Izimo Privacy Policy

Effective Date: 1st, December 2025

This Privacy Policy (“Privacy Policy”) is issued by Keystone Loom Horizon Ltd., registered in Seychelles under number 248030, with its registered address at House of Francis, Room 303, Ile du Port, Mahé, Seychelles, and operating under the brand name “Izimo” (“Izimo”, “Company”, “we”, “our”).

For consistency, all capitalised terms used in this Privacy Policy shall have the same meaning as the corresponding terms defined in the Customer User Agreement, unless expressly stated otherwise. This ensures that the terminology used throughout both documents is aligned and interpreted in a uniform manner.

In order to comply with applicable laws, perform identity verification, and reduce the risk of fraud, the data controller of Izimo may require you to provide certain information about yourself, including your mobile phone number, email address, identification documents, and details relating to any Payment Instruments you use. By accepting and agreeing to the terms of this Privacy Policy, you expressly consent to Izimo processing Your Data in the manner set out herein.

This Privacy Policy describes the categories of information we collect, how we use that information, the purposes for which we process it, and the rights you have in relation to Your Data. Izimo takes the protection of Your Data seriously and will process Your Data only in accordance with this Privacy Policy. For the purposes of this Privacy Policy, “Your Data” means any confidential, personal, or identifiable information relating to users of the Izimo Platform and Services, including both individuals and legal entities.

We are committed to respecting your privacy and to complying with all applicable data protection and privacy laws and regulations. The purpose of this Privacy Policy is to explain how we obtain, use, store, and protect Your Data when you visit the Izimo Website or use the Izimo Platform, or otherwise use our Services. This Privacy Policy does not apply to websites or services operated by third parties, and we encourage you to review the privacy policies of such third parties before providing any personal information to them.

This Privacy Policy forms part of our Customer User Agreement, and it sets out the basis on which we collect and process Your Data in connection with the provision of the Izimo Services. By using the Izimo Platform or Services, you confirm that you have read and understood this Privacy Policy and that you agree that Your Data may be processed as provided herein and, in the Terms, & Conditions.

Izimo may review and update this Privacy Policy from time to time at its sole discretion to reflect changes in applicable laws, regulatory requirements, or our operational practices. When updated, the changes will be highlighted or otherwise communicated to ensure you are aware of the amendments. We may modify this Privacy Policy at any time by posting a revised version on the Website, and such revised version shall be deemed received by all Clients. Unless required otherwise by law, we will provide you with at least 30 days’ prior notice before the revised Privacy Policy becomes effective. We may notify you of changes by posting a notice on the Website and/or by sending a communication via email. As of the effective date of the amended Privacy Policy, your continued use of the Services constitutes your acceptance of all changes. We therefore recommend that you review this page regularly to stay informed.

If you do not agree with this Privacy Policy, you must not register for or use the Izimo Services. If you disagree with any updates to this Privacy Policy, you may close your Client Account at any time by providing us with notice.

Please note: Izimo Services are not available to minors. Individuals under the age of 18 must not submit any personal information to us or use the Izimo Platform or Services.

1. Information Izimo collects from Clients

1.1 Information You Provide Directly
Izimo collects information that you submit when registering for, accessing, or using the Izimo Platform or Services. This includes:
(a) contact details such as your mobile phone number and email address;
(b) Identity Authentication Data, including login credentials, passwords, one-time passwords (OTPs), and any other security features used to access the Client Account or authorize transactions;
(c) information and documents required for Client Identification, Know Your Customer (KYC), and Due Diligence procedures, including identification documents and any other information needed to comply with Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) legislation;
(d) information you provide when completing the Registration Process or updating your Client profile;
(e) information submitted when communicating with customer service or when submitting a complaint.

1.2 Information Collected Automatically
When you use the Website, Platform, or Services, Izimo automatically collects:
(a) access and usage data related to your interactions with the Platform;
(b) session information, including access logs and device interaction records;
(c) technical and security-related data required to support Strong Customer Authentication (SCA) and fraud-prevention systems.

1.3 Financial and Transactional Information
To provide the Services, Izimo collects information relating to your financial activity on the Platform, including:
(a) Client Account balance information;
(b) details of uploads, Withdrawals, Payment Transactions, and currency exchange operations;
(c) Payment Transactions reference numbers, Payment Transaction amounts, applicable fees, and statuses;
(d) information relating to disputed, reversed, rejected, or blocked Payment Transactions.

