on information most relevant to an individual's decision-making. REIA supports this objective.

In a multi-party property technology environment, however, the notice must make clear:

- which entity is collecting the information;
- which purposes belong to the agency;
- which purposes belong to the platform;
- whether information will be used for marketing, profiling, analytics, or product development;
- whether information will be disclosed or traded; and
- how long each organisation will retain the information.

A platform should be responsible for notifying individuals about its own purposes. It should not be able to shift that responsibility to an agency through contractual terms.

The legislation and guidance should permit layered notices. A concise primary notice should be able to direct an individual to more detailed information without requiring every operational detail to be displayed on a single screen.

10. Consent

REIA generally supports the objective of ensuring that consent is genuine and meaningful. However, consent should remain a practical concept and should not be made unnecessarily complex through additional legal tests that do not address a clearly identified problem.

Existing privacy guidance describes valid consent as voluntary, informed, current, specific, and given by a person with capacity. Consent may be express or implied, although implied consent must arise clearly from the circumstances.

The exposure draft would codify and expand these concepts. Without careful drafting, this could require businesses to make fine legal distinctions about each interaction even where the consumer and business have a clear shared understanding of the requested service.

The legislation should clarify that:

- separate consent is not required for every data field or closely related step in a real estate transaction or tenancy process;
- consent does not expire merely because time has passed, unless the context or proposed use has materially changed;

- implied consent remains available where it is clear and unambiguous;
- evidence requirements must be proportionate to the risk and sensitivity of the activity; and
- information handling reasonably necessary to provide the requested real estate, leasing, or property management service should not depend on artificial or compelled consent.

Separate and specific consent is appropriate for genuinely optional activities, including:

- unrelated marketing;
- optional commercial referrals;
- trading in personal information;
- a platform's independent secondary uses;
- profiling unrelated to the requested service; and
- product development using identifiable customer information.

Regulator guidance should provide practical property-sector examples dealing with related purposes, re-consent, bundled workflows, referrals, platform services, and evidence of consent.

11. De-identification and aggregated property information

REIA supports de-identification as an important privacy protection. The applicable standard should be contextual, proportionate, and risk-based.

The consultation paper proposes a revised definition based on whether there is only a remote risk that an individual could be identified or reidentified, having regard to available information and practical steps.

This should not become a zero-risk test based on theoretical possibilities. Such a standard would be impractical and could discourage responsible de-identification.

The assessment should recognise:

- aggregation;
- suppression and generalisation;
- separation of identifying information;
- restricted access;
- secure data environments;

- contractual and governance controls;
- the purpose and likely recipients of the data; and
- the practical likelihood of reidentification.

Real estate institutes and other organisations may use appropriately de-identified or aggregated property information to understand market conditions, tenancy patterns, housing supply, and broader industry trends.

These activities can provide industry and public policy benefits without requiring access to identified personal information.

REIA does not seek a broad exemption from de-identification requirements. It recommends a workable standard that permits beneficial and low-risk uses while requiring reasonable safeguards against reidentification.

12. Existing records and transitional arrangements

The reforms should not impose retrospective liability for acts that were lawful when undertaken.

Businesses should not be required to obtain fresh consent for every existing record solely because the statutory definition of consent has changed.

Such a requirement would be costly, confusing for consumers, and impractical for historical property and customer records.

REIA recommends that:

- there be no liability for a pre-commencement collection, use, or disclosure that complied with the law at the time;
- existing consent remain effective for its original purpose unless the circumstances or proposed use materially change;
- new uses and disclosures after commencement comply with the new law; and
- data de-identified in good faith under the existing law receive transitional protection unless a material change or known reidentification risk arises.

The legislation should continue to recognise that records relating to a real estate sale, purchase, tenancy, or property management activity may need to be retained under legislation, contracts, professional obligations, limitation periods, litigation requirements, or electronic execution systems.

Information should not be destroyed where its retention is required or reasonably necessary for those purposes.

13. Access, erasure, and platform-held information

Access exception

REIA supports the proposed exception where giving access is technically impossible or technically infeasible, provided appropriate safeguards remain.

