MADE4TRADING
WHERE TRADERS TRADE

Made4Trading

Confidentiality Policy

Made4Capital Limited
Level 1, IconEbene 1, Reduit Road,
Cybercity, Ebene. 72201, Mauritius.

www.made4trading.com

1. Overview

Made4Capital Limited, trading as Made4Trading (hereinafter the "Company" or the "Firm") is a financial services company duly incorporated and registered under the laws of the Republic of Mauritius bearing company number 234336GBC, authorised and regulated by the Financial Services Commission of Mauritius ("FSC") with license number GB26205996. The Company's registered office is Level 1, IconEbene 1, Reduit Road, Cybercity, Ebene 72201, Mauritius.

Confidentiality is one of the most important legal obligations of the fiduciary industry. Besides being regulated by laws and legislation, confidentiality is also the cornerstone of a sound and trustworthy client relationship. A breach of confidentiality occurs when information provided in confidence to the Company by a client is disclosed to a third party without the client's consent. While most confidentiality breaches are unintentional, clients can still suffer significant financial losses as a result.

Important: A breach of client confidentiality can result in a sizeable award for damages, loss of reputation, and regulatory action against the Company.

---

2. Regulatory Framework

This Confidentiality Policy ("the Policy") adheres to Mauritian legislation, including the Banking Act 2004 and the Financial Services Act 2007 ("FSA 2007").

In the course of their duties, employees may have access to personal and private information pertaining to clients, partners, and the Company. It is of paramount importance that the Company takes the necessary measures to ensure robust protection of this information.

The protection of confidential information is vital for two significant reasons:

- **Legal Obligation:** Certain information may be subject to legal obligations, such as sensitive customer data that must be handled in accordance with relevant regulations.

- **Business Integrity:** Confidential information serves as the bedrock of our business operations, providing us with a competitive advantage, such as proprietary business processes that set us apart in the industry.

The Company and its employees shall not disclose the data of its financial consumers and shall protect the confidentiality of its non-public data. Client data shall only be utilised for the purposes specified and agreed with the financial consumer, for onboarding and assessing clients, or as required under any applicable law.

The Company may only disclose information to the FSC where required or requested, in accordance with the applicable laws and regulations. This includes complying with the power of the FSC to request information and conduct inspections under Sections 42 and 43 of the FSA 2007, respectively.

3. Non-Public Data

This Policy is formulated to comply with the strict confidentiality obligations under Section 64 of the Banking Act 2004 and Section 83 of the FSA 2007. As the Company is licensed and regulated by the FSC, it is bound by these laws to protect all non-public data and information relating to the affairs of its customers.

The types of non-public data collected and processed by the Company include, but are not limited to:

- Personal information such as name, surname, residential address, email address, phone number, date of birth, gender, citizenship, occupation and employment details;
- Information for the construction of the client's economic profile, including source of income and wealth, and details about source of funds;
- Information on whether a client holds a prominent public function (Politically Exposed Persons (PEPs);
- Bank account and/or credit card details; and

Documents provided to the Company for verification of the client's identity, including passport/identity card, company incorporation details, utility bills, and other identifiable documents. Other documents such as business plans, intellectual property, customer lists, financial records, software, marketing strategies, and any information which, if disclosed, could harm the organisation.

4. Sensitive Data

The Company considers the following categories of personal data to be sensitive, including but not limited to:

- Personal data revealing racial, gender or ethnic origin, political opinions, or religious or philosophical beliefs;
- Trade-union membership;
- Genetic data and biometric data processed solely to identify a human being; and
- Health-related data.

The Company does not intentionally collect and/or process sensitive data from clients or potential clients during the provision of its services unless required for legal or regulatory compliance purposes.

5. Non-Public Data Collection & Verification

The non-public data collected by the Company is utilised at all stages of the business relationship to provide services and products as defined in the Client Services Agreement. The collection and processing of this data are essential for the Company to perform its contractual obligations and to complete mandatory client onboarding procedures.

Consequently, the Company is legally required to collect specific data during onboarding and through ongoing monitoring of transactions for risk mitigation and management purposes.

5.1 Identity Verification & Fraud Prevention

At the start of the business relationship, the Company requires non-public data to authenticate and verify the identity of the client. Establishing the identity of a client is a mandatory requirement under Mauritian law and is crucial for identifying, assessing, mitigating, and investigating potential fraudulent activities or financial crimes.

