

Acacia Law — Privacy Policy

Version 2.1 — June 2026

1. About us and this policy

1.1 C Warburton and M Warburton t/as Acacia Law ("we", "us", "our") provides trans-Tasman patent and trade mark attorney services. Our contact details are: Level 1, 16 McDougall Street, Milton, QLD, 4064, Australia, tel: +61 7 3418-0974, ABN 34 461 295 912.

1.2 Our Privacy Officer is Mark Warburton, who can be contacted at privacy@acacialaw.com. The Privacy Officer is responsible for privacy compliance, access and correction requests, and complaints under this policy.

1.3 This policy explains how we collect, hold, use and disclose personal information in the course of our practice and through our website, and how you may access and correct your information or make a complaint. It is provided free of charge and is available on our website at all times.

2. Legal framework

2.1 **Australia.** We handle personal information in accordance with the Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Cth). Although we may fall within the small business exemption in that Act, we comply with the APPs as a matter of policy and professional practice. In addition, our handling of personal information in connection with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) is subject to the *Privacy Act 1988* (Cth) as of right, notwithstanding that exemption (clause 7). We do not disclose personal information to any third party for a benefit, service or advantage, and we do not buy, sell or trade personal information.

2.2 **New Zealand.** We act directly for New Zealand clients and act as address for service before the Intellectual Property Office of New Zealand (IPONZ). Our New Zealand-related activities are subject to the *Privacy Act 2020* (NZ) and its Information Privacy Principles (IPPs).

2.3 **Professional obligations.** We are bound by the confidentiality obligations in the Code of Conduct for Trans-Tasman Patent and Trade Marks Attorneys 2018. Communications made for the dominant purpose of intellectual property advice attract statutory privilege under section 200 of the *Patents Act 1990* (Cth) and section 229 of the *Trade Marks Act 1995* (Cth), and under corresponding New Zealand law. Nothing in this policy displaces privilege or our duty of confidence.

3. Kinds of personal information we collect and hold

3.1 Depending on our relationship with you, we may collect and hold:

- identity and contact details of clients, applicants, inventors, designers, authors, directors and authorised representatives;

- information necessary to your matter, including details of inventions, brands, designs, ownership, assignments, declarations, evidence of use, and technical and commercial information (which may incidentally contain personal information);
- billing and payment information (we do not hold complete payment card numbers);
- correspondence and communications, including email and, where applicable, audio recordings of consultations (clause 13);
- website server logs and client login credentials (clause 11);
- images and recordings taken at our events (clause 14);
- conflict-check, identity-verification and customer due diligence information, including date of birth, government-issued identity documents, beneficial ownership and control information and, where required, source of funds or wealth (clause 7).

3.2 We do not usually collect sensitive information. Where subject matter incidentally involves sensitive information about an identifiable individual (for example, health information in life sciences matters), we handle it only with consent or as otherwise permitted by law.

4. How we collect personal information

4.1 We collect personal information directly from you wherever practicable — by email, telephone, our online forms, and in consultations.

4.2 We also collect personal information from third parties where necessary for your matter, including from your authorised representatives, our foreign associates, IP Australia, IPONZ, WIPO, foreign intellectual property offices, public registers, search providers and investigators.

4.3 **Anonymity and pseudonymity.** You may make general enquiries anonymously or under a pseudonym. This is not practicable once you instruct us, because official filings and registers require accurate identity details.

5. Purposes of collection, holding and use

5.1 We collect, hold and use personal information to: provide patent and trade marks attorney services and act on your instructions; obtain, maintain, enforce and defend intellectual property rights in Australia, New Zealand and abroad; conduct conflict checks and verify identity; administer billing and accounting; meet our legal, regulatory and professional obligations; maintain and improve our services; and, with an opt-out, keep you informed of relevant developments (see clause 9 below).

6. Disclosure of personal information

6.1 **Public registers — important.** When we file applications or documents on your instructions, identity details (including applicant and inventor names and addresses) are

provided to government and international treaty organisations. Depending on your instructions, we may need to supply your information to: IP Australia, The Intellectual Property Office of New Zealand (IPONZ), The World Intellectual Property Organisation (WIPO), foreign intellectual property offices, tribunals and courts in various jurisdictions. Details are published on public registers. Register publication is permanent, searchable and accessible worldwide. Disclosure of these details is an inherent and unavoidable consequence of instructing us to seek registered rights.

