Privacy Policy
Orinoco (Pty) Ltd
(FSP Number: 51913)

Approval date	Reviewed By	Approved By
25.12.2025	**Compliance Officer**	**Key Individual**

This Privacy Policy ("**Policy**") applies to the processing of Personal Data when individuals access the website at www.finorinoco.com and use the services as described in the Terms of Use. Processing of Personal Data is carried out by Orinoco Capital (Pty) Ltd ("**Company**", "**we**", "**our**", or "**us**"), a private company incorporated under the laws of the Republic of South Africa and authorised as a Financial Services Provider (FSP No. 51913).

Company Details

Company Name	Orinoco (Pty) Ltd
Physical Address	Spaces Umhlanga Office 154 1st Floor 2 Ncondo Place Ridgeside Durban, KZN 4320
License Number	51913
Website	finorinoco.com

Please read this Privacy Policy carefully. By accessing or using our Website and Services, you acknowledge that you have read and understood its provisions. Where required under applicable law, your use of the Website and Services constitutes your acceptance of this Privacy Policy. If you do not agree with this Privacy Policy or any part of it, you must discontinue use of the Website and Services.

We are committed to respecting your privacy, recognising its importance, and protecting the confidentiality and integrity of your Personal Data. All processing of Personal Data is carried out in accordance with applicable South African law, including the Protection of Personal Information Act 4 of 2013 (POPIA), the Financial Advisory and Intermediary Services Act 37 of 2002 (FAIS), and the Financial Intelligence Centre Act 38 of 2001 (FICA), as well as the principles outlined in this Privacy Policy.

To ensure lawful and secure processing, we implement and maintain appropriate technical and organisational measures having regard to the nature, scope, context, and purposes of processing, as well as the risks to Data Subjects, in accordance with applicable legal and regulatory requirements.

This Privacy Policy establishes the key principles and responsibilities that govern our processing of Personal Data and is intended to provide transparency regarding how and why Personal Data is collected, used, disclosed, and retained. For any questions or

concerns about this Privacy Policy or our data handling practices, you may contact us at compliance@finorinoco.com

Product Supplier Details

The Company acts as a financial services intermediary services, meaning it helps clients open trading accounts through an online platform, and offers customer support, but does not execute trades. The Company does not act as a market maker, product issuer, or provider of the underlying instruments and operates solely in an intermediary capacity between the client and Octa Markets Incorporated, a company incorporated in Saint Lucia under registration number 2023-00092 (herein referred to as the "Execution Venue").

The Company does not act as the Execution Venue for client trades and does not assume the role of principal or counterparty to any client trades. The Company does not provide discretionary portfolio management, investment advice, or execute trades on behalf of clients.

Name	Octa Markets Incorporated
Physical Address	Ground Floor, Rodney Court Building Gros-Islet Saint Lucia
Business Address	Parcel 132/1, Block 2938B Road Town, VG1110 Wickham's Cay ii, Tortola British Virgin Islands
Business Registration Number	2023-00092
Email	support@octabroker.com
Website	https://www.octabroker.com/

1. Definitions

For this Privacy Policy, the following terms shall have the meanings set out below:

1.1. **Company/Us/We/Our -** Orinoco Capital (Pty) Ltd, a company incorporated in the Republic of South Africa and licensed as a Financial Services Provider, including its affiliates where applicable, acting as a Responsible Party for purposes of the Protection of Personal Information Act 4 of 2013 (the "POPIA") in relation to the processing of Personal Data described in this Privacy Policy.

1.2. **Consent** - Any voluntary, specific, and informed expression of will by which a Data Subject agrees to the processing of Personal Data, where such consent is required under POPIA. Consent does not apply where processing is carried out on the basis of legal obligation or contractual necessity.

1.3. **Responsible Party -** The natural or juristic person that determines the purpose of and means for processing Personal Data, as defined under POPIA. For purposes

of this Privacy Policy, Company acts as the Responsible Party unless expressly stated otherwise.

1.4. **Operator -** A natural or juristic person that processes Personal Data for or on behalf of the Responsible Party in terms of a contract or mandate, without coming under the direct authority of the Responsible Party, as defined under POPIA.

