HFM Investments Ltd

Privacy Policy

The Oval Building, Corner of Jalaram Road/Ring Westlands
5th Floor, Office 2-7, P.O. Box 39397-00623, Parklands, Kenya
T. +254-203894292
support.ke@hfm.com
www.hfm.com/ke

Table of Contents

1. Introduction 3
2. Collection of Personal Data 3
3. No Children's Data Collection 5
4. Use of Personal Data 5
5. Cookies 7
6. Links to other websites 8
7. Client Records Retention Periods 8
8. Sharing and Disclosure of Personal Data 8
9. Business Transfers Legal Requirements 9
10. Personal Data Transfers outside Kenya 10
11. Marketing Communications – Services Subscriptions Preferences 11
12. Personal Data Rights 12
13. Automated decision-making and profiling 13
14. Artificial Intelligence and Machine Learning (AI) 14
15. Confidentiality and Security of Personal Data 14
16. Amendments to this Policy 15
17. Enquiries and Contact Details 15

1. Introduction

1.1. HFM Investments LTD is a member of HFM Group, incorporated under the laws of the Republic of Kenya with Registration Number PVT-BEUJQBA (hereinafter the **"Company"**). The Company is authorised and regulated by the Capital Markets Authority ("**CMA**") to act as a non-dealing foreign exchange broker under the Capital Markets (Online Foreign Exchange Trading) Regulations, 2017 with License No 155.

1.2. This privacy statement covers the website www.hfm.com/ke and all its related sub-domains and mobile applications that are registered and operated by HFM Investments Ltd.

1.3. The Company acting in its capacity as non-dealing foreign exchange broker and in accordance with the Data Protection Act No. 24 of 2019 (the "**Law**") outlines in the Privacy Policy (herein the "**Policy**") how the Company collects, maintains, handles, protects and discloses (if applicable) personal information of the Client.

1.4. This Policy applies to existing clients, prospective clients, clients who have terminated their contractual relationship with the Company and website visitors (hereinafter jointly referred to as the "**Clients**" or "**you**") who are accessing or using the Company's website(s) and mobile applications (hereinafter referred to as the "**Platforms**").

1.5. The Company is committed to protecting the privacy of all Clients' Personal Data which it processes in accordance with the provisions of the Law, the Data Protection (General) Regulations 2021, this Policy and the Company's Client Agreement.

1.6. For the purposes of this Policy, references to "Personal Data" shall mean data which identifies or may identify Clients and which may include, for example, a Client's name, address, identification number, telephone number and date of birth.

2. Collection of Personal Data

2.1. The Company collects different types of Personal Data through the Company's Platforms from Clients who visit such Platforms or access, use or request products and services offered by the Company.

2.2. The provision of certain Personal Data is required for establishing a contractual relationship with the Company. Clients not wishing to provide such Personal Data will not be able to open an account with the Company or be provided with other products and/or services of the Company.

2.3. Clients have a responsibility to ensure that the Personal Data they provide to the Company and recorded in their personal account (Client Area) remain accurate and up to date throughout the period of their contractual relationship with the Company.

2.4. In addition to the information provided by Clients, the Company also lawfully collects and processes Personal Data from publicly available sources (including, inter alia, the press, social media and the internet) and third- party compliance databases for fraud prevention and KYC verification The Personal Data received from the Client, collected and processed by the Company are required for the communication, identification, verification and assessment for the business relationship establishment with the Client, contract performance, legitimate interest, and legal compliance. The following Personal Data may be collected from Clients depending on the product and/or service the Company provides to him:

(a) Contact details such as the Client's name, e-mail address and phone number.
(b) Identification details such as the Client's identification or passport number.
(c) Biographical and demographic data such as gender, age, ethnicity, education, occupation, the Client's financial trading experience and whether he has a prominent public function status (PEP).
(d) Financial information such as the Client's income status, bank account number and account details, tax information and other financial information.
(e) Information relevant to the services that the Company provides to the Client such as the Client's transactions and communication records with the Company.
(f) Details of visitors' and Clients' visits to the Company's website and information collected through cookies and other tracking technologies including IP address and domain name, browser version, operating system and geolocation.

(g) Information in relation to criminal convictions and offences to the extent required and/or permitted by applicable law.

(h) Information in relation to the client's mobile device Call log with the permission of the client.

(i) Your marketing preferences.

(j) Data derived from your activity.

(k) Information and logs from your interactions with the conversational AI Bots.

