ThinkMarkets is the trading name of the
TF Global Markets group of companies

THINKMARKETS GROUP

Group Privacy Statement

Document	Group Privacy Statement
Version	1.0
Issued	May 2026
Issuer	ThinkMarkets Group

Contact

compliance@thinkmarkets.com
www.thinkmarkets.com

Last updated: 8 October 2026

ThinkMarkets is a registered trademark of the group, that operates among various entities such as TF Global Markets Int Limited, Think Capital Limited and TF Global Markets (STL) Limited.

Group Privacy Statement

Version 1.0 | Issued: May 2026

About This Statement

ThinkMarkets is the trading name of the TF Global Markets group of companies (together, **"ThinkMarkets"**, **"we"**, **"us"**, or **"our"**). This Group Privacy Statement sets out how we collect, use, store, share, and protect personal data across all ThinkMarkets entities and platforms worldwide.

This Statement operates as the top-level privacy document for the ThinkMarkets Group. Each regulated ThinkMarkets entity may also issue its own entity-level privacy notice to address jurisdiction-specific requirements in greater detail. Where an entity-level notice exists, it should be read alongside this Statement. In the event of any conflict between this Statement and an entity-level notice, the entity-level notice takes precedence for clients of that entity.

This Statement applies to personal data we process in connection with our trading platforms, websites, mobile applications, and other services we provide to clients, prospective clients, website visitors, and others who interact with us (collectively referred to as **"you"**).

We may update this Statement from time to time. We will notify you of material changes by posting the updated version on our website at www.thinkmarkets.com. We encourage you to review this Statement periodically. The version published on our website at the relevant time governs the personal data we hold.

1. Who We Are

1.1 The ThinkMarkets Group

ThinkMarkets is a multi-regulated global provider of online trading services, established in 2010 and operating across more than 165 countries. The ThinkMarkets Group is comprised of multiple legal entities, a complete list of which is available upon request, and each of which acts as a separate data controller in respect of the personal data it processes for its own clients and users. Each entity is responsible for complying with applicable data protection requirements in its own jurisdiction.

1.2 Contact and Data Enquiries

If you have any questions about this Statement or wish to exercise your rights in relation to your personal data, if you are unsure which entity to contact, you may write to us at compliance@thinkmarkets.com, as outlined in Section 10 below, and we will direct your enquiry appropriately.

1.3 Your ThinkMarkets Website

ThinkMarkets operates regional websites for different jurisdictions. We ask that you visit www.thinkmarkets.com and select the version most relevant to your location and circumstances, or contact us at support@thinkmarkets.com if you require assistance identifying the correct regional entity for your needs.

2. Personal Data We Collect

We collect personal data that we need to provide our services, meet our regulatory obligations, and operate our business responsibly. The categories of personal data we collect include:

Identity data: full name, date of birth, gender, nationality, tax identification number, and information from identity documents such as passports or driving licences.

Contact data: residential or business address, email address, and telephone number.

Financial and economic data: information about your income, source of funds, source of wealth, assets and liabilities, account balances, bank account details, tax and financial statements, and investment objectives.

Trading and suitability data: trading experience, knowledge of financial instruments, appropriateness and suitability assessment responses, and transaction history.

Verification and screening data: information generated in the course of identity verification, anti-money laundering checks, sanctions screening, politically exposed person (PEP) checks, and client risk categorisation.

Technical and usage data: internet protocol (IP) address, browser type and version, device identifiers, pages visited, time and date of access, session recordings, and other information about how you access and use our platforms.

Communications data: records of communications between you and ThinkMarkets, including telephone call recordings, live chat transcripts, email correspondence, and records of in-person interactions.

Location data: where you interact with our services or visit our premises.

Premises visitor data: name, employer, contact details, vehicle registration, and the date, time, and purpose of your visit, where you visit our offices.

AI interface data: where you activate our AI Trading Interface, data transmitted to a third-party AI platform in connection with your use of that feature, as further described in Section 7.

We collect most personal data directly from you. We may also collect personal data from third parties, including identity verification providers, credit reference agencies, sanctions screening services, introducing brokers, and publicly available sources, where we are legally permitted to do so.

We do not collect sensitive personal data (such as data revealing racial or ethnic origin, religious beliefs, political opinions, health data, or biometric data used for identification) unless you have provided explicit consent, we are required to do so by applicable law, or an applicable legal exemption applies.

