PRIVACY POLICY

Version 1.0 | Effective Date: 24 March 2026

Last Updated: 24 March 2026

---

1. INTRODUCTION

1.1 About This Policy

This Privacy Policy explains how Sovereign Assets Limited (NZBN 9429052993879), trading as StackMotive ("**we**", "**us**", "**our**", "**StackMotive**") collects, uses, stores, discloses, and protects your personal information when you use the StackMotive platform, website, applications, and related services (collectively, the "**Platform**").

1.2 Our Commitment

We are committed to protecting your privacy and handling your personal information in accordance with the Privacy Act 2020 (NZ) and the Information Privacy Principles ("**IPPs**"). Where we have users in Australia, we also comply with the Privacy Act 1988 (Cth) and the Australian Privacy Principles ("**APPs**") to the extent they apply to us.

1.3 Scope

This policy applies to all individuals who:

(a) visit our website;

(b) create an account on the Platform;

(c) subscribe to any service tier;

(d) interact with Stack AI;

(e) subscribe to The Sovereign Signal newsletter or podcast;

(f) contact us for support; or

(g) otherwise provide us with personal information.

1.4 Agreement

By using the Platform, you acknowledge that you have read and understood this Privacy Policy. This policy is incorporated into and forms part of the StackMotive Terms of Service.

2. INFORMATION WE COLLECT

2.1 Information You Provide Directly

Category	Examples	Purpose
Account Information	Full name, email address, country of residence, timezone	Account creation and management
Billing Information	Payment method details (processed and stored by Stripe — we do not store card numbers)	Subscription billing
Profile Information	Display name, account preferences, notification settings	Platform personalisation
Support Communications	Emails, chat messages, feedback submissions	Customer support and service improvement
Newsletter/Podcast	Email address, name (if provided)	Content delivery for The Sovereign Signal

2.2 Information Generated Through Platform Use

Category	Examples	Purpose
Configuration Data	Watchlists, alert parameters, signal thresholds, panel layouts	Providing the Services
Usage Data	Pages viewed, features used, panels accessed, session duration, click patterns	Platform improvement and analytics
Stack AI Interaction Data	Queries submitted to Stack AI, conversation history within sessions	Providing AI functionality, service improvement
Device and Technical Data	IP address, browser type and version, operating system, device identifiers, screen resolution	Security, platform optimisation

2.3 Information from Third Parties

Source	Information	Purpose
Stripe	Payment confirmation, billing status, transaction IDs (not card numbers)	Billing management
Analytics providers	Aggregated usage patterns	Platform improvement

2.4 Sensitive Information

We do not intentionally collect sensitive personal information as defined under the Privacy Act 2020 (NZ) or the Privacy Act 1988 (Cth) (AU), such as racial or ethnic origin, political opinions, religious beliefs, health information, sexual orientation, or biometric data.

If you voluntarily provide sensitive information through Stack AI interactions or support communications, we process it only as necessary to respond to your query and do not use it for any other purpose.

2.5 Information We Do NOT Collect

We do **not** collect:

(a) credit card numbers or CVVs (these are processed and stored exclusively by Stripe);

(b) tax file numbers, social security numbers, or equivalent national identifiers;

(c) brokerage or exchange account passwords. Where you connect a brokerage account (e.g., via IBKR Flex), API credentials are encrypted at rest using per-user encryption keys and are never accessible in plaintext after initial entry;

(d) information about individuals other than you, unless you provide it to us for a specific purpose (e.g., referral programme).

3. HOW WE USE YOUR INFORMATION

3.1 Primary Purposes

We use your information for the following primary purposes:

(a) **Providing the Services:** operating the Platform, processing your configurations, generating Signal Data, and displaying analytical outputs;

(b) **Account Management:** creating and managing your account, authenticating your identity, and managing your subscription;

(c) **Billing:** processing payments, managing subscriptions, issuing invoices, and handling refunds;

(d) **Communication:** sending transactional emails (account confirmations, billing receipts, security alerts), responding to support queries, and delivering The Sovereign Signal newsletter (where subscribed);

(e) **Platform Improvement:** understanding how users interact with the Platform to improve functionality, fix bugs, and develop new features;

(f) **Security:** detecting and preventing fraud, unauthorised access, and other security threats;

(g) **Legal Compliance:** complying with applicable laws, regulations, and legal processes.

