Privacy Policy

WBH Legal ABN 41 311 475 562

Summary of this Privacy Policy

We are a law practice. The Privacy Act applies to us only for personal information we handle in connection with anti-money laundering and counter-terrorism financing (AML/CTF) laws. All other information you give us remains protected by our usual duties of confidentiality and legal professional privilege.

Before providing certain services, the law requires us to collect and verify information about clients and some other people, such as proof of identity and information about who owns or controls a company or trust. We collect this information directly from you where we can, and sometimes from other people or public records.

We use this information to verify identities, assess risk and meet our legal obligations. We may be required to report some of it to AUSTRAC, the financial crime regulator, and in some cases we are not allowed to tell you that a report has been made.

We protect this information, keep it for at least seven years as the law requires, and then destroy or de-identify it. You can ask to see or correct the information we hold about you, and you can complain to us or to the Office of the Australian Information Commissioner. The full policy below explains all of this in more detail.

1. Definitions

AML/CTF Act means the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

AML/CTF Framework means the AML/CTF Act, the AML/CTF Rules and AUSTRAC issued guidance.

AML/CTF Rules means the *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025* (Cth), made under the AML/CTF Act.

APPs means the Australian Privacy Principles in Schedule 1 of the Privacy Act.

AUSTRAC means the Australian Transaction Reports and Analysis Centre.

Designated Services means the services listed in Table 6 of Section 6 of the AML/CTF Act that are provided by a legal practitioner, law practice or other relevant professional.

KYC Information means information sufficient to establish initial customer due diligence matters on reasonable grounds, or to fulfil ongoing customer due diligence obligations, under the AML/CTF Framework.

OAIC means the Office of the Australian Information Commissioner.

Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not. The Scope section below explains the personal information to which this Privacy Policy applies.

Privacy Act means the *Privacy Act 1988* (Cth).

SALPCR means the South Australian Legal Practitioners Conduct Rules as adopted in South Australia under the *Legal Practitioners Act 1981* (SA).

Sensitive Information means personal information that includes information or an opinion about an individual's racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, membership of a professional or trade association or trade union, sexual orientation or practices, criminal record, or health, genetic or biometric information.

We, us and our means WBH Legal.

2. Introduction

WBH Legal respects the privacy of personal information collected and handled in connection with our legal practice.

We will take reasonable steps to ensure that:

- personal information collected for AML/CTF purposes is handled responsibly, transparently and securely;
- individuals are given information about how their personal information may be collected, held, used and disclosed for AML/CTF purposes; and
- individuals are informed about how they may request access to, or correction of, personal information we hold about them.

We will keep personal information confidential, except if disclosure is authorised by you, necessary for the conduct of your matter, required or authorised by law, or otherwise permitted under our professional obligations.

3. Purpose

This Privacy Policy explains how we manage personal information that we collect, hold, use and disclose for the purposes of, or in connection with, our obligations under the AML/CTF Framework.

For the purposes of this Privacy Policy, personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.

4. Scope

We are a small business operator under section 6D of the Privacy Act. We are subject to the Privacy Act only in relation to our AML/CTF related activities, by operation of section 6E(1A) of that Act.

This Privacy Policy applies only to personal information that we collect, hold, use or disclose for the purposes of, or in connection with, our obligations under the AML/CTF Framework. It applies to clients and to other individuals whose personal information we collect for these purposes, including beneficial owners, persons acting on behalf of clients, and other individuals connected with a designated service.

If personal information is collected for the purposes of our obligations under the AML/CTF Framework and subsequently incorporated into our broader client or matter records, we will, to the extent required by law, continue to handle that information in accordance with the Privacy Act and applicable APPs.

Other personal information handled by us remains outside the Privacy Act if it is not collected or held for the purposes of, or in connection with, the AML/CTF Framework, and if no other exception to the small business exemption applies.