3. No Children's Data Collection

3.1. The Company understands the importance of protecting children's privacy. The Company's services are not intended for children under eighteen (18) years of age nor is the Company's website designed for use by children. Therefore, the Company does not knowingly or specifically collect children's personal data. If the Company collects such data mistakenly or unintentionally, the Company shall delete the information at the earliest possible once it obtains knowledge thereof. If the Client becomes aware of such data collection he/she shall notify the Company at privacy.ke@hfm.com.

4. Use of Personal Data

4.1. The Company collects and processes Personal Data which are required for the evaluation, establishment and maintenance of the contractual relationship between the Company and the Client and in order to comply with this Policy and applicable laws and regulations governing the provision of financial services. In some cases, the Company may also process the Client's Personal Data to pursue its legitimate interests or those of third parties, provided that the Clients' interests and fundamental rights are not overridden by those of the Company or the third party.

4.2. Specifically, the Client's Personal Data will most commonly be used in the following circumstances:

(a) Where the Company needs to perform the contract it has entered with the Client or in order to take certain steps prior to entering into a contract with the Client

Processing is necessary for the Company in order to provide the Client with its products and services, and more specifically in order:

- To verify the Client's identity and carry out any required credit checks;
- To ensure that the Client meets the suitability requirements to use the Company's products and services;
- To manage the account the Client holds with the Company;
- To process the Client's transactions; and
- To send to the Client any information about transactions/post-transactions services.

If the Client does not provide the requested Personal Data, the Company may be unable to offer the Client with its products and/or services.

(b) Where the Company needs to comply with a legal obligation

As an investment firm, the Company is required to comply with certain legal and regulatory obligations which may involve the processing of Personal Data. Such obligations and requirements impose on the Company necessary data processing activities for identify verifications, compliance with court orders, tax law or other reporting obligations and anti-money laundering controls.

(c) Where the Company has legitimate interests to use the Client's Personal Data

More specifically, the Company may process the Personal Data for the following purposes:

- To develop or enhance its products and services;
- To enhance the security of the Company's network and information systems;
- To identify, prevent and investigate fraud and other unlawful activities, unauthorised transactions and other liabilities and manage risk exposure;
- To maintain its accounts and records;
- To manage its business operations and comply with internal policies and procedures;
- To defend, investigate or prosecute legal claims;

- To receive professional advice (such as legal advice);
- For the analysis of statistical data which helps the Company in providing its Clients with better products and services in the future. It should be noted that the Company anonymises and aggregate such data so that they do not directly or indirectly reveal the Clients' identities. The Company may provide this statistical data to third parties (as described in more detail in Section 8) solely for statistical purposes and in an effort to improve the Company's marketing campaign;
- To measure campaign effectiveness;
- To provide AI-powered analytics: The Company uses proprietary machine learning modules to analyse commercial metrics;
- To collect reviews/feedback for improving the services of the Company.

(d) Where the Client has given his consent

- The Company will ask for the Client's consent when the Company wishes to provide marketing information to its Clients in relation to its products or services which may be of interest to the Client.
- The Company will ask for Clients' permission to access their mobile device call log for the sole purpose of completing the phone number verification process.
- The Company will ask for Clients' permission to electronically verify their identity by providing their personal information to identity verification providers.
- The Company will obtain the Client's prior consent in any other circumstance where such consent is required by law or deemed necessary by the Company.

The Client may withdraw such consent at any time. This right doesn't affect the lawfulness of processing that was based on that consent before its withdrawal.

5. Cookies

5.1. A cookie is a small text file that is stored on a user's computer for record-keeping purposes. The Company uses cookies on its website(s) to ensure and provide the Client with a good experience when he browses our website and allows us to improve our website.

5.2. To understand more about the kind of cookies we use and how you can control and delete cookies, please see our Cookie Policy.

6. Links to other websites

6.1. The Company's website contains or may contain links to other websites or social media platforms of interest. However, once you have used these links to leave the Company's website, you should note that the Company does not have any control over those other websites. Therefore, the Company cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this Policy. You should exercise caution and look at the privacy statement applicable to the website in question.

6.2. The Company will not be liable for the unlawful or unauthorized use of the Client's Personal Data due to misuse and/or malicious use and/or negligence and/or misplacement of the Client's passwords either by him/her or any third party.

7. Client Records Retention Periods

7.1. Under the applicable laws and regulations, the Company is required to keep records containing Client Personal Data, trading information, account opening documents, communications and anything else which relates to the Client for 7 (seven) years after the execution of the last transaction or the termination of the business relationship.

8. Sharing and Disclosure of Personal Data

8.1. In the course of the performance of the Company's contractual and statutory obligations, the Client's Personal Data may be disclosed to third parties. Most of such third parties enter into contractual arrangements with the Company by which they observe data protection and confidentiality according to applicable law and regulations.

