PRIVACY STATEMENT

Intercept Law (ABN 64 124 650 942) are committed to handling personal information in accordance with the *Privacy Act 1988* (Cth), the Australian Privacy Principles (**APPs**), the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), the AML/CTF Rules and applicable professional obligations.

This Statement is intended as our public privacy statement. It summarises how we collect, hold, use and disclose personal information and how individuals may access or correct their information or make a privacy complaint.

1. Scope

This Statement applies to personal information collected and handled in connection with our legal services, client onboarding and matter administration, conflict checking, AML/CTF compliance, recruitment, events, publications, website use and practice operations.
We maintain practices, procedures and systems designed to support APP compliance, including controls relating to confidentiality, information security, records management, direct marketing, access and correction requests, complaints and AML/CTF compliance.

2. Personal information we collect

The kinds of personal information we collect and hold depend on the nature of your relationship with us, including whether you are a client, prospective client, person connected with a client matter, supplier, service provider, job applicant, employee, contractor, subscriber, event attendee or website user. The information may include:

- identification and contact details, including name, date of birth, address, email and telephone details;
- occupation, role, employer, business activity and professional information;
- identity documents and verification information, including document numbers, issuing authorities, expiry dates, photographs and signatures;
- government-related identifiers where required or authorised by law;
- financial, banking, payment, transaction, source of funds, source of wealth and ownership information;
- matter-related information, including instructions, communications, evidence, documents and information about relationships between persons involved in a matter;
- information about companies, trusts, partnerships and other arrangements, including beneficial owners, controllers, directors, trustees, beneficiaries, shareholders and other connected persons;
- information relevant to politically exposed persons, sanctions screening, AML/CTF risk assessment and transaction monitoring;
- recruitment, employment and contractor information;
- event, subscription, alumni, marketing and communication preferences; and
- website usage information, including IP address, browser type, device information, cookies, pixels and analytics information.

We collect sensitive information only where permitted by law, including where you consent and the information is reasonably necessary for our functions, where collection is required or authorised by law, where necessary for legal claims or legal services, or where another Privacy Act exception applies.

3. How we collect personal information

We collect personal information by lawful and fair means. We usually collect it directly from you when you instruct us, provide information or documents, communicate with us, complete a form or verification process, subscribe to publications, register for events, interact with our website or apply for employment or engagement.

We may also collect personal information from third parties where permitted by law, including clients, counterparties, witnesses, representatives, advisers, courts, tribunals, regulators, government bodies, public registers, commercial databases, identity verification providers, AML/CTF screening providers, financial institutions, recruitment agencies, referees, former employers, social media, online searches and technology or analytics providers.

If you provide us with personal information about another individual, you should take reasonable steps to ensure that the individual is aware their information has been provided to us and of this Statement. You should only provide sensitive information about another individual where you have authority or consent to do so, or where otherwise permitted by law.

4. How we use and disclose personal information

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

- providing legal services and carrying out instructions;
- conflict checks, client onboarding, matter opening and administration;
- communications, legal advice, due diligence, transactions, litigation and dispute resolution;
- trust accounting, payments, billing, debt recovery and practice management;
- compliance with professional, court, tribunal, regulatory and AML/CTF obligations;
- customer due diligence, ongoing customer due diligence, sanctions and politically exposed person screening, risk assessment, reporting, record-keeping and monitoring for AML/CTF purposes;
- responding to notices, audits, investigations and lawful requests from AUSTRAC, courts, regulators, law enforcement agencies and government bodies;
- risk management, insurance, complaints and professional indemnity matters;
- recruitment, employment, contractor and human resources administration;
- operating, securing and improving our business, systems, website and services;
- sharing information with partnership, service, administration and employing entities that support our practice for authorised business support functions; and
- legal updates, publications, event invitations and information about our services where permitted by law.

We may disclose personal information to barristers, experts, advisers, courts, tribunals, regulators, AUSTRAC, government agencies, counterparties, financial institutions, insurers, identity verification and AML/CTF service providers, technology and cloud providers, recruitment providers, payment providers, internal service entities and other persons where you have consented or disclosure is required or authorised by law.

5. AML/CTF compliance

From 1 July 2026, we will be reporting entities under the AML/CTF Act when providing certain designated services. Where AML/CTF laws apply, we may be required to collect, verify, use, disclose and retain personal information about clients and other relevant persons before providing services and during a matter.

This may include information required to verify identity, understand the nature and purpose of a service, identify beneficial owners or persons on whose behalf a person acts, assess risk, verify authority to act, establish source of funds or source of wealth, conduct sanctions and politically exposed person checks, and monitor transactions or behaviours.

If required information is not provided, we may be unable to provide the requested service or may need to pause, limit or terminate work, subject to professional obligations and applicable law. We may disclose information to AUSTRAC or another authority where required or authorised by AML/CTF laws, and those laws may restrict what we can say about certain reports, notices, investigations, requests or disclosures.

