



● OFFICIAL DOCUMENT

GLOBAL DATA GOVERNANCE

RockGlobal Privacy Policy

Privacy, Data Handling and Individual Rights

DOCUMENT

RG-LEGAL-PRIVACY-001

VERSION

1.0

LAST UPDATED

2 September 2026

ROUTE-AWARE POLICY

RockGlobal Legal and Compliance

Document control

Control field	Approved value
Document	RockGlobal Privacy Policy
Document ID	RG-LEGAL-PRIVACY-001
Version	1.0
Effective date	2 September 2026
Last updated	2 September 2026
Document owner	Legal and Compliance
Review cycle	At least annually and after any material change
Status	Approved master copy

Contents

This directory follows the approved master copy. Section headings are retained exactly for reliable legal review and future version comparison.

Section	Subject
—	Privacy at a glance
1	Who is responsible for your information
2	What personal information means
3	Personal information we collect
4	How we collect personal information
5	Why we use personal information
6	Automated tools, profiling, and human review
7	When we disclose personal information
8	International transfers
9	Security and data breaches
10	Cookies and similar technologies
11	Direct marketing and communication choices
12	How long we retain personal information
13	Your privacy rights
14	Complaints
15	Children
16	Third-party sites and services
17	Changes to this policy
18	Contact us

RockGlobal respects your privacy. This Privacy Policy explains how the RockGlobal entity responsible for your relationship collects, uses, holds, shares, transfers, and protects personal information, and the choices and rights available to you.

This policy applies to RockGlobal websites, client portals, trading and account services, applications, tools, events, promotions, communications, and other services that link to it (together, the **Services**). It should be read with any collection notice, cookie notice, product disclosure, client agreement, terms of business, or other notice presented when personal information is collected.

Privacy at a glance

- The RockGlobal entity responsible for your information depends on the website, jurisdiction, onboarding route, or agreement through which you receive Services.
- We collect information needed to provide and secure the Services, administer accounts, meet legal and regulatory obligations, and communicate with you.
- Financial-services laws may require us to verify identity, source of funds or wealth, tax residence, and other eligibility information.
- We do not sell personal information for money. Where a law gives a broader meaning to “sell” or “share,” you may exercise any applicable opt-out right as described below.
- We use service providers and may transfer information internationally with appropriate safeguards.
- You may have rights to access or correct your information and, depending on your location, additional rights.
- Privacy requests may be sent to the relevant route contact in section 18.

1. Who is responsible for your information

RockGlobal is a brand used by separate legal entities. The entity responsible for your personal information is normally the entity identified in the website footer, application form, client agreement, account opening documents, or other service notice provided to you.

Route	Responsible RockGlobal entity	Registration details	Primary privacy contact
International	RockGlobal International LLC	Company No. 3108 LLC 2023, registered in Saint Vincent and the Grenadines	info@rockglobal.com
Australia	ROCKGLOBAL CAPITAL MARKETS PTY LTD	ABN 12 108 915 233; Australian Financial Services Licence No. 282 288	support@rockglobaltrading.com
New Zealand	Rockfort Markets Limited , trading as RockGlobal	NZBN 9 429 042 010 807; FSP509 766	support@rockglobal.co.nz

For the New Zealand route, registration on the Financial Service Providers Register does not itself mean that Rockfort Markets Limited is licensed or actively supervised for every financial service. This policy describes privacy handling only and does not expand the services any entity is authorised or permitted to provide.

Each RockGlobal entity generally acts as an independent controller or agency for its own clients, prospects, users, personnel, and business contacts. RockGlobal entities may also share systems, personnel, or service providers and may exchange information as described in this policy. Where two or more entities jointly determine why and how particular information is processed, they will allocate responsibilities as required by applicable law. You may contact any RockGlobal route if you are unsure which entity is responsible; we will direct your request to the appropriate entity.

2. What personal information means

In this policy, **personal information** means information or an opinion about an identified individual, or an individual who is identifiable or reasonably identifiable. It includes “personal data,” “personal information,” and similar terms under applicable privacy laws.