1.4 Information Obtained from Third Parties
Izimo may receive information about you from third-party Service Providers strictly for the purpose of enabling or supporting the Services. This includes information obtained from:
(a) banks, correspondent institutions, and Payment Instrument providers processing your transactions;
(b) third-party identity verification and compliance-screening services assisting with Client Identification, AML, and CTF checks;
(c) merchants where you choose Izimo as a payment method;
(d) regulatory or governmental authorities where disclosure is required by law.

1.5 Optional Information
If permitted by law and only with your consent where required, Izimo may collect voluntary information such as:
(a) your communication or marketing preferences;
(b) feedback or information you choose to provide through surveys or similar tools.

1.6 Special Categories of Data
Izimo does not intentionally collect or process sensitive categories of personal information unless specifically required to fulfil regulatory obligations (such as identity verification) and only where legally permitted.

2. How Izimo Collects Your Data

2.1 Information Provided Directly by You
Izimo collects Your data when you interact directly with the Platform or with us, including when you:
(a) complete the Registration Process to open a Client Account;
(b) provide information or documentation for Client Identification, KYC, or Due Diligence requirements;
(c) upload documents requested by Izimo to verify identity or comply with AML/CTF regulatory obligations;
(d) update or modify your details in the client accounts;
(e) submit Orders for uploads, Withdrawals, or Payment transactions;
(f) communicate with customer service, report an error, submit a complaint, or otherwise engage with Izimo's support channels.

2.2 Information Collected Automatically Through Platform Use
Certain information is collected automatically when you access, navigate, or use the Website or Platform. This includes:
(a) technical information generated by your device or browser when connecting to the Platform;
(b) session, access, authentication, and security logs generated during login attempts or use of Identity Authentication Data;
(c) behavioral and operational data created through your interactions with Platform features;
(d) information generated as part of Strong Customer Authentication (SCA) and used to ensure account security and prevent unauthorized access.

2.3 Information Received from Third Parties
Izimo may receive Your Data from third parties where necessary to provide the Services or fulfil regulatory obligations, including:
(a) banks, payment service providers, correspondent institutions, and other financial intermediaries involved in processing your Payment Transactions;
(b) identity verification, compliance, and sanctions screening providers supporting Client Identification, KYC, AML, and CTF processes;
(c) merchants or partners where you select Izimo as a payment method on external platforms;
(d) regulatory, supervisory, or governmental authorities where disclosure or cooperation is required by law.

2.4 Information Generated Through Your Activity
Izimo also collects data created as a direct result of your use of the Services, including:
(a) Transaction histories, including pending, executed, rejected, or reversed Payment Transactions;
(b) information relating to limits, compliance checks, and risk assessments applied to your Client Account;
(c) internal records generated by fraud monitoring, risk scoring, or automated security systems.

2.5 Information Collected via Cookies and Similar Technologies
When you visit the Website or Platform, Izimo may use cookies or similar tracking technologies to collect certain technical and usage data. These technologies help improve Platform performance, support security mechanisms, and enable certain features. A separate cookies notice may apply, where relevant.

2.6 Information Required by Law or Compliance Obligations
Izimo may collect additional information where necessary to:
(a) comply with AML/CTF legislation and regulatory reporting requirements;
(b) respond to legal orders, supervisory requests, or investigations;
(c) verify the legitimacy of Transactions or Payment Instruments;

(d) meet obligations imposed by Service Providers, partner financial institutions, or correspondent banks.

3. How Izimo Uses Your Data

3.1 To Provide and Maintain the Services
Izimo uses the data you provide, and the data generated through your use of the Platform, to:
(a) open, manage, and maintain your Client Account;
(b) process uploads, Withdrawals, Payment Transactions, and currency exchange operations;
(c) enable secure login, identity authentication, and the use of Identity Authentication Data;
(d) provide you with access to your account balance, transaction history, and Platform features;
(e) communicate with you regarding the status of your Payment Transactions and Client Account operations.

3.2 To Comply with Legal and Regulatory Requirements
Izimo processes Your Data where necessary to comply with obligations under applicable laws, including:
(a) Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) legislation;
(b) Client Identification, Know Your Customer (KYC), and Due Diligence checks;
(c) transaction monitoring, verification, and record-keeping requirements;
(d) responding to lawful requests from regulatory, supervisory, or governmental authorities.

