

DATA PROTECTION · PRIVACY NOTICE

Privacy Notice

How Algotoria Limited collects, uses, stores and protects personal data — and the rights you have over it. This notice covers prospective clients, clients, introducers and website visitors.

CONTROLLER	CONTACT	VERSION	EFFECTIVE
Algotoria Limited BVI Reg. No. 2161048	compliance@algotoria.com	1.0	27 August 2026

1. Who we are

Algotoria Limited ("Algotoria", "we") is a company incorporated in the British Virgin Islands under number 2161048, with its registered office at Quijano Chambers, P.O. Box 3159, Road Town, Tortola, British Virgin Islands. Algotoria is an Approved Investment Manager and provides discretionary algorithmic trading management over accounts that clients own and control in their own name at third-party cryptocurrency exchanges.

For the personal data described in this notice, Algotoria is the **data controller** — we decide what is collected and why. Our home data-protection law is the **BVI Data Protection Act, 2021**, which applies to us as a BVI-established controller wherever the data is physically held. Where we offer services to individuals in the United Kingdom or the European Economic Area, we also apply the standards of the UK GDPR and the EU GDPR to that processing.

2. The short version

Your identity documents never leave the European Union. Everything we hold to verify who you are — passport or ID, proof of address, evidence of source of funds and source of wealth, and your signed agreements — is stored on our own servers in a Tier III, ISO/IEC 27001-certified data centre in **Germany**. That store is segregated from the trading platform and is never placed in a public cloud.

Only trading data sits near the exchanges. The platform that places your orders holds an anonymised account identifier, your exchange API credentials in encrypted form, and the record of trades. It runs in Google Cloud in **Tokyo** because it has to be within milliseconds of the exchange matching engines; every extra millisecond of round-trip widens slippage and raises the chance of a failed order.

We never hold your funds and cannot move them. The API credentials you give us carry trade-only permissions. No part of our system is able to withdraw, transfer or pledge your assets.

3. What we collect

3.1 Identity and onboarding data

To meet our anti-money-laundering and know-your-client obligations we collect your full name, date of birth, nationality, residential address, contact details, government identity document, proof of address, tax status declarations (including FATCA and CRS), politically-exposed-person status, and evidence of your source of funds and source of wealth. For corporate and institutional clients we collect the equivalent for the entity and its beneficial owners and authorised signatories.

3.2 Account and trading data

An internal account identifier, the exchange-side account or sub-account identifier, your exchange API credentials, and the resulting record of positions, orders, fills, transfers and performance.

3.3 Communications and messaging identifiers

Records of our correspondence with you, and the identifiers of the channel you use to reach us. Where you use our Telegram bot — which is our client-facing monitoring interface — we store your **Telegram account identifier, Telegram username and Telegram display name**, together with a language preference, so the bot can recognise you and show you the right accounts. This is the only personal data of yours that our cloud trading platform holds.

3.4 Website data

Information you submit through forms on algotoria.com, including the compliance declaration form. Our website does not run advertising trackers or third-party analytics profiling.

4. Why we use it, and on what legal basis

PURPOSE	DATA USED	LEGAL BASIS
Verifying your identity; anti-money-laundering, sanctions and PEP screening	Identity and onboarding data	Legal obligation
Entering into and performing the asset management agreement	Identity, account and trading data	Performance of a contract
Placing and reconciling orders on your exchange account	Account identifier, API credentials, trading data	Performance of a contract
Reporting to you — statements, quarterly reports, monitoring alerts	Account, trading and messaging data	Performance of a contract
Fee calculation, accounting and statutory financial reporting	Identity, account and trading data	Legal obligation; contract
Security monitoring, fraud prevention and incident investigation	Account, trading, communications data	Legitimate interests
Responding to enquiries from prospective clients	Contact details and enquiry content	Legitimate interests; consent
Complying with regulatory requests and court orders	Any of the above, as required	Legal obligation

Where we rely on **legitimate interests**, we have considered the effect on you and use the minimum data needed for the purpose. Where we rely on **consent** — for example marketing communications — you may withdraw it at any time without affecting the lawfulness of what came before.

