

FINARIUM

01000110 01001001 01001110

PRIVACY POLICY

VER. 1.0

Document Information

Document Property	Document Details
Document Title:	Privacy Policy
Document file name:	FINARIUM S.A. Privacy Policy VER. 1.0
Revision Number:	Version 1.0
Issued by:	FINARIUM S.A.
Issue date:	25/08/2026
Status:	Final

Document Revision History

Version	Date	Author	Description of change
1.0	25/08/2026	Board of Directors / Privacy Officer	First issued version

TABLE OF CONTENTS

1. Introduction	5
2. Purpose and Scope	5
3. About FINARIUM	5
4. Applicable Data Protection Framework	6
5. Definitions	6
6. Data Protection Principles	6
7. Categories of Personal Data Processed	7
7.1 Identification and Verification Information	7
7.2 Contact and Address Information	7
7.3 Corporate and Beneficial Ownership Information	7
7.4 Financial and Transaction Information	8
7.5 Source of Funds, Source of Wealth and Source of Virtual Assets	8
7.6 Compliance and Risk Information	8
7.7 Technical and Security Information	9
7.8 Correspondence and Relationship Information	9
8. How Personal Data Is Collected	9
9. Purposes for Processing Personal Data	9
10. Legal Grounds for Processing	10
10.1 Consent	10
10.2 Contractual Relationship	10
10.3 Compliance with Law	10
10.4 Legitimate Interests	11
10.5 Public Interest, Legal Authority and Judicial Requirements	11
10.6 Vital Interests	11
11. KYC, AML/CFT, Sanctions and Financial-Crime Processing	11
12. Sensitive Personal Data	12
13. Disclosure of Personal Data	12
14. Service Providers and Data Processors	12
15. International Transfers of Personal Data	13
16. Data Security	13
17. Data Retention	14
18. Rights of Data Subjects	14
18.1 Right of Access	14
18.2 Right of Rectification	14
18.3 Right of Cancellation	14
18.4 Right of Opposition	14

FINARIUM

01000110 01001001 01001110

Global Bank Tower, 18th Floor, Suite No. 1801, 50th Street, Panama City, Republic of Panama

18.5 Right of Portability	14
19. Exercising Data-Subject Rights	14
20. Automated Processing, Risk Scoring and Profiling	15
21. Confidentiality	15
22. Personal Data Breaches and Security Incidents	16
23. Regulatory, Judicial and Legal Disclosures	16
24. Accuracy of Personal Data	16
25. Changes to this Privacy Policy	16
26. Contact and Complaints	17
27. Governance and Responsibility	17
28. Effective Date and Approval	17

1. INTRODUCTION

FINARIUM S.A. ("**FINARIUM**", the "**Company**", "**we**", "**us**" or "**our**") respects the privacy of individuals whose Personal Data it processes and recognises the importance of handling such information lawfully, fairly, securely and transparently.

This Privacy Policy explains how FINARIUM collects, uses, stores, discloses, transfers, protects and otherwise processes Personal Data in connection with its business activities.

FINARIUM is incorporated in the Republic of Panama and has its registered office at Global Bank Tower, 18th Floor, Suite No. 1801, 50th Street, Panama City, Republic of Panama.

For the purposes of applicable Panamanian data-protection legislation, FINARIUM will act as the Responsible Party for the processing of Personal Data where it determines the purposes, means and scope of that processing.

2. PURPOSE AND SCOPE

This Privacy Policy applies to Personal Data processed by FINARIUM in connection with its business and operations, including information concerning, as applicable:

- customers and prospective customers;
- individuals acting on behalf of corporate customers;
- directors, shareholders, ultimate beneficial owners and authorised representatives of legal entities;
- counterparties and their representatives;
- users of FINARIUM's services;
- originators and beneficiaries of transactions;
- suppliers and service-provider representatives;
- directors, officers, employees, contractors and applicants;
- persons who communicate or otherwise interact with FINARIUM; and
- other natural persons whose Personal Data is legitimately processed in connection with the Company's activities.