3.3 To Ensure the Security of the Platform and Client Accounts
Izimo uses Your Data to protect the integrity and security of the Platform, including:
(a) verifying your identity during login and Payment Transaction approval;
(b) detecting and preventing fraud, suspicious activity, and unauthorized Payment Transactions;
(c) applying risk-management measures, including Payment Transaction limits and monitoring;
(d) taking actions such as blocking, suspending, or restricting Payment Transactions or Client Accounts when necessary for safety or compliance reasons.

3.4 To Improve and Optimise the Platform
Izimo may use technical and usage-related data to:
(a) diagnose and troubleshoot performance issues;
(b) enhance Platform functionality and user experience;
(c) develop new features, services, or security enhancements;
(d) analyse trends and usage patterns in anonymised or aggregated form (which does not identify individual Clients).

3.5 To Communicate with You
Izimo may use your contact details to:
(a) send operational communications, such as service updates, notifications, alerts, and authentication codes;
(b) provide support responses to your requests, complaints, or inquiries;
(c) notify you of changes to the Customer User Agreement, the Privacy Policy, or other important updates;
(d) send marketing communications only where permitted by law and only if you have not opted out.

3.6 To Enforce the Customer User Agreement
Izimo may process your data to:
(a) investigate breaches under the Customer User Agreement;
(b) assert or defend legal claims;
(c) prevent prohibited or high-risk activities;
(d) fulfill contractual obligations between you and Izimo.

3.7 For Legitimate Business Purposes

Where permitted by law, Izimo may process Your Data for internal business purposes, including audits, reporting, internal governance, and maintaining proper business records, provided such purposes do not override your rights and freedoms.

4. Legal Basis for Processing

Izimo processes personal data only to the extent necessary to operate the Platform and provide the Services to the Client. As a Seychelles-based company, Izimo follows the legal, regulatory, and operational requirements applicable to its activities, together with its internal Compliance policies and risk-management procedures.

Izimo processes personal data in order to deliver the Services requested by the Client. This includes opening, operating, and maintaining the Client Account, enabling and executing Payment Transactions, supporting Orders, and ensuring secure access to the Platform through the use of Identity Authentication Data and other security measures. The proper functioning of the Client Account and the availability of the Services require Izimo to handle personal data provided by the Client and generated during the Client's ongoing use of the Platform.

Izimo also processes personal data to comply with obligations related to Client Identification, KYC, AML, and CTF requirements and other regulatory duties applicable to financial-related service providers. This includes verifying documentation, monitoring Payment Transactions, assessing risk, identifying unusual or prohibited activities, and cooperating with lawful requests, inspections, or inquiries from competent authorities or financial institutions that support Izimo's operations.

Additionally, Izimo processes personal data for legitimate internal purposes that are necessary to protect the integrity, security, and proper functioning of the Platform. These purposes include preventing fraud, applying Transaction or operational limits, enforcing the Customer User Agreement, maintaining internal audit and governance processes, and ensuring the ongoing reliability and performance of the Services.

In certain cases, Izimo may rely on the Client's consent to process specific types of information. Where consent is required, Izimo will clearly indicate this at the point of collection. The Client may withdraw such consent at any time, provided Izimo is not required to retain or continue processing the personal data to comply with legal, regulatory, or operational obligations.

Izimo does not rely on any single statutory legal framework as the exclusive basis for processing personal data. Instead, data is processed only when it is reasonably necessary to operate the Services, meet obligations applicable to Izimo as a Seychelles-based company, and maintain the security, integrity, and continuity of the Platform for all Clients.

5. Sharing and Disclosure of Personal Data

5.1 Sharing with Affiliated Companies
Izimo may share personal data with companies that form part of the same corporate group as Izimo, including subsidiaries, parent entities, or any entities under common ownership or control. Where such sharing occurs, Izimo requires these affiliated companies to handle personal data in accordance with the same standards of confidentiality, security, and internal Compliance procedures that apply within Izimo.

