PRIVACY AND DATA PROTECTION STATEMENT

This **Privacy and Data Protection Statement** *(hereinafter referred to as the "Agreement")* sets forth the guiding principles and legal framework through which FINAUREX *("Company," "we," "our," or "us")* processes, stores, discloses, and protects personal data collected from clients, users, or visitors (collectively referred to as "you" or "your") through its website, mobile applications, and affiliated digital interfaces *(collectively referred to as the "Site").*

CHAPTER I – COLLECTION AND PROCESSING OF PERSONAL DATA

I.I In the context of account registration and the provision of regulated services, we shall lawfully request and collect personal identifiers, including but not limited to: full name, email address, telephone number, date of birth, nationality, domicile, government-issued identification credentials, financial status, and income source. Such data is collected to assess service eligibility and risk parameters.

I.II To fulfil our obligations under Know Your Customer *(KYC)* and Anti-Money Laundering *(AML)* statutes, the Company shall request documentation that may include identification cards, utility bills, bank records, and other verification instruments. This data shall also serve to ensure lawful communication, detect risk exposure, and mitigate fraudulent conduct.

I.III By engaging with the Site, you implicitly authorize the Company to collect technical information including but not limited to: IP addresses, geolocation data, device specifications, browser details, and behavioral usage data. This information facilitates optimization of the digital platform and supports regulatory compliance.

CHAPTER II – SECURITY SAFEGUARDS AND RETENTION FRAMEWORK

II.I The Company employs rigorous information security protocols, including but not limited to: cryptographic encryption standards, secure socket layer *(SSL)* technologies, and real-time threat monitoring systems. All electronic transmissions and data exchanges are secured against unauthorized interception.

II.II As an added layer of user authentication, we implement two-factor authentication (2FA). This mechanism requires a secondary verification token, transmitted via secured channels, in addition to your primary login credentials.

II.III All data is retained strictly for the duration necessary to fulfill the lawful purposes for which it was collected, or as otherwise mandated by regulatory or legal obligations. Upon expiration of such period, personal data shall be securely erased or anonymized in accordance with industry best practices.

II.IV Should you require restoration of access due to account inaccessibility, our account recovery procedures mandate identity re-verification prior to the reinstatement of account privileges. This ensures continued protection against identity fraud.

CHAPTER III – DATA USE, TRANSFER, AND DISCLOSURE

III.I Personal data collected shall be used exclusively for operational purposes including service delivery, client management, fraud detection, compliance enforcement, and the resolution of legal disputes.

III.II Subject to contractual safeguards, the Company may share your personal information with service providers, affiliates, or agents engaged to perform functions on our behalf. Any such disclosure shall remain consistent with applicable data protection laws.

III.III We may be compelled by statute or judicial process to disclose personal data to public authorities or law enforcement agencies. Such disclosures shall occur only to the extent required by law and will be duly documented.

III.IV Requests made by one client regarding information on another shall be denied unless supported by valid legal justification, presented in writing, and compliant with relevant data protection frameworks. The Company retains the sole discretion to decline such requests.

III.V By accessing our services, you acknowledge that your personal data may be stored or transmitted across international jurisdictions. The Company shall ensure such transfers are conducted under binding legal mechanisms ensuring adequate levels of data protection.

CHAPTER IV – RIGHTS, CONSENT, AND NOTICES

IV.I You retain the right to request the deletion of your personal data. The Company shall comply with such requests except where retention is necessary for compliance with legal obligations, dispute resolution, or fraud prevention.

IV.II The Company may issue periodic marketing communications, promotional offers, or updates related to its services. You reserve the right to opt out from receiving such communications at any time, without affecting your relationship with the Company.

IV.III You agree to indemnify and hold harmless the Company and its officers from any third-party claims arising from your breach of this Agreement or applicable data protection laws.

IV.IV Failure by the Company to enforce any provision of this Agreement shall not be construed as a waiver of any of its rights under applicable law. No waiver shall be deemed effective unless formally executed in writing by an

authorized representative.

IV.V This Agreement may be revised from time to time. All material amendments shall be published on the Site and shall take effect upon such publication. Your continued use of the Site shall constitute acceptance of the revised Statement.

CHAPTER V – MISCELLANEOUS PROVISIONS

V.I You acknowledge that links to third-party platforms provided on the Site are for convenience only. The Company does not endorse or assume responsibility for the privacy practices of such third parties.

V.II To ensure transparency and ongoing compliance, the Company shall periodically audit its data protection mechanisms. This includes system monitoring, breach reporting, and internal policy review.

V.III For inquiries, complaints, or data-related requests, you may contact the Company through the designated communication channels published on the Site. All correspondence must originate from your registered email address.