This Privacy Policy applies regardless of whether Personal Data is obtained electronically, through documentation, through communication with the individual, from authorised third parties or through legitimate compliance and verification sources.

3. ABOUT FINARIUM

FINARIUM is a Panamanian company whose activities include virtual-asset-related services.

Depending upon the relevant product, transaction and customer relationship, its activities may involve:

- virtual asset exchange activities;
- virtual asset transfers;
- custodial and wallet-related activities;
- virtual asset safekeeping or administration;
- virtual-asset-to-virtual-asset transactions;
- fiat on-ramp and off-ramp activities;
- interaction with counterpart virtual asset service providers;
- blockchain-based transactions;
- related value-transfer services; and
- compliance, transaction-monitoring and financial-crime prevention activities supporting those services.

Because these activities may involve financial transactions, virtual assets and cross-border counterparties, FINARIUM undertakes customer identification, due diligence, transaction monitoring, sanctions screening, financial-crime risk assessment and other controls appropriate to its business.

4. APPLICABLE DATA PROTECTION FRAMEWORK

FINARIUM processes Personal Data principally in accordance with the laws of the Republic of Panama, including:

- Law No. 81 of 26 March 2019 on Personal Data Protection; and
- Executive Decree No. 285 of 28 May 2021, which regulates and develops Law No. 81 of 2019.

These rules establish the general principles, rights, obligations and procedures governing Personal Data protection in Panama.

The Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) is the competent authority responsible for supervision of the general Personal Data protection framework in Panama.

FINARIUM may also be required to comply with other Panamanian laws relating to corporate administration, anti-money laundering, counter-terrorist financing, proliferation financing, sanctions, crime prevention, record keeping, judicial processes, regulatory cooperation and other legal obligations insofar as those requirements lawfully require or permit the processing of Personal Data.

Where information is processed in connection with a cross-border activity, FINARIUM will also take account of mandatory legal requirements applicable to that particular activity, recipient or transaction where those requirements lawfully apply.

5. DEFINITIONS

Personal Data: means information concerning a natural person that identifies or makes that person identifiable.

Data Subject: means the natural person to whom Personal Data relates.

Processing: includes any operation or set of operations performed on Personal Data, including its collection, recording, organisation, storage, adaptation, consultation, use, transmission, disclosure, combination, restriction, deletion or destruction.

Sensitive Personal Data: means Personal Data relating to the intimate sphere of an individual whose misuse may give rise to discrimination or a serious risk to that individual, including categories recognised as sensitive under applicable Panamanian law.

Responsible Party: means the natural or legal person responsible for decisions concerning the processing of Personal Data and determining the purposes, means and scope of such processing.

Service Provider: means a person or entity engaged by FINARIUM to perform services involving Personal Data under appropriate instructions and safeguards.

6. DATA PROTECTION PRINCIPLES

FINARIUM processes Personal Data in accordance with the principles established under applicable Panamanian law.

Accordingly, Personal Data will be processed in a manner consistent with the principles of:

- lawfulness;
- fairness and loyalty;
- transparency;
- purpose limitation;
- proportionality;
- accuracy;
- confidentiality;
- security;
- responsibility; and
- respect for the rights of Data Subjects.

FINARIUM seeks to collect and process Personal Data that is appropriate, relevant and reasonably necessary for the legitimate purpose for which it is processed.

Personal Data must not knowingly be used for a materially incompatible purpose unless the additional processing is legally permitted and the applicable requirements have been satisfied.

7. CATEGORIES OF PERSONAL DATA PROCESSED

The categories of Personal Data processed by FINARIUM depend upon the nature of the relationship, service, transaction and applicable legal requirements.

7.1 Identification and Verification Information

FINARIUM may process:

- full legal name;
- date of birth;
- nationality;
- citizenship information;
- passport information;
- national identification information;
- copies or details of identification documents;
- photographs;
- signatures;
- identity-verification results;
- document-authentication information; and
- other information required to establish or verify identity.

Where identity-verification technology is used, verification may include document-security checks, machine-readable document information, identity matching, biometric comparison and liveness verification where appropriate.

