

N1 Accounting Pty Ltd (ABN 13 169 557 162) | Effective 1 July 2026

Privacy contact	Penny He
Email	pennyhe@n1accounting.com.au
Telephone	02 9262 1295

1. About this policy

N1 Accounting Pty Ltd (N1 Accounting, we, us or our) is an Australian accounting practice and registered tax agent (#24765522). We are also enrolled with AUSTRAC and may provide designated services regulated by the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act).

This policy explains how we collect, hold, use and disclose personal information under the Privacy Act 1988, the Australian Privacy Principles (APPs), the Tax File Number Rule, the AML/CTF Act and other applicable laws. It applies to clients, prospective clients, representatives, beneficial owners, suppliers, website visitors, job applicants and other individuals whose information we handle.

This policy is available free of charge on our website and in another reasonable form on request. It should be read with any collection notice, engagement terms or consent presented when information is collected.

2. Personal information we collect

The kinds of information we collect depend on our relationship with you and the services requested. They may include:

- identity and contact information, including name, date of birth, address, telephone number, email, signature and photographs;
- government identifiers and identity documents, including tax file number, ABN, passport, driver licence, Medicare or other identification details, where lawful and necessary;
- taxation, accounting and financial information, including income, assets, liabilities, bank details, investments, superannuation, employment, transactions and tax records;
- business, trust, company, partnership and beneficial ownership information, including details of directors, shareholders, trustees, appointors, beneficiaries, partners and authorised representatives;
- AML/CTF information, including identity-verification results, politically exposed person and sanctions screening, source of funds, source of wealth, transaction purpose, risk assessments and information relevant to regulatory reporting;
- sensitive information where relevant and lawful, including biometric information used for automated biometric verification, criminal history, citizenship or immigration information, racial or ethnic origin inferred from identity documents, and health information relevant to taxation or service delivery;
- technical and online information, including IP address, device and browser information, login and audit records, website interactions, cookies and approximate or precise geolocation where enabled and notified;
- communications, instructions, consents, complaints, call notes and records of our professional relationship;
- payment and billing information processed through us or payment providers if applicable; and
- employment or contractor information for staff, contractors and applicants.

We do not adopt government identifiers as our own identifiers. We use and disclose them only where permitted by law.

3. How we collect information

We usually collect personal information directly from you through meetings, telephone calls, email, our website, online forms, portals, questionnaires, identity-verification processes and documents you provide. Website-form submissions are delivered to our Google environment.

We may also collect information from your authorised representative, employer, spouse or family member, related entities, previous adviser, banks and financial institutions, government agencies and registers, the ATO and other revenue authorities, ASIC, AUSTRAC, credit-reporting or screening databases, publicly available sources, referrals, and service providers acting for us.

Identity information may be collected through an authorised provider. Depending on the verification method selected, the provider may collect or generate identity-document data, photographs or facial images, biometric verification results, device data and geolocation data. A specific collection notice or consent may also be presented during that process.

Where lawful and practicable, you may deal with us anonymously or using a pseudonym. This is generally not practicable where we must identify you to provide tax-agent, accounting, company-formation, registered-office or AML/CTF-regulated services.

4. Why we collect, use and disclose information

We collect, hold, use and disclose personal information where reasonably necessary to:

- respond to enquiries, establish and administer our relationship and provide accounting, taxation, corporate secretarial and related professional services;
- verify identity and authority, identify beneficial owners, assess eligibility to act and manage conflicts and professional risk;
- comply with the AML/CTF Act, taxation laws, the Tax Agent Services Act 2009, professional standards, court orders, notices and other legal or regulatory obligations;
- conduct customer due diligence, ongoing monitoring, PEP and sanctions screening, fraud prevention and, where required or permitted, regulatory reporting;
- communicate with you, obtain approvals, lodge documents, deal with the ATO, ASIC, AUSTRAC and other authorities, and maintain engagement records;
- process invoices and payments, recover debts and manage insurance, legal claims, quality reviews, complaints and disputes;
- manage our systems, cybersecurity, data quality, business continuity, training and internal administration;
- engage and manage staff, contractors, suppliers and job applicants; and
- send service updates or direct marketing where permitted. You may opt out of marketing at any time.

If we cannot collect required information, we may be unable to verify identity, accept instructions, provide or continue a service, meet a deadline, or comply with law. We may not be permitted to explain some AML/CTF-related actions or disclosures.

5. Disclosure of personal information

We may disclose personal information, where appropriate, to:

- the ATO, ASIC, AUSTRAC, the Tax Practitioners Board, state revenue offices and other government, regulatory, law-enforcement or judicial bodies;
- your authorised representatives and other persons or entities involved in the engagement;
- banks, superannuation funds, auditors, lawyers, valuers, financial advisers and other professional advisers where authorised or legally permitted;
- technology, cloud, data-storage, communications, identity-verification, screening, payment, cybersecurity and document-management providers;
- our overseas contractors and outsourced accounting service providers, subject to contractual, confidentiality, security and access controls;
- CPA Australia or another authorised reviewer for professional standards or quality-review purposes;
- our insurers, legal advisers, debt-recovery providers and prospective purchasers or successors of our business, subject to appropriate safeguards; and
- other recipients with your consent or where required or authorised by law.