Erasure

The proposed erasure right would principally apply to large digital platforms rather than every real estate business.

Where a platform maintains its own applicant profile, analytics record, or marketing account, it should be responsible for responding to an erasure request concerning that information.

The right should remain subject to clear exceptions for records that must be retained under property, tenancy, financial, taxation, AML/CTF, professional, litigation, or other legal requirements.

14. Direct marketing

The reforms should distinguish between legitimate follow-up arising from a property enquiry and unrelated direct marketing.

An individual who asks about a property will ordinarily expect the agent to:

- respond to the enquiry;
- arrange an inspection;
- provide relevant property information; and
- communicate about closely related properties or steps in the requested real estate transaction or tenancy process.

These activities should not automatically be treated in the same way as unrelated or ongoing marketing.

Consumers should nevertheless receive a clear and simple way to opt out of ongoing marketing communications.

The Government should clarify the interaction between:

- the Privacy Act;
- the Spam Act;
- the Do Not Call Register;

- the fair and reasonable test; and
- the proposed trading-in-personal-information provisions.

15. Data breaches and the 72-hour notification period

REIA supports prompt action to contain data breaches, reduce harm, and provide affected individuals with useful information. However, the proposed 72-hour notification period must reflect the practical realities of investigating incidents involving multiple organisations and technology systems.

Under the current framework, an entity that has reasonable grounds to suspect an eligible data breach must undertake a reasonable and expeditious assessment, generally within 30 days. Once an entity has reasonable grounds to believe that an eligible data breach has occurred, notification must be made as soon as practicable.

The exposure draft would retain the assessment requirement but introduce a fixed requirement to notify the privacy regulator within 72 hours after the entity becomes aware of reasonable grounds to believe that an eligible data breach has occurred.

The 72-hour period does not commence merely because an entity receives an unverified technical alert or first suspects that a breach may have occurred. Nevertheless, the distinction between suspicion and reasonable grounds for belief may be difficult to apply during a developing incident.

Real estate agencies commonly rely on:

- property management and rental application platforms;
- franchise and corporate systems;
- CRM and forms providers;
- identity verification services;
- Digital ID and financial verification providers;
- cloud and email services; and
- external information security providers.

An agency may initially know only that a system is unavailable, suspicious activity has occurred, or a provider is investigating an incident. It may not have access to the technical logs or forensic evidence needed to determine:

- whether personal information was accessed or disclosed;
- which agencies, systems, or records were affected;
- which individuals are at risk;

- the categories of information involved;
- whether serious harm is likely;
- whether the incident has been contained; or
- what protective action affected individuals should take.

This is particularly problematic where a large platform holds information on behalf of hundreds of agencies. Individual agencies may receive incomplete or changing information from the provider while being expected to assess their own notification obligations.

The exposure draft would permit an incomplete initial statement where providing complete information within 72 hours is impossible or impracticable. However, the entity must identify what is missing, explain the omission, provide outstanding information as soon as practicable, and correct subsequent material changes or errors.

Staged notification is sensible, but it may still result in premature, inconsistent, or duplicative communications. Consumers may receive several notices about the same platform incident from the platform, individual agencies, franchise groups, identity providers, and other participants.

The Privacy Commissioner has acknowledged that it may take an organisation many months to understand the full cause of a breach, even though enough information may be available earlier to determine that notification is required. The legislation should therefore distinguish clearly between an initial notification intended to enable early protective action and the completion of a full forensic investigation.⁵

REIA recommends that the Government not proceed with the proposed fixed 72-hour notification period. Instead, the Government should retain the existing requirement to notify the privacy regulator and affected individuals as soon as practicable after an entity has reasonable grounds to believe that an eligible data breach has occurred. If the Government proceeds with a fixed notification period, provide appropriate extensions for complex and third-party incidents, protect good-faith preliminary notifications, impose rapid platform-to-agency notification and cooperation obligations, and facilitate coordinated notification where multiple entities are affected by the same breach.

