FUSION MARKETS

Privacy Policy

FMGP Trading Group Pty Ltd trading as Fusion Markets (Fusion Markets)

ABN: 74 146 086 017
AFSL: 385620
Date: November 2026

FMGP Trading Group Pty Ltd (ABN 74 146 086 017) trading as Fusion Markets, is the issuer of the Fusion Markets Products described in this communication. Trading in Fusion Markets Products involves the potential for profit as well as the risk of loss which may vastly exceed the amount of your initial deposit and is not suitable for all investors. You should read all of the Privacy Policy, the Product Disclosure Statement (PDS) and the Financial Services Guide (available on our website) carefully, consider your own financial situation, needs and objectives for investing in these Fusion Markets Products and obtain independent financial advice.

Contents

1. Types of personal information We collect 3
2. How We collect and hold personal information 4
3. Notifying you 4
4. The purposes for which We collect, hold, use and disclose personal information 4
5. How you can access your personal information that We hold and seek the correction of such information 6
6. Additional rights that may apply under GDPR or UK GDPR 7
7. How you can complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds Us, and how We will deal with such a complaint 8
8. Which overseas recipients and countries are We likely to disclose personal information to 8
9. Government Identifiers 9
10. Data Retention 9
11. Automated decision-making and computer programs 9

1. Types of personal information We collect

In this Privacy Policy, “Fusion Markets”, “We”, “Us” and “Our” refer to FMGP Trading Group Pty Ltd (ABN 74 146 086 017) trading as Fusion Markets.

We only collect personal information that is reasonably necessary for one or more of Our functions or activities, whether you interact with Us through Our website or Our mobile application (the “App”). The types of personal information that We collect and hold about you could include:

- ID information such as your name, postal or email address, telephone numbers, and date of birth;
- other contact details such as social media handles;
- financial information, such as your income, net worth, employment details, source of funds and source of wealth, and bank account or payment card details;
- identity documents, such as your passport or driver licence, and information obtained when We verify your identity electronically;
- tax information, such as your country of tax residence and your tax file number or other taxpayer identification number;
- information about your trading knowledge and experience, including your responses to Our onboarding questions; and
- other information you provide to Us, or that is reasonably necessary for Us to provide Our services to you and meet Our legal obligations.

Information We collect through the App

Where you access Our services through the App, We may also collect the following, either automatically or where you grant the relevant device permission:

- device and technical information, including device identifiers, operating system and version, IP address and mobile network information, used for account security and diagnostics;
- location data, where you have granted the App permission to access your device’s location, used to help meet regulatory obligations (such as verifying your trading jurisdiction) and to prevent fraud;
- images or documents captured or uploaded via the App’s camera or photo library, including identification documents provided for identity verification purposes;
- a facial image or short video captured during a liveness check, which We may ask you to complete as part of identity verification, a withdrawal or account recovery. This may involve biometric information, which is sensitive information under the Privacy Act 1988 (Cth). We will only collect it with your consent and will use it only to verify your identity and prevent fraud;
- a push notification token, used to send you alerts about your account, trading activity and service updates;
- confirmation that biometric authentication (such as Face ID or fingerprint login) was successful — the underlying biometric data is captured, matched and stored locally on your device by your device’s operating system, and is not collected or held by Us; and
- analytics and diagnostic information about how you use the App, including crash reports, used to improve App performance.

We will do all that We can to ensure that the personal information that We collect, use and disclose is accurate, up-to-date, complete and relevant.

2. How We collect and hold personal information

We must collect personal information only by lawful and fair means.

We must collect your personal information from you unless it is unreasonable or impracticable to do so. For example, if We are unable to contact you and We then rely on publicly available information to update your contact details or if, at your request, We exchange information with your legal or financial advisers or other representatives.

We might collect your information when you fill out a form with us (either in hard copy or via our website or the App), when We speak with you on the telephone, use Our website or the App, or face to face. We may also collect information automatically through your use of the App, or where you grant the App permission to access your device's camera, photo library, location or notifications, as described above. We may also verify your information via electronic means, such as email.

We hold personal information in electronic form in secure systems, including systems operated by Our service providers, and in limited cases in hard copy. We take reasonable steps to protect the personal information We hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. These steps include access controls, encryption, staff training and regular review of Our security practices.

If a data breach involving your personal information is likely to result in serious harm to you, We will notify you and the Office of the Australian Information Commissioner in accordance with the Notifiable Data Breaches scheme under the Privacy Act 1988 (Cth).

