

This Privacy Policy explains how FinRep Advisory collects, holds, uses and discloses personal information in connection with its financial reporting, technical accounting, training and advisory services. It should be read together with our engagement documents and Standard Terms and Conditions.

1. Who we are

FinRep Advisory is the business name of Robert G Mackay ABN 52 122 123 521, Melbourne, Victoria, Australia (FinRep Advisory, we, us or our).

This Policy applies to personal information collected or handled by us when you interact with us as a client, prospective client, supplier, contractor, employee, website visitor, professional adviser, auditor, regulator, beneficial owner, director, officer, trustee, partner, authorised representative or other person connected with a client or engagement.

2. Legal and professional framework

We handle personal information in accordance with the Privacy Act 1988 (Cth), including the Australian Privacy Principles, to the extent those laws apply to us. We also handle personal information consistently with our professional and ethical obligations as a member of Chartered Accountants Australia and New Zealand and applicable APESB pronouncements, including APES 110 Code of Ethics for Professional Accountants, APES 305 Terms of Engagement, APES 320 Quality Management for Firms that provide Non-Assurance Services, APES 325 Risk Management for Firms and APES GN 30 Outsourced Services where relevant.

Where we provide, or may provide, a designated service under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act), we may also be required to collect, verify, use, disclose and retain personal information for customer due diligence, ongoing due diligence, enhanced due diligence, sanctions-related checks, risk assessment, reporting and record-keeping.

3. Kinds of personal information we collect

The kinds of personal information we may collect and hold depend on your relationship with us and the nature of the engagement. It may include:

- identity and contact details, including name, position, employer, business address, residential address, email address, telephone number and signature;
- business and professional information, including role, authority to instruct us, qualifications, employment details, company or trust relationships and communications with us;
- client and engagement information, including financial reporting information, accounting records, audit queries, board papers, accounting memoranda, working papers, calculations, draft reports and related correspondence that may contain personal information;
- tax, payment and billing information, including ABN, TFN where lawfully collected, bank account details, invoice information and payment history;
- identity verification and AML/CTF information, including date of birth, identification documents, beneficial ownership and control information, details of directors, officers, trustees, partners and authorised representatives, source of funds or source of wealth information and risk assessment records;
- website and technology information, including IP address, browser type, device information, cookies, usage logs and metadata where collected through our website or technology systems;
- sensitive information only where reasonably necessary for our functions or activities, required by law, or where you have consented. This may include professional membership information, health or accessibility information relevant to meetings or services, or identity documents containing sensitive information.

4. How we collect personal information

Where practicable, we collect personal information directly from you. We may also collect personal information from:

- clients, prospective clients, their officers, staff, auditors, accountants, lawyers, bankers, insurers and other advisers;
- public registers and publicly available sources, including ASIC, ABN Lookup, websites, professional directories and published reports;
- identity verification, sanctions screening, AML/CTF, credit, fraud prevention or electronic signing providers;

- technology platforms, cloud services, email systems, document management systems, AI-assisted tools and analytics tools used in connection with our services;
- government agencies, regulators, courts, tribunals, professional bodies or law enforcement bodies where lawful and relevant.

If you provide us with personal information about another individual, you must take reasonable steps to ensure that you are authorised to do so and, where required, that the individual is aware of this Policy.

5. Why we collect, hold, use and disclose personal information

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

- assessing whether to accept or continue a client relationship or engagement;
- providing financial reporting, technical accounting, compilation, training and advisory services;
- communicating with you and managing client relationships;
- verifying identity, authority, beneficial ownership and control for AML/CTF, sanctions, fraud prevention and risk management purposes;
- preparing workpapers, technical memoranda, financial reports, calculations, training materials, engagement documents, proposals and invoices;
- billing, payment processing, debt recovery, insurance, quality management, file review and internal administration;
- complying with law, professional standards, CA ANZ membership obligations, APESB pronouncements, court or tribunal orders, regulator requests and lawful notices;
- protecting our legal rights, managing disputes, complaints, conflicts of interest and professional indemnity matters;
- improving our services, systems and processes, including through quality reviews, research, analytics and de-identified analysis;
- sending service updates, technical updates or marketing communications where permitted by law. You may opt out of marketing communications at any time.

6. Anonymity and pseudonymity

You may deal with us anonymously or using a pseudonym where it is lawful and practicable. However, for most client engagements this will not be practicable because we need to identify the client, confirm authority to instruct us, manage conflicts, issue invoices, comply with professional obligations and, where relevant, complete AML/CTF customer due diligence.

7. AI-assisted tools, cloud services and outsourced service providers

We may use secure technology platforms, cloud services, outsourced service providers, software tools and AI-assisted tools to provide services, communicate, prepare documents, perform research, analyse data, manage records, administer our practice and improve our services.

Where we use AI-assisted tools or external technology providers, we take reasonable steps to limit unnecessary personal information, use de-identified or redacted information where practicable, select appropriate service providers, and apply confidentiality, security and access controls. We do not intentionally use client confidential information to train public AI models unless you have expressly agreed or the relevant service terms and safeguards are appropriate for the engagement.

