

Privacy Policy

Truo Securities

Version: V1 | Last updated: 8 July 2026

In brief

We are Truo Securities. Truo Securities is a multi-asset financial services platform operated by Truo Markets Limited ("Truo Securities", "we", "us" or "our"). We respect your privacy and are committed to protecting the confidentiality and security of personal data that you provide to us or that we collect when you use our website, client portal, applications, trading platform access, account services, support channels and related services.

This Privacy Policy explains what personal data we collect, why we collect it, how we use it, the circumstances in which we may disclose it, how long we retain it, and the rights that may be available to you under applicable data protection laws.

About us

For the purposes of this Privacy Policy, Truo Securities is responsible for the personal data collected through www.truosecurities.com, secure client portals, applications, account registration forms, customer support channels and other services that we operate or make available to clients and prospective clients.

This Privacy Policy applies when you visit our website, create or access an account, submit onboarding or verification information, use our client portal, use our applications, communicate with us, subscribe to updates, participate in promotional activities, or otherwise use any service provided by us.

As used in this Privacy Policy, "personal data" means any information relating to an identified or identifiable individual.

Updates

We may update this Privacy Policy from time to time by publishing a revised version on our website or by notifying you through appropriate channels where required by applicable law. You should review this Privacy Policy periodically to remain informed about how we process personal data.

The current version of this Privacy Policy was published on 8 July 2026.

Personal data that we collect

Website and general browsing data

You may browse certain parts of our website without creating an account. When you do so, we may still collect limited technical and usage information, including IP address, browser type, device type, operating system, pages viewed, referring pages, session duration, cookie identifiers, language settings and other similar analytics or log data.

Account registration and client onboarding data

When you register for an account or request access to our services, we may ask you to provide personal data required to create, review, approve, maintain and administer your account. This may include your name, email address, phone number, date of birth, nationality, residential address, country of residence, account username, password, preferred language, client portal details and communication preferences.

Where required for regulatory, anti-money laundering, counter-terrorist financing, fraud prevention, suitability, account classification or ongoing due diligence purposes, we may also collect identity documents, proof of address, tax information, source of funds, source of wealth, employment information, financial background, trading experience, investment objectives, risk tolerance, product knowledge and related declarations.

Payment, funding and transaction data

If you make deposits, withdrawals, internal transfers or other account-related transactions, we may process information relating to your payment method, bank account, payment account, wallet details, transaction identifiers, amount, currency, transaction status, payment partner, funding source and related records.

Where a third-party payment processor, bank, payment partner or other financial institution is involved, that party may independently process your payment or transaction information in accordance with its own terms, policies and applicable regulatory obligations.

Contact and support data

We process personal data that you choose to provide when you contact us by email, phone, website form, client portal, live chat, social media, support ticket or any other communication channel. This may include your contact details, message content, attachments, screenshots, recordings, device information, server logs, case notes and any other information needed to review and respond to your inquiry.

Cookies and similar technologies

We use cookies, pixels, tags, local storage and similar technologies to operate our website and services, remember user preferences, maintain session security, detect fraud or abuse, measure website performance, improve user experience, support analytics and, where permitted, deliver or measure marketing communications.

You may be able to manage cookies through your browser settings. Disabling certain cookies may affect website functionality, login sessions, security features or service availability.

Log files and device information

Like most online services, we collect server log information. This may include IP addresses, browser types, internet service providers, referring and exit pages, platform type, date and time stamps, device identifiers, application version, network information and security event records.

We use this information to administer our services, monitor technical performance, maintain security, prevent spam, fraud and abuse, diagnose errors, support compliance checks and improve service reliability.

Analytics and marketing data

When you use our website, applications or online services, we may collect analytics information automatically. This information may include website and application interaction events, campaign source, page views, clicks, conversion events, device identifiers and pseudonymous usage data.

We use analytics and marketing data to understand how users interact with our services, improve website and application performance, measure campaign effectiveness and provide information that may be relevant to existing or prospective clients, subject to applicable consent and opt-out requirements.

How personal information is used

Account operation and service delivery

We use personal data to create, review, approve, manage and secure accounts; authenticate users; provide access to the client portal and applications; process account requests; provide customer support; enable deposits, withdrawals and account administration; deliver service notifications; maintain operational records; and provide services that you request from us.

Verification, compliance and risk management

We use personal data to verify identity, conduct due diligence, perform anti-money laundering and counter-terrorist financing checks, prevent fraud, assess account eligibility, review account activity, respond to regulatory requests, maintain audit records, comply with applicable laws and enforce our terms, policies and contractual rights.

Communications

We may use your contact details to send account-related messages, security alerts, onboarding updates, service announcements, policy updates, operational notices, support responses and other communications necessary for the administration of your account or services.

Where permitted by law, we may also send marketing communications about our services, market events, campaigns, promotions or educational content. You may opt out of marketing emails by using the unsubscribe link provided in those emails or by contacting us through the official channels listed below.