Regardless of whether the Privacy Act applies, we continue to handle all client information confidentially in accordance with our professional obligations, including under the *Legal Practitioners Act 1981* (SA) and the *South Australian Legal Practitioners Conduct Rules* as they apply in South Australia. Nothing in this Privacy Policy limits our duties of confidentiality or client legal privilege.

5. Description

WBH Legal is a South Australian law practice that provides legal services to clients.

We provide designated services under the AML/CTF Act. If we provide, prepare to provide, or reasonably anticipate providing a designated service, we will be required to collect and verify information about clients and in some instances, other relevant persons.

The designated services we provide may include:

- assisting with the buying, selling or transferring of real estate, other than under an order of a court or tribunal;
- assisting with the buying, selling or transferring of a body corporate or legal arrangement, other than under an order of a court or tribunal;
- assisting with a transaction to provide equity or debt financing in relation to a body corporate or legal arrangement;
- assisting with the creation or restructuring of a body corporate or legal arrangement;
- acting as, or arranging for another person to act as, a director or secretary of a company, a power of attorney, a partner, a trustee or an equivalent position, on behalf of another person;

6. Policy

6.1 Collection of personal information

We collect personal information only by lawful and fair means, and directly from you wherever it is reasonable and practicable to do so.

We may collect personal information if you, your organisation, or someone acting on your or its behalf:

- engages us to provide legal services;
- provides information or documents to us for AML/CTF purposes;
- visits our office or meets with us;
- communicates with us by post, email, telephone, text message, video conference or other means; or
- completes forms or provides documents to us.

We may collect personal information from third parties if you have consented, if it is unreasonable or impracticable to collect it from you directly, or if we are required or authorised by law to do so.

Third party sources may include:

- our clients;
- persons acting on behalf of a client;

- other parties to a matter and their representatives;
- courts, tribunals, regulators, law enforcement bodies and government agencies;
- publicly available sources, including public registers; and
- identity verification, screening, information technology and other service providers.

We also collect personal information through our website and through online identity verification platforms, for example when you complete an enquiry or intake form or upload identification documents. This is required, for instance, by PEXA, the LTO registration platform.

We will provide a collection notice at or before the time we collect personal information for AML/CTF purposes, or as soon as practicable afterwards.

6.2 KYC information and sensitive information

We are required by the AML/CTF Framework to collect and verify certain information. We may be prohibited from providing designated services if we cannot collect or verify that information.

The personal information we collect for AML/CTF purposes may include:

- name;
- date of birth;
- residential address;
- contact details;
- photographic identification;
- occupation;
- business holdings and structures;
- information about beneficial ownership and control;
- information about persons acting on behalf of a client;
- information about source of funds and source of wealth;
- information about the nature and purpose of the business relationship or transaction; and
- details of the legal services or transactions sought or provided.

We will only collect sensitive information if required under the AML/CTF Framework, with your consent if required, or if an exception under the Privacy Act applies.

Sensitive information may include information or an opinion about an individual's racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, membership of a professional or trade association or trade union, sexual orientation or practices, criminal record, health information, genetic information or biometric information.

We may collect government related identifiers, such as passport, driver licence or Medicare details, if required for identity verification or other AML/CTF purposes.

We will not adopt a government related identifier as our own identifier. We will only use or disclose a government related identifier if required or authorised by law, or if otherwise permitted by the Privacy Act.

If you do not provide requested Personal Information, we may be unable to provide Designated Services and/or comply with our legal obligations.

6.3 Personnel due diligence

We collect personal information about employees and prospective employees if required for personnel due diligence under the AML/CTF Framework. This may include identity information, employment history, and information about criminal history or regulatory action, collected with the individual's consent or as otherwise permitted by law.

We use this information to assess whether a person is suitable for a role that could be used to facilitate money laundering, terrorism financing or proliferation financing, and to comply with our AML/CTF program. We handle it in accordance with this Privacy Policy and our professional obligations.

6.4 Anonymity and pseudonymity

if lawful and practicable, you may interact with us anonymously or using a pseudonym.

