TF GLOBAL MARKETS (AUST) PTY LTD

Privacy Policy and Collection Statement

Document	Privacy Policy and Collection Statement
Date	26th of August 2026
Entity	TF Global Markets (Aust) Pty Ltd
Regulator	Financial Markets Authority (FMA), New Zealand
FSP number	FSP623289
NZBN	9429050705597

Contact

compliance@thinkmarkets.com
Phone: +64 3 668 4583
www.thinkmarkets.com/nz

Last updated: 24 September 2026

Privacy Policy and Collection Statement (Privacy Policy)

1. Introduction

TF Global Markets (Aust) Pty Ltd (referred to as ***ThinkMarkets***, ***we***, ***our***, ***us***) is bound by the relevant *Privacy Acts* in Australia and New Zealand (***Privacy Act***). This policy adheres to the Privacy Principles (***PPs***) and recognises the importance of ensuring the confidentiality and security of your personal information.

All third parties (including clients, suppliers, sub-contractors, or agents) that have access to or use personal information collected and held by ThinkMarkets, must abide by this Privacy Policy and Collection Statement (**Privacy Policy**). ThinkMarkets makes this Privacy Policy available free of charge and can be downloaded from its website https://www.thinkmarkets.com/nz/.[1]

In this Privacy Policy:

- ***Disclosure*** of information means providing information to persons outside of ThinkMarkets;
- ***Personal information*** means information or an opinion relating to an individual, which can be used to identify that individual;
- ***Privacy Officer*** means the contact person within ThinkMarkets for questions or complaints regarding ThinkMarkets' handling of personal information;
- ***Sensitive or personal information*** is information that includes information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences, and criminal record, and includes health information; and
- ***Use*** of information means use of information within ThinkMarkets.

2. What kind of personal information do we collect and hold?

We may collect and hold a range of personal information about you to provide you with our services, including:

- your full name;
- contact details;
- date of birth;
- employment details;
- country of residency;
- financial and trading information;
- identification details such as passport or driver's licence details;
- proof of address such as utility bills and banks statements;
- trading preferences;
- banking details; and
- other personal information we require to meet your needs and provide our services to you.

3. How do we collect personal information?

We generally collect personal information directly from you. For example, personal information will be collected through our application processes, forms, and other interactions with you while providing you

with our products and services, including when you visit our website, use a mobile app from us, call us or send us correspondence.

We may also collect personal information about you from a third party, such as electronic verification services, referrers, and marketing agencies. If so, we will take reasonable steps to ensure that you are made aware of this Privacy Policy. We may also use third parties to analyse traffic at our website, which may involve the use of cookies. Information collected through such analysis is anonymous.

We will not collect sensitive information about you without your consent unless an exemption in the APPs applies. These exceptions include if the collection is required or authorised by law, or necessary to take appropriate action in relation to suspected unlawful activity or serious misconduct.

If the personal information we request is not provided by you, we may not be able to provide you with the benefit of our services or meet your needs appropriately.

We do not give you the option of dealing with them anonymously, or under a pseudonym. This is because it is impractical, and, in some circumstances, illegal for ThinkMarkets to deal with individuals who are not identified.

4. Unsolicited personal information

We may receive unsolicited personal information about you. We destroy or de-identify all unsolicited personal information we receive unless it is relevant to our purposes for collecting personal information. We may retain additional information we receive about you if it is combined with other information we are required or entitled to collect. If we do this, we will retain the information in the same way we hold your other personal information.

5. Who do we collect personal information about?

The personal information we may collect, and hold includes (but is not limited to) personal information about:

- clients;
- potential clients;
- visitors to our website via online enquiry forms;
- introducing brokers; and
- service providers or suppliers;

6. Website collection

We collect personal information when we receive completed online generated forms from our website (www.thinkmarkets.com). We may also use third parties to analyse traffic at that website, which may involve the use of cookies. Information collected through such analysis is anonymous.

To use our web site, you must consent to our use of cookies. You can withdraw or modify your consent to our use of cookies at any time. If you want to restrict or block the cookies we set, you can do this through your browser settings. The 'help' function within your browser should tell you how. Please note that if you set your browser to refuse cookies, you may not be able to use all the features of our website.

Cookies do not contain personal information in themselves but can be used to identify a person when combined with other information. Cookies are small text files which are transferred to your computer's hard drive through your web browser that enables our website to recognise your browser and capture and remember certain information.

We also use cookies to

- To protect our customers and prevent fraudulent activity. Without cookies enabled you can't use the Management Portal or online trading platforms.
- In our online application forms. Without cookies enabled you won't be able to apply for our products.
- In web analytics. We also use web analytics services from other companies to track how visitors reach our site and the path they take through it. These companies use cookies to help us improve our service to you.