1.5. **Data Subject** - Any identifiable, living natural person to whom Personal Data relates and whose Personal Data is processed by Company.

1.6. **KYC/AML Checks** - Customer due diligence, ongoing monitoring, and verification procedures carried out by Company or authorised third parties in order to comply with the Financial Intelligence Centre Act 38 of 2001 (the "FICA"), the Financial Advisory and Intermediary Services Act 37 of 2002 (the "FAIS"), and related regulatory requirements. Such checks may include the processing of identity documents, proof of address, tax identifiers, source of funds and source of wealth information, authority to act, employment details (including public office or politically exposed person status), sanctions screening, and adverse media checks.

1.7. **Personal Data** - Any information relating to an identifiable, living natural person, as defined under POPIA, including but not limited to identification details, contact information, financial information, and transaction or trading-related data.

1.8. **Processing** - Any operation or activity concerning Personal Data, whether or not by automated means, including collection, receipt, recording, organisation, storage, updating, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, erasure, or destruction.

1.9. **Applicable Law** - The Protection of Personal Information Act 4 of 2013 (the "**POPIA**"), the Financial Intelligence Centre Act 38 of 2001 (the "**FICA**"), the Financial Advisory and Intermediary Services Act 37 of 2002 (the "**FAIS**"), and any other applicable South African laws, regulations, or binding guidance relating to data protection, financial services, or anti-money laundering.

1.10. **Special Personal Information** - Personal Data as defined under POPIA that requires enhanced protection due to its sensitive nature, including biometric information, criminal behaviour records, and other categories designated as special personal information under POPIA.

1.11. **Services** - All products, features, functionalities, platforms, tools, and support services offered or facilitated by the Company in its capacity as a financial intermediary, as described in the Terms of Use.

1.12. **Terms of Use -** The rules that govern how users access and use the Services, as published on the Website.

1.13. **Third Party / Service Provider** - Any external natural or legal person engaged by Company to provide services, support operations, or otherwise process Personal Data under Company's instructions.

1.14. **User/You/Your** - Any natural person who accesses the Website or uses the Services provided by Company, whether as a visitor, applicant, or client.

1.15. **Website** - The website operated by Company at https://finorinoco.com, together with any related subdomains.

2. Data protection principles

2.1. As Responsible Party for purposes of the Protection of Personal Information Act 4 of 2013 (POPIA), the Company determines the purposes and means of processing

Personal Data and is responsible for ensuring compliance with applicable data protection and financial sector legislation, including POPIA, FAIS, and FICA.

2.2. The applicability of data-protection obligations depends on the nature and context of processing, including whether processing occurs in the context of Company's establishment in the Republic of South Africa, whether Company intentionally targets or provides services to individuals in other jurisdictions, and whether any applicable law has extraterritorial effect. Where such obligations apply, the Company implements appropriate measures and safeguards in accordance with this Policy, applicable law, and the Terms.

2.3. This Policy is governed by the fundamental principles of lawful processing established under POPIA. Accordingly, Company ensures that Personal Data is:

(a) processed lawfully and in a reasonable manner that does not infringe the privacy of Data Subjects;

(b) collected for specific, explicitly defined, and lawful purposes related to Company's services and regulatory obligations, and not further processed in a manner incompatible with those purposes;

(c) adequate, relevant, and not excessive in relation to the purposes for which it is processed;

(d) accurate, complete, and, where necessary, kept up to date, with reasonable steps taken to correct or delete inaccurate Personal Data;

(e) retained only for as long as is necessary to achieve the purposes for which it was collected or processed, subject to statutory retention obligations under applicable law;

(f) processed in accordance with the rights of Data Subjects as provided under POPIA.

