AML/CFT customer due diligence and privacy notice

Last updated: 4 June 2026

Who is collecting and holding your information:

Della Realty Group Limited, 203 Rosetta Road, Raumati South, Paraparaumu 5032 / care@dellarandall.co.nz

Privacy contact: Carmen Elliott / +64 4 9027708

AML service provider: AMLHUB Ltd, acting on behalf of *Della Realty Group Limited*

1. Why we need this information

Della Realty Group Limited is required to comply with New Zealand anti-money laundering and countering financing of terrorism laws, including the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 and related regulations.

To meet these obligations, we need to collect and verify information about our customers and, where relevant, other people connected with a customer or transaction. This may include beneficial owners, directors, trustees, settlors, beneficiaries, attorneys, authorised representatives, people acting on behalf of a customer, and other individuals whose information is relevant to our AML/CFT checks.

This notice explains how we collect, use, verify, share, store, and retain personal information for AML/CFT purposes. It applies whether we collect information directly from you or indirectly from another person or source.

2. Who this notice applies to

This notice applies to you if you are:

- a customer or prospective customer of *Della Realty Group Limited*;
- a beneficial owner of a customer;
- a director, shareholder, partner, trustee, settlor, protector, beneficiary, or other controller of a customer;
- a person acting on behalf of a customer, including under a power of attorney or other authority;
- a person whose identity, role, ownership interest, source of funds, source of wealth, authority, or relationship to a customer or transaction needs to be checked for AML/CFT purposes.

In this notice, “you” means any of the people listed above.

3. What information we may collect

We collect only the information we reasonably need for AML/CFT checks, verification, screening, risk assessment, record keeping, audit, and legal compliance.

Depending on the customer, transaction, and level of risk, this may include:

Identity and contact information

- full name;
- date of birth;
- residential address, registered office, or other relevant address;
- phone number, email address, and other contact details;
- nationality, citizenship, residency, or tax residency information where relevant;
- relationship to the customer or transaction;
- role, authority, ownership, control, or beneficial ownership information.

Identity documents and verification information

- copies or details of passports, driver licences, birth certificates, certificates of incorporation, trust deeds, company records, authority documents,
- or other identification and verification documents;
- document numbers, issue and expiry dates, issuing country or authority;
- results of electronic identity verification checks;
- records showing how your identity or authority was verified.

Biometric or liveness information, where electronic identity verification is used

Where we use electronic identity verification, we may ask you to provide a live selfie, video, or similar liveness check so your identity document can be matched to you and to help prevent impersonation or fraud.

This may involve the collection and processing of facial images, liveness results, facial matching results, and related verification information by our identity verification provider. If you cannot or do not wish to complete a liveness or facial matching check, contact us to discuss whether an alternative verification method is available.

Screening and risk information

- politically exposed person, or PEP, status;
- sanctions, watchlist, adverse media, and other screening results;
- country, geographic, transaction, customer type, product/service, delivery channel, and other AML/CFT risk factors;
- information needed to assess whether enhanced due diligence is required.

Source of funds and source of wealth information

Where enhanced due diligence is required, we may collect information about your source of funds and/or source of wealth. This may include:

- bank statements;
- sale and purchase agreements;
- loan or mortgage documents;
- inheritance documents;
- trust, company, or partnership records;
- pay slips or employment records;
- accounting, tax, or financial statements;
- gift declarations;
- evidence of savings, investments, business income, asset sales, or other sources of wealth;
- other documents or explanations reasonably needed to understand where funds or wealth have come from.

Transaction and relationship information

- information about the nature and purpose of the business relationship or transaction;
- property, transaction, and settlement information;
- information about related parties;
- records of communications, checks, risk assessments, decisions, and reviews.

4. Where we may collect information from

We may collect information directly from you. We may also collect information indirectly from other people or sources, including:

- the customer, prospective customer, or their representatives;
- beneficial owners, directors, trustees, settlors, beneficiaries, attorneys, authorised representatives, or people connected with the customer;
- lawyers, conveyancers, accountants, mortgage advisers, banks, financial institutions, or other professional advisers involved in the transaction;
- Companies Office, NZBN, LINZ/property records, and other public registers;
- identity verification providers;
- address verification providers;
- credit reporting or electronic verification sources, where used for identity or address verification;
- sanctions, PEP, watchlist, and adverse media screening providers;
- government-issued identity document verification sources;
- publicly available websites, media, and public records;
- AMLHUB Ltd and its approved sub-processors, acting on our behalf.

We may collect information indirectly because AML/CFT checks often require information about people other than the direct customer, such as beneficial owners or people acting on behalf of a customer.

