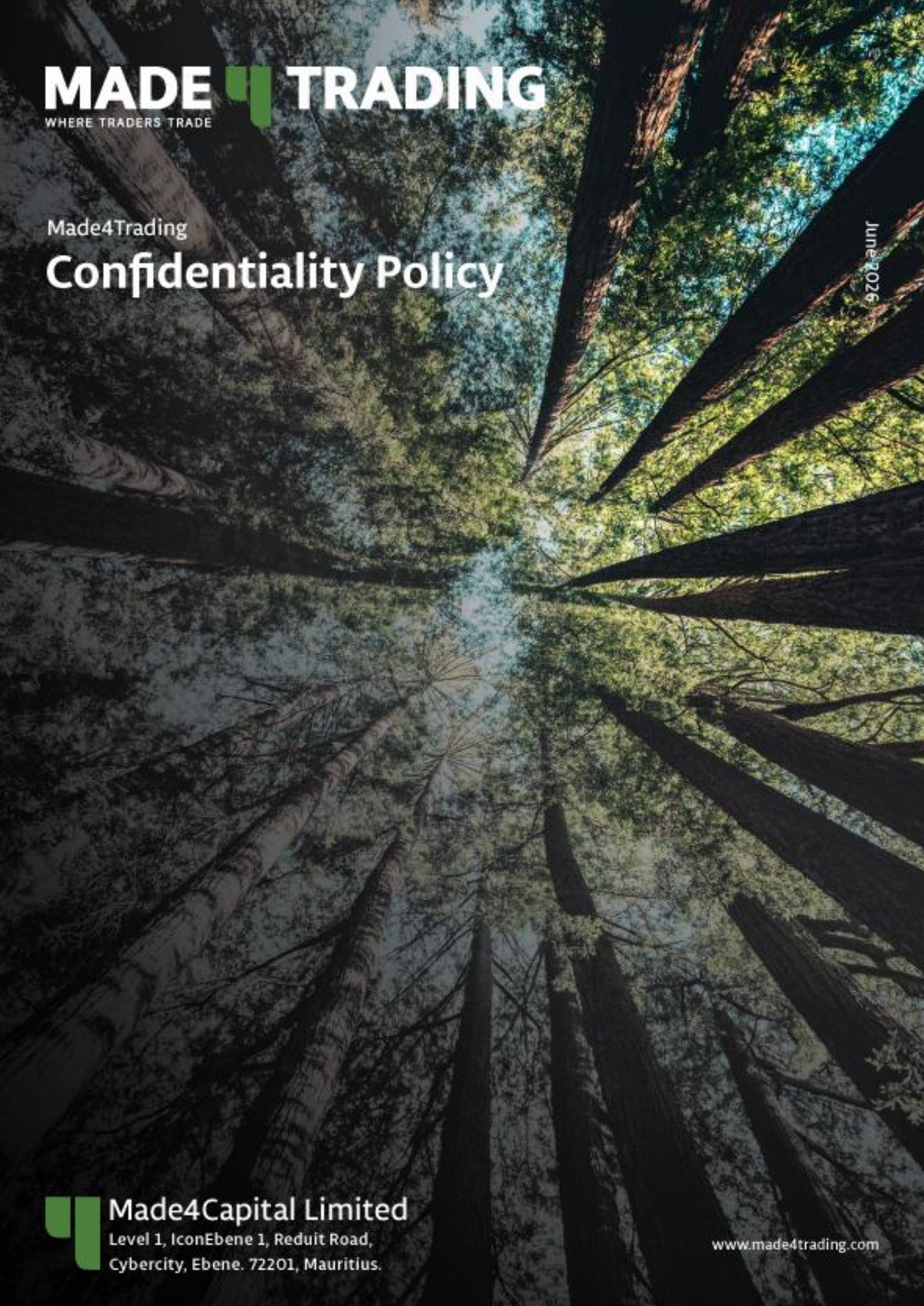
MADE TRADING
WHERE TRADERS TRADE

Made4Trading

Confidentiality Policy

June 2026



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

www.made4trading.com

Definitions

"The Company" refers to Made4Capital Limited.
"FSA 2007" means the Financial Services Act 2007, as amended from time to time.
"FSC" means the Financial Services Commission in Mauritius.
"FIU" means the Financial Intelligence Unit in Mauritius
"Non-public consumer data" means the data provided by the financial consumer to the Company, which shall not be made available to the public at large.