8.2. Under the circumstances referred to above, recipients of Personal Data may be, for example:

(a) third party payment service providers who help the Company provide its Clients the services of securely deposit and withdrawal to and from a Client's account;

(b) other service providers that the Company has chosen to support it in the effective provision of its products and services by offering technological expertise, solutions and support;

(c) governmental and regulatory bodies, including law enforcement authorities and FSCA, in connection with enquiries, proceedings or investigations by such parties or in order to enable the Company to comply with its legal and regulatory requirements;

(d) credit reference and fraud prevention agencies, third party authentication service providers and other financial institutions for the purposes of credit checking, fraud prevention and anti-money laundering controls;

(e) third party service providers for the provision of the required customer support services through live chat and the Company's website visits and traffic monitoring through cookies;

(f) external consultants including legal and tax consultants;

(g) data reporting service providers;

(h) market research companies and call centers;

(i) affiliates of the Company; and

(j) AI Technology Providers.

8.3. In accordance with the recommendations of Payment Card Industry Security Standards Council, customer card details are protected using Transport Layer encryption — TLS 1.2 and application layer with algorithm AES and key length 256 bit.

8.4. The Company does not collect, store or process any personal credit or debit card information. All payment transactions are processed through payment gateway providers.

9. Business Transfers Legal Requirements

9.1. If the Company is involved in a merger, acquisition, financing due diligence, reorganization, bankruptcy, receivership, sale of company assets, or transition of service to another

provider, Client's Personal Data and other information may be transferred to a successor or affiliate as part of that transaction along with other assets.

10. Personal Data Transfers outside Kenya

10.1. The Company is committed to protecting Personal Data especially when these are to be transferred outside Kenya. The Law allows personal data to be transferred outside of Kenya if the transfer is necessary.

10.2. The Company may transfer, disclose or make available Clients' Personal Data to companies within the HFM Group and to third-party service providers, including data processors, located within or outside Kenya, where such transfers are necessary for the provision of its services, the performance of its contractual obligations, compliance with applicable legal and regulatory requirements, or other legitimate business purposes permitted by law.

10.3. Any transfer of Personal Data outside Kenya shall be carried out in accordance with the Law, and any other applicable data protection requirements.

10.4. Where Personal Data is transferred outside Kenya, the Company shall ensure that an appropriate legal basis or transfer mechanism applies and that relevant safeguards are implemented to protect the confidentiality, integrity and security of the Personal Data.

10.5. Depending on the nature of the transfer, the Company shall apply appropriate safeguards, including:

- Contractual Safeguards: Ensuring that appropriate contractual arrangements are in place with recipients of Personal Data, requiring them to maintain appropriate standards of data protection, confidentiality and security, and to process Personal Data only for authorised purposes.
- Assessment of Data Protection Standards: Assessing the level of data protection afforded by the recipient and the destination country, including the existence of applicable data protection laws and the technical and organisational measures implemented to protect Personal Data.

- Technical and Organisational Security Measures: Implementing appropriate security measures, including encryption during transmission, access controls, restrictions on unauthorised disclosure and other measures designed to protect Personal Data against accidental loss, unlawful access, alteration or unauthorised processing.
- Access Restrictions and Confidentiality: Ensuring that access to transferred Personal Data is limited to authorised personnel and service providers who require such access for legitimate business purposes and are subject to appropriate confidentiality and data protection obligations.
- Monitoring and Accountability: Maintaining appropriate oversight of international data transfers and, where required by applicable law, documenting the transfers and the safeguards implemented to ensure compliance with relevant data protection requirements.

10.6. Where the Company relies on the necessity of a transfer, the Client's consent or another legally recognised transfer mechanism, the relevant requirements under applicable law shall be observed.

10.7. The Company shall take reasonable steps to ensure that Personal Data transferred outside Kenya continues to receive an appropriate level of protection and that recipients process such Personal Data only for the purposes for which it was lawfully disclosed.

11. Marketing Communications – Services Subscriptions Preferences

11.1. The Company may process Personal Data to tell its Clients about products, services and offers that may be of interest to the Client. The Company may only process such Personal Data if it has obtained the Client’s explicit consent to do so.

11.2. If the Client no longer wishes to receive any promotional communications, he may opt-out of receiving them by following the instructions included in each communication or by updating his email subscription preferences within the Client account area.