5. We do not sell your data, and we do not profile you for advertising

We do not sell, rent or trade personal data. We do not use your data to build advertising profiles, and we do not make automated decisions that produce legal effects for you. Our trading algorithms act on market data and your account configuration; they do not evaluate you as a person.

6. Where your data is held

We deliberately separate identity data from trading data and store each where it belongs.

WHAT	WHERE	WHY THERE
Identity, onboarding and contractual records	Germany (EU) — Algotoria's own servers in a Tier III, ISO/IEC 27001-certified data centre	EU-grade protection; segregated from the trading platform; never in a public cloud
Account identifiers, encrypted API credentials, trading records, Telegram identifiers	Japan — Google Cloud, Tokyo region	Must sit within milliseconds of the exchange matching engines to limit slippage and failed orders
The same trading data, mirrored	Qatar — Google Cloud, Doha region	A standby copy of the platform, kept ready so service can be restored if the Tokyo region is lost
Backups of critical data	Netherlands (EU) — Google Cloud Storage	Geographic separation of backup copies

6.1 International transfers

Because we are established in the British Virgin Islands and our infrastructure is in Germany, Japan, Qatar and the Netherlands, personal data crosses borders. Every transfer is covered by a written data processing agreement with the provider. Germany and the Netherlands are within the EEA. Japan benefits from a UK and EU adequacy decision. **Qatar does not benefit from an adequacy decision**; that transfer relies on the Standard Contractual Clauses incorporated into our Google Cloud data processing agreement, supported by a transfer risk assessment and by the technical measures described in section 7 — in particular, that the credentials held there are encrypted and the key that unlocks them is held in a different system.

You may request a copy of the safeguards applying to any transfer by writing to compliance@algotoria.com.

7. How we protect it

- **Trade-only credentials.** The API keys you issue to us cannot withdraw, transfer or pledge assets. We programmatically reject any key that carries withdrawal permission.
- **Encryption of your credentials.** Your exchange API credentials are encrypted by our platform before they are written to the database. The master key that unlocks them is held in a separate cloud secrets manager, so access to the database alone yields nothing usable.
- **IP binding.** Trading credentials are restricted to the fixed address of our execution server, so a copied credential cannot be used from anywhere else.
- **Encryption in transit.** All data moves over TLS. Sensitive material you send us travels through the encrypted channel described in section 8.
- **Access control.** Access is role-based, least-privilege, logged, and protected by multi-factor authentication. Our staff have no physical access to the trading servers.
- **Monitoring.** A 24/7 network and security operations centre monitors the platform, with alerting and a documented incident-response procedure.

8. Who we share it with

We share personal data only with parties who need it to deliver our service or where the law requires it. We require every processor to act on our instructions under a written agreement.

RECIPIENT	ROLE	WHAT THEY RECEIVE
Sumsub	Identity verification and KYC screening	Identity and onboarding data
AMLBot	Sanctions, PEP and wallet screening	Identity data; wallet addresses
Google Cloud	Hosting of the trading platform	Account, trading and Telegram identifier data
Hetzner	Hosting of our own servers holding identity records	Identity and contractual records, encrypted at rest
Telegram	Messaging channel for the client interface and for secure document exchange	Messages you send; your Telegram identifiers
Cryptocurrency exchanges you have chosen	Your own counterparty and custodian	Order and account data, via your own API credentials
Auditors, accountants and legal advisers	Professional advisers	Only what the engagement requires
Regulators, tax authorities and courts	Where legally compelled	Only what is legally required

8.1 Our secure channel for sensitive documents — and a change coming

Sensitive material such as identity documents and API credentials should never be sent by ordinary e-mail. Today we ask you to send it through **Telegram**, using its end-to-end encrypted secret-chat mode where possible. Telegram therefore acts as a processor for the message content and sees your Telegram identifiers.

Planned change. We intend to move secure document exchange and client messaging to **Sover** (sover.app), a self-hosted, end-to-end encrypted messaging platform, once its programmatic interface is available to us. Sover is self-hosted, which means the message content would sit on infrastructure we control rather than a third-party consumer messaging service. We will update this notice, and tell affected clients, before that change takes effect. Until then, Telegram remains the channel described above.