If We receive personal information that We did not solicit, then within a reasonable period after receiving the information, We must determine whether or not We could have collected the information under Australian Privacy Principle 3 (collection of solicited personal information) if We had solicited the information and We may use or disclose the personal information to make this determination.

Then, if We determine that We could not have collected the personal information and the information is not contained in a Commonwealth record, We must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified. If however this does not apply in relation to the personal information, then Australian Privacy Principles 5 to 13 apply in relation to the information as if We had collected the information by solicitation.

3. Notifying you

When We receive personal information from you directly, We will take reasonable steps to notify you how and why we collected your information, who We may disclose it to and outline how you can access it, seek correction of it or make a complaint.

Sometimes We collect your personal information from third parties. You may not be aware that We have done so. If We collect information that can be used to identify you, We will take reasonable steps to notify you of that collection.

4. The purposes for which We collect, hold, use and disclose personal information

We may collect information about you because We are required or authorised by law to collect it. There are laws that affect Us, including company and tax law, which require Us to collect personal information.

For example, We may require personal information to verify your identity under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).

We collect, hold, use and disclose your personal information to:

- assess your application and open, operate and administer your account;
- verify your identity and meet Our obligations under anti-money laundering, counter-terrorism financing, sanctions, tax and financial services laws;
- assess whether Our products are likely to be consistent with your objectives, financial situation and needs, in line with Our design and distribution obligations;
- process deposits, withdrawals and transactions;
- detect and prevent fraud, unauthorised access and other unlawful activity;
- communicate with you, respond to your enquiries and handle complaints;
- send you marketing communications, where permitted (see below);
- improve Our website, the App and Our services; and
- respond to requests from regulators, courts and law enforcement bodies.

We may disclose your personal information to:

- Our related entities;
- service providers that help Us operate Our business, including identity verification, payment, technology, cloud hosting, analytics and customer support providers;
- banks and payment service providers;
- Our professional advisers, auditors and insurers;
- regulators, government agencies, law enforcement bodies and courts, including ASIC, AUSTRAC and the Australian Taxation Office, where We are required or authorised to do so; and
- any other person you have authorised Us to disclose it to.

If We collect and hold your personal information for a primary purpose, We will not use or disclose the information for a secondary purpose unless:

- you have consented to the use or disclosure of the information;
- you would reasonably expect Us to use or disclose the information for the other purpose and the other purpose is related to the first particular purpose;
- the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order;
- a permitted general situation exists in relation to the use or disclosure of the information by Us; or
- We reasonably believe that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

If We collect personal information from any of our related bodies corporate, this principle applies as if Our primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information. This principle does not apply to the use or disclosure by Us of personal information for the purpose of direct marketing or government related identifiers.

If We hold personal information about an individual, We must not use or disclose the information for the purpose of direct marketing, unless We collected the information from the individual and the individual would reasonably expect Us to use or disclose the information for that purpose, and We provide a

simple means by which the individual may easily request not to receive direct marketing communications from Us and the individual has not made such a request to Us.

We may also use or disclose personal information about an individual for the purpose of direct marketing if We collected the information from the individual and the individual would not reasonably expect Us to use or disclose the information for that purpose or someone other than the individual and either the individual has consented to the use or disclosure of the information for that purpose, or it is impracticable to obtain that consent, and We provide a simple means by which the individual may easily request not to receive direct marketing communications from Us, and in each direct marketing communication with the individual, We include a prominent statement that the individual may make such a request, or We otherwise draw the individual's attention to the fact that the individual may make such a request and the individual has not made such a request from Us.

You can opt out of receiving marketing communications from Us at any time by using the unsubscribe link in Our emails or by contacting Us at help@fusionmarkets.com.

If you have general enquiry type questions, you can choose to do this anonymously or use a pseudonym. We might not always be able to interact with you this way however as we are often governed by strict regulations that require us to know who We are dealing with. In general, We will not be able to deal with you anonymously or where you are using a pseudonym when it is impracticable or we are required or authorised by law or a court/tribunal order to deal with you personally.