7. Why do we collect and hold personal information?

We may use and disclose the information we collect about you for the following purposes:

- provide you with our products and services;
- review and meet your ongoing needs;
- provide you with information we believe may be relevant or of interest to you;
- let you know about other products or services we offer, send you information about special offers or invite you to events;
- consider any concerns or complaints you may have;
- comply with relevant laws, regulations and other legal obligations;
- help us improve the products and services offered to our customers and enhance our overall business;

We may use and disclose your personal information for any of these purposes. We may also use and disclose your personal information for secondary purposes which are related to the primary purposes set out above, or in other circumstances authorised by the Privacy Act.

Sensitive information will be used and disclosed only for the purpose for which it was provided (or a directly related secondary purpose), unless you agree otherwise, or an exemption in the Privacy Act applies.

8. Who might we disclose personal information to?

We may disclose personal information to:

- a related entity of ThinkMarkets;
- an agent, contractor, or service provider we engage with to carry out our functions and activities, such as our External Legal Advisors, accountants, debt collectors; etc.
- organisations involved in a transfer or sale of all or part of our assets or business;
- organisations involved in managing payments, including payment merchants and business banking Partners.

- Internal and External Auditors, Regulators (such as ASIC or the FMA), government bodies, law enforcement agencies, courts and Federal Courts;
- financial product issuers;

If we disclose your personal information to service providers that perform business activities for us, they may only use your personal information for the specific purpose for which we supply it. We will ensure that all contractual arrangements with third parties adequately address privacy issues, and we will make third parties aware of this Privacy Policy.

9. Sending information overseas

We may disclose personal information to our affiliates that are located outside Australia or New Zealand in some circumstances.

This list is not exhaustive as our affiliates are located around the glove.

We will not send personal information to recipients outside of Australia or New Zealand unless:

- we have taken reasonable steps to ensure that the recipient does not breach the Act and the PPs,
- the recipient is subject to an information privacy scheme like the Privacy Act; or
- the individual has consented to the disclosure.

When we share your data with a third party, we have contracts in place with them which requires them to have in place the technical and organisational measures necessary to protect your personal data, however many such providers are subject to different privacy laws and controls to Australia and/or New Zealand and hence we cannot provide absolute surety that those providers will not comply with their obligations to us and divulge your personal data.

If you consent to your personal information being disclosed to an overseas recipient, and the recipient breaches the PPs, we will not be accountable for that breach under the Privacy Act, and you will not be able to seek redress under the Privacy Act.

10. Management of personal information

We recognise the importance of securing the personal information of our customers. We will take steps to ensure your personal information is protected from misuse, interference or loss, and unauthorised access, modification, or disclosure.

Your personal information is generally stored in our computer database. Any paper files are stored in secure areas. In relation to information that is held on our computer database, we apply the following guidelines:

- passwords are required to access the system, and passwords are routinely checked;
- data ownership is clearly defined;
- we change employees' access capabilities when they are assigned to a new position;
- employees have restricted access to certain sections of the system;
- the system automatically logs and reviews all unauthorised access attempts;
- unauthorised employees are barred from updating and editing personal information;
- all computers which contain personal information are secured both physically and electronically;

- data is encrypted during transmission over the network; and
- print reporting of data containing personal information is limited.

Where our employees work remotely or from home, we implement the following additional security measures:

- two-factor authentication is enabled for all remote working arrangements;
- password complexity is enforced, and employees are required to change their password at regular intervals;
- we ensure that employees only have access to personal information which is directly relevant to their duties;
- we use audit trails and audit logs to track access to an individual's personal information by an employee;
- we monitor access to personal information, and will investigate and take appropriate action if any instances of unauthorised access by employees are detected;
- employees must ensure that screens are angled so that they cannot be used by anyone else, and are locked when not in use;
- employees must ensure that no other member of their household uses their work device;
- employees must store devices in a safe location when not in use;
- employees may not make hard copies of documents containing personal information, nor may they email documents containing personal information to their personal email accounts; and
- employees may not disclose an individual's personal information to colleagues or third parties via personal chat groups.

11. Direct marketing

We may only use personal information we collect from you for the purposes of direct marketing without your consent if:

- the personal information does not include sensitive information; and
- you would reasonably expect us to use or disclose the information for the purpose of direct marketing; and
- we provide a simple way of opting out of direct marketing; and
- you have not requested to opt out of receiving direct marketing from us.
- we provide a simple way of opting out of direct marketing; and
- We believe our other products are suitable for you and enhance your experience with ThinkMarkets.

If we collect personal information about you from a third party, we will only use that information for the purposes of direct marketing if you have consented (or it is impracticable to obtain your consent), and we will provide a simple means by which you can easily request not to receive direct marketing communications from us. We will draw your attention to the fact you may make such a request in our direct marketing communications.