Some laws give additional protection to **sensitive information** or **special-category data**, such as biometric identifiers, health information, racial or ethnic origin, religious beliefs, political opinions, trade-union membership, sexual orientation, criminal-history information, or precise geolocation. We collect sensitive information only where it is reasonably necessary and permitted by law, and where any required consent or other legal condition is satisfied.

Information that has been irreversibly anonymised so that no individual can reasonably be identified is not personal information. We may use anonymised or aggregated information for lawful business purposes.

3. Personal information we collect

The information we collect depends on your route, the Services you use, and legal requirements. It may include:

3.1 Identity and contact information

- name, title, date and place of birth, age, gender, nationality, citizenship, signature, and photograph;
- residential, postal, and business addresses;
- email address, telephone number, preferred language, and communication preferences; and
- username, client or account number, and other identifiers.

3.2 Verification, eligibility, and compliance information

- passport, national identity card, driver licence, tax number, visa or residency information, and proof of address;
- identity-verification results, document authenticity checks, facial image or liveness check where used and permitted, and fraud-risk signals;
- occupation, employer, employment status, source of funds, source of wealth, income, assets, liabilities, financial position, and investment objectives;
- trading knowledge, experience, risk tolerance, product eligibility, and appropriateness or suitability responses;
- tax residence and status, beneficial ownership, corporate ownership or control, authorised representatives, and powers of attorney;
- politically exposed person, sanctions, adverse-media, watchlist, insolvency, criminal-history, and other due-diligence results, where lawful; and
- information required for anti-money laundering, counter-terrorism financing, sanctions, fraud prevention, tax reporting, and other legal or regulatory checks.

3.3 Account, transaction, and service information

- application and onboarding information, agreements, consents, acknowledgements, and account settings;
- deposits, withdrawals, payment methods, bank-account details, wallet or payment identifiers, transaction history, balances, and billing records;
- orders, positions, trades, instrument and platform activity, timestamps, instructions, execution information, and account performance;
- product subscriptions, feature use, competition or promotion entries, rewards, and eligibility records; and
- complaints, disputes, claims, investigations, support requests, and service history.

We do not normally need full payment-card credentials because payment providers may collect them directly. If we receive payment information, we handle it in accordance with applicable security and retention requirements.

3.4 Device, technical, and usage information

- IP address, device identifiers, operating system, browser type, language, time zone, and approximate location derived from IP;
- login events, session identifiers, authentication records, security events, crash reports, and diagnostic information;
- pages viewed, links selected, referral source, feature use, date and time of access, and interaction data; and
- cookie identifiers, pixels, local storage, and preference data as described in section 10.

3.5 Communications and recordings

- emails, chat messages, form submissions, survey responses, social-media interactions, and correspondence;
- telephone or video-call recordings and transcripts where recording is permitted and notice has been provided; and
- marketing preferences, event attendance, and campaign interactions.

3.6 Business, partner, and professional information

- employer, role, professional contact details, qualifications, and business relationship;
- introducing broker, affiliate, supplier, contractor, representative, or institutional-client information;
- commission, referral, performance, and due-diligence records; and
- information about directors, officers, employees, shareholders, beneficial owners, trustees, partners, or authorised persons connected with an organisation.

3.7 Inferences and risk indicators

We may derive risk scores, fraud indicators, client segments, service preferences, and similar inferences from the information above. We do not treat an inference as fact without appropriate context and review where it may materially affect you.

Please do not provide personal information about another person unless you are authorised to do so and, where required, have told them how RockGlobal will handle it.

