

FINORA GLOBAL, Inc., (Finora Exchange)

PRIVACY POLICY

1. Introduction and Scope

FINORA GLOBAL, Inc. ("FINORA GLOBAL," "the Company," "we," or "us") recognizes the fundamental right to privacy and is committed to the protection of personal data in accordance with Republic Act No. 10173, otherwise known as the *Data Privacy Act of 2012*, its Implementing Rules and Regulations, National Privacy Commission ("NPC") issuances, and other applicable laws and regulations of the Republic of the Philippines.

This Privacy Policy governs the collection, processing, storage, retention, disclosure, and protection of personal data of all data subjects, including but not limited to customers, prospective customers, business partners, counterparties, employees, contractors, and website users, whose personal data is processed by the Company in the course of its operations.

2. Definitions

Unless otherwise stated, terms used in this Policy shall have the meanings assigned to them under the Data Privacy Act of 2012 and its Implementing Rules and Regulations.

3. Legal Basis for Processing

The Company processes personal data strictly on lawful grounds, including:

- Compliance with legal and regulatory obligations, including AML/CTPF, licensing, reporting, and recordkeeping requirements;
- Performance of a contract or steps necessary prior to entering into a contract with the data subject;
- Legitimate interests pursued by the Company, provided such interests are not overridden by the fundamental rights and freedoms of the data subject;
- Consent of the data subject, where expressly required by applicable law.

4. Categories of Personal Data Processed

The Company may collect and process personal data including, but not limited to:

- **Personal identifiers:** full legal name, date and place of birth, nationality, government-issued identification details;
- **Contact information:** residential and mailing address, email address, telephone and mobile numbers;

- **Financial and transactional information:** account records, transaction history, wallet addresses, payment details;
- **Compliance and risk data:** KYC/KYB documentation, risk profiles, sanctions and watchlist screening results;
- **Technical and usage data:** IP addresses, device identifiers, access logs, security logs, and system activity records.

5. Purposes of Processing

Personal data is processed for legitimate and specified purposes, including:

- Customer onboarding, identification, and verification;
- Compliance with AML/CTPF laws, sanctions requirements, and regulatory directives;
- Provision, operation, and maintenance of the Company's digital asset exchange services;
- Risk management, fraud detection, transaction monitoring, and security assurance;
- Regulatory reporting, audits, examinations, and lawful disclosures;
- Internal governance, compliance monitoring, and recordkeeping.

6. Data Sharing and Disclosure

The Company may disclose personal data, strictly on a need-to-know basis, to:

- Government authorities, regulators, or law enforcement agencies as required by law or lawful order;
- Third-party service providers engaged for compliance, identity verification, technology, cybersecurity, or operational support, subject to appropriate contractual safeguards;
- Professional advisers, auditors, and consultants bound by confidentiality obligations.

The Company does not sell or commercially exploit personal data.

7. Cross-Border Data Transfers

Where personal data is transferred or accessed outside the Philippines, the Company ensures that:

- Such transfer is lawful, necessary, and proportionate;
- Appropriate organizational, contractual, and technical safeguards are in place;
- The recipient jurisdiction affords a level of data protection comparable to Philippine standards.

8. Data Retention and Disposal

Personal data shall be retained only for as long as necessary to fulfill the purposes for which it was collected or as required by applicable laws and regulations, including AML/CTPF record

retention requirements. Upon expiration of the applicable retention period, personal data shall be securely disposed of or anonymized.

9. Data Security Measures

The Company implements reasonable and appropriate administrative, technical, and physical security measures to protect personal data against unauthorized access, disclosure, alteration, loss, or destruction. These measures include access controls, encryption, monitoring, logging, and incident response protocols.

10. Personal Data Breach Management

Personal data breaches are handled in accordance with NPC Circular No. 16-03 and the Company's internal incident response procedures. Where required, the Company shall notify the National Privacy Commission and affected data subjects within the prescribed timeframes.

11. Rights of Data Subjects

Data subjects are entitled to rights under the Data Privacy Act, including the right to be informed, access, correction, objection, erasure or blocking, data portability, and the right to lodge a complaint with the National Privacy Commission, subject to applicable legal limitations.

12. Amendments

This Privacy Policy may be amended from time to time to reflect changes in laws, regulations, or Company operations. Updated versions shall take effect upon publication through official Company channels.

13. Contact Information

For privacy-related inquiries or requests, data subjects may contact:

[Compliance Officer]

[compliance@finora.exchange]

Eugene Choi