Electronic communications, cloud processing and AI-assisted tools involve inherent risks, including unauthorised access, transmission error, service interruption, loss of confidentiality, inaccurate outputs and processing or support outside Australia. We use reasonable safeguards, but we cannot guarantee that electronic systems are error-free, uninterrupted or immune from cyber risk.

8. Disclosure of personal information

We do not sell, rent or trade personal information. We may disclose personal information where reasonably necessary for the purposes described in this Policy, including to:

- our staff, contractors, consultants, subcontractors and professional advisers;
- your representatives, auditors, accountants, lawyers, bankers, insurers, directors, officers or other persons you authorise or who are reasonably involved in the engagement;
- technology, cloud, email, hosting, document management, accounting, electronic signing, identity verification, AML/CTF, sanctions screening, payment, billing and data storage providers;
- CA ANZ, APESB or other professional bodies where required or appropriate for professional, ethical, disciplinary, quality management, complaints or membership purposes;

- regulators and government agencies, including AUSTRAC, OAIC, ATO, ASIC, law enforcement bodies, courts and tribunals, where required or permitted by law;
- insurers and legal advisers for professional indemnity, claims, dispute, risk management or legal purposes;
- a purchaser or prospective purchaser of all or part of our business, subject to appropriate confidentiality safeguards.

9. Overseas disclosure and storage

Some service providers we use may store, process, support or access information from locations outside Australia. This may include the United States, United Kingdom, European Union or European Economic Area, New Zealand, Singapore and other countries where our providers or their subprocessors operate.

Before disclosing personal information to an overseas recipient, we take reasonable steps in the circumstances to address applicable Privacy Act requirements, including by using reputable providers, contractual safeguards, security controls, access restrictions and due diligence appropriate to the nature of the information and the service.

10. Government identifiers, TFNs and sensitive information

We will only collect, use or disclose government-related identifiers, including TFNs, where permitted or required by law or where reasonably necessary for the engagement. We do not use government-related identifiers as our own identifier of an individual.

We collect sensitive information only where reasonably necessary for our functions or activities and where we have consent, or where collection is required or authorised by law. Sensitive information and identity documents are subject to heightened security and access controls.

11. Security of personal information

We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. These steps may include:

- restricting access to personal information to people who need access for legitimate purposes;
- using secure cloud services, password protection, multi-factor authentication, encryption where practicable, backups, anti-malware tools and access controls;
- maintaining confidentiality obligations with staff, contractors and service providers;
- using document management, file naming, retention and deletion practices designed to reduce unnecessary exposure;
- training and awareness appropriate to our size, services and risk profile;
- reviewing and responding to suspected data breaches, including under the Notifiable Data Breaches scheme where applicable.

12. Notifiable Data Breaches

If we become aware of a suspected data breach involving personal information, we will assess and respond to it in accordance with our legal obligations and internal procedures. Where the Privacy Act requires notification of an eligible data breach, we will notify affected individuals and the Office of the Australian Information Commissioner as required.

13. Retention, destruction and de-identification

We retain personal information for as long as reasonably required for the purposes for which it was collected, including providing services, maintaining engagement records and working papers, complying with legal, tax, AML/CTF, professional, insurance and dispute-management obligations, and managing our business.

Where we no longer need personal information for a lawful purpose, we will take reasonable steps to destroy it or de-identify it, unless we are required or permitted by law, a court or tribunal order, professional standards, insurance requirements or our legitimate business needs to retain it.

AML/CTF records, where applicable, may need to be retained for at least seven years or for another period required by law.

14. Access to personal information

You may request access to personal information we hold about you by contacting the Privacy Officer using the details below. We may need to verify your identity before providing access. We will respond within a reasonable time and may refuse access where the Privacy Act or another law allows us to do so. If we refuse access, we will explain our reasons where reasonable and lawful.

15. Correction of personal information

You may ask us to correct personal information we hold about you if you believe it is inaccurate, out of date, incomplete, irrelevant or misleading. We will take reasonable steps to correct personal information where appropriate. If we refuse a correction request, we will explain our reasons where reasonable and lawful.

16. Direct marketing

We may use your contact details to send you technical updates, service information or other communications about our services where permitted by law. You may opt out of marketing communications at any time by using the unsubscribe function, replying to the communication, or contacting us.

17. Cookies and website analytics

Our website may use cookies, analytics tools and similar technologies to operate the website, understand usage and improve content. You may be able to disable cookies through your browser settings, although some website features may not function properly.

18. Complaints

If you have a privacy concern or complaint, please contact us first so we can investigate and respond. Please provide enough detail for us to understand the issue and contact you.

We will acknowledge privacy complaints within a reasonable time and aim to respond in writing within 30 days. If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner at www.oaic.gov.au.

19. Contact details

Privacy Officer: Robert Mackay

Email: support@finrep.com.au

Telephone: +61 412 824 087

Website: www.finrep.com.au

20. Changes to this Policy

We may update this Policy from time to time. The current version will be published on our website or otherwise made available on request. This Policy was last updated on 24 July 2026.