9. How long we keep it

CATEGORY	RETENTION	REASON
Identity, onboarding and AML records	7 years after the relationship ends	BVI SIBA and AML record-keeping obligations
Agreements and contractual records	7 years after termination	Statutory and limitation periods
Trading and financial records	7 years	Tax, audit and regulatory reporting
Exchange API credentials	Deleted on termination or on your request	No longer needed once trading stops
Correspondence	7 years	Evidence of advice and instructions
Enquiries that do not become a relationship	12 months	Follow-up, then deletion

Backups follow their own rotation and are overwritten in the ordinary course rather than deleted on demand; we explain this in section 10.3.

10. Your rights

You may exercise any of the following by writing to compliance@algotoria.com. We respond within **30 days**, or 45 days for a complex request, and we will tell you if we need the longer period. We do not charge for a first request. We may ask you to verify your identity before we act.

10.1 Access, correction and portability

- **Access** — a copy of the personal data we hold, what we use it for, who we share it with, and how long we keep it.
- **Correction** — rectification of anything inaccurate or incomplete; we correct it across our systems and tell recipients where feasible.
- **Portability** — the data you provided to us, in a machine-readable format such as CSV or JSON.

10.2 Objection, restriction and withdrawal of consent

- **Object** to processing based on legitimate interests. We will stop unless we have compelling grounds that override your interests. For marketing, we always stop.
- **Restrict** processing while a dispute about accuracy or lawfulness is resolved.
- **Withdraw consent** at any time where consent is the basis we rely on.

10.3 Erasure — and its honest limits

You may ask us to delete your personal data, and we will do so from our live systems. Two limits apply and we would rather state them plainly than imply a stronger right than exists:

- **Legal retention wins.** We cannot delete identity, AML or financial records that we are required to keep for seven years. We will delete them when the obligation expires.
- **Backups age out rather than being surgically edited.** Once data is removed from live systems it may persist in encrypted backups until those backups are overwritten on their normal rotation. We do not perform accelerated deletion inside historical backups, because doing so would compromise the integrity of the backup set.

10.4 Complaints

If you are unhappy with how we have handled your data, tell us first at compliance@algotoria.com and we will investigate. You also have the right to complain to a supervisory authority — the Office of the Information Commissioner in the British Virgin Islands, or, if you are in the United Kingdom or the EEA, your national data-protection authority.

11. Personal data breaches

We maintain a documented incident-response procedure. Where a breach is likely to result in a risk to your rights and freedoms, we will notify the relevant supervisory authority without undue delay and, where the risk is high, notify you directly and explain what happened, what data was involved, what we have done, and what you can do.

12. Children

Our services are for professional investors and are not offered to anyone under 18. We do not knowingly collect personal data from children. If you believe we hold data about a child, write to us and we will delete it.

13. Cookies and the website

algotoria.com uses only what is necessary to serve the site and remember your language choice. We do not run advertising trackers, cross-site profiling or third-party analytics that build a profile of you. Forms on the site use a bot-protection challenge to prevent automated abuse; it does not profile you for advertising.

14. Changes to this notice

We review this notice at least annually and whenever our processing changes materially. The version number and effective date at the top of page one tell you which version you are reading. Where a change materially affects how we handle your data — such as the move to Sover described in section 8.1 — we will tell affected clients before it takes effect rather than relying on a silent update.

15. How to reach us

CONTROLLER	Algotoria Limited, BVI Reg. No. 2161048
REGISTERED OFFICE	Quijano Chambers, P.O. Box 3159, Road Town, Tortola, British Virgin Islands
DATA PROTECTION ENQUIRIES	compliance@algotoria.com
SECURITY MATTERS	security@algotoria.com
GENERAL ENQUIRIES	ops@algotoria.com

This notice describes our processing as at the effective date shown on page one. It is written to be read, not to be hidden behind. If anything here is unclear, or if you want to know exactly what we hold about you, write to compliance@algotoria.com and ask.