6.2 Foreign associates. To obtain or enforce protection outside Australia and New Zealand, we disclose relevant information to our associates (patent and trade mark attorneys and agents) in the relevant countries, who in turn disclose it to their intellectual property offices and other bodies to which they must report. Our associates are subject to the professional obligations of their own jurisdictions.

6.3 Regulators, courts and law. We may disclose personal information to the Trans-Tasman IP Attorneys Board, courts, tribunals and government agencies where required or authorised by law, including in connection with regulatory, disciplinary or audit processes.

6.4 Service providers. We disclose personal information to the service providers listed in clause 8 solely so that they can provide services to us, on terms protecting the information.

7. Anti-money laundering and counter-terrorism financing

7.1 From 1 July 2026, certain professional services are "designated services" under the AML/CTF Act. Where we provide a designated service — for example, receiving, holding or managing client money or other property (beyond payment of our professional fees), assisting in transactions for the sale or transfer of a business or of assets (including assignments of intellectual property in that context), or assisting with the creation or restructuring of companies or other legal arrangements — we are a reporting entity regulated by AUSTRAC.

7.2 Collection and verification. To meet our customer due diligence obligations we collect and verify identity information before, and periodically during, the provision of a designated service. This may include your full name, date of birth, residential address and government-issued identity documents and, for companies, trusts and other entities, information about beneficial ownership and control and the identity of individuals acting on the entity's behalf, together with information about the source of funds or wealth where required. We may use an electronic identity verification service, which may check the information you provide against official records with your consent. If we cannot verify your identity as required, we may be unable to provide, or continue to provide, the designated service.

7.3 Use and disclosure. AML/CTF information is used to conduct initial and ongoing customer due diligence and transaction monitoring, and may be disclosed to AUSTRAC — including in suspicious matter reports and threshold transaction reports — and to other agencies where required or authorised by law. The AML/CTF Act may prohibit us

from disclosing to you that a report has been made or that information has been sought by AUSTRAC (the tipping-off provisions), and to that extent your rights of access under clause 18 are qualified by law.

7.4 Records. We retain AML/CTF records in accordance with clause 16.3. Personal information collected for AML/CTF purposes is not used for any other purpose except as permitted by the AML/CTF Act and the *Privacy Act 1988* (Cth).

8. Service providers, storage and overseas disclosure

8.1 We use the following providers and systems:

- **Proton** (email and document services) — data hosted in Switzerland, with end-to-end and zero-access encryption where applicable;
- **Google Workspace / Google Drive** (email, documents and storage) — data hosted on Google's global infrastructure;
- **Xero** (accounting) — data hosted overseas, principally in the United States;
- **Stripe and PayPal** (payment processing — clause 12);
- an internally hosted open-source client relationship management system, hosted on our own infrastructure in Australia and on virtual servers in the USA;
- Locally hosted AI large language models on our own infrastructure in Australia (clause 10); and
- **Anthropic (Claude)** — hosted in the United States (clause 10).

8.2 Accordingly, personal information may be stored in or disclosed to recipients in Australia, New Zealand, Switzerland, the United States, and the countries in which Google operates data centres, together with each country in which you instruct us to seek or enforce intellectual property rights. Because foreign filings depend on your instructions and our associate network spans most jurisdictions worldwide, it is not practicable to list every country or service that will store your information. We will identify the relevant countries for your matter on request.

8.3 We take reasonable steps, including contractual and technical safeguards, to ensure overseas recipients handle personal information consistently with the APPs and, for New Zealand-related information, with IPP 12. Where you instruct us to file or act in a particular country, disclosure to recipients in that country under its laws is a necessary incident of your instructions.

9. Direct marketing

9.1 We may send existing clients and contacts information about legal and practice developments and our services. Every electronic message includes a functional unsubscribe facility, consistent with the *Spam Act 2003* (Cth) and the *Unsolicited Electronic Messages Act 2007* (NZ). You may opt out at any time by using that facility or contacting the Privacy Officer, and we will give effect to the opt-out promptly. We do not provide mailing lists to any third party.

10. Artificial intelligence and automated processing

10.1 We use a large language model hosted entirely on our own infrastructure; information processed by it does not leave our systems. We also use Claude (Anthropic) under commercial terms which prohibit the use of our data to train Anthropic's models; that processing occurs in the United States.

10.2 AI tools are used only as assistive tools — for example, transcription, summarisation and drafting support — under the review and control of a registered attorney. No decision that produces a legal effect or otherwise significantly affects you is made by automated means without substantive human review. We will update this policy as required by the automated decision-making transparency requirements of the *Privacy Act 1988* (Cth) commencing 10 December 2026.

