PRIVACY POLICY & INTERNAL PRIVACY CONTROLS

Base Markets

An Investment Dealer (Full-Service Dealer Excluding Underwriting) and Global Business Company Licensed by the Financial Services Commission

License No: GB25204723
Company No: 223521 /GBC
Date: October 2025
Version: 1.0

DOCUMENT HISTORY			
VERSION	DATE OF CHANGES	COMMENTS	DATE OF BOARD APPROVAL
1.0	15 SEP 25	First Manual – Licensing Phase	14 OCT 25

Table of Contents

1. Foreword

Base Markets (the "Company") is incorporated in Mauritius on the 4th of July 2025 as a private company limited by shares. The Company is regulated by the Financial Services Commission (FSC) of Mauritius under the Financial Services Act 2007 and is licensed as an Investment Dealer (Full Service, excluding Underwriting) with the License Number GB25204723 and a Global Business Licensee, with the Company Number 223521.

The Company has its principal place of effective management in Mauritius, which proposes to conduct its business principally outside Mauritius. The registered office address of the Company is at C/O Credentia International Management Ltd, The Cyberati Lounge, Ground Floor, The Catalyst, Silicon Avenue, 40 Cybercity, 72201 Ebène, Republic of Mauritius.

The Company shall perform such activities and duties as are customarily authorised and performed by the holder of an Investment Dealer (Full-Service Dealer excluding Underwriting) Licence under the Securities Act 2005, in particular, carrying out the following activities:

- Act or hold itself as an intermediary in the execution of securities transactions for clients;
- Trade or hold itself to trade in securities as principal with the intention of reselling these securities to the public;
- Distribute or hold itself out to distribute securities on behalf of an issuer or holder of securities;
- Solicit any investor (person or institutional or body corporate) to enter into securities transactions;
- Give investment advice which is ancillary to the normal course its business activities;
- Manage portfolios of clients.

This Privacy Policy sets out how the Company collects, uses, stores, and protects personal data in accordance with the Mauritius Data Protection Act 2017 and applicable international standards. The Policy applies to all directors, officers, employees, contractors, consultants, and third parties who have access to Company systems or client information.

The purpose of this Policy is to:

- Ensure lawful, fair, and transparent processing of personal data.
- Protect client and employee information against unauthorised access, loss, or misuse.
- Define roles and responsibilities for data protection within the Company.
- Explain the rights of clients and how these can be exercised.

2. Data Protection Principles and Responsibilities

The Company adheres to the principles of the Mauritius Data Protection Act 2017, ensuring that personal data is:

- Processed lawfully, fairly, and transparently.
- Collected for specified and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Limited to what is necessary for the stated purpose ("data minimisation").
- Accurate and kept up to date.
- Stored only for as long as necessary, after which it is securely deleted or destroyed.
- Protected by appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss, destruction, or damage.

Responsibilities:

- **Board of Directors** – Holds ultimate accountability for compliance with data protection laws and approves this Policy.
- **Compliance Officer / Data Protection Officer** – Oversees implementation of the Policy, monitors compliance, advises management and employees, and acts as the primary contact for data subjects and regulators.
- **Employees and Contractors** – Must comply with this Policy and related procedures, ensure data is handled responsibly, and immediately report any suspected breaches or misuse.

3. Collection, Use, and Retention of Data

The Company collects and processes personal data strictly for lawful and legitimate business purposes, in line with the Mauritius Data Protection Act 2017. Personal data may include client identification documents, contact details, financial information, transactional records, and employee HR data.

Purposes of Processing

Personal data is collected and used for:

- Meeting legal and regulatory obligations, including Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements.
- Managing client relationships, including account opening, execution of transactions, and communication.
- Fulfilling contractual obligations with clients, employees, and service providers.
- Monitoring, detecting, and preventing fraud or suspicious activities.
- Internal business operations such as HR management, payroll, performance reviews, and training.
- Marketing and client engagement, where explicit consent has been obtained.

Lawful Basis of Processing

Data is processed on the basis of:

- Legal or regulatory obligation.
- Performance of a contract.
- Legitimate business interest, balanced against the rights of data subjects.
- Consent, where required (e.g., for marketing communications).

Data Retention and Disposal

The Company retains personal data only for as long as necessary to fulfil the purpose for which it was collected and to meet legal or regulatory obligations. Retention schedules are defined in internal procedures, with specific periods set for client, transaction, and employee records.

Once data is no longer required, it must be securely destroyed or deleted using approved methods to prevent unauthorised recovery. Paper records are shredded or incinerated, while electronic data is erased using secure deletion tools.

Accuracy and Updating

Employees and clients are responsible for ensuring that their personal data held by the Company remains accurate and up to date. The Company will take reasonable steps to update or correct data where inaccuracies are identified.