5. How you can access your personal information that We hold and seek the correction of such information

We will always give you access to your personal information unless there are certain legal reasons why We cannot do so. We do not have to provide you with access to your personal information if:

- We believe there is a threat to life or public safety;
- there is an unreasonable impact on other individuals;
- the request is frivolous;
- the information wouldn't be ordinarily accessible because of legal proceedings;
- it would prejudice negotiations with you;
- it would be unlawful;
- it would jeopardise taking action against serious misconduct by you;
- it would be likely to harm the activities of an enforcement body (e.g. the police); or
- it would harm the confidentiality of our commercial information.

If we cannot provide your information in the way you have requested, we will tell you why in writing. If you have concerns, you can complain by contacting us on +61 3 8376 2706 or you can send us an email to help@fusionmarkets.com

If you believe there is something wrong with the information, for example if you think that the information We hold is inaccurate, out of date, incomplete, irrelevant or misleading, please send us an email to help@fusionmarkets.com so we can update your details.

If you are worried that We have given incorrect information to others, you can ask us to tell them about the correction. We will correct this if We can or We will notify you if We are unable to change the details.

You can ask us to access your personal information that We hold by sending us an email to help@fusionmarkets.com

We will give you access to your information in the form you want it where it is reasonable and practical to do so. We may charge you a small fee to cover our costs when giving you access, but We will always notify you of this first and this fee will not relate to you making a request for your information, only to give you access to the information.

We are required to help you ask for the information to be corrected if We cannot correct this for you. Accordingly, We may need to talk to third parties. However, the most efficient way for you to make a correction request is to send it to the organisation which you believe made the mistake.

If We are able to correct the information, We will notify you within five business days of deciding to do this. We will also notify the relevant third parties as well as any others you notify Us about. If there are any instances where We cannot do this, then We will notify you in writing. If We are unable to correct your information, We will explain why in writing within five business days of making this decision. If We cannot resolve this with you internally, you can make a complaint to the Office of the Australian Information Commissioner (OAIC) or the Australian Financial Complaints Authority (AFCA), as set out in section 7.

If We agree to correct your information, we will do so within 30 days from when you asked us, or a longer period as agreed between Us and you.

If We are unable to make corrections within a 30 day time frame or the agreed time frame, We must notify you of the delay, the reasons for it and when we expect to resolve the matter, ask you to agree in writing to give us more time and let you know you can complain to OAIC.

6. Additional rights that may apply under GDPR or UK GDPR

Where GDPR or UK GDPR applies to your personal information, you may have the following rights:

- Ask what personal data We are collecting and how it is being used (“Right to be Informed”)
- Unsubscribe from any of our emails at any time (“Right to Object”)
- Access the personal data We have collected about you (“Right to Access”)
- Ask Us to correct any inaccurate personal data (“Right to Rectification”)
- Export your personal data in an electronic format (“Right to Data Portability”)
- Require Us to restrict processing of specific types of personal data (“Right to Restrict Processing”)
- Not be subject to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects for you, subject to the exceptions in the GDPR or UK GDPR (“Rights in Relation to Automated Decision-Making”). Section 11 describes the automated decisions We make; and
- Ask for your personal data to be deleted (and be provided with an audit trail if requested) and third parties to stop using the data (“Right to be Forgotten”).

These rights apply equally to personal data We collect through Our website and through the App.

7. How you can complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds Us, and how We will deal with such a complaint

If an individual feels that We have breached our obligations in the handling, use or disclosure of their personal information, they may raise a complaint. We encourage individuals to discuss the situation with one of Our representatives in the first instance, before making a complaint.

The complaints handling process is as follows: The individual should make the complaint including as much detail about the issue as possible, in writing to Us:

Complaints Department
Fusion Markets
Email: help@fusionmarkets.com

Post: Level 10, 627 Chapel Street, South Yarra VIC 3141, Australia

We will investigate the circumstances included in the complaint and respond to the individual as soon as possible (and within 30 calendar days) regarding Our findings and actions following this investigation. After considering this response, if the individual is still not satisfied they may escalate their complaint directly to the Information Commissioner for investigation:

Office of the Australian Information Commissioner
Website: www.oaic.gov.au
Phone: 1300 363 992

When investigating a complaint, the OAIC will initially attempt to conciliate the complaint, before considering the exercise of other complaint resolution powers.

Alternatively, if an issue has not been resolved to your satisfaction, you can lodge a complaint with the Australian Financial Complaints Authority, or AFCA. AFCA provides fair and independent financial services complaint resolution that is free to customers.