1. Overview

Made4Capital Limited, trading as “Made4Trading” (hereafter the “Company”, the “Firm”, “we”, “us” or “our”) is a financial services Company duly incorporated and registered under the laws of the Republic of Mauritius bearing company number 234336GBC, authorized and regulated by the Financial Services Commission of Mauritius (FSC) with licence number GB26205996. Our registered office is Level 1, IconEbene 1, Reduit Road, Cybercity, Ebene 72201, Mauritius.

2. Regulatory Framework and Purpose of This Policy

The Company’s confidentiality Policy adheres to Mauritian legislation such as the **Banking Act 2004** and the **FSA 2007.**

As employees carry out their responsibilities, they may encounter personal and private information pertaining to clients, partners, and our company. It is of paramount importance that Made4Capital takes the necessary measures to ensure the robust protection of this information.

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

- Certain information may be subject to legal obligations, such as sensitive customer data that must be handled in accordance with relevant regulations.
- 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 consumer data. Consumer data shall only be utilized 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 financial regulator if and when requested for, given the power of the FSC to request information and conduct inspections, as stated under section 42 and 43 of the FSA 2007, respectively.

3. Non-Public Data Collected and Processed

This policy is formulated to comply with the strict confidentiality obligations under **Section 64 of the Banking Act 2004** and **Section 83 of the Financial Services Act 2007**. As an FSC-regulated broker, Made4Capital is bound by these laws to protect all non-public consumer data and information relating to the affairs of its customers.

- A list of non-public data collected and processed by the Company includes but are not limited to:
- Personal information such as: Name, surname, residential address, e-mail address, phone number, date of birth, gender, citizenship, occupation and employment details;
- Information for the construction of client’s economic profile, including source of income and wealth, details about source of funds;
- Information on whether a client holds a prominent public function (PEPs);
- Bank Account and/or Credit card details;
- Documents provided to the Company for verification of the client’s identity i.e. passport/identity card, Company incorporation details as applicable, utility bills and other identifiable documents for verification purposes. Other documents such as

business plans, intellectual property, customer lists, financial records, software, marketing strategies, and any information that, if disclosed, could pose harm to our organization.

4. Sensitive Data Collected and/or Processed

The Company considers the following personal data to be 'sensitive':

- personal data revealing racial, gender or ethnic origin, political opinions, religious or philosophical beliefs;
- trade-union membership;
- genetic data, biometric data processed solely to identify a human being;
- health-related data.

The Company does not collect and/or process any sensitive data from clients or potential clients during the provision of the services.

5. Purpose of Collecting and Using Non-Public Consumer Data

The non-public consumer data collected by the Company is utilized 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 and acceptance procedures.
Furthermore, the Company operates under the laws of **Mauritius** and is subject to several regulations, including anti-money laundering and counter-terrorism financing laws. The Company is supervised by competent authorities, primarily the **FSC**, and must comply with the **Banking Act 2004**, the **FSA 2007**, and the **FIAMLA 2002**. 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 and Fraud Prevention

At the start of the business relationship, the Company requires non-public consumer data, such as full name, address, and telephone number, to authenticate and verify the identity of the client. Establishing the true identity of a client is a mandatory requirement under Mauritian law and is crucial for identifying, assessing, mitigating, and investigating potentially fraudulent activities or financial crimes.

5.2 Assessment of Appropriateness and Account Management

Throughout the business relationship, the Company collects data regarding a client's risk aversion, 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 interests, and perform statistical analyses to improve service quality.

5.3 Termination of Relationship and Record Retention

Non-public consumer 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 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, magnetic, or electronic formats as permitted by the regulator.

6. Security Practices for Safeguarding Non-Public Consumer Data

The Company implements the required procedures for safeguarding the security, integrity, and confidentiality of information, considering the nature of the information to be stored.