Children's Data / Age Restriction

The Company's services are intended only for individuals aged 18 and above, or the age of legal capacity in their jurisdiction. The Company implements age verification during onboarding to prevent the collection of data from minors. Where false information is identified, the account will be suspended, and any associated data will be securely deleted. The Company does not knowingly collect or process personal data of minors. If such data is inadvertently collected, it will be deleted as soon as practicable.

Automated Decision-Making / Profiling

Certain processes, such as KYC verification, transaction monitoring, or fraud detection, may involve automated decision-making or profiling. These measures are designed to comply with legal obligations and to protect the Company and its clients against financial crime. Data subjects have the right to request human intervention, to express their point of view, and to contest automated decisions that have legal or significant effects. Where personal data is used for marketing-related profiling, individuals have the right to object and to opt out of such processing at any time.

4. Internal Privacy Controls

The Company maintains internal controls to ensure that personal data is handled securely and in compliance with applicable laws and policies. These controls apply to all employees, contractors, and third parties with access to Company systems.

Access Restrictions

- Access to personal data is strictly limited to individuals with a legitimate business need.
- Privileged accounts and administrative rights are restricted to authorised IT personnel.
- Access rights are reviewed regularly, and accounts are revoked immediately upon termination of employment or contract.

Data Handling Procedures

- Data classified as Confidential or Restricted must only be accessed, stored, and transmitted on approved systems.
- Personal data may not be transferred to removable media, personal devices, or unauthorised cloud storage.
- Physical files containing personal information must be kept in secure cabinets with controlled access.

Technical Safeguards

- Encryption is applied to sensitive data both in transit and at rest.
- Systems are protected by firewalls, endpoint protection, intrusion detection, and monitoring tools.
- Logs of access to personal data are maintained and monitored for unusual activity.

Monitoring and Oversight

- The Compliance Officer (acting as Data Protection Officer) conducts periodic reviews of data protection practices.
- Internal audits and spot checks are performed to verify adherence to privacy requirements.
- Findings from reviews are reported to senior management and corrective measures implemented promptly.

Employee Responsibilities

- Employees must complete mandatory privacy and data protection training.
- Any suspected misuse, loss, or unauthorised disclosure of personal data must be reported immediately to the Compliance Officer.
- Breaches of internal privacy controls may result in disciplinary action, including termination of employment or contract.
- All employees must complete privacy and data protection training at least annually, with additional refresher sessions provided as required.

5. Cookies and Online Tracking

This Policy also applies to personal data collected from website visitors, including through cookies, online forms, and analytics tools. Such data is processed in accordance with this Policy and applicable laws, and visitors have the same rights described herein.

The Company's website uses cookies and similar technologies to enhance functionality, improve user experience, and collect information about how visitors interact with the site. Cookies may include:

- **Essential cookies** – required for core website functions such as secure login and navigation.
- **Analytics cookies** – used to gather anonymous statistics on website usage to improve services.
- **Marketing cookies** – used, with consent, to deliver relevant advertising and measure campaign effectiveness.

Visitors are notified of the use of cookies when they access the Company's website. Consent is obtained for non-essential cookies, and visitors may withdraw or modify their consent at any time through browser settings or cookie management tools.

6. Customer Rights, Consent and Policy Updates

By accessing the Company's website, using its services, or otherwise providing personal data, clients and users consent to the collection, use, and processing of their information as set out in this Privacy Policy, subject to their rights under the Data Protection Act 2017.

In accordance with the Data Protection Act 2017, individuals whose personal data is processed by the Company ("data subjects") are entitled to specific rights. These rights ensure that personal information is handled fairly, transparently, and with due respect to individual privacy.

Consent must be explicit where required by law, for example by ticking a box, signing an agreement, or affirmatively selecting a preference. Silence, inactivity, or continued use of services without such confirmation does not constitute consent.

The Company may share personal data with third parties only where it is lawful, necessary, and consistent with the purposes for which the data was collected.

Right of Access

Data subjects may request confirmation of whether the Company holds their personal data, and if so, receive a copy along with information about how it is being processed.

Right to Rectification

If personal data is inaccurate or incomplete, data subjects have the right to request correction or completion.

Right to Erasure ("Right to be Forgotten")

Individuals may request the deletion of their personal data where there is no legal or regulatory obligation for the Company to retain it.

Right to Restrict Processing

In certain circumstances, data subjects may request that the Company limit the use of their personal data, for example, while accuracy is being verified or in the context of a legal claim.

Right to Object

Data subjects may object to the processing of their data for specific purposes, including direct marketing.

Right to Data Portability

Where applicable, individuals may request a copy of their personal data in a structured, commonly used, and machine-readable format, and may request that it be transmitted directly to another data controller.

