# PRIVACY POLICY

**Residence Pty Ltd trading as Residence**
ABN 81 079 342 939
NSW Corporation Licence No. 972 646
119 Willoughby Rd, Crows Nest NSW 2065

**Licensee in Charge:** Richard Damian Rawle
**Licence No.:** 883 993

**Version:** 2.0
**Effective date:** 14 August 2026
**Document owner:** Licensee in Charge

---

## 1. Purpose

Residence Pty Ltd trading as Residence ("Residence", "we", "us" or "our") is committed to protecting the privacy, confidentiality and security of personal information entrusted to us.

This Privacy Policy explains how Residence collects, holds, uses, discloses, protects, accesses, corrects and disposes of personal information.

Residence handles personal information in accordance with applicable privacy legislation, including the **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)** where they apply.

From 1 July 2026, certain real estate services are regulated under the **Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act)**. Residence's handling of personal information in connection with its AML/CTF obligations is subject to the Privacy Act and APPs.

This Policy should be read with Residence's:

- Supervision Guidelines;
- Operational Procedures Manual;
- AML/CTF Program;
- Customer Due Diligence procedures;
- Data Breach Response Procedure;

- Information Security procedures; and
- records retention requirements.

---

## 2. Scope

This Policy applies to personal information handled by Residence concerning individuals including:

- vendors;
- purchasers and prospective purchasers;
- landlords and tenants, if applicable;
- prospective clients;
- customers;
- bidders;
- property owners;
- beneficial owners;
- company directors and officeholders;
- trustees and beneficiaries where relevant;
- persons acting for or on behalf of customers;
- employees and contractors;
- suppliers and service providers;
- professional advisers;
- persons making enquiries or complaints; and
- other individuals with whom Residence deals in conducting its business.

---

## 3. What is Personal Information?

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Depending upon the circumstances, information collected by Residence may include:

### Identification and contact information

- full name;

- residential and postal address;
- telephone number;
- email address;
- date of birth;
- occupation;
- signature;
- previous names;
- nationality or country of residence where relevant;
- government-issued identification details; and
- information necessary to verify an individual's identity.

## Property and transaction information

- property ownership information;
- property address;
- purchase or sale information;
- offers and negotiations;
- agency agreements;
- contracts and transaction documentation;
- inspection and enquiry history;
- property preferences;
- settlement information;
- tenancy information where applicable; and
- communications with Residence.

## Financial information

Where reasonably necessary, Residence may collect:

- bank account details;
- deposit information;
- payment information;
- trust-account transaction information;
- source-of-funds information;
- source-of-wealth information where required;
- financial capacity information provided in connection with a transaction; and
- other financial information necessary for a transaction or regulatory requirement.

## 4. AML/CTF Information

From 1 July 2026, Residence may be required to collect additional information to comply with the AML/CTF Act and AML/CTF Rules.

Depending upon the customer, transaction and assessed money-laundering or terrorism-financing risk, this may include information necessary to:

- establish and verify a customer's identity;
- identify and verify beneficial owners;
- identify persons acting on behalf of a customer;
- establish a person's authority to act;
- understand the nature and purpose of the business relationship;
- assess money-laundering and terrorism-financing risk;
- conduct ongoing customer due diligence;
- conduct enhanced customer due diligence;
- understand the source of funds or source of wealth where required;
- identify politically exposed persons where applicable;
- identify relevant geographic or jurisdictional risks;
- monitor transactions and customer behaviour;
- investigate unusual or suspicious activity; and
- comply with reporting and record-keeping obligations.

Residence may obtain identification information from documents including passports, driver licences and other government-issued identification.

Residence may also use electronic identity-verification services.

---

## 5. Minimisation of Identification Documents

Residence recognises that identity documents such as passports and driver licences contain sensitive and valuable personal information and create increased privacy and identity-fraud risks if unnecessarily retained.

Accordingly, Residence will seek to collect and retain **only the personal information reasonably necessary** for its functions and legal obligations.

Where an identification document is sighted or electronically verified for AML/CTF purposes, Residence will generally record information necessary to demonstrate compliance, which may include:

- the person's name;
- date of birth;
- residential address;
- type of identification document;
- issuing authority or country;
- document number where required;
- expiry date where relevant;
- date the document was sighted or verified;
- method of verification;
- verification result; and
- other information required by applicable AML/CTF obligations.

Residence will not routinely retain a complete scanned or photocopied passport, driver licence or other identification document merely because the document was used for AML/CTF verification.