3. Why We Use Personal Data

We process personal data only where we have a lawful basis to do so. The primary lawful bases on which we rely are:

Performance of a contract: We process personal data to the extent necessary to open, administer, and maintain your trading account, process your instructions and transactions, and provide you with our products and services.

Compliance with legal obligations: We are subject to regulatory requirements across multiple jurisdictions, including anti-money laundering, counter-terrorist financing, financial crime prevention, and client due diligence requirements. We process personal data to meet these obligations.

Legitimate interests: We process personal data where it is necessary for our legitimate interests, including improving our services, ensuring the security and integrity of our platforms, managing our business operations, and, where permitted, marketing our services to existing and prospective clients. We conduct this processing in a manner that does not override your interests or fundamental rights.

Consent: Where we rely on your consent as the lawful basis for processing, we will request your consent separately and clearly. You may withdraw consent at any time; withdrawal does not affect the lawfulness of processing carried out before withdrawal.

The purposes for which we process personal data include:

- verifying your identity and assessing your eligibility to open and maintain an account;
- assessing the appropriateness or suitability of our products and services for you;
- processing your instructions, orders, and transactions;
- managing your account, including calculating and monitoring margin requirements;
- complying with our legal and regulatory obligations, including record-keeping requirements;
- detecting, investigating, and preventing financial crime, fraud, and market abuse;
- monitoring and recording communications as required by applicable regulation;
- responding to requests from regulatory authorities, courts, or law enforcement agencies;
- managing and improving our platforms, products, and services;
- providing you with customer support;
- sending you service communications and, where you have consented or we have a legitimate interest, marketing communications about our products and services; and
- conducting surveys, research, and analysis to improve client outcomes.

4. How Long We Keep Personal Data

We retain personal data for as long as is necessary for the purposes for which it was collected, subject to any longer period required by applicable law or regulation.

In particular, anti-money laundering and financial services regulations across our operating jurisdictions require us to retain client due diligence records and transaction documentation for a minimum period, typically five years from the end of our relationship with you, though longer retention periods may apply in certain jurisdictions.

Telephone call recordings and electronic communications records are retained for the periods required by the applicable regulatory framework for each entity.

Where we determine that personal data is no longer required, we securely delete or anonymise it in accordance with our data retention procedures.

5. How We Share Personal Data

We share personal data only where we have a lawful basis to do so, and only to the extent necessary for the relevant purpose.

Within the ThinkMarkets Group: We may share personal data between group entities for operational, compliance, and administrative purposes, where permitted by applicable law.

Service providers and technology partners: We engage third-party providers to support our business, including technology and platform providers, payment processors, identity verification services, cloud storage providers, and customer support providers. These providers act under our instruction and we take steps to ensure they maintain appropriate data protection standards.

Regulators and authorities: We disclose personal data to applicable regulators, financial intelligence units, law enforcement agencies, courts, and other public authorities where we are required to do so by applicable law, court order, or regulatory obligation, or where we have a good-faith belief that disclosure is necessary to protect the safety of individuals or to defend our rights.

Introducing brokers and marketing partners: Where you have been introduced to us by a third party, or where we work with authorised marketing partners, we may share relevant data with those parties in accordance with applicable data protection requirements and, where required, with your consent.

Financial counterparties: In cases involving suspected fraud, price manipulation, payment abuse, money laundering, or similar conduct, we reserve the right to share relevant personal data with other financial institutions, payment providers, and appropriate regulatory and legal agencies.

AI platform providers: Where you activate the AI Trading Interface, certain account data is transmitted to the third-party AI platform provider you have selected. Please refer to Section 7 for further details.

We do not sell or rent personal data to third parties.

6. International Data Transfers

ThinkMarkets operates globally, and personal data may be transferred to, stored in, or processed in countries outside the country in which it was originally collected. This may occur because our group entities, servers, or third-party service providers are located in different jurisdictions.

Where personal data is transferred across borders, we take steps to ensure that appropriate safeguards are in place to protect your data, consistent with applicable data protection requirements. Such safeguards may include, depending on the applicable jurisdiction:

- transfers between group entities or to third parties in countries that have been recognised as providing an adequate level of data protection;
- the use of contractual protections, such as data transfer agreements or equivalent instruments, between the data exporter and the recipient;
- other safeguards permitted by applicable law in the relevant jurisdiction.

By using our services and providing us with your personal data, you acknowledge that your data may be transferred, stored, and processed internationally in accordance with this Statement.

If you wish to obtain further information about the specific safeguards applicable to your personal data, please contact us at compliance@thinkmarkets.com.