5. How we use your information

We use your information to:

- identify and verify customers, beneficial owners, and people acting on behalf of customers;
- verify authority to act;
- carry out standard, simplified, enhanced, and ongoing customer due diligence;
- check PEP, sanctions, watchlist, and adverse media status;
- assess AML/CFT risk;
- understand source of funds and source of wealth where required;
- decide whether we can start, continue, or complete a business relationship or transaction;
- meet record keeping, audit, reporting, and regulatory obligations;
- protect against fraud, impersonation, money laundering, terrorism financing, and other unlawful activity;
- respond to lawful requests or requirements from regulators, supervisors, courts, or other authorities.

We do not sell AML/CFT information, and we do not use AML/CFT information for unrelated marketing.

6. What happens if information is not provided

If we cannot collect or verify the information we need, we may be unable to:

- complete AML/CFT checks;
- act for a customer;
- continue acting for a customer;
- proceed with a transaction;
- complete settlement or other requested services.

We may also need to take other steps required or permitted by law.

7. Who we may share information with

We may share your information where reasonably necessary for AML/CFT checks, verification, screening, legal compliance, audit, security, or related business purposes.

This may include sharing information with:

- AMLHUB Ltd, which provides AML/CFT software and services to us;
- identity verification, biometric/liveness, address verification, PEP, sanctions, watchlist, and adverse media screening providers;
- secure cloud hosting, storage, support, monitoring, and technology providers;
- our professional advisers, auditors, insurers, and legal advisers;
- parties involved in a transaction where sharing is necessary to complete or manage the transaction;
- AML/CFT supervisors, regulators, courts, government agencies, or other authorities where legally required or permitted.

AMLHUB Ltd processes AML/CFT information on our behalf. AMLHUB Ltd is not our privacy contact. Please contact *Della Realty Group Limited* using the details at the top of this notice.

8. AMLHUB Ltd and sub-processors

We use AMLHUB Ltd to help us collect, verify, screen, manage, and store AML/CFT information. AMLHUB Ltd acts on our behalf and must only process personal information for authorised AML/CFT service purposes.

AMLHUB Ltd may use approved sub-processors to provide parts of the AML/CFT service, such as identity verification, liveness checks, sanctions/PEP/adverse media screening, address verification, hosting, storage, security, support, and system monitoring.

Current sub-processor information is available at: amlhub.co.nz/sub-processors

We may update this list from time to time. The current list will identify the relevant provider or provider category, purpose, location, and the type of information processed.

9. Overseas storage and processing

AML/CFT information is stored in Australia. Some service providers or sub-processors may process or access information from other countries, including the United States and the European Union.

Where information is stored, processed, or accessed outside New Zealand, we take steps designed to ensure that appropriate privacy, confidentiality, and security safeguards apply.

10. Security

We take reasonable steps to protect AML/CFT information from loss, unauthorised access, misuse, disclosure, alteration, and destruction.
Those steps may include access controls, audit logs, encryption, secure hosting, staff training, contractual protections, and controls over service providers and sub-processors.

11. How long we keep information

We keep AML/CFT records for as long as required for AML/CFT compliance, audit, regulatory, legal, dispute, insurance, and business record purposes.
In general, AML/CFT identity and verification records must be kept for at least five years after the end of the business relationship or after completion of the relevant occasional transaction or activity. We may keep information longer where required or permitted by law, or where reasonably necessary for audit, regulatory, legal, dispute, insurance, or compliance purposes.

12. Your access and correction rights

You have the right to ask us for access to personal information we hold about you. You can also ask us to correct it if you think it is wrong.
To request access or correction, contact:
Della Realty Group Limited
Email: homes@dellarandall.co.nz
Phone: +64 4 9027708
Address: 203 Rosetta Road, Raumati South, Paraparaumu 5032

In some cases, the law may allow or require us to withhold information or limit what we can say about certain compliance matters. We will respond to access and correction requests in accordance with the Privacy Act 2020.

13. If you provide information about someone else

If you provide us with personal information about another person, you must take reasonable steps to make sure that person is aware of this notice.
This includes, where relevant, beneficial owners, directors, shareholders, trustees, settlors, beneficiaries, attorneys, authorised representatives, people acting on behalf of a customer, and anyone else whose information you provide for AML/CFT purposes.
You should give them a copy of this notice.
You must also make sure you have the authority to provide their information where authority is required. If you cannot make another person aware of this notice, please tell us.

14. Questions or complaints

For questions about this notice or how we handle AML/CFT information, contact:
Della Realty Group Limited
Email: homes@dellarandall.co.nz
Phone: +64 4 9027708
You can also contact the Office of the Privacy Commissioner if you have a privacy concern that we have not resolved.