Australian Financial Complaints Authority
Website: www.afca.org.au
Email: info@afca.org.au
Phone: 1800 931 678 (free call)
Post: GPO Box 3, Melbourne VIC 3001

8. Which overseas recipients and countries are We likely to disclose personal information to

We may store your information in cloud or other types of networked or electronic storage. As electronic or networked storage can be accessed from various countries via an internet connection, it is not always practicable to know in which country your information may be held. We are likely to disclose personal information to recipients located in the Philippines, Seychelles and Vanuatu, including Our

related entities and service providers. Where We use cloud or networked storage, personal information may also be held in other countries.

This includes information collected through the App: where We use App analytics, crash-reporting, push-notification or cloud storage service providers, information collected through the App may also be stored or processed overseas on the same basis.

Overseas organisations may be required to disclose information We share with them under a foreign law. Before disclosing personal information to an overseas recipient, We take reasonable steps to ensure that the recipient handles it consistently with the Australian Privacy Principles.

9. Government Identifiers

Sometimes We may be required to collect government-related identifiers such as your tax file number. We will not use or disclose this information unless We are authorised or required to do so by law or the use or disclosure of the identifier is reasonably necessary for Us to verify your identity for the purposes of Our business activities or functions.

10. Data Retention

Fusion Markets retains personal information collected through our website and the App for as long as necessary to provide our services and to comply with our legal, regulatory and record-keeping obligations. In particular, client account records, transaction records, identification and due diligence documentation, and related correspondence are retained for a period of seven (7) years from the end of the business relationship or the date of the relevant transaction, consistent with applicable anti-money laundering and financial services record-keeping requirements. Where applicable laws require a longer or shorter period for particular records, that period will apply instead. On expiry of the applicable retention period, Fusion Markets will securely delete or anonymise the relevant personal information.

11. Automated decision-making and computer programs

Fusion Markets uses computer programs and automated systems to support certain operational, compliance, risk management, fraud prevention and client onboarding activities. Some of these programs make decisions, or do things that are substantially and directly related to making decisions, that could reasonably be expected to significantly affect your rights or interests. This section explains the kinds of personal information these programs use and the kinds of decisions they make or support.

Personal information used by these programs

The kinds of personal information used in the operation of these computer programs include:

- identification information, such as your name, date of birth, residential address and identity document details;
- contact information, such as your email address and telephone number;
- location information, such as your country of residence, IP address and, where you have granted the App permission, your device location;

- transaction information, such as deposits, withdrawals, payment method details and trading activity;
- device information, such as device identifiers, operating system and browser details; and
- account activity, such as login history, account settings and changes to your account details.

Decisions made solely by computer programs

Some decisions are made solely by the operation of a computer program, without a member of Our staff reviewing the decision before it takes effect. These are:

- verifying your identity electronically against independent data sources during onboarding, where that verification is successful;
- declining an account application, or restricting access to Our services, where the information you provide, your IP address or your device location indicates that you are located in a jurisdiction in which We do not offer Our services;
- temporarily locking or restricting access to your account, or requiring additional authentication, where Our security systems detect unusual login activity, repeated failed login attempts or a device not previously associated with your account; and
- closing out open positions where your account falls below the required margin level, in accordance with Our terms and conditions.

Decisions supported by computer programs

For other decisions, a computer program does something substantially and directly related to making the decision, such as screening, scoring or flagging, but a member of Our staff reviews the outcome and makes the final decision. These include:

- screening you against sanctions, politically exposed person and adverse media sources, with any potential matches reviewed by Our compliance team;
- assigning a money laundering and terrorism financing risk rating to your account, which determines the level of due diligence We apply to you;
- referring your application for manual identity verification where electronic verification is unsuccessful;
- assessing whether you are likely to be within the target market for Our products, based on your responses to Our onboarding questions;
- monitoring transactions and account activity to detect potentially suspicious, fraudulent or unusual activity; and
- deciding whether to restrict, suspend or close your account, or to decline or delay a deposit or withdrawal, for compliance, fraud prevention or risk management reasons.

Asking for a review

If you believe a decision made or supported by a computer program has affected you, you can contact Us using the details in section 7 to ask for more information about the decision or for it to be reviewed by a member of Our staff. Where We are able to, We will explain the main factors that led to the decision. We may not be able to provide this information where doing so would be unlawful, including where it would breach Our obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), or where it would compromise Our fraud prevention or security controls. You may also make a complaint as set out in section 7.

We review the computer programs We use periodically and will update this Privacy Policy if the kinds of decisions they make or support change.