7.2 Contact and Address Information

This may include:

- residential address;
- registered or business address;
- telephone number;
- email address; and
- other contact information provided to the Company.

7.3 Corporate and Beneficial Ownership Information

Where an individual is associated with a legal entity, FINARIUM may process information concerning:

- directors;
- officers;
- shareholders;
- ultimate beneficial owners;
- controllers;
- authorised signatories;
- trustees, partners or similar persons;
- ownership percentages;

- organisational relationships; and
- the individual's authority to represent or control an entity.

7.4 Financial and Transaction Information

Depending upon the service provided, FINARIUM may process:

- bank-account information;
- payment information;
- transaction history;
- transaction amount, currency and date;
- originator and beneficiary information;
- account or customer identifiers;
- virtual asset details;
- blockchain and transaction identifiers;
- wallet addresses;
- blockchain or network information;
- counterparty information;
- transaction timestamps; and
- information concerning the economic purpose of a transaction.

7.5 Source of Funds, Source of Wealth and Source of Virtual Assets

Where required for due diligence or risk-management purposes, FINARIUM may process information and supporting documentation concerning:

- source of funds;
- source of wealth;
- source of virtual assets;
- employment or business income;
- corporate revenues;
- investments;
- sale proceeds;
- gifts;
- inheritances;
- mining activities;
- transaction history; and
- other evidence reasonably necessary to establish the legitimate provenance of funds or virtual assets.

7.6 Compliance and Risk Information

FINARIUM may process:

- customer-risk classifications;
- due-diligence findings;
- sanctions-screening results;
- politically exposed person screening results;
- adverse-media information;
- financial-crime risk indicators;
- suspicious transaction indicators;
- compliance alerts;
- investigative records;
- information concerning high-risk jurisdictions or counterparties; and
- information required for internal or external regulatory reporting.

7.7 Technical and Security Information

Where relevant to the services used or security and fraud-prevention controls, FINARIUM may process technical information such as:

- IP address;
- device-related information;
- access information;
- transaction-device information;
- approximate geolocation indicators;
- session and security information;
- electronic authentication information; and
- information generated by fraud-prevention or cybersecurity systems.

7.8 Correspondence and Relationship Information

FINARIUM may also retain:

- communications with customers and counterparties;
- requests and enquiries;
- complaints;
- contractual correspondence;
- due-diligence communications;
- records of instructions;
- regulatory correspondence; and
- other communications relevant to the relationship.

8. HOW PERSONAL DATA IS COLLECTED

FINARIUM may obtain Personal Data:

- directly from the Data Subject, including through onboarding documentation, transaction instructions, due-diligence requests and communications;
- from a legal entity represented by the Data Subject, for example where a company provides information regarding its directors, shareholders or beneficial owners;
- from counterparties and financial or virtual-asset service providers, where information is required to process or assess a transaction;
- from public and legally accessible sources, including official registries and other sources recognised or permitted by applicable law;
- from screening, verification and compliance systems, including identity-verification, sanctions, PEP, adverse-media and blockchain-analytics tools;
- from transaction and blockchain information, including information associated with wallet addresses and transaction flows; and
- from Service Providers acting for FINARIUM, where they are authorised to collect or process information on the Company's behalf.

9. PURPOSES FOR PROCESSING PERSONAL DATA

FINARIUM may process Personal Data for purposes including:

- establishing and administering a business relationship;
- verifying identity;
- onboarding customers;
- identifying directors, shareholders and ultimate beneficial owners;
- assessing customer and transaction risk;