2.4. In line with these principles, Company is committed to:

(a) ensuring transparency, fairness, and accountability in all Personal Data processing activities;

(b) implementing appropriate technical and organisational measures to safeguard Personal Data against unauthorised or unlawful processing, accidental loss, destruction, or damage;

(c) limiting the collection and processing of Personal Data to what is strictly necessary for the stated purposes;

(d) ensuring that Personal Data remains accurate and up to date, and rectifying or deleting inaccuracies without undue delay;

(e) applying defined retention periods and securely deleting or anonymising Personal Data once the purposes for which it was collected have been achieved, subject to mandatory legal and regulatory retention requirements;

(f) ensuring that third parties processing Personal Data on behalf of Company act as operators under POPIA, are bound by written agreements, and comply with applicable data protection and confidentiality obligations.

2.5. The Services are not intended for individuals under eighteen (18) years of age. The Company does not knowingly collect Personal Data relating to minors. If the Company becomes aware that Personal Data of a minor has been collected, such data will be deleted as soon as reasonably practicable, unless retention is required by applicable law. Company reserves the right to restrict or terminate access to the Services where it reasonably believes that a User does not meet the applicable legal age requirements.

2.6. Certain categories of Personal Data are mandatory for compliance with legal and regulatory obligations, including obligations under FICA and FAIS, and for the establishment and maintenance of a client relationship. Failure to provide such Personal Data may result in the Company being unable to provide the Services or being required to suspend or terminate the relationship in accordance with applicable law.

2.7. Additional rights, obligations, or limitations may apply depending on the User's jurisdiction, the nature of the services provided, and applicable mandatory laws.

3. Data processed

3.1. Company processes Personal Data only where such processing is lawful and permitted under POPIA. Depending on the purpose and context of processing, Company relies on one or more of the following lawful bases:

(a) **Consent.** Company obtains a User's consent to the processing of Personal Data where consent is required under POPIA, including through consent forms or explicit actions within the Services. Consent is not relied upon where processing is carried out in order to comply with a legal obligation.

(b) **Contractual necessity.** Company processes Personal Data where such processing is necessary for the conclusion, performance, or enforcement of an agreement entered into between Company and the User.

(c) **Legitimate interests.** Company processes Personal Data where such processing is necessary to pursue its legitimate business interests, including the operation, security, and improvement of the Services, provided that such interests are not overridden by the rights and legitimate interests of the Data Subject.

(d) **Legal obligations.** Company processes Personal Data where such processing is required to comply with applicable laws and regulatory obligations, including obligations under the Financial Intelligence Centre Act 38 of 2001 (FICA) and the Financial Advisory and Intermediary Services Act 37 of 2002 (FAIS). Processing on this basis is mandatory and cannot be withdrawn by User.

3.2. Categories of Personal Data Company processes the following types of Personal Data:

	Category of data	**Purpose**	**Legal ground**
(a)	Identity information (name, date and place of birth, age, gender, citizenship, tax residency, occupation)	Identify User, assess suitability for Services, comply with legal and regulatory obligations	Contractual necessity; Legal obligations
(b)	Government identifiers and supporting documents (passport and ID numbers, tax identifiers, passport scans, identity cards, utility bills, bank statements, power of attorney or agent details)	Verify identity and comply with AML/KYC and financial regulatory requirements	Legal obligations; Contractual necessity

(c)	Contact details (postal address, email address, telephone number, messaging accounts)	Communicate with User, provide updates, verify identity	Contractual necessity; Legitimate interests
(d)	Account and access data (usernames, passwords, authentication credentials)	Provide secure access to Website and Services	Contractual necessity; Legitimate interests
(e)	Trading and transaction data (account history, trading activity, orders, demo or simulated accounts, reporting references)	Deliver Services and meet reporting and record-keeping obligations	Contractual necessity; Legal obligations
(f)	Financial and background information (bank account details, payment details, income, source of funds, source of wealth, assets, liabilities, employer details, job title)	Process payments, assess suitability, and comply with AML and financial regulations	Contractual necessity; Legal obligations
(g)	Compliance screening results (PEP checks, sanctions screening, adverse media checks)	Comply with AML, counter-terrorist financing, and sanctions obligations	Legal obligations
(h)	Communication records (telephone recordings, chat transcripts, emails)	Customer service, verification, complaint handling, compliance monitoring, and dispute resolution; records are retained for statutory or evidential purposes and protected through access controls	Legal obligations; Legitimate interests
(i)	Technical and device data (IP address, device ID, operating system, browser type, advertising identifiers)	Ensure security, prevent fraud, optimise system performance, and marketing attribution	Legitimate interests; Consent (where required by law)
(j)	Cookies, analytics, and usage data (cookie identifiers, analytics data, usage metrics, marketing tags)	Optimise Website, measure marketing effectiveness, analyse engagement, and improve Services	Legitimate interests; Consent (where required by law)
(k)	Other information voluntarily provided by User (feedback, inquiries, suggestions)	Respond to inquiries and enhance Services	Legitimate interests; Consent (where applicable)
(l)	Geolocation information	Restrict access from prohibited jurisdictions and ensure compliance with licensing requirements	Legal obligations; Legitimate interests