Service improvement and business operations

We may use personal data to improve our website, client portal, mobile and desktop applications, customer service processes, product experience, cybersecurity controls, internal reporting, business planning, marketing performance and operational efficiency.

We may anonymize, pseudonymize, aggregate or de-identify information for internal analytics, statistical reporting, product development, research, security monitoring and business performance review. Such information will not be used to identify you where it has been properly anonymized.

Lawful basis for processing

Depending on the jurisdiction and the nature of the processing, we may process your personal data on one or more lawful bases, including performance of a contract with you, compliance with legal or regulatory obligations, our legitimate business interests, protection of legal rights and interests, consent where required, or other lawful bases permitted under applicable data protection laws.

Where we rely on legitimate interests, we consider whether our interests are overridden by your rights and interests. Where we rely on consent, you may withdraw that consent at any time, subject to legal or contractual restrictions and the lawfulness of processing carried out before withdrawal.

When we may share personal information

We do not sell your personal data. We may share personal data only where necessary for the purposes described in this Privacy Policy, where permitted by law, or where you have provided instructions or consent.

We may share personal data with affiliated companies, service providers, technology vendors, data hosting providers, cybersecurity providers, banks, payment processors, payment partners, liquidity or platform providers, identity verification providers, analytics providers, marketing and customer relationship management providers, professional advisers, auditors, insurers, regulators, law enforcement authorities, courts, government agencies, dispute resolution bodies or other parties where required or permitted by law.

Where third parties process personal data on our behalf, we require them to process such data in accordance with our instructions and to apply appropriate confidentiality, security and data protection safeguards.

Business transfers

If we undergo a merger, acquisition, restructuring, transfer of assets, financing, sale of business, change of control or similar corporate transaction, personal data may be transferred as part of that transaction, subject to applicable law and appropriate safeguards.

International transfers

Because we operate online services and may use service providers, affiliates and business partners in different jurisdictions, your personal data may be processed, stored or transferred outside your country of residence. Where required by applicable law, we will implement appropriate safeguards for such transfers.

Security of personal data

We use technical, organizational and administrative safeguards designed to protect personal data against unauthorized access, loss, misuse, alteration or disclosure. These measures may include access controls, authentication systems, encryption in transit, security monitoring, network protection, internal policies, employee access restrictions and vendor due diligence.

No method of electronic transmission or storage is completely secure. Although we take reasonable steps to protect personal data, we cannot guarantee absolute security. You are responsible for keeping your account credentials confidential and for notifying us promptly if you suspect unauthorized access to your account.

Children and sensitive personal data

Our website and services are not directed to persons under the age of 18. We do not knowingly collect personal data from children under 18. If you believe that a child has provided personal data to us, please contact us so that we can take appropriate steps.

We do not intentionally collect sensitive personal data unless required for identity verification, legal compliance, regulatory obligations, fraud prevention, account administration or where you voluntarily provide such information. Sensitive data may include information contained in identity documents or other verification materials.

Third-party websites and services

Our website, client portal, applications or communications may contain links to third-party websites, platforms, payment providers, trading platforms, application stores or other external services. These third parties operate independently and may have their own privacy policies and data handling practices. We are not responsible for the privacy practices, content or security of third-party websites or services.

Your rights

Depending on the laws that apply to you, you may have rights to access, correct, update, delete, restrict, object to or obtain a copy of your personal data. You may also have the right to withdraw consent, object to direct marketing, request data portability or lodge a complaint with a competent data protection authority.

To protect account security and personal data, we may need to verify your identity before responding to a rights request. Some requests may be limited by legal, regulatory, contractual, security, fraud prevention, audit or legitimate business requirements.

Viewing and correcting data

Where account functionality allows, you may view, manage or update certain personal data through your account or client portal. If you believe that personal data held by us is inaccurate, outdated or incomplete, you may contact us to request correction.

Deleting data and account closure

You may request account closure or deletion of certain personal data by contacting us through the official support channels. We will review such requests in accordance with applicable law and our regulatory, contractual, security, accounting, tax, audit, fraud prevention and legitimate business obligations.

Certain records may need to be retained after account closure, including records required for compliance, dispute resolution, transaction history, security monitoring, legal claims, audit requirements or other legitimate business purposes.

Data retention

We retain personal data for as long as necessary to provide services, maintain your account, comply with legal and regulatory obligations, resolve disputes, prevent fraud or abuse, maintain security, enforce agreements and support legitimate business purposes.

When personal data is no longer required, we will delete, anonymize or securely dispose of it in accordance with applicable laws, internal retention policies and operational requirements.

Contact information

If you have questions, requests or concerns regarding this Privacy Policy or the way we process personal data, you may contact us through the details below:

Truo Securities

Operated by: Truo Markets Limited

Registered Office: C/o Credentia International Management Ltd, The Cyberati Lounge, Ground Floor, The Catalyst, Silicon Avenue, 40 Cybercity, 72201 Ebene, Republic of Mauritius.

Email: support@truosecurities.com

Website: www.truosecurities.com