We do not sell personal information.

6. Service providers and overseas disclosures

We use cloud and technology systems such as Quickbooks, MYOB, Xero, Microsoft, Google, Dropbox. These providers may process or store information in Australia and in overseas locations used by their service and support infrastructure. Their own privacy terms may also apply to information they process as independent organisations.

We also use overseas-based dedicated service provider for accounting support. Personal information is therefore likely to be disclosed to recipients outside Australia. The countries or regions currently applicable are set out in the Schedule at the end of this policy and must be completed and maintained by us based on our actual contractor locations and provider arrangements.

Before disclosing personal information overseas, we take reasonable steps required by APP 8, which may include due diligence, contractual privacy and confidentiality obligations, restricted access, security controls and supervision. In some circumstances, an exception under the Privacy Act may apply. Overseas recipients may be subject to different privacy laws, and we may remain accountable for their handling of information as provided by law.

7. Sensitive information and biometric verification

We collect sensitive information only where reasonably necessary for our functions and with consent, or where another legal basis permits or requires collection. Biometric information may be collected where facial or document verification is selected. It is used for identity verification, fraud prevention, AML/CTF compliance and security.

We do not use biometric information for marketing. Access is restricted to authorised persons and providers. Retention depends on the verification method, provider settings and applicable law. Individuals should be offered a reasonable alternative verification method where required by law or where biometric consent is not provided, although this may take longer or require in-person or certified documentation.

8. Automated systems and decisions

We may arrange for computer programs to use personal information to perform or assist with identity and document verification, biometric matching, duplicate or anomaly detection, PEP and sanctions screening, fraud checks, transaction monitoring and AML/CTF risk assessment. Information used may include identity and document data, facial images or biometric results, contact details, beneficial ownership, transaction information, source-of-funds information, device data and geolocation data.

These systems may produce a verification result, match, alert, score or recommendation that is substantially and directly related to our decision to accept, delay, restrict or continue a service, request further information, or make a legally required report. Where practicable and lawful, significant adverse decisions are reviewed by an authorised person rather than made solely by a computer program. We may be unable to provide details where disclosure would compromise security or breach AML/CTF or other laws.

9. Direct marketing and cookies

We may use contact details to send information about our services where permitted by the Privacy Act and Spam Act 2003. You may opt out using the unsubscribe facility or by contacting us. We will action an opt-out request within a reasonable time.

Our website may use cookies and similar technologies for essential functions, security, preferences and analytics. Browser settings can restrict cookies, but some website functions may not operate correctly. Where required, we will provide a separate cookie notice or consent tool identifying the categories and providers used.

10. Data quality, security and retention

We take reasonable technical and organisational steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. Measures may include access controls, multifactor authentication, encryption, secure portals, logging, backups, staff training, confidentiality obligations, vendor due diligence and incident-response procedures. No system or transmission method is completely secure.

We retain personal information for as long as needed for the purpose collected and to meet taxation, tax-agent, AML/CTF, corporate, professional, insurance and limitation-period requirements. Different records have different statutory periods.

When information is no longer required, we take reasonable steps to destroy it securely or de-identify it, unless retention is required or authorised by law.

11. Access and correction

You may request access to personal information we hold about you or ask us to correct information that is inaccurate, out of date, incomplete, irrelevant or misleading. Contact the Privacy Officer using the details at the start of this policy. You do not need to use a particular form, although we may ask you to verify your identity and clarify the request.

We will respond within a reasonable period. We generally do not charge for making a request, but may charge reasonable access costs where permitted after giving notice. Access or correction may be refused or limited where permitted by law. If so, we will generally provide written reasons and available complaint mechanisms, unless it would be unlawful to do so.

12. Privacy complaints and data breaches

If you have a privacy concern or complaint, contact the Privacy Officer at admin@n1accounting.com.au or 02 7259 5637. Please describe the issue and the outcome sought. We will acknowledge the complaint, investigate it fairly and aim to respond within 30 days. We may contact you for further information.

If you are not satisfied after giving us a reasonable opportunity to respond, you may complain to the Office of the Australian Information Commissioner (OAIC) at <https://www.oaic.gov.au/privacy/privacy-complaints> or by telephone on 1300 363 992.

We maintain procedures to assess and respond to suspected data breaches. Where an eligible data breach is likely to result in serious harm and remedial action does not prevent that risk, we will notify affected individuals and the OAIC as required by the Notifiable Data Breaches scheme. Other regulators may also be notified where required.

13. Changes to this policy

We may update this policy to reflect changes in law, technology, providers and our information-handling practices. The current version will be published on our website with its effective date. We will take reasonable steps to communicate material changes where appropriate. We review this policy at least annually and when a material change occurs.