3.3. The Company does not process special personal information as contemplated under POPIA except where such processing is permitted by law and strictly necessary for the stated purposes, including biometric data used for identity verification during onboarding. In such cases, the Company applies enhanced safeguards, including data minimisation, restricted access, limited retention periods, and, where required under POPIA, prior assessments and explicit consent. Processing relating to vulnerable client circumstances is carried out only where permitted by law, limited to what is necessary, and subject to the same safeguards.

4. Your personal data rights and controls

4.1. As a Data Subject for purposes of POPIA, You may exercise specific rights in relation to Your Personal Data, subject to applicable legal limitations. The Company undertakes to respect these rights and to provide clear and effective means for their exercise. In particular, You may:

	Action	Description
(a)	**Request access**	obtain confirmation of whether Company processes Personal Data relating to You and, where applicable, receive information regarding the categories of Personal Data processed, the purposes of processing, and the recipients or categories of recipients to whom Personal Data has been disclosed
(b)	**Request correction**	request Company to correct or update Personal Data that is inaccurate, incomplete, misleading, or outdated
(c)	**Request restriction**	request that the processing of Your Personal Data be restricted or limited where permitted under POPIA
(d)	**Object to processing**	object to the processing of Your Personal Data on reasonable grounds where such processing is based on legitimate interests or for purposes of direct marketing
(e)	**Withdraw consent**	withdraw any consent previously provided for the processing of Personal Data, provided that such withdrawal shall not affect the lawfulness of processing carried out prior to withdrawal and does not apply to processing required by law, including processing under FICA or FAIS
(f)	**Submit a complaint**	lodge a complaint with the Information Regulator of South Africa.

4.2. **How to exercise rights.** You may exercise Your rights by contacting the Company at compliance@finorinoco.com. Company will consider and respond to requests in accordance with POPIA and within the time periods prescribed by applicable law. To protect Personal Data, the Company may request additional information to verify identity before acting on a request. Certain rights apply only in specific circumstances, and any applicable limitations will be explained in the response.

4.3. **Scope and limitations.** The exercise of Data Subject rights may be limited or restricted where permitted under POPIA or other applicable law. This includes circumstances where the Company is required to retain Personal Data to comply

with statutory or regulatory obligations (including record-keeping under FICA or FAIS), to establish, exercise, or defend legal claims, or where granting a request would prejudice the rights and freedoms of other persons.

4.4. **Verification of requests.** Where a request relates to access, correction, or deletion of Personal Data, Company may require sufficient information to verify identity and locate the relevant data. If You do not maintain an account with Company, Company may be unable to associate the request with prior interactions. The Company may refuse or charge a reasonable fee for requests that are manifestly unfounded, excessive, or repetitive, as permitted under POPIA.

4.5. **Representation by agents.** You may authorise another person to act on Your behalf by providing written authorisation or a valid power of attorney in accordance with applicable law. The Company may require proof of such authority and, where appropriate, confirmation directly from You to verify the legitimacy of the request.

4.6. **Review of decisions.** If Company refuses a request or limits the exercise of a right, You may, where provided under POPIA, refer the matter to the Information Regulator or pursue any other remedies available under applicable law.