12. Personal Data Rights

12.1. Clients have the following rights in relation to their Personal Data:

- **Right of access:** The Client has the right to be informed whether the Company is processing his/her Personal Data, and if so, to provide the Client with a copy of that Personal Data.
- **Right to rectification:** The Client is entitled to request that the Company corrects or completes his/her Personal Data if it is inaccurate, outdated, incomplete or misleading.
- **Right to erasure:** This enables the Client to request the deletion or destruction of their personal data without undue delay when the Company no longer has a lawful basis to retain it.
- **Right to restrict processing:** This enables the Client to ask the Company to restrict the processing of the Client's Personal Data if:
  - accuracy of the personal data is contested by the Client, for a period enabling the Company to verify the accuracy of the data;
  - personal data is no longer required for the purpose of the processing, unless the Company requires the personal data for the establishment, exercise or defence of a legal claim;
  - processing is unlawful and the Client opposes the erasure of the personal data and requests the restriction of their use instead; or
  - Client has objected to the processing, pending verification as to whether the legitimate interests of the Company overrides those of the data subject.
- **Right to data portability:** The Client has the right to obtain his/her Personal Data provided to the Company in a structured, commonly used and machine-readable format.
- **Right to object:** The Client has the right to object to the processing of his/her personal data, unless the Company demonstrates compelling legitimate interest for the processing which overrides the Client's interests, or for the establishment, exercise or defence of a legal claim.

- **Rights in relation to automated decision-making and profiling:** The Client has the right to be free from decisions based solely on automated processing of his/her Personal Data, including profiling, that affect him/her, unless such profiling is necessary for entering into, or the performance of, a contract between Client and the Company or the Client provides explicit consent.
- **Right to withdraw consent:** If the Company relies on the Client's consent to process his/her Personal Data, the Client has the right to withdraw that consent at any time. This will not affect the lawfulness of the processing that took place on the basis of the Client's prior consent.
- **Right to lodge a complaint with the data protection authority:** If the Client has a concern about the Company's privacy practices, including the way in which the Company handled his/her Personal Data, the Client can report it to the relevant data protection authority.

To exercise any of the above rights, the Client may contact the Company at privacy.ke@hfm.com.

13. Automated decision-making and profiling

13.1. When you make an application for account opening we will use systems to make an automated assessment of your knowledge and experience through the evaluation of an appropriateness test. In such cases, you have the right to contact us to:

(a) give you information about the processing of your personal data (please also see Section 12 of this Policy in relation to your rights); and/or

(b) request that one of our employees examines your application and obtain an explanation for the automated decision reached. You also have the right to challenge such a decision. Following such a request, we will reassess your application, taking into consideration both the reasons that a particular automated decision was reached as well as your own point of view.

14. Artificial Intelligence and Machine Learning (AI)

14.1. The Company utilizes proprietary and third-party artificial intelligence (AI) and machine learning (ML) technologies (hereinafter "AI tools") to provide enhanced services to the Clients.

14.2. These AI tools are used based on our Legitimate Interests to improve platform efficiency, provide state-of-the-art analytical tools, and enhance the user experience for the Clients.

14.3. The AI tools are designed to support, not replace, human decision-making. The Company implements safeguards to ensure that AI-generated insights do not result in automated decisions with significant effects without appropriate human review.

15. Confidentiality and Security of Personal Data

15.1. Personal Data which the Company holds is to be treated by the Company as confidential and will not be used for any purpose other than those specified in this Policy.

15.2. Any Personal Data that the Client provides to the Company will be treated as confidential and shared only with the parties set out in Section 8 of this Policy.

15.3. Such Personal Data will not be disclosed to any other third party except if such disclosure is required under any regulatory or legal proceedings.

15.4. The Personal Data that the Client provides in connection with registering as a user of the website(s) or for the Services is classified as Registration Information. The Company offers high protection of the Registration Information provided by the Client. The Client can access his Registration Information through a password selected by him which is encrypted and known only to the Client. The Client must be careful and protect his password from any third parties. Registration Information is safely stored on secure servers that only authorized personnel have access to via password. The Company encrypts all Personal Data as it is transferred to the Company and thus makes all necessary effort to prevent unauthorized parties from viewing any such information.

15.5. Personal Data provided to the Company that is not Registration Information also resides on secure servers and is again accessible only to authorized personnel via password. This

information is not accessible by the Client; therefore, no password is provided to view or modify this information.

16. Amendments to this Policy

16.1. The Company reserves the right to review and amend this Policy from time to time for any reason and notify the Clients of any such amendments accordingly by posting an updated version of this Policy on the Company's website(s). The Company will notify you about any material changes to this Policy by placing a notice on its website or by communicating with you directly.

16.2. The Client is responsible for regularly reviewing the Policy and any amendments thereof.

17. Enquiries and Contact Details

17.1. For any general enquiries regarding this Policy or for any data subject requests, as set out in Section 12 of this Policy, or questions about how the Company processes Client's Personal Data, please contact us at privacy.ke@hfm.com .

Version: 2026/02