However, this will generally not be lawful or practicable if we are required to identify or verify a client or another person under the AML/CTF Framework. Our professional obligations also ordinarily require us to know who we are acting for and who is giving instructions.

We may be able to provide general information on an anonymous basis. We will usually be unable to act in a legal matter anonymously or pseudonymously.

6.5 Use and disclosure of personal information

We use and disclose personal information for the purpose for which it was collected, and for related purposes that you would reasonably expect.

For sensitive information, any secondary purpose must be directly related to the primary purpose of collection.

We may use and disclose personal information for AML/CTF purposes, including to:

- identify and verify clients and other relevant persons;
- identify beneficial owners;
- confirm the authority of persons acting on behalf of clients;
- assess money laundering, terrorism financing and proliferation financing risks;
- conduct sanctions, politically exposed person and other screening checks;
- conduct ongoing customer due diligence;
- monitor transactions and matter activity where required;
- comply with record keeping obligations;
- comply with reporting obligations; and
- comply with directions, notices, requests or requirements from AUSTRAC or another lawful authority.

We may also use or disclose personal information if necessary for the conduct of your matter, with your express or implied authority, or as required or authorised by law.

We will not use personal information collected for AML/CTF purposes for direct marketing.

6.6 Unsolicited personal information

If we receive personal information that we did not request, we will determine whether we could have collected that information under the Privacy Act.

If we could not have collected the information and it is lawful and reasonable to do so, we will take reasonable steps to destroy or de-identify it as soon as practicable and in accordance with APP 4.

6.7 Disclosure to third parties

Subject to our duties of confidentiality, privilege and any applicable court rules or undertakings, we may disclose personal information to:

- barristers, mediators, experts, investigators, consultants and other legal practitioners engaged in relation to a matter;
- other parties to proceedings or transactions and their representatives;
- courts, tribunals, government agencies, regulators and law enforcement bodies;
- AUSTRAC and other agencies if required or authorised by the AML/CTF Framework;
- professional indemnity insurers;
- costs assessors or the Supreme Court costs adjudication process if relevant;
- contracted service providers who assist us to operate our practice, including information technology, document management, data storage, archiving, identity verification and screening providers; and
- related entities, where applicable.

We take reasonable steps to ensure that contracted service providers handle personal information appropriately and do not use or disclose it for unauthorised purposes.

We may use technology tools (including artificial intelligence tools) to assist in processing information. We take reasonable steps to ensure such tools are used in a manner consistent with our privacy and confidentiality obligations.

6.8 Legal requirements and AUSTRAC reporting

There may be circumstances where we are required or authorised by law to use or disclose personal information without your consent.

This may include where:

- disclosure is required by warrant, subpoena, court order, statutory notice or other lawful requirement;
- disclosure is required or authorised under the AML/CTF Framework;
- we form a suspicion about a matter or transaction that must be reported to AUSTRAC;

- disclosure is necessary to lessen or prevent a serious threat to life, health or safety;
- disclosure is necessary for us to take appropriate action in relation to suspected unlawful activity or serious misconduct; or
- disclosure is otherwise permitted by the Privacy Act.

In some cases, it is an offence for us to disclose that we have made a report to AUSTRAC.

Nothing in this Privacy Policy limits our obligations of confidentiality or client legal privilege. However, there may be circumstances where we are compelled to disclose confidential information to AUSTRAC under the AML/CTF Framework. In some circumstances, we may be prohibited from notifying you that a disclosure has been made.

6.9 Data Quality

We take reasonable steps to ensure that personal information we collect, use and disclose for AML/CTF purposes is accurate, current, complete and relevant.

We rely on you to provide accurate information and to tell us if your information changes during the course of your matter or business relationship with us.

Records held after our work has concluded will not usually be monitored or updated unless further instructions are received or we are required to do so by law.

6.10 Storage and information security

We hold personal information in hard copy and electronic formats.

Our electronic systems include practice management, document management and storage systems operated by third party providers, including cloud based services.