3.2 Secondary Purposes

With your consent or where otherwise permitted by law, we may also use your information for:

(a) **Aggregated Analytics:** creating anonymised, aggregated data sets for internal research and product development (this data cannot identify you);

(b) **Marketing:** sending marketing communications about new features, tier upgrades, or related content (you may opt out at any time — see section 8).

3.3 Stack AI Data Use

Queries you submit to Stack AI are processed by Anthropic, PBC ("**Anthropic**") through their Claude API. We use Stack AI interaction data to:

(a) provide AI-powered responses within the Platform;

(b) improve the quality and relevance of Stack AI responses; and

(c) monitor for misuse of the AI functionality.

We do not use your Stack AI interactions to train third-party AI models. Our agreement with Anthropic specifies that data submitted through the API is not used for model training. However, you should review Anthropic's own privacy policy for their data handling commitments.

3.4 Lawful Basis for Processing

Under the Privacy Act 2020 (NZ), we collect and process personal information in accordance with the Information Privacy Principles, particularly:

- **IPP 1 (Purpose):** We collect information only for a lawful purpose connected with our functions and where collection is necessary for that purpose;
- **IPP 3 (Collection from Subject):** We collect information directly from you wherever practicable;
- **IPP 6 (Access):** You may request access to your personal information (see section 8);
- **IPP 10 (Use):** We use information only for the purpose for which it was collected, or a directly related purpose.

For Australian users, we process your personal information in accordance with the APPs, including on the basis of consent and where processing is reasonably necessary for our functions and activities.

4. HOW WE SHARE YOUR INFORMATION

4.1 We Do Not Sell Your Information

We do not sell, rent, or trade your personal information to third parties for their marketing or advertising purposes.

4.2 Service Providers (Data Processors)

We share your information with the following categories of third-party service providers who process data on our behalf:

Provider	**Purpose**	**Data Shared**	**Location**
Stripe, Inc.	Payment processing	Billing information, transaction data	United States
Anthropic, PBC	Stack AI functionality (queries processed via Claude API; under our	Stack AI queries and conversation context	United States

Provider	Purpose	Data Shared	Location
	current agreement, API-submitted data is not used for model training)		
DigitalOcean	Platform hosting and infrastructure	All Platform data (encrypted at rest)	Sydney, Australia (SGP/SYD region)
Stytch / Google OAuth	User authentication and magic link login	Email address, authentication tokens	United States
Market data providers (including Marketaux, Finlight, Massive.com)	Market data feeds	Platform requests for data (no user personal information shared)	Various
Resend	Transactional and marketing emails	Email address, name	United States

4.3 Contractual Protections

All service providers are bound by data processing agreements that require them to:

(a) process your information only as instructed by us;

(b) implement appropriate technical and organisational security measures;

(c) not use your information for their own purposes; and

(d) delete or return your information upon termination of the relationship.

4.4 Legal and Regulatory Disclosure

We may disclose your information where required or permitted by law, including:

(a) in response to a court order, subpoena, or legal process;

(b) to comply with requests from regulatory bodies (including the Financial Markets Authority, the Office of the Privacy Commissioner, or ASIC);

(c) to enforce our Terms of Service;

(d) to protect the rights, property, or safety of StackMotive, our users, or the public; and

(e) to comply with any applicable regulatory obligations.

4.5 Business Transfers

If StackMotive is involved in a merger, acquisition, sale of assets, or bankruptcy, your information may be transferred to the successor entity. We will notify you by email and/or prominent notice on the Platform before your information becomes subject to a different privacy policy.

4.6 With Your Consent

We may share your information with third parties where you have given us explicit consent to do so.

5. CROSS-BORDER DATA TRANSFERS

5.1 Transfer Locations

Your personal information may be transferred to, stored, and processed in jurisdictions outside New Zealand, including the United States, where our service providers (including Stripe, Anthropic, and [Cloud Provider]) operate.

5.2 New Zealand Users

Under the Privacy Act 2020, we may transfer personal information outside New Zealand where the recipient is subject to privacy protections comparable to those in New Zealand, or where one of the permitted exceptions applies. We take reasonable steps to ensure overseas recipients protect your information consistently with the IPPs.