5. Purposes of processing personal data

5.1. Company processes Personal Data for the following specific and lawful purposes, in accordance with the Protection of Personal Information Act 4 of 2013, the Financial Advisory and Intermediary Services Act 37 of 2002, the Financial Intelligence Centre Act 38 of 2001, and other applicable laws:

(a) **Onboarding and account management** to consider applications, verify identity, perform KYC and AML checks, establish and manage User accounts, and verify User instructions.

(b) **Provision of services** to deliver requested Services and products, enable access to Website and platforms, facilitate transactions, provide customer support, and respond to User inquiries.

(c) **Risk and compliance** to perform risk assessments, monitor suitability and appropriateness, comply with legal and regulatory obligations (including transaction reporting, tax, record-keeping, and licensing requirements), and cooperate with competent authorities where lawfully required.

(d) **Customer relationship administration** to manage and maintain the client relationship, address complaints, provide evidence in disputes, recover amounts payable, and resolve queries or issues.

(e) **Security and fraud prevention** to detect, investigate, and prevent fraud, unauthorised access, or other unlawful activity, and to ensure the integrity, availability, and security of Services and systems.

(f) **Internal operational purposes** to train staff, improve customer service, conduct internal research, undertake product and service development, and analyse the use of Services in order to enhance performance and reliability.

(g) **Communications** to provide service-related notices, security alerts, and operational updates, and, where permitted under POPIA and applicable marketing laws, to send marketing or promotional communications, subject to User rights to object or withdraw consent. Marketing communications

may be delivered via channels such as email, telephone, SMS, push notifications, or messaging applications used by Company.

(h) **Business operations** to fulfil contractual and operational obligations with partners, contractors, and service providers, including reporting, system integrations, and operational support.

(i) **Payment processing and chargebacks** to process payments, monitor transactions, detect irregularities, manage chargebacks, and prevent misuse of payment methods.

(j) **Legal claims and proceedings** to establish, exercise, or defend legal rights, comply with court orders, or respond to lawful requests or directions from competent authorities.

(k) **Vulnerable clients** to assess and, where permitted by law, take into account personal circumstances indicating vulnerability, for the purpose of ensuring fair treatment, applying appropriate safeguards, and delivering outcomes consistent with regulatory and legal requirements.

(l) **Suitability and appropriateness assessments** to conduct suitability and appropriateness testing, client classification, and risk profiling as required under applicable financial services regulation.

(m) **Communication records** to record and retain telephone or electronic communications (including calls, chats, and emails) for compliance, verification, quality monitoring, complaint handling, and dispute resolution purposes, in accordance with applicable laws. Such records are stored securely with restricted access, retained only for the period required by law, and disclosed to competent authorities where legally required.

(n) **Compliance monitoring and analytics** to conduct monitoring, surveillance, and analytics aimed at detecting suspicious activity, market abuse, or misuse of Services, limited to what is necessary and proportionate to the relevant compliance purpose.

(o) **Service diagnostics and telemetry** to collect and analyse technical logs, diagnostics, and telemetry data for system availability, performance optimisation, error investigation, and service reliability, subject to data minimisation and defined retention limits.

5.2. Company does not process Personal Data for purposes that are incompatible with the purposes listed above, unless such further processing is permitted or required by law or is based on a lawful ground under POPIA.

6. Disclosing your personal data

6.1. Company may disclose Personal Data to authorised third parties where such disclosure is necessary and lawful for the provision of Services, compliance with legal or regulatory obligations, or the pursuit of legitimate interests that are not overridden by the rights of Data Subjects. Categories of recipients may include:

(a) **Company group entities** - parent companies, affiliates, and subsidiaries of Company, where necessary to ensure consistent operations, governance, regulatory compliance, and delivery of Services, subject to appropriate safeguards.

(b) **Execution Venue and trading counterparties** - the Execution Venue, being Octa Markets Incorporated, a company registered in Saint Vincent and the Grenadines (Reg. 19776 IBC 2011) or Saint Lucia (Reg. 2023-00092), acting as the principal to all trades, for the purposes of enabling account

creation on the trading platform, execution of transactions, margin management, risk controls, regulatory reporting, and ongoing administration of trading activities. Such disclosure is necessary for the performance of the contractual relationship between Company, User, and the Execution Venue, and to comply with applicable legal and regulatory obligations.