5.2 Sharing with Service Providers and Partners
Izimo may share personal data with selected Service Providers who support the operation of the Platform or the delivery of the Services. These may include:

- payment processors, correspondent financial institutions, and other entities involved in executing Transactions;
- identity verification providers and compliance-screening partners assisting with Client Identification, KYC, AML, and CTF obligations;
- technical and operational service partners that host systems, maintain infrastructure, or support Platform functionality;
- merchants or third-party partners where the Client chooses Izimo as a payment method.
- When personal data is shared with Service Providers, such providers may retain certain information to comply with their own regulatory, legal, or contractual obligations.

5.3 Sharing Between Clients for Transaction Purposes
In certain circumstances, Izimo may share limited information between Clients to facilitate a Payment Transaction or confirm that a payment has been sent or received. This may include identifiers such as a name or email address to ensure that the Client is paying or receiving funds from the correct party. Izimo does not disclose financial information—such as details of a Client's Payment Instrument—to another Client unless expressly authorised or required by law.

5.4 Interactions with Third-Party Platforms
If a Client uses the Platform in connection with a third-party website, merchant, or platform, Izimo may share limited personal data that is necessary to authenticate the Client, validate a Payment Transaction, or complete the requested service. Such third parties may have their own privacy practices for which Izimo is not responsible.

5.5 Information Received from Third Parties
Merchants, financial institutions, or third-party platforms may provide information to Izimo (such as email addresses or phone numbers) to help verify that a Client is registered with Izimo, initiate a Payment Transaction, or deliver Transaction-related notifications.

5.6 Cross-Border Transfers
Because payment processing often involves international networks and correspondent financial institutions, personal data may be transferred to and processed in jurisdictions outside the Client's country of residence. Izimo ensures that personal data transferred internationally is handled with reasonable safeguards and only to the extent necessary to operate the Services, meet legal or operational obligations, or engage with required Service Providers.

5.7 Disclosure for Legal, Regulatory, or Security Reasons
Izimo may disclose personal data where necessary to comply with applicable law, respond to lawful requests or investigations, or meet obligations imposed by financial institutions or supervisory authorities. Personal data may also be disclosed to protect the security of the Platform, prevent fraud, enforce the Customer User Agreement, or resolve disputes or claims involving a Client.

5.8 No Sale of Personal Data
Izimo does not sell, rent, or trade personal data to third parties for marketing or commercial purposes.

6. International Transfers and Storage of Data

Izimo operates through infrastructure, financial networks, and Service Providers that may be located in various jurisdictions. As a result, Your Data may be transferred to, stored in, or processed in countries outside the Client's country of residence and outside Seychelles. Such

transfers occur only to the extent necessary for Izimo to provide the Services, support the operation of the Platform, or comply with applicable operational or regulatory obligations.

Izimo may store Your Data on servers operated by trusted third-party hosting providers. These providers may be located in regions where data-protection standards differ from those in the Client's home country. When Your Data is transferred internationally, Izimo ensures that such transfers are carried out with reasonable safeguards and internal Compliance measures designed to protect confidentiality, integrity, and security.

In some cases, Your Data may also be transferred to correspondent financial institutions, payment processors, or technical infrastructure partners who assist Izimo in executing Payment Transactions, maintaining operational continuity, or supporting verification, monitoring, and fraud-prevention functions. These entities may in turn be required to retain certain information to comply with their own legal, regulatory, or operational obligations.

International transfers are an essential component of providing global payment and financial-related services. By using the Services or maintaining a Client Account, the Client acknowledges that such transfers may occur and that personal data may be processed in jurisdictions that may not offer the same data-protection framework as the Client's country of residence. Despite this, Izimo applies commercially reasonable administrative, technical, and organisational measures to ensure that personal data remains protected throughout its lifecycle, regardless of where it is processed or stored.

7. Data Security and Protection Measures

Izimo takes the security of personal data seriously and applies reasonable administrative, technical, and organisational measures designed to protect the confidentiality, integrity, and availability of the information processed through the Platform. These measures are intended to prevent unauthorised access, misuse, loss, alteration, or disclosure of personal data.

To protect Client Accounts, Izimo uses various security controls, including the use of Identity Authentication Data, encryption of communications where appropriate, monitoring tools, and other mechanisms to safeguard access to the Platform. Clients may be required to complete Strong Customer Authentication (SCA) steps or additional verification procedures when accessing their accounts or initiating a Payment Transaction. These measures aim to ensure that only authorised individuals can access or operate a Client Account.