- providing services requested by customers;
- processing and administering transactions;
- verifying ownership or control of virtual asset wallets;
- identifying counterparties;
- conducting customer due diligence and enhanced due diligence;
- establishing source of funds, source of wealth or source of virtual assets;
- screening against sanctions, PEP and other relevant risk databases;
- detecting fraud and other unlawful activity;
- conducting blockchain analysis;
- monitoring customer and transaction behaviour;
- identifying unusual or suspicious transactions;
- investigating compliance alerts;
- meeting anti-money laundering, counter-terrorist financing and proliferation-financing obligations;
- complying with sanctions requirements;
- complying with lawful regulatory, judicial or governmental requests;
- maintaining appropriate records and audit trails;
- managing legal, compliance, financial and operational risk;
- establishing, exercising or defending legal rights;
- protecting the Company's systems and information;
- preventing unauthorised access, cybercrime or misuse of services;
- administering contracts and commercial relationships;
- managing complaints, enquiries and customer communications;
- conducting internal governance, audit and assurance activities; and
- complying with applicable laws and legitimate corporate obligations.

Personal Data will not knowingly be processed for an incompatible purpose without an appropriate legal basis and compliance with applicable transparency requirements.

10. LEGAL GROUNDS FOR PROCESSING

FINARIUM will process Personal Data only where a lawful condition for processing exists under applicable Panamanian law. Depending upon the circumstances, processing may be justified by one or more of the following grounds.

10.1 Consent

Where required, FINARIUM will obtain the Data Subject's prior, informed and unequivocal consent. Where processing relies on consent, FINARIUM will maintain appropriate evidence of that consent where required. Consent may be withdrawn in accordance with applicable law. Withdrawal does not retrospectively invalidate processing lawfully undertaken before the withdrawal.

10.2 Contractual Relationship

Personal Data may be processed where reasonably necessary to establish, administer or perform a contractual or commercial relationship involving the Data Subject.

10.3 Compliance with Law

FINARIUM may process Personal Data where processing is required or authorised by applicable legislation, judicial process or another legally binding obligation. This includes processing necessary for lawful compliance, corporate governance, record keeping, financial-crime prevention, regulatory cooperation and reporting.

10.4 Legitimate Interests

Where permitted by Panamanian law, FINARIUM may process Personal Data where necessary for a legitimate interest pursued by the Company or a third party, provided that the relevant interest has been evaluated against the rights and fundamental freedoms of the Data Subject and appropriate measures are adopted to mitigate the resulting privacy risks.

Such interests may include:

- fraud prevention;
- security;
- risk management;
- establishment or defence of legal rights;
- protecting the integrity of the Company's services;
- internal governance; and
- preventing misuse of the Company's systems.

10.5 Public Interest, Legal Authority and Judicial Requirements

Processing may occur where required by a competent public authority acting within its lawful powers, where necessary to safeguard a legally recognised public interest or pursuant to a valid judicial order.

10.6 Vital Interests

Where permitted by law, Personal Data may be processed where necessary to protect the vital interests of the Data Subject or another natural person.

11. KYC, AML/CFT, SANCTIONS AND FINANCIAL-CRIME PROCESSING

Financial and virtual-asset services may present heightened risks relating to money laundering, terrorist financing, proliferation financing, fraud, sanctions evasion and other unlawful activity. FINARIUM therefore processes Personal Data for financial-crime prevention and compliance purposes where legally permitted or required.

Such processing may include:

- identity verification;
- customer due diligence;
- enhanced due diligence;
- verification of corporate ownership and control;
- verification of ultimate beneficial owners;
- sanctions and watchlist screening;
- PEP screening;
- adverse-media screening;
- source-of-funds verification;
- source-of-wealth verification;
- source-of-virtual-assets verification;
- wallet ownership or control verification;
- blockchain analysis;
- transaction monitoring;
- counterparty assessment;
- risk scoring;
- investigation of alerts;
- retention of compliance records; and
- preparation of reports or disclosures to competent authorities where legally required.

Where Personal Data must be retained or processed in order to meet a legal obligation or legitimate financial-crime control requirement, a request to delete or restrict such information may be limited to the extent permitted by law.

12. SENSITIVE PERSONAL DATA

Certain information may constitute Sensitive Personal Data under Panamanian law. This may include, among other categories recognised by law, biometric information used to identify a natural person.

FINARIUM will process Sensitive Personal Data only where there is a lawful basis for doing so and where the additional protections required by applicable law are satisfied.

