

Stratocumulus Legal Privacy Policy

As at 7 July 2026

1. Introduction

- 1.1 **Stratocumulus Tuesday Pty Ltd (ACN 639 204 710), an incorporated legal practice trading as Stratocumulus Legal (ABN 78 639 204 710)**, of 79 St Georges Terrace, Perth, is committed to protecting personal information and handling it in accordance with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles.
- 1.2 We are a reporting entity, or may act as an authorised agent of a reporting entity, for the purposes of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and related rules. Section 6E(1A) of the *Privacy Act 1988* (Cth) applies the Privacy Act to small business operators that are reporting entities or authorised agents of reporting entities, for the purposes of, or in connection with, activities relating to their AML/CTF obligations.
- 1.3 This Privacy Policy explains how and why we collect, use, hold and disclose personal information, including personal information used to verify identity and comply with AML/CTF obligations.
- 1.4 We publish a separate [Website Privacy Policy](#) that applies to information collected via our website and online forms. It can be found on our website.

2. What is personal information?

- 2.1 Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not the information or opinion is true and whether or not it is recorded in a material form. Some personal information is sensitive information, including biometric information used for automated biometric verification or identification.

3. What personal information we collect

- 3.1 We collect personal information that is reasonably necessary for our business activities, to provide services, to manage our relationship with you, and to comply with our legal and regulatory obligations, including AML/CTF obligations. This may include your full name, date and place of birth, residential or business address, email address, telephone number, details of services provided to you, records of enquiries or complaints, transaction-related information and any other information you choose to provide.
- 3.2 For identity verification and customer due diligence, we may collect identity document details such as driver licence, passport, Medicare card or other government-issued identification numbers, document expiry dates, verification results and related evidence that verification occurred. We may also collect biometric information, such as a facial image or short video, where this is reasonably necessary for identity verification and related compliance purposes and where consent is required.

3.3 We may also collect information about how you access, use and interact with our website and online services, including IP address, device information, browser type, operating system, pages visited and information collected through cookies or similar technologies. You may disable cookies through your browser settings, but doing so may affect the functionality of our website.

4. Why we collect, use and disclose personal information

4.1 We collect, use and disclose personal information to provide and manage our services, verify identity, conduct customer due diligence, assess and manage money laundering, terrorism financing, proliferation financing, fraud and related compliance risks, meet our AML/CTF and other legal obligations, communicate with you, respond to enquiries and complaints, maintain records, improve our services, keep our systems secure and protect our lawful interests.

4.2 We may use your contact details to provide information about our services that may be of interest to you. You can opt out of marketing communications at any time by using the unsubscribe facility in the communication or by contacting us.

5. How we collect personal information

5.1 We usually collect personal information directly from you when you interact with us, use our services, complete forms, communicate with us, provide identity documents or complete an identity verification process. We may also collect personal information from another person acting on your behalf, public registers, government record holders, courts, regulators, professional advisers, financial institutions, counterparties, service providers and identity verification providers.

5.2 If you do not provide personal information we reasonably require, we may not be able to verify your identity, comply with our legal obligations, provide services to you or the person you act for, communicate with you or respond to your enquiries.

6. Identity verification, DVS and biometric information

6.1 To verify your identity, we may use electronic identity verification services, including the Australian Government's Document Verification Service. With your consent where required, your name, date of birth and identity document details may be securely checked against records held by relevant Commonwealth, State or Territory authorities or official record holders. These authorities generally return a match result only, indicating whether the details match their records.

6.2 This process may be carried out through authorised identity verification providers, including Infotrack and its authorised sub-providers. We do not sell your personal information.

6.3 Where biometric information is collected, it may be used to confirm that you are a real person and physically present, match your image to an identification document, reduce the risk of fraud and identity theft, and support AML/CTF and related compliance purposes. We treat biometric information as sensitive information and use it only for identity verification and related compliance purposes, with consent where required.

7. Consent and alternatives

7.1 By providing personal information and completing an identity verification process, you consent to the collection, use and disclosure of your personal information for identity

verification, AML/CTF and related compliance purposes, including checks against official records and sharing with authorised identity verification providers. Your consent is voluntary and may be withdrawn by contacting us, although withdrawal may affect our ability to verify your identity electronically or provide services. If electronic verification is not available or you do not consent, we may need to verify your identity in another way.

8. Disclosure of personal information

- 8.1 We may disclose personal information to our employees and authorised representatives, related entities, professional advisers, technology and service providers, identity verification providers including Infotrack and authorised sub-providers, Commonwealth, State and Territory authorities and official record holders through identity verification services, regulators including AUSTRAC, law enforcement agencies, courts, counterparties and other persons where required or authorised by law, where you consent, or where disclosure is otherwise permitted by the Privacy Act.
- 8.2 If ownership or control of all or part of our business changes, we may transfer relevant personal information to the new owner or controller, subject to applicable law.

9. Overseas disclosure

- 9.1 Some of our service providers may store or process personal information outside Australia. Where this occurs, we take reasonable steps to ensure that personal information is handled consistently with the Australian Privacy Principles, including through contractual and security arrangements where appropriate.

10. Security, storage and retention

- 10.1 We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. These steps may include secure systems, access controls, encryption in transit and at rest where appropriate, staff confidentiality obligations, training, monitoring and regular review of our information security practices.
- 10.2 We retain personal information only for as long as reasonably required for the purposes for which it was collected, for any secondary purpose permitted by the Australian Privacy Principles, or as required or authorised by law. When we no longer need personal information, we take reasonable steps to destroy or de-identify it. For AML/CTF purposes, we seek to retain evidence of verification and compliance rather than unnecessary copies of full identity documents, unless retention is required or authorised by law.

11. Access and correction

- 11.1 You may request access to the personal information we hold about you and ask us to correct it if it is inaccurate, out of date, incomplete, irrelevant or misleading. We will respond within a reasonable time. We may refuse access or correction where permitted by law, but if we do so we will explain why, where reasonable.

12. Complaints

- 12.1 If you have a complaint about how we have handled your personal information, please contact us first. We will acknowledge your complaint, consider whether further investigation is required, investigate where appropriate and respond within a

reasonable time. If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner for guidance on available options.

13. Contact details

Privacy contact: Stratocumulus Tuesday Pty Ltd (ACN 639 204 710), trading as Stratocumulus Legal (ABN 78 639 204 710)
Postal Address: PO Box 142, Subiaco, Western Australia, 6904

14. Changes to this policy

- 14.1 We may update this Privacy Policy from time to time to reflect changes in our practices or in the law. The latest version will be made available on request or through our usual publication channels.

<end>