5.2 Appropriateness & Account Management

Throughout the business relationship, the Company collects data regarding a client's risk tolerance, income, and profession. This information is required to assess the appropriateness of the products and services provided. Additionally, this data enables the Company to manage the client's account effectively, inform the client of relevant products or services, and perform statistical analyses to improve service quality.

5.3 Termination of Relationship

Non-public data remains necessary when a client decides to terminate their relationship with the Company, particularly for assessing historical data or resolving complaints. In accordance with the Banking Act 2004 and the FSA 2007, the Company is required to maintain all records, including account files and business correspondence, for a period of at least seven (7) years from the date of the client's last transaction or the completion of the relevant transaction. These records may be stored in written or electronic formats as permitted by the FSC.

---

6. Staff Conduct

All staff members of the Company are expected to adhere to the following confidentiality practices:

- Any information concerning companies, their promoters, beneficial owners, officers or related parties is confidential and shall not be released in any way to anyone unless authorised by the client or otherwise required by law or under any other agreements entered into by or on behalf of the Government of Mauritius.

Unless specifically authorised by a director to do otherwise, staff must not:

- Disclose information to any person unless it forms part of the normal practice of day-to-day work;

- Disclose to any person the names of clients for whom the Company acts, except where such disclosure, such as to banks and the like, is normal and necessary;

- Disclose to relatives, friends, contractors, or other unauthorised persons any matter relating to the Company's clients or their affairs; or

- Disclose any discussions with their supervisor to any other staff member or third party, unless specifically authorised to do so by their supervisor.

7. Security Practices

The Company implements the required procedures for safeguarding the security, integrity, and confidentiality of information, taking into account the nature of the information being stored. Agents or third parties that assist the Company in providing its services to clients shall maintain the confidentiality of non-public data and use such information only while providing their services, based on the Company's directions. The Company monitors the activities of agents and third parties acting on its behalf, based on the relevant agreements that are in place for each business relationship.

Specifically, non-public data is only accessible by employees who require access to such information to perform their duties. Such individuals are bound by confidentiality and are subject to internal disciplinary procedures, as well as legal consequences under the Banking Act 2004 and the FSA 2007, in case they fail to meet their obligations.

The accessibility of non-public data by employees is based on the following principles:

- Differentiation of access rights according to the level of each employee;

- Protection of systems by defining access privileges, control structures, and resources;

- Responsibility measures for the unlawful disclosure of information, applicable to Company employees and individuals outside the Company; and

- Encryption of sensitive information.

7.1 Employee Responsibilities

Employees must understand and comply with this Policy and any additional confidentiality agreements they have signed.

In particular, employees shall:

- protect and maintain the confidentiality of all information entrusted to them during and after their employment;

- not disclose confidential information to unauthorised individuals unless required by law or with proper authorisation;

- take appropriate security measures to prevent unauthorised access to confidential information, such as using strong passwords and secure storage methods; and

- report any suspected breach or unauthorised disclosure of confidential information promptly to their supervisor, Compliance Officer, or other designated person in accordance with the Company's internal reporting procedures.

7.2 Management Responsibilities

Management has the following responsibilities in relation to the protection of confidential information.

Management shall:

- ensure that employees are fully informed about this Policy and receive comprehensive training and guidance on its implementation;
- regularly review and update access controls and security measures to safeguard confidential information from unauthorised access or disclosure; and
- promptly investigate and take appropriate action in response to any reported breaches or unauthorised disclosures of confidential information.

8. Data Protection & Privacy

The Company is registered as a Data Controller with the Data Protection Office in Mauritius, in line with Section 14 of the Data Protection Act 2017 of Mauritius ("DPA 2017"). Accordingly, the Company adheres to the requirements of the DPA 2017 in relation to the collection, processing, storage, and sharing of personal data of clients, to ensure the privacy, confidentiality and integrity.