Where explicit consent is legally required for processing a particular category of Sensitive Personal Data, such consent will be obtained in the form required by applicable law unless another statutory exception applies.

FINARIUM applies enhanced safeguards to Sensitive Personal Data having regard to its nature and the risks associated with unauthorised disclosure or misuse.

13. DISCLOSURE OF PERSONAL DATA

FINARIUM does not disclose Personal Data indiscriminately. Personal Data may be disclosed where reasonably necessary and legally permitted to:

- banks and payment counterparties;
- virtual asset service providers and transaction counterparties;
- identity-verification providers;
- screening and financial-crime prevention providers;
- blockchain analytics providers;
- technology and infrastructure providers;
- professional advisers;
- accountants and auditors;
- insurers where relevant;
- corporate service providers;
- contractors and other Service Providers;
- competent regulatory or supervisory bodies;
- courts and judicial authorities;
- law-enforcement authorities;
- financial-intelligence authorities; and
- other persons where disclosure is required or permitted by applicable law.

Information disclosed to Service Providers must be limited to what is reasonably necessary for the relevant purpose and be subject to appropriate confidentiality, security and data-protection requirements.

14. SERVICE PROVIDERS AND DATA PROCESSORS

FINARIUM may engage specialist third parties to support aspects of its operations, including identity verification, screening, compliance, transaction monitoring, blockchain analysis, technology, hosting, security, professional advice and other legitimate business functions.

Where a third-party processes Personal Data on FINARIUM's behalf, the Company will take reasonable measures to ensure that:

- processing takes place for legitimate and defined purposes;
- access is limited appropriately;
- confidentiality obligations apply;
- reasonable security measures are maintained;
- processing is undertaken consistently with applicable law; and
- Personal Data is not used for unauthorised purposes.

FINARIUM remains responsible for ensuring that the use of external Service Providers is consistent with its obligations under applicable Panamanian law.

15. INTERNATIONAL TRANSFERS OF PERSONAL DATA

The nature of virtual-asset and cross-border financial activities may require Personal Data to be transferred or made available outside Panama.

FINARIUM will undertake an international transfer of Personal Data only where the transfer satisfies at least one legally recognised condition under applicable Panamanian law.

Depending upon the circumstances, this may include where:

- the Data Subject has provided valid consent;
- the receiving jurisdiction or international organisation provides an equivalent or higher level of Personal Data protection;
- appropriate safeguards have been put in place;
- the transfer is provided for by applicable law or an international treaty binding on Panama;
- the transfer is necessary for a contract concerning the Data Subject;
- the transfer is necessary for the legitimate administration of a relationship with the Data Subject;
- the transfer is necessary for an applicable financial transaction;
- the transfer is required in connection with legal proceedings or the administration of justice;
- the transfer is necessary to protect a legally recognised public interest; or
- another condition recognised by Law No. 81 of 2019 or its implementing regulation applies.

FINARIUM will apply appropriate contractual, technical and organisational safeguards to international transfers where required.

Cross-border accessibility of Personal Data will not, by itself, permit the recipient to use the information for purposes unrelated to the purpose for which it was legitimately disclosed.

16. DATA SECURITY

FINARIUM applies reasonable technical, organisational and administrative safeguards having regard to the nature of the Personal Data processed, the purpose of processing and the risks arising from unauthorised access, alteration, disclosure, loss or destruction.

Measures may include, as appropriate:

- access controls;
- authentication;
- segregation of duties;
- encryption;
- secure transmission;
- activity logging;
- transaction and security monitoring;
- access limitation;
- incident escalation;
- internal approval controls;
- vendor-security controls;
- business-continuity arrangements; and
- periodic assessment of relevant systems and controls.

Access to Personal Data is limited to persons who require access for legitimate business or legal purposes and who are subject to appropriate confidentiality obligations.

No electronic or physical security measure can eliminate all risk. FINARIUM therefore maintains procedures designed to identify, assess, contain and respond to suspected security incidents.