5.3 Australian Users

If you are located in Australia, you acknowledge and consent to the transfer of your personal information outside Australia as described in this section. In accordance with APP 8, before disclosing your information overseas, we take reasonable steps to ensure that overseas recipients do not breach the APPs. However, you acknowledge that by consenting to this cross-border transfer, we may not be accountable under the Privacy Act 1988 (Cth) for the actions of overseas recipients, and you may not be able to seek redress under that Act for any breach by an overseas recipient.

The countries to which your information may be transferred include:

- **United States:** Stripe (payment processing), Anthropic (AI services), Stytch (authentication), Resend (email delivery)
- **Australia:** DigitalOcean (platform hosting — Sydney region)
- **New Zealand:** Sovereign Assets Limited primary operations

5.4 Safeguards

We implement the following safeguards for cross-border transfers:

(a) contractual protections requiring recipients to handle information in accordance with this policy;

(b) encryption of data in transit and at rest;

(c) access controls limiting who can access personal information; and

(d) regular review of our service providers' security practices.

6. DATA SECURITY

6.1 Security Measures

We implement technical and organisational measures to protect your personal information, including:

(a) **Encryption:** All data transmitted between your browser and the Platform is encrypted using TLS 1.2 or higher. Data at rest is encrypted using AES-256 or equivalent;

(b) **Access Controls:** Access to personal information is restricted to authorised personnel on a need-to-know basis;

(c) **Authentication:** The Platform uses magic link authentication powered by Stytch, with Google OAuth available as an alternative sign-in method. Session tokens are used for authenticated access;

(d) **Infrastructure Security:** The Platform is hosted on [SPECIFY] with [SPECIFY security features — e.g., VPC isolation, firewall rules, intrusion detection];

(e) **Monitoring:** We monitor for unauthorised access attempts and security anomalies; and

(f) **Incident Response:** We maintain an incident response plan for security events.

6.2 No Guarantee

While we take reasonable steps to protect your information, no method of electronic transmission or storage is completely secure. We cannot guarantee absolute security of your information.

6.3 Your Responsibilities

You are responsible for:

(a) maintaining the confidentiality of your account credentials;

(b) using strong, unique passwords; and

(c) notifying us immediately if you suspect unauthorised access to your account.

7. DATA RETENTION

7.1 Retention Periods

We retain your personal information for the following periods:

Data Category	**Retention Period**	**Rationale**
Account Information	Duration of account + 12 months	Service delivery and post-termination queries
Billing and Transaction Records	Duration of account + 7 years	Tax and financial record-keeping obligations (Tax Administration Act 1994)
Configuration Data	Duration of account + 30 days	Service delivery; deleted 30 days after account closure
Usage Data	24 months (rolling)	Platform improvement and analytics
Stack AI Interactions	90 days	Service quality monitoring; then deleted or anonymised
Support Communications	Duration of account + 24 months	Service continuity and dispute resolution
Marketing Consent Records	Duration of consent + 24 months	Compliance evidence

7.2 Anonymisation

Where possible, we anonymise data rather than delete it, so that we can use it for aggregated analytics without identifying you.

7.3 Deletion

Upon expiry of the relevant retention period, we delete or anonymise your personal information. Deletion from backup systems may take up to an additional 90 days.

7.4 Legal Holds

We may retain information beyond the standard retention period where required to comply with legal obligations, resolve disputes, or enforce our agreements.

8. YOUR RIGHTS

8.1 New Zealand Users

Under the Privacy Act 2020, you have the following rights:

(a) **Access (IPP 6):** You may request access to your personal information held by us. We will respond within 20 working days;

(b) **Correction (IPP 7):** You may request correction of inaccurate personal information. If we decline to correct it, we will attach a statement of the correction sought;

(c) **Deletion:** While not an express right under the Privacy Act, we will delete your personal information upon request, subject to our legal retention obligations;

(d) **Complaints:** You may complain to the Office of the Privacy Commissioner if you believe we have breached the Privacy Act.

8.2 Australian Users

Under the Privacy Act 1988 (Cth) and the APPs, you additionally have the right to:

(a) **Access (APP 12):** Request access to your personal information. We will respond within 30 days;

(b) **Correction (APP 13):** Request correction of inaccurate, out-of-date, incomplete, irrelevant, or misleading information;

(c) **Complaints (APP 1):** Complain to us about a breach of the APPs. If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner (OAIC);

(d) **Opt Out of Direct Marketing (APP 7):** Request that we stop using your information for direct marketing purposes.