Izimo employs internal Compliance processes and risk-management procedures to detect and prevent fraudulent or suspicious activity. This includes monitoring of Payment Transactions, applying operational or Transaction limits, reviewing identified risks, and taking actions such as blocking access, suspending activity, or restricting the Client Account when necessary to protect the Client, Izimo, or third parties.

Personal data may be stored using third-party hosting or cloud-service providers that support the operation of the Platform. Izimo requires these providers to implement reasonable security safeguards and to maintain systems designed to protect personal data from unauthorised access or disclosure. These measures form part of Izimo's broader commitment to maintaining a secure operational environment.

Despite Izimo's efforts, no online service or system can guarantee absolute security. Clients are responsible for maintaining the confidentiality of their Identity Authentication Data and for ensuring that any devices used to access the Platform are secure and protected against malware, unauthorised access, and other threats. Clients should notify Izimo immediately using the official Customer Service channels if they suspect any compromise of their account or Identity Authentication Data.

Izimo continuously reviews and updates its security practices to adapt to emerging risks, technological changes, and legal or operational requirements. These efforts form part of Izimo's ongoing commitment to maintaining a secure and resilient Platform for all Clients.

8. Data Retention

Izimo retains personal data only for as long as necessary to operate the Platform, provide the Services, fulfil the purposes for which the data was collected, or comply with applicable legal, regulatory, and operational requirements. The specific retention period for any category of personal data will depend on the type of information, the nature of the Services provided, and the obligations that apply to Izimo or its Service Providers.

Certain information must be retained to comply with obligations relating to Client Identification, KYC, AML, and CTF requirements. This may include identification documents, Payment Transaction records, and information relating to the operation of the Client Account, which may need to be stored for a period after the Client Account is closed. Retention of such information ensures that Izimo can meet record-keeping requirements, respond to lawful requests, assist in financial investigations, and protect the integrity of the Services.

Izimo may also retain Your Data for internal Compliance purposes, risk management, fraud-prevention activities, or the resolution of disputes, complaints, or legal claims. Information necessary to enforce the Customer User Agreement or to protect Izimo's rights may be kept for a reasonable period, even after a Client Account has been closed.

Where Your Data is no longer required for the purposes for which it was collected and no legal or operational obligations require its continued retention, Izimo will take reasonable steps to securely delete, anonymise, or otherwise remove Your Data from its systems. In some cases, data may remain stored in backup systems for a limited period as part of routine business continuity processes, after which it will also be removed in accordance with Izimo's data-retention procedures.

9. Your Rights

Izimo respects the ability of each Client to understand and control how their Data is used. While the specific rights available to Clients may depend on the laws applicable in their country of residence, Izimo aims to provide every Client with a reasonable level of transparency and control over their information.

Clients may request access to the personal Data that Izimo holds about them. This includes information provided during Client Identification, Registration Process and information generated through the use of the Platform and Services, such as Payment Transaction records and communications with Customer Service.

Clients may also request that Izimo correct any inaccurate or incomplete personal Data associated with their Client Account. It is the Client's responsibility to ensure that information provided to Izimo is accurate and kept up to date. Izimo may request additional documentation to verify changes to personal information, particularly when updates may affect Compliance or security measures.

In certain circumstances, Clients may request the deletion or restriction of their personal Data. Izimo will consider such requests in line with its legal, regulatory, and operational obligations. Some information cannot be deleted if it is necessary for Izimo to:

- comply with KYC, AML, or CTF requirements;
- maintain records of Payment Transactions;

- respond to legal or regulatory requests;
- enforce the Customer User Agreement;
- resolve disputes or protect Izimo's rights.

Clients may also contact Izimo if they have concerns about how their personal Data is being processed or if they wish to better understand how data is handled across the Platform. Izimo will provide reasonable assistance and information where appropriate.

Requests regarding your Data may be submitted through the official communication channels listed on the Website or directly to Customer Service. Izimo may take steps to verify the identity of the Client before responding to any request, particularly where access to sensitive information or changes to account details are involved.

10. Cookies and Tracking Technologies

Izimo may use cookies and similar tracking technologies when you visit the Website or access the Platform. These technologies help Izimo understand how Clients use the Services, improve Platform functionality, support security and authentication processes, and enhance overall user experience.