17. DATA RETENTION

FINARIUM retains Personal Data only for as long as reasonably necessary for the legitimate purpose for which it was collected and for any additional period required or permitted by applicable law.

Retention periods are determined having regard to matters including:

- the nature of the information;
- the purpose for which it was collected;
- the duration of the customer or contractual relationship;
- applicable statutory record-keeping requirements;
- AML/CFT and financial-crime obligations;
- regulatory expectations;
- audit requirements;
- actual or potential legal proceedings;
- limitation periods;
- investigation requirements; and
- security or fraud-prevention needs.

Personal Data that is no longer required will be deleted, anonymised, blocked or otherwise securely disposed of in accordance with applicable law and the Company's information-governance procedures.

Information will not be retained indefinitely merely because it may potentially be useful

18. RIGHTS OF DATA SUBJECTS

Subject to applicable law and any statutory limitations or exceptions, Data Subjects have rights in relation to their Personal Data.

18.1 Right of Access

A Data Subject may request confirmation regarding Personal Data held or processed concerning that person and obtain information regarding its origin, processing and purpose.

18.2 Right of Rectification

A Data Subject may request correction of Personal Data that is inaccurate, incomplete, outdated, irrelevant, false or otherwise requires correction.

18.3 Right of Cancellation

A Data Subject may request deletion or cancellation of Personal Data in circumstances recognised by applicable law.

18.4 Right of Opposition

A Data Subject may object, on legitimate grounds relating to that person's circumstances, to specified processing and may withdraw consent where processing is based upon consent, subject to applicable legal exceptions.

18.5 Right of Portability

Where the statutory requirements are satisfied, a Data Subject may request a copy of Personal Data in a structured, generic and commonly usable format allowing the information to be operated by different systems or transmitted to another Responsible Party.

These rights are subject to limitations arising under applicable law. For example, FINARIUM may be required to retain or continue processing certain information in order to comply with a legal obligation, regulatory requirement, investigation, legitimate legal claim or financial-crime prevention requirement.

19. EXERCISING DATA-SUBJECT RIGHTS

Requests concerning Personal Data may be submitted to FINARIUM through its official corporate contact channels or delivered to its registered office:

FINARIUM S.A.
Global Bank Tower
18th Floor, Suite No. 1801
50th Street
Panama City
Republic of Panama

FINARIUM may take reasonable steps to verify the identity of the person making a request and, where applicable, the authority of a representative acting on that person's behalf.

Requests will be handled within the periods required by applicable Panamanian law.

In particular, subject to applicable exceptions:

- requests for access are to be addressed within the legally prescribed period, which is generally no more than ten business days;
- correction of inaccurate or incomplete information is to be undertaken within the legally prescribed period, which is generally no more than five business days; and
- other statutory rights will be dealt with in accordance with the corresponding requirements of Law No. 81 of 2019 and its implementing regulation.

FINARIUM does not charge for the exercise of statutory Data Subject rights except where a charge is expressly permitted by applicable law.

20. AUTOMATED PROCESSING, RISK SCORING AND PROFILING

FINARIUM may use technology-supported systems as part of its compliance, fraud-prevention and transaction-monitoring framework.

These systems may analyse information such as:

- customer-risk attributes;
- transaction history;
- transaction amount and frequency;
- transaction velocity;
- customer behaviour;
- geographic indicators;
- device information;
- sanctions or watchlist information;
- blockchain activity;
- wallet attribution;
- counterparty risk; and
- other indicators associated with financial-crime risk.

Such systems may generate risk scores, alerts or cases requiring investigation.

Automated indicators are intended to assist FINARIUM in identifying risk and allocating compliance resources. Where an alert or assessment requires a material compliance decision, FINARIUM's internal controls provide for appropriate escalation and human review in accordance with the nature and level of the risk.

FINARIUM will ensure that technology-supported processing remains subject to applicable legal requirements concerning fairness, transparency, proportionality, security and individual rights.

21. CONFIDENTIALITY

Directors, officers, employees, contractors, advisers and other persons authorised to process Personal Data must maintain the confidentiality of non-public Personal Data to which they obtain access.