Agents or third parties that assist the Company to provide its services to clients shall maintain the confidentiality of non-public consumer 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.
The security of non-public consumer data is of utmost importance for the Company. For this reason, the Company implements several procedures on the accessibility and protection of data.

Specifically, non-public consumer data is only accessible by employees who need the specific information to operate, develop or improve the Company's services. Such individuals are bound by confidentiality and are subject to internal disciplinary procedures, as well as legal consequences as per The Banking Act and The FSA, in case they fail to meet their obligations.

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

a) Differentiation of the access rights according to the level of each employee
b) Protect systems by defining access privileges, control structures and resources
c) Responsibility measures for the illegal rendering of the information to the employees of the Company and by individuals outside the Company.
d) Encryption of sensitive information

Further to the above, the employees and management of the Company have the following responsibilities.

6.1 Employee's Responsibilities:

a) Employees must understand and comply with this policy and any additional confidentiality agreements they have signed.
b) Employees must protect and maintain the confidentiality of all information entrusted to them during and after their employment.
c) Employees should not disclose confidential information to unauthorized individuals unless required by law or with proper authorization.
d) Employees must take appropriate security measures to prevent unauthorized access to confidential information, such as using strong passwords and secure storage methods.
e) Employees should report any suspected breaches or unauthorized disclosure of confidential information to the appropriate authority.

6.2 Management Responsibilities:

a) Management must ensure that employees are fully informed about this policy and receive comprehensive training and guidance on its implementation.

b) Management should regularly review and update access controls and security measures to safeguard confidential information from unauthorized access or disclosure.
c) Management must promptly investigate and take appropriate action in response to any reported breaches or unauthorized disclosures of confidential information.

7. Storage of Non-Public Consumer Data

The Company undertakes all reasonable and appropriate organisational, physical and technical measures for the protection of non-public consumer data against unlawful access, destruction, misuse or accidental loss.

Non-public consumer data are being stored on the various databases of the Company, on its CRM platform.

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

- **Automatic Save** (Systems performs automatic save of critical data of the server). The backup data will be saved on the second hard disc within the server as well as on a hard disc of a separate hard disc. This method is used for quick recovery of the data in case of loss of the server only.
- **On cloud and or USB** etc. daily. This method is primarily used for the creation of back up files for reference. The said items, when physically saved, will be kept in a fireproof safe not located on the same premises as the rest of the computer hardware.

The IT Function is responsible for the creation of the backup files and the change of the Back-up hard disks. The software which backs up the data issues a report, which needs to be checked by the Head of the IT Function. The hard disks, which are numerous in number and on several servers, are checked daily.

In case of information loss that cannot be retrieved from the USB/Cloud back up data of the previous day, the representative officer shall retrieve any available information from the Company's CRM system.

The Company keeps client's non-public consumer data on record for a period of at least seven (7) years from the date of the last transaction of the client with the Company. In case there is an investigation against any customers the documents will be kept according to the instructions of the investigating authority.

The Company will be able to retrieve the relevant documents/data without undue delay and present them at any time to the local authorities if requested.

8. Disclosure of Non-Public Consumer Data

The Company may disclose non-public consumer data to a third party in the following circumstances:

a) If the financial customer has been informed about the disclosure and he/she has consented in writing to the disclosure.
b) If the third party to which the data will be disclosed has been authorized by the financial consumer to obtain the data from the Company.

c) If the Company is required to disclose the non-public consumer data to the Credit Information Bureau, The 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 Made4Capital to disclose only the minimum amount of information required, avoiding unnecessary or excessive disclosures, unless required by Law.

9. Client Consent

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

The Company may obtain the consumer's consent electronically in the form of a general agreement through the acceptance of the client services agreement and/or consider clients who have received and agreed to this policy electronically as clients who have given their consent to the disclosure of their non-public consumer data.

10. Amendments to Policy

The Company reserves the right to make changes to this Confidentiality Policy from time to time for any reason and the client will be notified of such changes by posting an updated version of this Confidentiality Policy on the website. The client is responsible for regularly reviewing this Policy from company's website after any such changes are published, shall constitute an agreement to such changes.

11. How to Contact Us

The Consumer can extend any questions or requests he/she might have in relation to his/her data stored by the Company by sending an email at Compliance@made4trading.com.