Cookies are small data files stored on a device or browser when accessing online services. Izimo may use cookies to remember login preferences, maintain the operation of the Client session, support features that require Identity Authentication Data, and ensure that the Platform functions efficiently across devices. Certain cookies are essential for the operation of the Platform and cannot be disabled without affecting the ability to use the Services.

Izimo may also use analytical or performance-related technologies that help monitor usage patterns, identify technical issues, and optimise the Platform. These technologies may collect information such as device type, browser information, access times, or interaction data, but do not allow Izimo to directly identify Clients unless they are logged into the Platform.

If permitted by your device or browser settings, you may manage or delete cookies at any time. However, disabling certain cookies may limit the functionality of the Platform or affect the ability to access specific Services or features.

Where Services Provider support the operation of the Website or Platform, they may use their own cookies or tracking tools as part of their service delivery. Such technologies are used under their own practices and may not be controlled directly by Izimo.

Izimo may provide a separate Cookies Notice where required or where additional details about specific cookie types or technologies are needed.

11. Complaints and Contact Information

Izimo aims to ensure that all personal data is handled responsibly and in accordance with this Privacy Policy. If you have questions, concerns, or complaints about how your personal data is processed, or if you wish to exercise any of the rights described in this Privacy Policy, you may contact Izimo using the official communication channels listed on the Website or by reaching out directly to our support team.

Clients may submit inquiries or complaints regarding personal data through the following dedicated contact point:

Email: support@izimo.io
Registered Office:
Keystone Loom Horizon Ltd.
House of Francis, Room 303

Ile du Port, Mahé
Seychelles

Izimo will review and respond to questions or complaints within a reasonable timeframe and may request additional information where necessary to verify the identity of the Client or to understand the nature of the inquiry. Where a complaint relates to a matter governed by legal or regulatory requirements, Izimo will take appropriate steps to address the issue in accordance with its internal Compliance procedures, operational policies, and obligations under applicable law.

If a Client is dissatisfied with Izimo's response or believes that personal data has not been handled in accordance with this Privacy Policy, the Client may escalate the matter by contacting Izimo's management or by following any dispute-resolution procedures outlined in the Customer User Agreement.

12. Changes to This Privacy Policy

Izimo may update or amend this Privacy Policy from time to time in order to reflect changes in its operational practices, legal or regulatory requirements, technological developments, or the Services offered through the Platform. Any updated version of the Privacy Policy will be published on the Website and will indicate the date on which the changes take effect.

Where changes are significant or impact the way personal data is collected, used, or stored, Izimo will take reasonable steps to inform Clients. This may include posting a notice on the Website, providing a notification through the Platform, or sending a communication to the Client's registered email address. Unless otherwise required by law, Izimo will provide at least 30 days' prior notice before any material amendment becomes effective, consistent with the approach described in the Customer User Agreement.

By continuing to use the Services after the effective date of an updated Privacy Policy, the Client acknowledges and accepts the revised terms. Clients who do not agree with the updated Privacy Policy may stop using the Services and may request to close their Client Account in accordance with the Customer User Agreement.

Izimo encourages Clients to review this Privacy Policy periodically to stay informed about how personal data is handled and protected.

13. Final Provisions

This Privacy Policy forms an integral part of the Customer User Agreement and should be read together with all other documents and policies referenced therein. In the event of any inconsistency between this Privacy Policy and the Customer User Agreement, the provisions of the Customer User Agreement shall prevail to the extent permitted by applicable law.

Nothing in this Privacy Policy limits Izimo's ability to comply with its legal, regulatory, or operational obligations, nor does it restrict Izimo from taking any measures necessary to protect the integrity of the Platform, safeguard the Client Account, or fulfil obligations arising under applicable Compliance, AML, or CTF requirements.

If any provision of this Privacy Policy is found to be invalid, unlawful, or unenforceable by a competent authority, the remaining provisions shall continue in full force and effect. Izimo's failure to enforce any provision shall not be construed as a waiver of that provision or of Izimo's rights.

This Privacy Policy is governed by the laws of Seychelles. Any disputes arising out of or relating to this Privacy Policy shall be handled in accordance with the dispute-resolution procedures set

out in the Customer User Agreement, and the courts of Seychelles shall have jurisdiction, without prejudice to Izimo’s right to seek relief in any other competent jurisdiction.