(c) **Payment service providers and financial institutions** - entities that process payments, deposits, withdrawals, and refunds, and assist with fraud detection, chargeback management, and reconciliation.

(d) **Service providers and business partners** - third-party providers engaged to support Company's operations, including IT hosting and cloud infrastructure providers, payment service providers, banks and financial institutions, identity verification and AML/KYC screening providers, customer support platforms, analytics providers. Such providers act as operators under POPIA, process Personal Data only on Company's instructions, and are bound by written confidentiality and data-protection obligations.

(e) **Professional advisers, auditors, and credit agencies** - legal, financial, tax, compliance, or regulatory advisers and auditors engaged to provide professional services, conduct audits, or support compliance, risk management, and verification activities.

(f) **Regulatory, supervisory, and reporting authorities** - regulators, supervisory bodies, courts, law-enforcement agencies, tax authorities, trade repositories, or other competent authorities, where disclosure is **required or permitted by law**, including disclosures made in response to lawful requests or reporting obligations.

(g) **Business transfers** - third parties involved in an actual or contemplated merger, acquisition, restructuring, reorganisation, or sale of assets or shares, subject to appropriate confidentiality and data-protection safeguards.

(h) **Advertising, marketing, and authentication providers** - selected third parties assisting with marketing communications, campaign measurement, analytics, or User authentication (for example, through third-party login services), where permitted by law and, where required, subject to User consent.

(i) **Dispute resolution and enforcement** - legal representatives, advisers, insurers, or other relevant parties where necessary to establish, exercise, or defend legal rights, enforce agreements or policies, or protect the rights, property, or safety of Company, Users, or others.

(j) **Publicly shared data** - where Services include community, social, or comparative features, limited information (such as usernames, avatars, or performance-related metrics) may be visible to other Users. The Company ensures that only information necessary for the operation of such features is disclosed and that Users are informed of such visibility.

(k) **Consent-based sharing** - any other third parties where User has provided valid consent for the specific disclosure, in accordance with POPIA.

6.2. The Company requires all third parties receiving Personal Data to be subject to confidentiality and data-protection obligations consistent with POPIA and applicable law. The Company takes reasonable steps to ensure that such third parties implement appropriate technical and organisational safeguards. The

Company does not sell Personal Data. Disclosures are made only in accordance with this Policy and applicable law.

6.3. **Anonymised or aggregated data.** The Company may disclose anonymised or aggregated information, which does not identify Users and cannot reasonably be re-identified, to third parties for research, statistical, analytical, or business purposes.

6.4. **Analytics and Advertising Data.** The Company may process device-based identifiers, cookie identifiers, and usage data for analytics, performance measurement, fraud prevention, and, where permitted by law, advertising purposes. Any sharing with analytics or advertising partners is limited to what is necessary, may involve pseudonymised data, and is carried out in accordance with POPIA and applicable consent requirements.

7. Data retention

7.1. Company retains Personal Data only for as long as is necessary to fulfil the purposes for which it was collected and processed, and to comply with applicable statutory, regulatory, contractual, and business obligations. Retention periods depend on the category of Personal Data and the requirements of applicable South African law.

7.2. **Client data.** Personal Data collected for client onboarding, KYC and AML procedures, trading activity, and transaction records is retained for **a minimum period of five (5) years after the termination of the business relationship** or the completion of a transaction, as required under section 23 of the Financial Intelligence Centre Act 38 of 2001, or for a longer period where required by other applicable laws or regulatory obligations. Personal Data necessary for the establishment, exercise, or defence of legal claims may be retained until the expiry of the applicable statutory limitation period.