4. How we collect personal information

We may collect personal information:

- **directly from you**, including through websites, forms, applications, portals, platforms, calls, emails, chats, events, surveys, competitions, and support interactions;
- **automatically**, through cookies, logs, security tools, analytics, and your use of websites, platforms, or applications;
- **from RockGlobal entities**, where needed to route an enquiry, administer a shared service, prevent fraud, meet group governance requirements, or support an authorised transfer of a relationship;
- **from service providers**, including identity-verification, screening, payment, banking, platform, hosting, analytics, customer-support, cybersecurity, and fraud-prevention providers;
- **from business partners**, including introducing brokers, affiliates, authorised representatives, employers, corporate clients, or referral partners;
- **from public and official sources**, including company, insolvency, court, electoral, sanctions, regulatory, and professional registers, and information you make public; and
- **from regulators, law-enforcement bodies, dispute-resolution schemes, financial institutions, counterparties, and other authorised third parties.**

Where required, we will provide a collection notice at or before collection, or within the period required when information is collected indirectly. If you do not provide information that is required by law, contract, or operational necessity, we may be unable to open or maintain an account, process a transaction, provide a requested feature, or respond fully to you.

Where lawful and practicable, you may interact with us anonymously or using a pseudonym for general website browsing or general enquiries. We cannot offer anonymity where identity is required by law or necessary to provide the requested Service.

5. Why we use personal information

We use personal information only where we have a lawful purpose and, where applicable, a legal basis.

Purpose	Examples	Legal basis where GDPR-style law applies
Provide and administer Services	Process applications; create and operate accounts; authenticate users; provide platforms, tools, subscriptions, support, payments, withdrawals, statements, and notices	Contract; steps requested before entering a contract; legitimate interests
Verify identity and eligibility	KYC and customer due diligence; verify documents; assess residency, eligibility, appropriateness, or suitability	Legal obligation; contract; substantial public interest where recognised; legitimate interests
Prevent financial crime and protect security	AML/CTF, sanctions and PEP screening; detect fraud, account abuse, cyber threats, market abuse, or suspicious activity; investigate incidents	Legal obligation; legitimate interests; substantial public interest where recognised
Execute and record activity	Receive and process instructions; maintain order, transaction, communications, and audit records; reconcile accounts	Contract; legal obligation; legitimate interests
Meet legal and regulatory obligations	Regulatory reporting; tax reporting; recordkeeping; complaints; audits; lawful requests; litigation and enforcement	Legal obligation; public interest where recognised; legitimate interests
Operate and improve our business	Troubleshooting; analytics; quality assurance; research; product development; training; business continuity; internal reporting	Legitimate interests; consent where required
Communicate with you	Service messages, security alerts, policy changes, support, surveys, and relationship management	Contract; legal obligation; legitimate interests
Market responsibly	Send news, education, events, promotions, or service information; measure campaign effectiveness; manage preferences	Consent where required; legitimate interests where permitted
Manage corporate relationships	Supplier, partner, affiliate, introducing-broker, institutional, recruitment, and professional relationships	Contract; legal obligation; legitimate interests
Corporate transactions and legal claims	Due diligence for a merger, financing, restructure, sale, or transfer; establish, exercise, or defend legal rights	Legitimate interests; legal obligation

Our **legitimate interests** include operating a secure and effective financial-services business, preventing fraud and misuse, protecting clients and systems, improving Services, managing relationships, and communicating about relevant Services. We balance those interests against your rights and reasonable expectations.

Where we rely on **consent**, you may withdraw it at any time. Withdrawal does not affect processing already carried out lawfully and may not affect processing supported by another legal basis.

We will not use personal information for a materially incompatible new purpose without taking the steps required by law, which may include giving further notice or obtaining consent.

6. Automated tools, profiling, and human review

We may use automated tools to support identity verification, sanctions and watchlist screening, fraud and cybersecurity detection, transaction monitoring, client classification, product eligibility, risk management, and service personalisation.

These tools may analyse identity, device, account, transaction, behavioural, and publicly available information and may generate alerts or risk indicators.

An alert or score may result in additional verification, delayed processing, a request for information, a restriction, or referral to trained personnel. Where applicable law gives you rights in relation to a decision based solely on automated processing that produces legal or similarly significant effects, we will provide the required information and a way to request human review, express your point of view, or contest the decision.

We do not use sensitive information to unlawfully discriminate. We periodically review material automated systems for accuracy, security, fairness, and legal compliance. Further information about a material automated decision may be provided at the point of collection or on request, subject to security, fraud-prevention, legal, and third-party rights.