Where a complete copy has been obtained, Residence will take reasonable steps to securely destroy or de-identify it when the copy is no longer reasonably required for an authorised purpose.

A copy may be retained where Residence is required or authorised to retain it for another legitimate legal or business purpose.

---

## 6. How We Collect Personal Information

Residence generally collects personal information directly from the individual concerned.

Information may be collected:

- in person;
- by telephone;
- by email;
- through our website;

- through property portals;
- through online enquiry forms;
- through agency agreements;
- during property inspections;
- during negotiations;
- through contracts and transaction documentation;
- through identity-verification processes;
- through electronic signature systems;
- through our CRM;
- through AML/CTF customer due diligence procedures; and
- through other communications with Residence.

Where permitted or required, information may also be obtained from third parties including:

- solicitors and conveyancers;
- accountants;
- mortgage brokers and financial institutions;
- government bodies and public registers;
- strata managers;
- property-data providers;
- identity-verification providers;
- credit reporting bodies where legally permitted;
- companies and beneficial ownership records;
- authorised representatives;
- other real estate agents;
- fraud-prevention services; and
- AML/CTF screening and verification providers.

---

## 7. Why Residence Collects Personal Information

Residence may collect, hold, use and disclose personal information for purposes including:

- providing real estate agency services;
- appraising, listing, marketing, selling, leasing or managing property;

- communicating with clients and customers;
- arranging inspections and open homes;
- receiving and communicating offers;
- negotiating transactions;
- preparing and administering agency agreements;
- facilitating contracts and settlements;
- administering deposits and trust money;
- maintaining transaction records;
- verifying instructions;
- preventing fraud and identity theft;
- managing complaints and disputes;
- maintaining business and compliance records;
- complying with NSW real estate legislation;
- complying with taxation and accounting obligations;
- complying with AML/CTF obligations;
- customer due diligence;
- ongoing customer monitoring;
- assessing money-laundering and terrorism-financing risk;
- detecting and investigating suspicious activity;
- making reports required by law;
- responding to regulators and law-enforcement authorities;
- maintaining information and cybersecurity;
- training and supervising personnel; and
- establishing, exercising or defending legal rights.

Residence will not collect personal information merely because it may be useful at some future time.

---

## 8. AML/CTF Customer Due Diligence

Residence may be legally required to verify a customer’s identity before providing particular services.

Depending on the circumstances, Residence may need to obtain information about:

- the customer;
- beneficial owners;
- directors;
- trustees;
- beneficiaries;
- partners;
- persons acting on behalf of the customer;
- persons on whose behalf a transaction is conducted; and
- other persons relevant to the customer due diligence process.

The extent of customer due diligence may vary according to the assessed risk.

Higher-risk circumstances may require Residence to obtain and verify additional information.

If Residence cannot satisfactorily complete customer due diligence, Residence may be unable to commence or continue providing a particular service and may be required to take other action under the AML/CTF Act.

---

## 9. Electronic Identity Verification

Residence may use a third-party electronic identity-verification provider to verify customer identity and perform AML/CTF screening.

This may involve providing identification information to the verification provider and comparing it against government, commercial or other reliable and independent data sources.

Where permitted by law, identity verification may include matching information such as:

- name;
- residential address; and
- date of birth.

Residence will take reasonable steps to ensure that service providers handling personal information have appropriate privacy, confidentiality and information-security arrangements.

Where required, Residence will provide an appropriate privacy collection notice before undertaking electronic verification.

---

## 10. AML/CTF Monitoring

Residence may be required to undertake ongoing customer due diligence and transaction monitoring.

This may involve reviewing existing personal information and obtaining additional information where:

- circumstances change;
- information appears inconsistent;
- a transaction is unusual;
- ownership or control changes;
- payment arrangements change;
- information requires updating;
- the customer's risk classification changes; or
- additional due diligence is required by law.

---

## 11. Disclosure of Personal Information

Residence may disclose personal information where reasonably necessary to conduct its business or comply with the law.

Recipients may include:

- vendors and purchasers;
- landlords and tenants where applicable;
- solicitors and conveyancers;
- accountants and auditors;
- mortgage brokers;
- financial institutions;
- strata managers;
- valuers;
- tradespeople and contractors;

- property portals;
- photographers and marketing providers;
- CRM and software providers;
- electronic signature providers;
- cloud-storage and IT providers;
- identity-verification providers;
- AML/CTF screening providers;
- insurers and insurance advisers;
- professional advisers;
- government agencies;
- courts and tribunals;
- regulators;
- law-enforcement agencies; and
- other parties where authorised or required by law.