7.3. **Account and service data**. Personal Data linked to User accounts is retained for the duration of the account relationship and for a limited period after account closure to enable account administration, dispute resolution, audit, and compliance with record-keeping obligations under applicable law

7.4. **Applications, demo accounts, and leads**. Where a User submits an application but no client relationship is established, Personal Data is retained for five (5) years from the date the application was processed or the date the business relationship would have commenced, in accordance with statutory record-keeping requirements under FICA. Personal Data relating to demo accounts, webinar registrations, or other pre-contractual interactions is retained for up to **five (5) years** from the date the Company determines the User has ceased using the demo account. This data is maintained to assist the Financial Intelligence Centre (FIC) in the event of an investigation into identity verification and account opening patterns.

7.5. **Marketing data**. Personal Data processed for marketing purposes is retained until consent is withdrawn or an objection is lodged, as applicable. Company may retain minimal Personal Data solely to record marketing preferences, opt-outs, or suppression lists, in order to ensure that further marketing communications are not sent.

7.6. **Backup and archival data**. Personal Data stored in encrypted backups for disaster recovery and business continuity purposes is retained in accordance with internal retention schedules and securely overwritten or deleted within **a**

maximum period of twelve (12) months, unless restoration is required following a system failure or emergency.

7.7. Notwithstanding any request for erasure or restriction of processing, **Company is required under applicable law, including section 23 of FICA, to retain certain records for the minimum statutory retention period following termination of the business relationship or completion of a transaction**. Where such statutory obligations apply, Company will retain Personal Data solely for compliance purposes, restrict access to such data, and securely delete or anonymise it once the applicable retention period has expired.

8. Data security and safeguards

8.1. Company implements appropriate technical and organisational measures, as required under section 19 of the Protection of Personal Information Act 4 of 2013 (POPIA), to safeguard Personal Data against unauthorised access, disclosure, alteration, loss, or destruction.

8.2. The Company regularly reviews, tests, and evaluates the effectiveness of its technical and organisational measures in order to ensure the ongoing confidentiality, integrity, availability, and resilience of Personal Data processing systems.

8.3. Such measures may include:

(a) encryption of Personal Data in transit and, where appropriate, at rest;
(b) firewalls, secure network architecture, and protected server infrastructure;
(c) role-based access controls, authentication mechanisms, and monitoring of system access;
(d) incident detection and response procedures, including logging and monitoring of administrative access;
(e) staff training, awareness programmes, and confidentiality undertakings;
(f) vendor due diligence and contractual obligations requiring third-party service providers to implement safeguards equivalent to those applied by Company;
(g) encrypted backups, disaster recovery, and business continuity procedures.

8.4. While the Company takes reasonable and appropriate measures to protect Personal Data, no system of data transmission or storage can be guaranteed to be completely secure. The Company maintains documented procedures to detect, manage, and respond to suspected or actual security incidents in accordance with applicable law.

8.5. In the event of a security compromise leading to the unauthorised access to, acquisition of, or loss of Personal Data, Company will assess the incident and take appropriate remedial measures without undue delay. Where required under section 22 of POPIA, Company will notify the Information Regulator of South Africa and affected Data Subjects, taking into account the nature of the breach, the risks posed, and applicable statutory requirements.

9. Transfers to other countries

9.1. Due to the nature of Company's operations and the Services provided, Personal Data may be transferred to, accessed from, or processed in jurisdictions outside the Republic of South Africa. Such transfers may involve Company group entities,

the Execution Venue, subcontractors, and trusted service providers as described in this Privacy Policy.

9.2. The Company ensures that any cross-border transfer of Personal Data is carried out in compliance with section 72 of POPIA. Personal Data is transferred outside South Africa only where the Company is satisfied that one or more of the conditions set out in section 72 of POPIA are met.

9.3. Where applicable, the Company implements appropriate safeguards to protect Personal Data transferred across borders. Such safeguards may include, without limitation:

(a) encryption of Personal Data during transmission and, where appropriate, during storage;

(b) role-based access controls and authentication procedures ensuring that only authorised personnel may access Personal Data;

(c) logging and monitoring of administrative access to systems processing Personal Data;

(d) intra-group data transfer arrangements requiring Company group entities to apply confidentiality, security, and data-protection standards consistent with this Policy and POPIA;

(e) contractual obligations imposed on third-party recipients to process Personal Data only for authorised purposes and to maintain safeguards substantially similar to those required under South African law;

(f) limiting cross-border transfers to the minimum categories of Personal Data necessary for the relevant purpose.