7. When we disclose personal information

We may disclose personal information where reasonably necessary to:

- another RockGlobal entity for authorised routing, shared operations, compliance, risk management, security, or relationship support;
- identity-verification, screening, fraud-prevention, cybersecurity, cloud, hosting, data-storage, communications, analytics, customer-support, document-management, and software providers;
- banks, payment providers, custodians, trading platforms, liquidity or execution providers, counterparties, brokers, and other parties involved in providing a requested Service or processing a transaction;
- introducing brokers, affiliates, authorised representatives, corporate-account administrators, employers, or partners connected with your relationship, subject to authority and applicable law;
- professional advisers, auditors, insurers, consultants, debt-recovery providers, and dispute-resolution services;
- regulators, supervisory authorities, tax authorities, courts, law-enforcement bodies, financial-intelligence units, sanctions authorities, and other government agencies when required or permitted by law;
- a prospective buyer, investor, financier, successor, or transaction adviser in connection with a proposed or completed merger, financing, restructure, transfer, or sale, subject to appropriate confidentiality and legal safeguards; or
- another person where you direct us, consent, or where disclosure is otherwise required or permitted by law.

Service providers may use personal information only for the services they provide to us or for another purpose permitted by law. We use due diligence, contractual controls, access restrictions, and oversight proportionate to the information and risk.

We may disclose anonymised or aggregated information that does not reasonably identify you.

8. International transfers

RockGlobal operates across jurisdictions and uses international technology and service providers. Personal information may therefore be accessed, processed, or stored outside the country where it was collected. Depending on your route and the providers used, recipient locations may include Australia, New Zealand, Saint Vincent and the Grenadines, Singapore, the United States, the United Kingdom, countries in the European Economic Area, and other locations disclosed at collection or in an applicable service notice.

Privacy protections may differ between countries. Where required, we use measures designed to protect transferred information, such as:

- transfer to a jurisdiction recognised as providing adequate or comparable protection;
- contractual privacy, confidentiality, security, and audit obligations;
- approved standard contractual clauses or equivalent transfer terms;
- verification that the recipient is subject to applicable privacy law;

- your informed authorisation where the law permits it; or
- another lawful transfer mechanism or exception.

New Zealand disclosures are handled with regard to Information Privacy Principle 12. Australian disclosures are handled with regard to Australian Privacy Principle 8 and related requirements. Where the EU or UK GDPR applies, information about the relevant transfer safeguard and how to obtain a copy is available on request, subject to lawful redactions.

9. Security and data breaches

We use administrative, technical, organisational, and physical safeguards designed to protect personal information against loss, misuse, interference, unauthorised access, alteration, disclosure, and destruction. Depending on risk, these measures may include access controls, authentication, encryption in transit or at rest, network and endpoint protection, logging and monitoring, secure development and change controls, vendor due diligence, staff training, confidentiality duties, backups, incident response, and business-continuity procedures.

No internet transmission or storage system is completely secure. You should protect account credentials, use unique passwords and available multi-factor authentication, keep devices secure, and contact us immediately if you suspect unauthorised account activity or a fraudulent communication.

We maintain procedures to identify, assess, contain, investigate, and remediate suspected personal-information breaches. We will notify affected individuals and relevant authorities when required by applicable law, including the Australian Notifiable Data Breaches scheme and New Zealand's privacy-breach notification requirements.

10. Cookies and similar technologies

We and authorised providers may use cookies, pixels, software development kits, local storage, tags, and similar technologies to:

- keep websites and portals functioning and secure;
- maintain sessions, remember preferences, and balance network traffic;
- understand performance, errors, and how Services are used;
- measure communications and campaign effectiveness; and
- provide or measure relevant content and advertising where permitted.

Cookies may be **strictly necessary**, **functional**, **analytics**, or **marketing and measurement** technologies. Non-essential technologies are used only with consent where required. You can use the cookie banner or **Cookie Settings** link to make or change available choices. You can also control cookies through your browser, although blocking necessary technologies may affect functionality.