The objective should be early and useful notification, rather than speculative reporting that diverts resources from containment or leaves affected individuals with incomplete and confusing information.

⁵ Carly Kind, Privacy Commissioner, evidence to the Joint Committee of Public Accounts and Audit, *Inquiry into the Management of Client Privacy in the Australian Public Sector*, Proof Committee Hansard (29 July 2026), 10.

16. Implementation and regulatory guidance

The reforms should not commence until businesses have received final legislation, an explanatory memorandum, final regulator guidance, and sufficient time to update systems, processes, and contracts.

REIA recommends:

- at least 24 months between passage and substantive commencement;
- final general and sector-specific regulator guidance at least 12 months before commencement;
- consultation on rental application guidance with state and territory regulators;
- specific guidance for data suppliers and purchasers concerning consent evidence, reliance on supplier evidence, referrals, and the small-business safe harbour;
- model contractual clauses for controllers, processors, suppliers, and purchasers; and
- practical examples for real estate businesses.

REIA's experience with AML/CTF implementation demonstrates that sector guidance issued with approximately six months remaining before commencement provides an extremely tight implementation period.

Privacy reform should avoid repeating that approach.

Guidance must supplement clear statutory protections. It should not be used as a substitute for addressing foreseeable power imbalances and liability issues in the legislation.

Conclusion

REIA supports effective privacy protections and recognises their importance to consumer trust. The reforms must, however, reflect the operating environment of real estate businesses.

Agencies are already managing a substantial and growing regulatory burden across federal, state, and territory frameworks. The retention of the small-business exemption is welcome, but that exemption must remain meaningful.

REIA does not support the proposed trading-in-personal-information provisions in their current form. They could expose small agencies to *Privacy Act* obligations because of consent and disclosure processes controlled by larger commercial data suppliers.

If the provisions proceed, the legislation should place the primary evidentiary obligation on entities whose primary business activity is trading in personal information. Those entities should be required to obtain, retain, substantiate, and provide evidence of the authority relied upon to disclose the information.

A small-business purchaser should be able to rely on that evidence unless it knows, or could reasonably be expected to know, that the evidence is false or the disclosure is unlawful. The legislation should not require an ordinary agency to conduct a separate legal audit of a process controlled by a larger supplier.

The framework must also avoid capturing small agencies that incidentally share information through genuine referrals, franchise networks, inter-agency cooperation, or other ordinary activities reasonably connected with a real estate transaction or tenancy process.

Any loss of the small-business exemption should remain limited to the relevant data-handling activity unless the conduct is knowing, reckless, repeated, or systemic.

Similar power imbalances arise under the proposed controller and processor framework. Large technology platforms should not be able to shift responsibility to small agencies while retaining practical control over data fields, interfaces, consent architecture, applicant profiles, retention, marketing, analytics, and product development.

Responsibility must follow actual control, conduct, and commercial benefit.

Activity-specific *Privacy Act* coverage arising from AML/CTF obligations must remain activity-specific. It should not become a basis for treating an otherwise exempt small business as an APP entity or controller for unrelated information handling.

REIA also remains concerned about the proposed fair and reasonable test. Without clearer statutory boundaries, it could impose an uncertain assessment above lawfulness and duplicate state and territory regulation.

Rental application processes require particular care, coordinated regulator guidance, and recognition of the information reasonably required to make sound and equitable tenancy decisions.

Digital ID and Consumer Data Right solutions offer a practical pathway to reducing unnecessary document collection while preserving reliable identity and financial-capacity checks. The Government should invest in the national implementation of these technologies alongside the legislative reforms.

These issues should be addressed in the legislation and not left solely to guidance.

The Government should release a complete bill, explanatory memorandum, transitional provisions, and regulatory impact analysis for further consultation. Final regulator and sector-specific guidance should be available at least 12 months before substantive commencement.

With these changes, the reforms can strengthen privacy protection without imposing disproportionate liability on businesses or undermining the effective operation of Australia's property market.



**OVER 100 YEARS OF SERVING
THE REAL ESTATE INDUSTRY**