You have the right to request us not to use or disclose your personal information for the purposes of direct marketing, or for the purposes of facilitating direct marketing by other organisations. We must give effect to the request within a reasonable period. You may also request that we provide you with

the source of their information. If such a request is made, we must notify you of the source of the information free of charge within a reasonable period.

12. Identifiers

We do not adopt identifiers assigned by the Government (such as drivers' licence numbers) for our own file recording purposes, unless one of the exemptions in the Privacy Act applies.

13. How do we keep personal information accurate and up to date?

We are committed to ensuring that the personal information we collect, use and disclose is relevant, accurate, complete and up to date.

We encourage you to contact us to update any personal information we hold about you. If we correct information that has previously been disclosed to another entity, we will notify the other entity within a reasonable period of the correction. Where we are satisfied information is inaccurate, we will take reasonable steps to correct the information within 30 days, unless you agree otherwise. We do not charge you for correcting the information.

14. Accessing your personal information

Subject to the exceptions set out in the Privacy Act, you may gain access to the personal information that we hold about you by contacting the ThinkMarkets' Privacy Officer. We will provide access within 30 days of the individual's request. If we refuse to provide the information, we will provide reasons for the refusal.

We will require identity verification and specification of what information is required. An administrative fee for search and photocopying costs may be charged for providing access.

15. Updates to this Privacy Policy

This Privacy Policy will be reviewed from time to time to take account of new laws and technology, and changes to our operations and the business environment.

16. Responsibilities

It is the responsibility of management to inform employees and other relevant third parties about this Privacy Policy. Management must ensure that employees and other relevant third parties are advised of any changes to this Privacy Policy. All new employees are to be provided with timely and appropriate access to this Privacy Policy, and all employees are provided with training in relation to appropriate handling of personal information. Employees or other relevant third parties that do not comply with this Privacy Policy may be subject to disciplinary action.

17. Non-compliance and disciplinary actions

Privacy breaches must be reported to management by employees and relevant third parties. Ignorance of this Privacy Policy will not be an acceptable excuse for non-compliance. Employees or other relevant third parties that do not comply with this Privacy Policy may be subject to disciplinary action.

18. Incidents/Complaints handling/Making a complaint

We have an effective complaint handling process in place to manage privacy risks and issues.

The complaints handling process involves:

- identifying (and addressing) any systemic/ongoing compliance problems;
- increasing consumer confidence in our privacy procedures; and
- helping to build and preserve our reputation and business.

You can make a complaint to us about the treatment or handling of your personal information by lodging a complaint with the Privacy Officer.

If you have any questions about this Privacy Policy, or wish to make a complaint about how we have handled your personal information, you can lodge a complaint with us by:

- writing – TF Global Privacy Officer, Baker Tilly Staples Rodway Auckland Ltd, Level 12, 23-29 Albert Street, Auckland, 1010, NZ
- emailing – compliance@thinkmarkets.com

If you are not satisfied with our response to your complaint, you can also refer your complaint to the Insurance and Financial Services Ombudsman Scheme ("IFSO"), an approved dispute resolution scheme under the Financial Service Providers (Registration and Dispute Resolution) Act 2008. Our participant details can be found at https://www.ifso.nz/ and our membership number is 5004399. Their contact details are below:

Freephone: 0800 888 202

Telephone: 04 499 7612

Office hours are 8.30am to 5.00pm Monday to Friday.

Email: info@ifso.nz

Address: Level 2, Solnet House, 70 The Terrace, Insurance & Financial Services Ombudsman Scheme, Wellington 6143, New Zealand.

19. Contractual arrangements with third parties

We ensure that all contractual arrangements with third parties adequately address privacy issues, and we make third parties aware of this Privacy Policy.

Third parties will be required to implement policies in relation to the management of your personal information in accordance with *the Privacy Act*. These policies include:

- regulating the collection, use and disclosure of personal and sensitive information;
- de-identifying personal and sensitive information wherever possible;
- ensuring that personal and sensitive information is kept securely, with access to it only by authorised employees or agents of the third parties; and

- ensuring that the personal and sensitive information is only disclosed to organisations which are approved by us.

20. Your rights

This Privacy Policy contains information about how:

- you may access the personal information we hold about you;
- you may seek the correction of your personal information;
- you may ask us to provide an alternative means of identity verification for the purposes of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)*;*
- you may complain about a breach of the Privacy Act, including the PPs; and
- we will deal with a privacy complaint.

---

21. Relevant Legislation

This policy has been designed to cover obligations across both Australia and New Zealand. Noted below is the relevant legislation for each jurisdiction.

- In Australia
    - Anti-Money Laundering and Counter-Terrorism Financing Act 2006
    - Privacy Act 1988
- In New Zealand
    - Anti-Money Laundering and Countering Financing of Terrorism Act 2009
    - Privacy Act 2020