We do not sell personal information for money. To the extent use of advertising or measurement technology is treated as a “sale,” “sharing,” or targeted advertising under applicable law, you may opt out through Cookie Settings or the route contact in section 18. Where legally required and technically supported, we process recognised browser-based opt-out preference signals.

Our separate Cookie Policy gives further information about active providers, purposes, and durations and forms part of this policy by reference.

11. Direct marketing and communication choices

We may send service-related communications that are necessary to administer your relationship, such as security, transaction, account, legal, and policy notices. You may not be able to opt out of these while you use the relevant Service.

We send direct marketing only where permitted. You can stop marketing emails by using the unsubscribe link, changing available account preferences, or contacting us. You may also ask us not to use your personal information for direct marketing and, where applicable, ask us to identify the source of the information. We will honour valid requests and may retain a minimal suppression record so that we do not contact you again through the opted-out channel.

Opting out of marketing does not stop service messages. Cookie-based advertising and measurement choices should be managed through Cookie Settings.

12. How long we retain personal information

We keep personal information only for as long as reasonably necessary for the purpose collected, including to provide Services, meet legal and regulatory duties, maintain security and audit trails, resolve complaints, and establish, exercise, or defend legal claims.

Retention depends on the information, route, relationship, and law. Our general criteria are:

Information	Typical retention approach
Unsuccessful or incomplete applications	For the period reasonably needed to manage the application, prevent fraud, answer queries, and meet legal duties, then deleted or anonymised unless a longer period is required
Client identity, due-diligence, account, and transaction records	For the relationship and the applicable statutory period afterwards; this is commonly at least five years for relevant New Zealand AML/CFT records and seven years for relevant Australian AML/CTF records
Trading instructions, communications, complaints, and legal records	For the applicable regulatory, limitation, audit, or dispute period, and longer where a matter remains active or a legal hold applies
Security logs and technical records	For a period proportionate to security, fraud, troubleshooting, and legal needs, with shorter periods used where practicable
Marketing records	Until you opt out or the information is no longer needed, with a minimal suppression record retained as necessary
Cookie data	For the duration described in the Cookie Policy or consent tool

At the end of the applicable period, we securely delete, destroy, anonymise, or place information beyond operational use, unless continued retention is required or permitted by law. Backup copies may remain until securely overwritten under normal cycles.

13. Your privacy rights

Rights vary by location and are subject to conditions and exceptions. Depending on applicable law, you may have the right to:

- know whether we process your personal information and receive information about that processing;
- access personal information we hold about you and receive a copy;
- correct inaccurate information or complete information that is incomplete;
- request deletion or erasure;
- restrict or object to certain processing, including direct marketing;
- withdraw consent at any time where processing relies on consent;
- receive certain information in a structured, commonly used, machine-readable format or ask for it to be transferred to another controller;
- opt out of sale, sharing, targeted advertising, or certain profiling where those concepts apply;
- limit certain uses or disclosures of sensitive personal information where applicable;

- request human review of certain solely automated decisions;
- complain to a privacy or data-protection authority; and
- not be discriminated against for exercising an applicable privacy right.

These rights are not absolute. For example, we may need to retain information to comply with AML/CTF, sanctions, tax, financial-services, recordkeeping, security, or legal-claims obligations. If we cannot fulfil a request in whole or in part, we will explain the reason where the law permits.

13.1 Australia

If the Privacy Act 1988 (Cth) and Australian Privacy Principles apply, you may request access to and correction of personal information. You may also complain about our handling of personal information. We will respond within the period required by law and, if access or correction is refused, provide reasons and available complaint pathways where required.

13.2 New Zealand

If the Privacy Act 2020 applies, you may request access to personal information and correction of information you believe is wrong. If we do not make a requested correction, you may ask us to attach a statement of correction as provided by law. You may complain to the Office of the Privacy Commissioner if you are dissatisfied with our response.