Exercising Rights

Requests relating to data subject rights must be submitted in writing to the Compliance Officer (acting as Data Protection Officer). The Company will respond within the timelines prescribed under the Data Protection Act 2017. Identification may be required to verify the requester's identity before actioning any request. The Company will respond to rights requests within 30 days of receipt, extendable by an additional 30 days where necessary due to complexity or volume, in accordance with the Data Protection Act 2017.

Marketing Communications

The Company will only send direct marketing communications (including email, SMS, or calls) where explicit consent has been provided. Clients and users may withdraw consent or opt out of marketing at any time by following the unsubscribe instructions in communications or by contacting the

Company directly. Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal.

Third-Party Service Providers

Personal data may be shared with service providers engaged by the Company to deliver services such as IT support, payment processing, KYC/AML verification, cloud hosting, and audit. These providers are contractually required to implement appropriate security measures, comply with applicable laws, and process data only on the Company's instructions.

Regulatory and Legal Obligations

The Company may disclose personal data to regulators, law enforcement agencies, courts, or other authorities where legally required, including under the Financial Services Act 2007, the Data Protection Act 2017, and applicable anti-money laundering legislation.

Group Companies and Affiliates

Where relevant, personal data may be shared within the Company's group entities to ensure efficient operations, compliance with group policies, or delivery of cross-border services. Such sharing is subject to equivalent data protection safeguards.

International Transfers

Where personal data is transferred outside Mauritius, the Company ensures that:

- The destination country offers adequate levels of protection; or
- Appropriate safeguards, such as contractual clauses, are in place; and
- Data subjects are informed of the transfer where required by law.

Where required, international transfers will rely on Standard Contractual Clauses (SCCs) or equivalent legal mechanisms to ensure adequate protection.

Prohibited Sharing

The Company does not sell, lease, or otherwise trade customer data to third parties for marketing or commercial gain.

Updates to the Policy

The Company may update this Privacy Policy from time to time to reflect changes in legal or regulatory requirements, business practices, or technology. The most current version will always be available on the Company's website.

Where changes are material, the Company will take reasonable steps to inform clients in advance through direct communication or prominent notices. Continued use of the Company's services after such notification will constitute acceptance of the revised Policy.

7. Data Sharing and Breach Management

The Company implements technical and organisational measures to safeguard personal data against loss, misuse, unauthorised access, disclosure, alteration, or destruction. These measures are proportionate to the sensitivity of the data and the risks posed by processing activities.

Data Security Measures

- Encryption of sensitive data both in transit and at rest, using industry-standard algorithms.
- Strong access controls, including Multi-Factor Authentication (MFA) for critical systems.
- Firewalls, intrusion detection/prevention systems, and endpoint protection tools.
- Regular patching, vulnerability scans, and penetration testing.
- Secure backup and disaster recovery arrangements.
- Ongoing employee training on data protection and cybersecurity awareness.

Breach Notification

A personal data breach is any incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Where a breach occurs:

- The IT Department and Compliance Officer will immediately investigate and assess the scope and impact.
- Material breaches will be reported without undue delay to the Data Protection Office and other relevant regulators, in line with statutory requirements.
- Affected individuals will be notified promptly if the breach is likely to result in significant risk to their rights or freedoms. Notifications will explain the nature of the breach, its likely consequences, and measures taken to mitigate harm.
- All breaches, regardless of severity, will be documented in the Company's internal incident log.

Continuous Improvement

Lessons learned from breaches or near misses will be incorporated into revised controls, updated training, and improvements to systems and processes.

8. Queries and Complaints

Individuals who have questions about this Privacy Policy, the Company's handling of personal data, or who wish to exercise their rights under the Data Protection Act 2017, may contact the Compliance Officer (acting as Data Protection Officer).

All queries or complaints should be submitted in writing to:

Compliance Officer / Data Protection Officer

Email: compliance@basemarkets.com

Telephone: +230 467 2000
Address: C/O Credentia International Management Ltd, The Cyberati Lounge, Ground Floor, The Catalyst, Silicon Avenue, 40 Cybercity, 72201 Ebène, Republic of Mauritius.

The Company will acknowledge all queries and complaints within **5 business days** and provide a substantive response within the statutory timelines prescribed under the Data Protection Act 2017. Where necessary, additional information may be requested to verify the identity of the data subject or to clarify the scope of the request.

If a data subject is not satisfied with the Company's response, they have the right to escalate the matter to the **Data Protection Office of Mauritius**. Contact details for the regulator can be found at: https://dataprotection.govmu.org.

The Company is committed to handling all privacy-related concerns promptly, fairly, and transparently, and to cooperating fully with the Data Protection Office where complaints are raised.