Privacy Policy

Laurent Law Ltd t/a Laurent Law Barristers and Solicitors

1. Introduction

Laurent Law Ltd (“we”, “us”, “our”) is committed to protecting your privacy and handling your personal information in accordance with the New Zealand Privacy Act 2020 and our professional obligations under the Rules of Conduct and Client Care for Lawyers.

2. Information We Collect

We collect personal information necessary to provide legal services, including immigration, property, and litigation advice

This may include:

- Identity Data: Names, dates of birth, passports, and visas.
- Contact Data: Email addresses, phone numbers, and physical addresses.
- Matter Data: Information relating to your legal issues, including family history or employment details for immigration cases.
- Compliance Data: Information required for Anti-Money Laundering (AML) and "Know Your Customer" (KYC) verification.

3. How We Collect Information

We generally collect information directly from you. However, we may also collect information from:

- Publicly available sources (e.g., Landonline, Companies Office).
- Third parties where authorised by you or permitted by law (e.g., Immigration New Zealand)

4. Purpose of Collection and Use

We use your information to:

- Provide legal advice and represent you in court or before tribunals.
- Verify your identity and perform customer due diligence.
- Communicate with you regarding your files and billing .
- Meet our statutory obligations under the Privacy Act and Law Society Rules of Conduct and Client Care.

5. Anti-Money Laundering (AML) Compliance

As a law firm, we are a "reporting entity" under the AML/CFT Act 2009. This law requires us to take specific steps to help detect and deter money laundering and terrorism financing in New Zealand.

Customer Due Diligence (CDD): Before we can provide certain legal services (known as "captured activities"), we must verify the identity of our clients, any beneficial owners (such as company directors or trust beneficiaries), and anyone acting on their behalf.

Information We Must Collect: To meet these requirements, we will ask you for specific documents, which may include:

- Certified ID: Current passport or driver's licence.
- Address Verification: Recent utility bills or bank statements.

- Nature of Business: Information about the purpose of your relationship with us.

Source of Wealth/Funds: In some cases (such as high-risk transactions or trust-related work), we must verify where your funds or wealth originated.

Ongoing Monitoring: We are required to conduct ongoing monitoring of our business relationship with you to ensure transactions remain consistent with your known risk profile.

Mandatory Reporting: Under the Act, we are legally required to report Suspicious Activity (SARs) or Prescribed Transactions (PTRs) (such as international wire transfers over $1,000) to the Financial Intelligence Unit (FIU) of the NZ Police.

Privacy & Privilege: AML information is held securely and used solely for compliance purposes. While we have strict confidentiality duties, the AML/CFT Act requires us to disclose non-privileged information to regulatory supervisors if requested. We will not disclose any information that we believe, on reasonable grounds, is protected by Legal Professional Privilege.

6. Digital Identity Verification (Verifi Identity GBG)

To streamline our onboarding process and meet our strict AML/CFT obligations, we use Verifi Identity (provided by GBG) to conduct digital identity verification and biometric screening.

Biometric Processing: When we use this service, we may be asked to provide a high-quality image of your government-issued ID (such as a passport) and a "selfie" or video to confirm a match. Verifi uses biometric technology to perform "liveness" checks and facial recognition.

Data Matching: Your information is checked against authoritative databases (such as the Department of Internal Affairs, NZTA, and international PEP/Sanctions lists) to confirm your identity and risk profile.

Security of Data: All data processed through Verifi is encrypted. While Laurent Law Ltd retains the results of these checks for our compliance records, GBG handles the technical processing of your biometric data in accordance with their own strict security standards and New Zealand privacy law.

Alternative Option: If you do not wish to use digital biometric verification, please let us know. You may instead provide certified physical copies of your identification documents to our office in person or via post.

7. Disclosure of Information

We may disclose your information to:

- Government agencies (e.g., Immigration NZ, Courts) as part of your legal matter.
- Third-party service providers (e.g., IT support, secure cloud storage) who assist our operations .
- Regulatory bodies where required by law (e.g., NZ Law Society or AML/CFT supervisors).

8. Website Cookies and Usage Data

When you visit our website (laurentlaw.co.nz), we may use "cookies" to improve your experience.

What are Cookies?: Small text files placed on your device to collect standard internet log and visitor behaviour information.

How We Use Them: We use cookies to understand how visitors interact with our site, track traffic patterns via tools like Google Analytics, and remember your preferences.

Managing Cookies: You can set your browser to not accept cookies; however, some website features may not function correctly as a result.

9. Marketing Communications

We may use your contact details to send you legal updates, newsletters, or information about our services that we believe may be of interest to you.

Consent: We will only send these communications if you have opted in or if we have an existing professional relationship with you.

Opting Out: You have the right to stop us from contacting you for marketing purposes at any time. Every marketing email will include an "Unsubscribe" link, or you can contact us directly at mdutoit@laurentlaw.co.nz to be removed from our mailing list.

No Third-Party Sales: We will never sell, trade, or rent your personal information to third parties for their own marketing purposes.

10. Security and Retention

Protection: We take all reasonable steps to protect your information from loss, unauthorised access, or disclosure.

Confidentiality: All client information is held in strict confidence, subject to legal professional privilege.

Retention: We retain files for at least 7 years (or longer if required) to comply with Law Society regulations, after which they are securely destroyed.

11. Your Rights

Under the Privacy Act 2020, you have the right to:

- Access the personal information we hold about you.
- Request correction of that information if it is inaccurate.

Note: Legal professional privilege may limit your right to access certain documents created for the purpose of legal advice.

12. Data Breach Notification

We take the security of your personal information seriously. In the unlikely event of a privacy breach (e.g., unauthorised access, loss, or disclosure of your data):

Assessment: We will immediately assess the breach to determine if it is likely to cause "serious harm" to any individual.

Notification: If we determine that a breach has caused or is likely to cause serious harm, we will notify the Office of the Privacy Commissioner and the affected individuals as soon as practicable.

Timeline: In accordance with the Privacy Act 2020, we aim to provide this notification within 72 hours of becoming aware of the breach.

Details Provided: Our notification will include a description of the breach, the steps we are taking to mitigate it, and advice on what you should do to protect yourself.

13. Contact Us

For any privacy-related queries, please contact our Privacy Officer:

Name: Simon Laurent

Email: slaurent@laurentlaw.co.nz

Address: 7A Maidstone Street, Grey Lynn, Auckland 1021