11. Website

11.1 Our web server logs the requesting IP address, browser type, date and time, and pages accessed. Logs are used for security, diagnostic and statistical purposes and are retained for 90 days.

11.2 We use only essential cookies, including session cookies required for client logins. If your browser rejects cookies, login-based services will not be available. We do not currently use analytics, advertising or tracking technologies. If we introduce any, we will update this policy before doing so.

11.3 Our website links to external websites and may include third-party content. Those sites and content are governed by their own terms and privacy policies, and links do not constitute endorsement.

11.4 **Online forms and surveys.** Information you submit through our online forms and surveys is used only for the purpose stated at the point of collection and, in aggregated or de-identified form, for service improvement.

12. Payments

12.1 Online and card payments are processed by Stripe and PayPal. Card details are transmitted directly to the processor and are not stored on our servers. The processors' own privacy policies apply to their handling of your information.

13. Audio and video recording of consultations

13.1 With your knowledge, we generally audio record consultations to ensure an accurate record and file note. You may request a copy of any recording of your consultation, or ask that a consultation not be recorded.

13.2 Recordings are stored on our secure systems, transcribed using our locally hosted tools (clause 10), used only as a record of the consultation, and deleted in accordance with clause 16 once a written record is settled.

14. Events

14.1 Photography or filming may occur at our events for the purpose of reporting on and promoting our services, including in print and online publications (which are accessible worldwide). Notice will be given at registration and at the venue.

14.2 If you do not wish to be photographed, filmed or to have your image published, tell us at registration, advise the photographer, or contact the Privacy Officer at any time, and we will give effect to your request in respect of future use. We do not publish identifiable images of children without the consent of a parent or guardian.

15. CCTV

15.1 Our premises are within a building protected by CCTV operated and controlled by our landlord, covering the main entrance, common areas and parking areas, for the safety and security of staff and visitors. We do not operate or control the system. Footage is held by the landlord and may be disclosed by it to police in relation to unlawful acts, for work health and safety purposes, or as otherwise required by law. Enquiries about the system may be directed to the Privacy Officer, who will refer them to the landlord.

16. Security, quality, retention and destruction

16.1 We take reasonable technical and organisational measures to protect personal information from misuse, interference, loss, and unauthorised access, modification or disclosure — including encryption in transit and at rest, access controls and multi-factor authentication, segregation of client matter data, and secure backup.

16.2 We take reasonable steps to keep personal information accurate, up to date and complete. Please advise us of changes to your details.

16.3 Client files are retained for at least seven years after a matter closes, and longer where rights remain in force or limitation, professional or regulatory requirements apply. Records made or obtained under the AML/CTF Act, including identification and verification records, are retained for at least seven years after the end of our relationship with you or after the record was made, as required by that Act. Consultation recordings are deleted once the written record is settled or within 12 months, whichever is earlier. When personal information is no longer required for any permitted purpose, we destroy or de-identify it.

17. Data breaches

17.1 If a data breach involving personal information occurs, we will contain and assess it, take remedial action, and notify the Office of the Australian Information Commissioner (OAIC) and affected individuals where the breach is an eligible data breach under Part IIIC of the *Privacy Act 1988* (Cth), and the Office of the Privacy Commissioner (NZ) and affected individuals where it is a notifiable privacy breach under the *Privacy Act 2020* (NZ).

18. Access and correction

18.1 You may request access to, and correction of, personal information we hold about you by contacting the Privacy Officer. For individuals in New Zealand, access and correction are legal rights under IPPs 6 and 7. We will respond within 30 days. We do not charge for making a request or for correction; a reasonable charge may apply to compiling and providing access. If we refuse access or correction, we will give written reasons and available review avenues; on request, we will attach a statement of correction to the record.

19. Complaints

19.1 If you have a complaint about our handling of your personal information, please contact the Privacy Officer in writing. We will acknowledge your complaint within 7 days and respond within 30 days.

19.2 If you are dissatisfied with our response, you may complain to the OAIC (www.oaic.gov.au, 1300 363 992) or, for New Zealand-related matters, the Office of the Privacy Commissioner (www.privacy.org.nz). Complaints about professional conduct may be made to the Trans-Tasman IP Attorneys Board (www.ttipattorney.gov.au).

20. Changes to this policy

20.1 We review this policy periodically and following relevant legislative change. The current version is published on our website; material changes will be notified to current clients. This version supersedes all previous versions.