The DPA 2017 was promulgated with a view to aligning with the EU General Data Protection Regulation (GDPR). As a Data Controller, the Company ensures compliance with the following six (6) principles when collecting, processing, and managing personal information owned by data subjects, in line with Section 21 of DPA 2017:

	Principle	Description
1	**Lawfulness, Fairness and Transparency**	Personal data must be processed lawfully, fairly, and in a transparent manner.
2	**Purpose Limitation**	Personal data must be collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes.
3	**Integrity and Confidentiality**	Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4	**Accuracy**	Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay.
5	**Storage Limitation**	Personal data must be kept in a form which permits identification of data subjects no longer than is necessary for the purposes for which the personal data are processed.
6	**Data Subjects' Rights**	Personal data must be processed in accordance with the rights of data subjects as provided under the DPA 2017.

The Company ensures that the DPA 2017 is respected by all its staff and that there is no breach. Appropriate training is provided to relevant employees on a regular basis on data privacy regulations, as they are the ones handling business relationships or transactions, including liaising directly with clients.

9. Non-Public Data Storage

The Company undertakes all reasonable and appropriate organisational, physical, and technical measures for the protection of non-public data against unlawful access, destruction, misuse, or accidental loss. Non-public data is stored on the databases of the Company, CUBE and HubSpot.

For safeguarding the Company's recorded data from possible loss, the Company implements consistent, reliable, and documented backup procedures. The backup procedure is automatic and takes place once per day across two different storage spaces, as follows:

- **Automatic Save:** critical data from the server is automatically saved to a secondary hard disc within the server as well as to a separate external storage device.

- **Cloud Backup:** backup files are stored in a secure cloud environment using Veeam services, on a daily, monthly and annual basis.

The IT Officer or Finance and Administration Manager shall ensure that accounting records and backup copies are stored so as to minimise any risk of their loss due to theft, fire, corruption or any unauthorised erasure; prevent unauthorised access; and are backed up or otherwise duplicated so that copies are available if the originals are lost, destroyed, corrupted or erased.

The Company retains client non-public data for a period of at least seven (7) years from the date of the client's last transaction. Where an investigation is ongoing against any clients, documents will be retained in accordance with the instructions of the investigating authority.
The Company will be able to retrieve relevant documents and data without undue delay and present them at any time to the local authorities if so requested.

10. Non-Public Data Disclosure

The Company may disclose non-public data to a third party where permitted or required by applicable law, including in the following circumstances:

- The client has been informed about the disclosure and has consented in writing to such disclosure;
- The third party to which the data will be disclosed has been authorised by the client to obtain the data from the Company; or

- The Company is required to disclose the non-public data to the Credit Information Bureau, the Financial Intelligence Unit (FIU), the FSC, under any other Mauritian law, or by court order.

In such cases, employees involved must follow a documented disclosure procedure and obtain all necessary approvals. It is essential for the Company to disclose only the minimum amount of information required, avoiding unnecessary or excessive disclosures, unless required by law.

---

11. Penalties

All employees and officers of the Company are bound by strict confidentiality obligations in the exercise of their duties. Any breach of confidentiality obligations may result in regulatory, civil, criminal, and/or internal disciplinary consequences, including penalties prescribed under applicable laws and regulations.

The Company may take appropriate internal disciplinary action against any employee or officer who breaches this Policy, which may include dismissal, where appropriate.

Protection from liability may apply in circumstances where a disclosure is made in good faith and in accordance with applicable Mauritian law. Such protection does not, however, excuse wilful or negligent disclosure.

---

12. Client Consent

At the stage of establishing a business relationship, the Company obtains the Client's voluntary consent to this Policy. Such consent is obtained before the offering of any services to the consumer.

The Company may obtain the client's consent electronically through the acceptance of the Client Service Agreement. Clients who have received and electronically agreed to this Policy shall be deemed to have consented to the collection, processing, use, and disclosure of their non-public personal data in accordance with this Policy and applicable law.

13. Amendments to Policy

The Company reserves the right to make changes to this Policy from time to time for operational, regulatory or legal reasons. Clients will be notified of any such changes by posting an updated version of this Policy on the Company's website. The client is responsible for regularly reviewing this Policy on the Company's website. Where required, clients will be notified of material changes to the Policy in accordance with applicable laws and regulations.

14. How to Contact Us

Any client wishing to raise questions or requests in relation to their data stored by the Company may do so by contacting the Support Team:

Support Team

Email: support@made4trading.com

Address: Level 1, IconEbene 1, Reduit Road, Cybercity, Ebene 72201, Mauritius