Residence does not sell personal information.

---

## 12. Disclosure to AUSTRAC and Other Authorities

Residence may be required or authorised to disclose personal information to the **Australian Transaction Reports and Analysis Centre (AUSTRAC)** under the AML/CTF Act.

Residence may also be required or authorised to disclose information to other regulators, government bodies or law-enforcement agencies.

In some circumstances, the law may prohibit Residence from informing an individual that particular information has been disclosed or that certain AML/CTF action has been taken.

Nothing in this Privacy Policy requires Residence to provide information where doing so would contravene the AML/CTF Act, including applicable restrictions concerning disclosure of suspicious-matter information.

---

## 13. Consequences of Not Providing Information

Individuals are generally free to decide whether to provide requested personal information.

However, if information required by law or reasonably required to provide our services is not provided, Residence may be unable to:

- verify identity;
- establish authority to act;
- complete customer due diligence;
- enter into an agency agreement;
- accept instructions;
- receive or release funds;
- proceed with a property transaction; or
- provide some or all requested services.

Where AML/CTF requirements apply, Residence may be legally prohibited from providing a designated service until required customer due diligence has been completed.

---

## 14. Marketing

Residence may use personal information to communicate with individuals concerning:

- properties;
- market information;
- property appraisals;
- real estate services; and
- other information reasonably connected with our business.

Individuals may request that Residence stop sending direct marketing communications at any time.

Marketing preferences do not affect communications that Residence is required to send concerning an existing transaction, contract, legal obligation or regulatory requirement.

## 15. Security of Personal Information

Residence takes reasonable steps to protect personal information from:

- misuse;
- interference;
- loss;
- unauthorised access;
- unauthorised modification; and
- unauthorised disclosure.

Controls may include:

- role-based system access;
- individual user accounts;
- password controls;
- multi-factor authentication where available;
- secure cloud systems;
- encryption where appropriate;
- staff privacy and cybersecurity training;
- controlled access to identity information;
- secure document transfer;
- system backups;
- malware and cybersecurity protection;
- monitoring of user access;
- secure disposal procedures; and
- incident-response procedures.

Employees and contractors must not store confidential customer information or identification documents on unauthorised personal devices, personal email accounts or unapproved cloud-storage services.

# 16. Data Breaches

Residence maintains procedures for responding to suspected loss, unauthorised access or disclosure of personal information.

Where a suspected data breach occurs, Residence will:

1. contain the breach where practicable;
2. assess what information is affected;
3. determine the individuals potentially affected;
4. assess the risk of serious harm;
5. take remedial action;
6. document the incident; and
7. make notifications required under the Privacy Act, including the Notifiable Data Breaches scheme, where applicable.

Residence may also notify other regulators or authorities where required.

---

# 17. Retention of Personal Information

Residence retains personal information only for as long as reasonably required for:

- the purpose for which it was collected;
- provision of agency services;
- legal and regulatory requirements;
- trust-account obligations;
- taxation and accounting requirements;
- AML/CTF requirements;
- insurance;
- complaints or disputes;
- litigation or anticipated litigation; or
- another permitted purpose.

Different categories of information may have different retention periods.

AML/CTF records will be retained for the period required under the AML/CTF Act and AML/CTF Rules.

Importantly, the obligation to retain an AML/CTF compliance record does not necessarily mean that Residence must retain a complete copy of the underlying identity document.

Where Residence no longer requires personal information and is not legally required or authorised to retain it, Residence will take reasonable steps to destroy or permanently de-identify it.

---

## 18. Overseas Disclosure

Some technology, cloud, software, identity-verification or other service providers used by Residence may process or store information outside Australia.

Before using such providers, Residence will take reasonable steps appropriate to the circumstances to assess privacy and information-security arrangements.

Where the Australian Privacy Principles require Residence to identify countries in which overseas recipients are likely to be located, this information will be included in the relevant collection notice or this Policy once those arrangements are identified.

Residence’s AML/CTF Collection Notice should identify any material overseas disclosures arising from its chosen identity-verification or AML screening provider.

---

## 19. Accuracy and Correction

Residence takes reasonable steps to ensure that personal information it holds is accurate, up to date, complete and relevant.