6. Automated tools
We use technology, including automated and computer-assisted tools, for functions such as identity verification, document verification, sanctions and politically exposed person screening, transaction monitoring, risk assessment and conflict checking.

We do not use computer programs to make solely automated decisions that significantly affect an individual's rights or interests. Automated outputs may inform decisions made by appropriately trained personnel, including whether we can act, whether enhanced customer due diligence is required, or whether AML/CTF or other legal steps are required.

7. Legal professional privilege, confidentiality and identifiers
Our duties of confidentiality and legal professional privilege remain important. Some laws, including AML/CTF laws, may require or authorise collection, use, disclosure or retention of personal information. Where privilege may apply to information or documents requested under AML/CTF laws or other laws, we manage privilege issues in accordance with applicable legal requirements.

We do not adopt a government-related identifier as our own identifier of an individual unless permitted by law. We may collect, use or disclose government-related identifiers where reasonably necessary for identity verification, legal services, AML/CTF compliance, court or tribunal processes, regulatory compliance, or where otherwise required or authorised by law.

8. Direct marketing and anonymity
We may use contact details to provide legal updates, publications, event invitations and information about our services where permitted by law. You may opt out at any time by using the unsubscribe function in an email or by contacting our firm. We do not use sensitive information for direct marketing without consent.

You may request to deal with us anonymously or by using a pseudonym. We will agree where lawful and practicable. Given the nature of legal services, conflict checks, court and tribunal requirements, billing, trust accounting and AML/CTF obligations, this will often be impracticable or unlawful unless ordered by a court or otherwise required by law.

9. Quality, security and retention
We take reasonable steps to ensure personal information we collect, use and disclose is accurate, up-to-date, complete and relevant, and to protect it from misuse, interference, loss and unauthorised access, modification or disclosure.

Personal information may be held in physical and electronic form. Safeguards may include access controls, secure document management systems, confidentiality obligations, staff training, cyber security measures, secure destruction processes, service provider due diligence and internal policies and procedures.

We retain personal information for as long as required or permitted by law and as necessary for our functions, including legal services, professional obligations, risk management, insurance, disputes and AML/CTF compliance. AML/CTF records may need to be retained for prescribed periods that may extend for at least 7 years. Where personal information is no longer required for a lawful purpose, we take reasonable steps to destroy or de-identify it, subject to applicable retention requirements.

10. Overseas disclosure
We may disclose personal information to overseas recipients where necessary or related to legal services, where you have consented, where we use overseas service providers or advisers, where a matter involves an overseas party, transaction, court, tribunal, regulator,

registry or authority, where disclosure is required or authorised by law, or where another Privacy Act exception applies.

The countries in which overseas recipients are located will depend on the particular matter, transaction, service provider or technology service used. Where APP 8 applies, we take reasonable steps to ensure that overseas recipients do not breach the APPs in relation to personal information, unless an exception applies.

11. Website, cookies and analytics
Our website may use cookies, pixels, analytics tools and similar technologies to enable functionality, understand website usage, improve our services and support communications. You may be able to change browser settings to refuse cookies or receive notice when cookies are used, although some website functions may not operate properly if cookies are disabled.

You may click-through to third party websites from this site, in which case we recommend that you refer to the privacy statement of the websites you visit. This Privacy Policy applies to this site only and this firm assumes no responsibility for the content of any third party websites.

12. Access and correction
You may request access to personal information we hold about you by contacting:
Intercept Law
3 Barralong Road, ERINA NSW 2250
E: reception@interceptlaw.com.au
T: (02) 43223223

We may require proof of identity before responding. We will respond within a reasonable period and endeavour to respond within 15 business days. Access or correction may be refused or limited where permitted by law, including where access would affect another person's privacy, prejudice proceedings or investigations, reveal commercially sensitive evaluative information, breach confidentiality, be unlawful, or be inconsistent with legal professional privilege or professional obligations. If we refuse a request, we will provide reasons where reasonable and lawful.

13. Data breaches and complaints
We respond to suspected or actual data breaches in accordance with the Privacy Act and our internal procedures. Where an eligible data breach occurs, we will notify affected individuals and the Office of the Australian Information Commissioner as required by the Notifiable Data Breaches scheme.

If you have a privacy complaint, please contact our office r in writing using the details above.

We will investigate and endeavour to respond within 14 business days, unless the matter is complex or further time is reasonably required. Where a privacy issue is substantiated, we will take reasonable steps to address it.

If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner by telephone on 1300 363 992 or through its website.

14. Changes to this Privacy Statement
From time to time, it may be necessary for us to revise this Privacy Statement. This Statement is subject to regular review and may be updated to reflect changes in law, regulatory guidance, technology, our business practices or the services we provide. The

current version can be obtained from our website or by contacting our firm at reception@interceptlaw.com.au

If you require any further information about the Privacy Act and the Australian Privacy Principles, you can visit the Federal Privacy Commissioner's website (see www.oaic.gov.au).