### EFG Holding's Commitment to Data Protection

EFG Holding and its subsidiaries ("the Group") are steadfastly committed to upholding the highest standards of data protection and privacy. The safeguarding of personal data is considered an integral component of our corporate responsibility to our clients, employees, and partners. To this end, the Group has instituted a comprehensive governance framework to ensure all personal data is processed with accountability and transparency, in full compliance with the General Data Protection Regulation (GDPR) and all applicable local laws within our operating jurisdictions.

### 1. Governance and Oversight Framework

A clearly defined organizational structure has been established to ensure robust and effective supervision of all data processing activities. Responsibilities are delegated as follows:

* **Board of Directors:** Assumes ultimate responsibility for the strategic oversight of the data protection framework, including resource allocation and the approval of Group-wide policies. The Board also monitors the organization's ongoing compliance with all applicable regulations.
* **Audit Committee:** Is mandated to review periodic compliance reports, assess the effectiveness of the Group's data protection risk management framework, monitor the implementation of corrective actions, and ensure the independent validation of internal controls.
* **Group Chief Legal & Compliance Officer:** Is charged with the implementation of the data protection framework across the Group, ensuring its alignment with regulatory requirements, reporting to the Board of Directors and Audit Committee, and managing the escalation of material incidents and breaches.
* **Data Protection Function:** This function, comprising a Data Protection Manager and Specialist, is responsible for the operational execution of the framework. Its duties include updating internal policies, preparing regular reports, identifying compliance vulnerabilities, developing remediation plans, and fostering a culture of data protection awareness through corporate training programs.

### 2. Core Data Protection Principles

All data processing activities undertaken by the Group are governed by the seven fundamental principles as stipulated in the GDPR, which ensure that personal information is handled ethically and responsibly:

* **Lawfulness, Fairness, and Transparency:** Processing data in a lawful, fair, and transparent manner.
* **Purpose Limitation:** Collecting data for specified explicit, and legitimate purposes only.
* **Data Minimization:** Ensuring that personal data collected is adequate, relevant, and limited to what is necessary.
* **Accuracy:** Maintaining the accuracy of personal data and ensuring it is kept up to date.
* **Storage Limitation:** Retaining personal data for no longer than is necessary for the intended purpose.
* **Integrity and Confidentiality:** Securing personal data against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
* **Accountability:** Demonstrating unwavering compliance with these principles.

### 3. Data Subject Rights and Data Management

The Group is fully committed to upholding the rights of individuals with respect to their personal data:

* **Lawful Basis for Processing:** Personal data is processed on various lawful bases, including contractual necessity and legal obligations (e.g., KYC/AML requirements), not solely upon consent. For non-essential processing activities, such as direct marketing, clear and accessible opt-out mechanisms are provided.
* **Data Subject Rights:** We guarantee the rights of individuals to access, rectify, erase, restrict processing of, and port their personal data, in addition to their right to object to processing.
* **Subject Access Requests:** The Group maintains a formal policy for managing Subject Access Requests, ensuring individuals can inquire about and receive copies of their data within the statutory timeframes.

### 4. Risk Management and Compliance Assurance

To ensure the highest level of security and compliance, the Group adheres to the following protocols:

* **Data Breach Management:** The Group has established robust procedures for the immediate containment and management of any data breach, including severity assessment, notification to regulatory authorities where required, and the implementation of corrective measures.
* **Cross-Border Data Transfers:** Personal data shall not be transferred outside of our jurisdictions unless the recipient country ensures an adequate level of data protection or appropriate contractual safeguards are in place, subject to necessary approvals.
* **Third-Party Data Processors:** When engaging third-party vendors to process personal data, we ensure that legally binding contracts are executed to enforce strict data protection obligations in line with regulatory standards.
* **Auditing and Assessment:** The Group relies on its internal Legal, Compliance, and Internal Audit functions, supplemented by independent external counsel where appropriate (e.g., Nigeria), to continuously review, test, and enhance the effectiveness of our data protection program.