8.3 Exercising Your Rights

To exercise any of these rights, contact us at:

Email: privacy@sovereignassets.org

We may need to verify your identity before processing your request. We will not charge a fee for a straightforward access or correction request, but we may charge a reasonable fee for manifestly unfounded or excessive requests.

8.4 Marketing Communications

You may opt out of marketing communications at any time by:

(a) clicking the "unsubscribe" link in any marketing email;

(b) adjusting your notification preferences in the Platform settings; or

(c) contacting us at privacy@sovereignassets.org.

Opting out of marketing does not affect transactional communications (billing confirmations, security alerts, service notifications).

9. COOKIES AND TRACKING

9.1 Cookies We Use

Cookie Type	Purpose	Duration	Can You Disable?
Essential/Session	Authentication, session management, security	Session / up to 24 hours	No — required for Platform to function
Preference	Remembering your settings (timezone, layout, theme)	Up to 12 months	Yes — but may degrade experience
Analytics	Understanding usage patterns (anonymised)	Up to 24 months	Yes

9.2 Third-Party Cookies

We may use third-party analytics services that set their own cookies. We do not use advertising cookies or tracking pixels from ad networks.

9.3 Managing Cookies

You can manage or disable non-essential cookies through:

(a) the cookie consent banner displayed on first visit;

(b) your browser settings; or

(c) the Platform's privacy settings (where available).

Disabling essential cookies will prevent you from using the Platform.

10. CHILDREN'S PRIVACY

The Platform is not intended for use by individuals under 18 years of age. We do not knowingly collect personal information from children. If we become aware that we have collected personal information from a child under 18, we will take steps to delete it promptly. If you believe a child has provided us with personal information, please contact us at privacy@sovereignassets.org.

11. NOTIFIABLE PRIVACY BREACHES

11.1 New Zealand

In accordance with Part 6A of the Privacy Act 2020, if we become aware of a privacy breach that we believe has caused, or is likely to cause, serious harm to any affected individual, we will:

(a) notify the Office of the Privacy Commissioner as soon as practicable; and

(b) notify you as soon as practicable, including a description of the breach, what information was affected, and what steps we are taking in response.

11.2 Australia

If we experience an eligible data breach under Part IIIC of the Privacy Act 1988 (Cth) that is likely to result in serious harm to any individual, we will:

(a) notify the Office of the Australian Information Commissioner; and

(b) notify affected individuals,

in accordance with the Notifiable Data Breaches scheme.

11.3 Our Approach

Regardless of legal thresholds, we adopt a presumption of notification — if we believe a breach may affect your data, we will err on the side of transparency and notify you promptly.

12. THIRD-PARTY LINKS AND SERVICES

The Platform may contain links to third-party websites, services, or resources. This Privacy Policy does not apply to those third parties. We encourage you to review the privacy policies of any third-party service you access. We are not responsible for the privacy practices or content of third-party services.

13. CHANGES TO THIS POLICY

13.1 Updates

We may update this Privacy Policy from time to time to reflect changes in our practices, the Platform, or applicable law. The "Last Updated" date at the top of this policy indicates when it was most recently revised.

13.2 Notification

We will notify you of material changes to this policy by:

(a) posting the updated policy on the Platform;

(b) displaying a prominent notice in the Platform interface; and

(c) sending an email to your registered email address for changes we consider significant.

13.3 Continued Use

Your continued use of the Platform after the effective date of an updated policy constitutes acceptance of the changes. If you do not agree, you should discontinue use of the Platform and contact us to close your account.

14. CONTACT US

If you have questions, concerns, or requests regarding this Privacy Policy or our handling of your personal information, please contact:

Privacy Officer Sovereign Assets Limited (NZBN 9429052993879), trading as StackMotive
Email: privacy@sovereignassets.org

For New Zealand privacy complaints: Office of the Privacy Commissioner PO Box 10094, Wellington 6143 Phone: 0800 803 909 Website: https://privacy.org.nz

For Australian privacy complaints: Office of the Australian Information Commissioner GPO Box 5218, Sydney NSW 2001 Phone: 1300 363 992 Website: https://www.oaic.gov.au

---

This Privacy Policy applies to all users of the StackMotive Platform.