We may link personal information collected for AML/CTF purposes with other information we hold about you in connection with your matter, for example in our client and matter records.

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

These steps may include:

- staff training on privacy, confidentiality and AML/CTF obligations;
- access controls limiting personal information to those who need it;
- multi factor authentication;
- password and passphrase controls;
- anti malware protections;
- secure document management systems;
- secure physical storage;
- backup procedures; and
- processes for managing cyber incidents and data breaches.

If a data breach occurs that is likely to result in serious harm, we will comply with the Notifiable Data Breaches scheme in the Privacy Act, including notifying the Office of the Australian Information Commissioner and affected individuals where required.

6.11 Retention and destruction

We retain personal information for as long as necessary to fulfil the purposes for which it was collected, comply with our legal and professional obligations, and ensure relevant evidence remains available if reasonably required.

Information collected for AML/CTF purposes including KYC information and transaction records will be kept for at least seven years after the business relationship ends or the transaction is completed, as required by the AML/CTF Framework.

Other personal information may be retained for longer periods if required by law, to comply with our professional obligations, insurance considerations or limitation periods.

If personal information is no longer needed for any permitted purpose, and we are not required by law, court order or professional obligation to retain it, we will take reasonable steps to destroy or deidentify it.

6.12 Access and correction

You may request access to, or correction of, personal information we hold about you by contacting our Privacy Officer.

We may ask you to verify your identity before giving access or making corrections.

We will respond to access and correction requests within a reasonable period, generally within 30 days.

We may charge a reasonable fee to cover the cost of locating, retrieving and providing information. We will not charge a fee for making a correction.

We may refuse access or correction where permitted by law. This may include where giving access would have an unreasonable impact on the privacy of others, would be unlawful, would prejudice enforcement activities or anticipated legal proceedings, would reveal commercially sensitive evaluative information, or would be inconsistent with our duties to another client.

If we refuse access or correction, we will provide written reasons unless it would be unreasonable or unlawful to do so.

6.13 Overseas Disclosure

We hold personal information physically and electronically within Australia, unless we have agreed with you to disclose it to a person or organisation overseas, or unless disclosure overseas is required for the conduct of your matter.

Some electronic services we use may store or process data overseas. We take reasonable steps to ensure that overseas recipients handle personal information consistently with the Australian Privacy Principles.

If we disclose personal information to an overseas recipient, we will take reasonable steps to ensure the recipient does not breach the APPs, unless an exception in APP 8.2 applies (for example, if you expressly consent after being informed that the APPs may not apply).

6.14 Business Transactions

If we are involved in a merger, acquisition, restructure or sale of practice assets, personal information may be disclosed in confidence as part of due diligence and may be transferred to the new owner.

Where practicable and lawful, we will provide notice before personal information is transferred and becomes subject to a different privacy policy.

7. Complaints and Questions

If you have a question about this Privacy Policy, or a complaint about how we have handled your personal information, please contact our Privacy Officer in writing:

Ms J White

Address: 51 Angas Street, Adelaide SA 5000

Email: admin@wbhlegal.com.au

Phone: (08) 8410 4420

We will acknowledge your complaint within 7 business days and investigate it promptly.

We aim to resolve complaints within 30 days. If we need more time, we will keep you informed of our progress.

If you are not satisfied with our response, or we do not resolve your complaint within 30 days, you may contact the Office of the Australian Information Commissioner:

Website: www.oaic.gov.au

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Post: GPO Box 5218, Sydney NSW 2001

8. Policy updates and version control

We may update this Privacy Policy from time to time to reflect changes in our practices or legal requirements.

The current version will be available free of charge at https://wbhlegal.com.au or on request from our Privacy Officer.

If you require a copy of this Privacy Policy in a particular form, for example large print or an accessible PDF, please contact our Privacy Officer.

Version: **1 July 2026**

Date adopted: **1 July 2026**

Date last reviewed: **1 July 2026**

Next review date: **1 July 2027**

Approved by: **WBH Legal**