7. AI Trading Interface and Data Processing

ThinkMarkets has launched an AI Trading Interface that enables clients to connect a third-party AI assistant to their trading account. This section sets out how this feature affects the processing of your personal data.

7.1 Data Transmitted to AI Platform Providers

When you activate the AI Trading Interface, certain account data, which may include your positions, balances, order history, and account information, is transmitted to the AI platform provider you have selected. The categories of data transmitted are limited to those necessary to operate the trading interface. We do not transmit identity documents, payment card details, or KYC documentation via this feature.

7.2 Third-Party AI Providers

Third-party AI platform providers are independent of ThinkMarkets and operate under their own terms and privacy policies. ThinkMarkets is not responsible for the data practices of those providers. We strongly recommend that you review the privacy policy of your chosen AI platform provider before activating this feature.

You should not share any personal, financial, or identity information with an AI assistant beyond what is necessary to operate the trading interface. ThinkMarkets will never request authentication credentials, passwords, or sensitive personal information via an AI assistant.

7.3 Your Consent

By activating the AI Trading Interface, you consent to the transmission of the account data described above to your chosen AI platform provider for the purpose of operating the interface. You may withdraw this consent at any time by disabling the AI Trading Interface in your account settings, without affecting the lawfulness of processing carried out before withdrawal.

7.4 Your Rights

Your rights in relation to your personal data, as set out in Section 8, are unaffected by your use of the AI Trading Interface.

The AI Trading Interface is governed by the AI Trading Interface Supplementary Terms, available at www.thinkmarkets.com.

8. Your Rights

Subject to applicable law in your jurisdiction, you have the right to:

- **be informed** about how we collect and use your personal data;
- **access** the personal data we hold about you;
- **correct** personal data that is inaccurate or incomplete;
- **request deletion** of your personal data, subject to our legal and regulatory obligations to retain certain records;
- **object** to certain types of processing, including processing based on our legitimate interests;
- **restrict** the processing of your personal data in certain circumstances;
- **data portability**, meaning the right to receive your personal data in a structured, commonly used format in certain circumstances;
- **withdraw consent** at any time where we rely on consent as the lawful basis for processing; and
- **opt out** of direct marketing communications at any time.

To exercise any of these rights, please contact the ThinkMarkets entity with which you hold an account, using the contact details in Section 10 below.

We will respond to your request in accordance with the timeframes required by applicable law. We may need to verify your identity before processing your request. We will not charge a fee for reasonable requests.

Where your request relates to a regulated record-keeping obligation, we may be unable to delete or restrict processing of certain data while our legal retention obligation persists. We will inform you of this where applicable.

9. How We Protect Personal Data

We apply appropriate technical and organisational measures to protect your personal data against unauthorised access, disclosure, alteration, loss, or destruction. Our measures include:

- access controls requiring authentication to access systems containing personal data;
- restricted access to personal data based on role and business need;
- encryption of data during transmission and at rest;
- automated logging and monitoring of access attempts and system activity;
- physical security controls for premises and equipment;

- secure destruction procedures for data that is no longer required; and
- regular staff training on data protection and information security responsibilities.

We treat breaches of data protection obligations seriously. Where a personal data breach occurs, we follow our incident response procedures and notify the applicable supervisory authority and affected individuals where required by law.

10. Complaints and Contact Details

Raising a Concern with Us

If you have a concern about how we handle your personal data, we ask that you contact us in the first instance. We will act on your concern promptly.

You may contact the relevant ThinkMarkets entity at compliance@thinkmarkets.com.

Raising a Concern with a Supervisory Authority

If you are not satisfied with our response, or if you believe we have not handled your personal data in accordance with applicable requirements, you have the right to complain to the supervisory authority in your jurisdiction. Each ThinkMarkets entity is registered with, or subject to the oversight of, the applicable data protection or privacy authority in its operating jurisdiction. Details of the relevant supervisory authority for your jurisdiction are available from the ThinkMarkets entity with which you hold an account, or by contacting us at compliance@thinkmarkets.com.

11. Cookies and Tracking Technologies

Our websites and email communications may use cookies, web beacons, pixel tags, and similar technologies to collect technical and usage data, to improve our services, and to measure the effectiveness of our communications. Our Cookie Declaration, available on the relevant ThinkMarkets regional website, provides further information about the cookies we use and how you can manage your preferences.

This Statement was issued by ThinkMarkets Group | Version [1.0] | May 2026

This Statement is subject to review and update. The current version is always available at www.thinkmarkets.com.