Confidentiality obligations continue after the person's employment, appointment, engagement or other relationship with FINARIUM has ended, to the extent required by applicable law or contractual obligation.

Personal Data may be accessed internally only where there is a legitimate business, compliance, legal or operational need.

22. PERSONAL DATA BREACHES AND SECURITY INCIDENTS

FINARIUM maintains procedures for identifying, escalating, investigating and responding to suspected or confirmed Personal Data security incidents.

A Personal Data security incident may include unauthorised or unlawful access, use, alteration, disclosure, destruction or loss of Personal Data, including where the event occurs accidentally.

Where a Personal Data security breach presents a risk requiring notification under applicable Panamanian law, FINARIUM will notify the competent authority and affected Data Subjects in accordance with the applicable legal requirements.

Where the statutory notification obligation applies, notification will be made within the legally required period and will include the information required by Executive Decree No. 285 of 28 May 2021.

FINARIUM will document relevant Personal Data security breaches and the measures implemented to contain, correct and mitigate their effects.

23. REGULATORY, JUDICIAL AND LEGAL DISCLOSURES

FINARIUM may be legally required to disclose Personal Data to public authorities, regulators, courts, law-enforcement agencies or other competent bodies.

Such disclosures will be made only where there is an appropriate legal basis, including where required:

- by applicable legislation;
- by a competent authority acting within its lawful powers;
- pursuant to a judicial order;
- in connection with criminal or regulatory investigations;
- for financial-intelligence or AML/CFT purposes;
- for sanctions compliance;
- to establish, exercise or defend legal rights; or
- to protect a legally recognised public interest.

FINARIUM will seek to limit the information disclosed to that reasonably necessary for the relevant lawful purpose.

24. ACCURACY OF PERSONAL DATA

FINARIUM takes reasonable measures to maintain Personal Data that is accurate, complete and current having regard to the purpose for which it is processed.

Customers and other Data Subjects are expected to notify FINARIUM where information previously supplied has materially changed.

FINARIUM may also update or correct information where reliable evidence demonstrates that existing information is inaccurate, incomplete or outdated and applicable law permits such action.

25. CHANGES TO THIS PRIVACY POLICY

FINARIUM may amend this Privacy Policy where necessary to reflect:

- changes in applicable legislation;
- regulatory guidance;
- changes to the Company's services or operations;
- new technological or security requirements;
- changes to Personal Data processing activities; or
- improvements to the Company's privacy and information-governance framework.

Material amendments will be communicated or made available through an appropriate Company communication channel having regard to the circumstances.

The current version of this Privacy Policy supersedes any earlier version relating to the same subject matter.

26. CONTACT AND COMPLAINTS

Questions, requests or complaints concerning the processing of Personal Data may be directed to FINARIUM through its official corporate contact channels or delivered to:

FINARIUM S.A.
Global Bank Tower
18th Floor, Suite No. 1801
50th Street
Panama City
Republic of Panama

A Data Subject who considers that his or her rights under Panamanian Personal Data protection law have not been respected may also exercise the remedies available under applicable law, including submitting an appropriate complaint to the Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI).

27. GOVERNANCE AND RESPONSIBILITY

FINARIUM is responsible for implementing this Privacy Policy throughout the areas of its operations to which it applies.

Senior management is responsible for supporting appropriate Personal Data governance and ensuring that personnel with access to Personal Data understand the confidentiality, security and compliance requirements applicable to their responsibilities.

Relevant personnel are expected to promptly escalate suspected Personal Data breaches, unauthorised disclosure, improper use of information or other potential violations of this Privacy Policy.

Compliance with this Privacy Policy may be reviewed as part of the Company's internal governance, compliance, risk-management, assurance or audit processes.

28. EFFECTIVE DATE AND APPROVAL

This Privacy Policy takes effect upon its formal approval by the Company and remains effective until amended or superseded in accordance with the Company's governance procedures.

This Privacy Policy is to be reviewed periodically and following any material change to applicable Personal Data protection requirements, the Company's processing activities or the nature of its services.