Individuals should notify Residence if their personal information changes or if they believe information held by Residence is inaccurate.

Residence will take reasonable steps to correct personal information where appropriate.

---

## 20. Access to Personal Information

An individual may request access to personal information Residence holds about them.

Residence will respond within a reasonable period and will generally provide access unless an exception under applicable law applies.

Residence may need to verify the identity of the person requesting access before releasing information.

There may be circumstances in which Residence cannot provide access to some information, including where disclosure:

- would affect another person’s privacy;
- would prejudice an investigation;
- is prohibited by law;
- relates to legal proceedings;
- would reveal commercially sensitive information; or
- would contravene restrictions under the AML/CTF Act.

Where access is refused, Residence will generally provide reasons where it is lawful and appropriate to do so.

---

## 21. Privacy Complaints

An individual who believes Residence has mishandled their personal information may make a privacy complaint.

Complaints should be directed to:

**Privacy Officer / Licensee in Charge**
Residence Pty Ltd trading as Residence
119 Willoughby Rd
Crows Nest NSW 2065

Residence will:

- acknowledge the complaint;
- investigate it appropriately;

- seek further information if required; and
- provide a response within a reasonable period.

Residence aims to respond to privacy complaints within **30 days**.

If an individual is dissatisfied with Residence's response, they may be entitled to complain to the **Office of the Australian Information Commissioner (OAIC)**.

---

## 22. AML/CTF Privacy Collection Notices

This Privacy Policy provides general information about Residence's handling of personal information.

Where Residence collects personal information for customer due diligence or another AML/CTF purpose, Residence may also provide a specific **AML/CTF Privacy Collection Notice** explaining:

- what information is being collected;
- why it is being collected;
- the legal authority for collection;
- consequences of not providing it;
- relevant third-party disclosures;
- possible disclosure to AUSTRAC;
- overseas disclosures where applicable; and
- how the individual can access or correct their information.

A collection notice may not contain information that Residence is prohibited from disclosing under the AML/CTF Act.

---

## 23. Automated Decision-Making

Residence will review this Policy before **10 December 2026** to determine whether any computer program used by Residence uses personal information to make decisions that could reasonably be expected to significantly affect an individual's rights or interests.

If Residence uses automated decision-making of that kind, this Policy will be updated to provide the information required by the Privacy Act.

Ordinary use of software, CRM systems, identity-verification tools or risk-screening tools does not remove the responsibility of Residence personnel to comply with Residence's legal and supervisory obligations.

---

## 24. Staff and Contractor Obligations

All Residence personnel who handle personal information must:

- comply with this Policy;
- complete required privacy and AML/CTF training;
- access information only when required for their duties;
- maintain confidentiality;
- follow approved identity-verification procedures;
- use only approved systems;
- immediately report suspected privacy or security incidents;
- follow records-retention and destruction requirements; and
- comply with instructions from the Licensee in Charge.

A serious or deliberate breach of this Policy may result in disciplinary action, termination of access or engagement, and regulatory or legal consequences.

---

## 25. Governance and Review

The Licensee in Charge is responsible for overseeing implementation of this Policy.

Residence will review the Policy:

- at least annually;
- following a material privacy or cybersecurity incident;
- when its AML/CTF Program materially changes;
- when a new technology or identity-verification provider materially changes information handling;

- when applicable privacy or AML/CTF legislation changes; and
- before 10 December 2026 in relation to the Privacy Act automated decision-making amendments.

The current version will be made available to clients and customers free of charge, including through Residence's website where appropriate.

---

# 26. Contact

Questions, requests for access or correction, and privacy complaints should be directed to:

**Privacy Officer / Licensee in Charge**
**Richard Damian Rawle**
Residence Pty Ltd trading as Residence
119 Willoughby Rd
Crows Nest NSW 2065

---

## Document Approval

**Document:** Residence Privacy Policy
**Version:** 2.0
**Effective:** 14 August 2026

**Approved by:** Richard Damian Rawle
**Position:** Licensee in Charge
**Licence No.:** 883 993

Signature: ___ Richard Rawle ____________________________

Date: _______________14 August 2026___________________

---

## Document Review Record

| Version | Date | Change | Approved by | Next Review |
|---|---|---|---|---|
| 2.0 | 14 August 2026 | New Privacy Policy incorporating AML/CTF obligations commencing 1 July 2026 | Richard Damian Rawle | 14 August 2027 or earlier following legislative change |