9.4. Depending on the nature and risk profile of the transfer, Company may also implement additional organisational or technical measures, including:

(a) segregation of operational, backup, and testing environments;

(b) data minimisation or pseudonymisation prior to transfer, where appropriate;

(c) assessment of requests for access to Personal Data by foreign public authorities and, where reasonably possible, resisting or challenging requests that appear unlawful or disproportionate.

9.5. Where required under POPIA, cross-border transfers of Personal Data may take place on the basis that:

(a) the recipient is subject to a law, binding corporate rules, or contractual obligations that provide an adequate level of protection substantially similar to that provided under POPIA;

(b) the transfer is necessary for the performance of a contract between Company and User, or for the implementation of pre-contractual measures taken at the request of User;

(c) the transfer is necessary for the establishment, exercise, or defence of legal rights;

(d) the transfer is required or permitted by law, or is necessary for reasons of public interest; or

(e) User has provided informed and specific consent to the transfer, after being made aware of the potential risks associated with such transfer.

10. Cookies and tracking technologies

10.1. The Company uses cookies and similar tracking technologies to enhance User experience, analyse Website usage, ensure security, and, where permitted by law, deliver personalised content or advertising. Information about the categories of

cookies used, their purposes, and options available to Users to manage cookie preferences is set out in Company's separate Cookie Policy, available on the Website.

11. Miscellaneous

11.1. **Automated decision-making and profiling.** The Company does not use fully automated decision-making processes that produce legal effects or similarly significant effects for Users without meaningful human involvement. Where automated analysis or profiling is applied (for example, for fraud prevention, risk monitoring, or service personalisation), such processing is subject to appropriate human oversight and safeguards and is carried out in accordance with POPIA and applicable financial services regulation.

11.2. Third-party websites and services. Services may contain links to websites, applications, or services operated by third parties. The company does not control and is not responsible for the privacy practices, content, or security of such third-party platforms. Users are encouraged to review the applicable privacy policies of those platforms before providing any Personal Data.

11.3. Changes to this policy. The Company may update this Privacy Policy from time to time to reflect changes in operations, legal requirements, or regulatory guidance. The updated version will be made available on the Website and will indicate the effective date. Where changes materially affect Data Subject rights or the manner in which Personal Data is processed, Company will provide appropriate notice and, where required under POPIA, obtain renewed consent.

11.4. Governing law and jurisdiction. This Privacy Policy is governed by and construed in accordance with the laws of the Republic of South Africa, without prejudice to any mandatory rights afforded to Data Subjects under applicable data-protection laws.

11.5. Severability. If any provision of this Privacy Policy is found to be invalid, illegal, or unenforceable under applicable law, the remaining provisions shall remain in full force and effect.

11.6. **Prevailing language**. This Privacy Policy may be translated into other languages for convenience. In the event of any inconsistency between the English version and a translated version, the English version shall prevail.

12. Contact and data protection officer

12.1. All requests, inquiries, or complaints relating to this Privacy Policy or the processing of Personal Data may be submitted to the Company using the contact details below. Requests are handled in accordance with Company's internal procedures and applicable law.

12.2. Company may be contacted regarding this Privacy Policy or the processing of Personal Data as follows:

(a) E-mail: compliance@finorinoco.com

(b) Registered address: Spaces Umhlanga, Office 154, 1st Floor, 2 Ncondo Place, Ridgeside, Durban, KwaZulu-Natal, 4320, Republic of South Africa.

(c) Business address: Spaces Umhlanga, Office 154, 1st Floor, 2 Ncondo Place, Ridgeside, Durban, KwaZulu-Natal, 4320, Republic of South Africa.

12.3. For the purposes of POPIA, the Company has designated an Information Officer responsible for overseeing compliance with data-protection obligations. Requests

and complaints relating to Personal Data will be escalated internally to the Information Officer where appropriate.