13.3 European Economic Area and United Kingdom

Where the EU GDPR or UK data-protection law applies, rights may include access, rectification, erasure, restriction, portability, objection, withdrawal of consent, and rights concerning solely automated decisions. You have an unconditional right to object to processing for direct marketing. You may complain to the supervisory authority where you live or work, or where you believe a breach occurred.

13.4 California and other United States jurisdictions

Where applicable United States state privacy law applies, rights may include confirming processing, access or knowledge, correction, deletion, portability, and opting out of sale, sharing, targeted advertising, or certain profiling. California residents may also have the right to limit certain uses of sensitive personal information and to receive information about categories of information, sources, purposes, and recipients. We will not unlawfully discriminate against you for exercising a right.

13.5 Exercising a right

Send your request to the relevant contact in section 18 and state the right you wish to exercise. We may ask for information reasonably necessary to verify your identity and authority. Do not send unnecessary identity documents by ordinary email; we will provide a secure method if documents are needed.

An authorised agent may submit a request where permitted. We may require evidence of authority and may verify the request directly with you. We generally do not charge a fee, but may do so or decline a request where permitted by law, including for manifestly unfounded, excessive, or repetitive requests.

We will respond within the time required by applicable law. You may appeal a refusal where applicable by replying to our decision or using the complaint process below.

14. Complaints

If you believe we have mishandled personal information, contact the responsible route first. Please describe the issue, relevant dates, the RockGlobal service or account involved, and the outcome you seek. We will acknowledge, investigate, and respond within a reasonable period and any period required by law.

If you remain dissatisfied, you may contact the competent authority, including:

- **Australia:** Office of the Australian Information Commissioner — <https://www.oaic.gov.au/>
- **New Zealand:** Office of the Privacy Commissioner — <https://www.privacy.org.nz/>
- **EEA:** the data-protection authority in the country where you live or work, or where the issue occurred;
- **United Kingdom:** Information Commissioner's Office — <https://ico.org.uk/>; or
- another privacy, consumer, financial, or data-protection authority with jurisdiction over your complaint.

Nothing in this section limits any right to use another complaint or dispute-resolution pathway available under a client agreement or applicable law.

15. Children

The Services are intended for adults aged 18 years or older and are not directed to children. We do not knowingly open trading or financial-services accounts for children or knowingly use children's personal information for targeted advertising.

Some business or verification records may incidentally contain information about a minor, such as a beneficiary or dependent, where lawful and necessary. In those circumstances we apply protections appropriate to the person's age and the sensitivity of the information. If you believe a child has provided personal information contrary to this policy, contact us so we can investigate and take appropriate action.

16. Third-party sites and services

The Services may link to websites, platforms, applications, social networks, or services operated by others. Their privacy practices are governed by their own notices. We are not responsible for a third party's handling of information unless we process it jointly, engage that party as our service provider, or applicable law provides otherwise. Review the relevant privacy notice before providing information.

17. Changes to this policy

We may update this policy to reflect changes in law, regulation, technology, providers, or our Services. The current version will be published with the effective or last-updated date. Where a change materially affects how we use personal information, we will take additional steps required by law, which may include a prominent notice, direct communication, renewed cookie choice, or consent.

We keep prior versions in our records. You may request an earlier version using the contacts below.

18. Contact us

Address privacy questions, requests, and complaints to **Privacy and Compliance** and include the RockGlobal website, route, or account to which your enquiry relates.

International route

RockGlobal International LLC

Company No. 3108 LLC 2023

2nd Floor, Reigate Building, P.O. Box 356

Kingstown, Saint Vincent and the Grenadines

Email: info@rockglobal.com

Australian route

ROCKGLOBAL CAPITAL MARKETS PTY LTD

ABN 12 108 915 233

Australian Financial Services Licence No. 282 288

Email: support@rockglobaltrading.com

New Zealand route

Rockfort Markets Limited, trading as RockGlobal

NZBN 9 429 042 010 807; FSP509 766

Level 5/187 Broadway

Newmarket, Auckland 1023, New Zealand

Email: support@rockglobal.co.nz

If you contact the wrong route, we may securely forward your request to the appropriate RockGlobal entity and tell you that we have done so.