Privacy Policy

Last updated: 06. 07. 2026

This Privacy Policy (the "Policy") explains how Metritax (MU) Ltd (the "Company", "We", "Us") processes Personal Data when you visit the Website at metritax.com or use the Services described in the Customer Agreement.

By accessing the Website or Services, you confirm you have read and understood this Policy and accept it as legally binding. If you disagree with any part of it, you must stop using the Website and Services.

1. About the Company

Metritax (MU) Ltd is incorporated in the Republic of Mauritius (registered number 235525 GBC) and licensed as an Investment Dealer (Full Service Dealer, excluding underwriting) by the Financial Services Commission of Mauritius (licence number GB26206169).

2. Our Commitment

We respect and protect the confidentiality and integrity of your Personal Data. This Policy applies to the Company and to its employees, agents, and anyone else acting on its behalf when handling information received from actual or prospective clients.

We will not disclose Non-public Consumer Data and will use it only for the purposes specified to, and agreed with, you, or as required under applicable law. All processing complies with applicable laws and the principles in this Policy, and we maintain technical and organisational measures proportionate to the nature and risks of our processing and to the legal requirements of each jurisdiction where we process Personal Data.

We are committed to protecting the privacy and confidentiality of client information and to handling Personal Data in a fair, transparent and secure manner throughout the client relationship.

Questions about this Policy or our data practices: support@metritax.com.

3. Relationship to Other Documents

This Policy supplements, and does not replace or override, any data-processing provisions in the Customer Agreement or any partnership or affiliate agreement. As amended from time to time and published on the Website, it governs how the Company collects, uses, stores, discloses, and

transfers your Personal Data, and your rights in respect of it, during and after the business relationship.

4. Definitions

4.1. Company / Us / We / Our — Metritax (MU) Ltd, together with its parents, affiliates, and subsidiaries, acting as Data Controller for the processing described in this Policy.

4.2. Consent — a freely given, specific, informed, and unambiguous indication of a User's agreement to the processing of their Personal Data.

4.3. Data Controller — a person and/or a company, that determines the purposes and means of processing Personal Data. Unless stated otherwise, this is the Company.

4.4. Data Processor — any person and/or a company, that processes Personal Data on the Data Controller's behalf.

4.5. Data Subject — any individual whose Personal Data the Company processes.

4.6. KYC/AML/Verification Checks — procedures by the Company or its authorised third parties to verify identity, assess risk, and meet anti-money laundering and counter-terrorist financing obligations. These may include, but not limited to, passport or ID details, social security or tax identifiers, source-of-wealth information, reasons for using corporate or trust structures, employment details (including public-office roles), and results of PEP checks, sanctions screening, and adverse media searches.

4.7. Non-public Consumer Data — data provided to the Company by a financial consumer and not made available to the public at large.

4.8. Personal Data — any information relating to an identified or identifiable natural person, including but not limited to name, contact details, identification, financial information, address, and trading history.

4.9. Processing — any operation performed on Personal Data, automated or not, including collection, storage, use, disclosure, and deletion.

4.10. Relevant Legislation — the Data Protection Act 2017 of Mauritius, as amended, together with related rules, regulations, and binding guidance of the Data Protection Commissioner of Mauritius, and any other privacy laws applicable where the Company operates or offers Services.

4.11. Sensitive Personal Data — special categories of Personal Data requiring enhanced protection under Relevant Legislation, for example, data on health, criminal records, racial or ethnic origin, religious or philosophical beliefs, sexual orientation, biometric, or any other category designated as sensitive under applicable law.

4.12. Services — all products, features, applications, content, and functionality the Company offers.

4.13. Third Party / Service Provider — any external person the Company engages to provide services, support operations, or process Personal Data on the Company's instructions.

4.14. User / You / Your — any natural person who accesses the Website or uses the Services, as a visitor, partner, affiliate, applicant, or client.

4.15. Website — the website the Company operates at metritax.com, including subdomains.

4.16. Client Data - Personal Data collected by the Company in connection with the provision of investment services, account administration, trading activities, onboarding procedures and regulatory compliance obligations.

5. Data We Process

5.1. We process Personal Data on the following grounds:

5.1.1. Consent — obtained through consent forms or your explicit actions within the Services.

5.1.2. Contractual necessity — to perform our obligations under agreements between you and the Company.

5.1.3. Legitimate interests — to operate, secure, and improve the Services, as described in the Customer Agreement.

5.1.4. Legal obligations — where processing is required to comply with applicable law.

5.2. Categories of Personal Data we process stated below. For each category below, we state what we collect and why:

5.2.1. Identity information - includes but is not limited to: name, date and place of birth, age, gender, marital status, citizenship, tax residency, occupation. To identify you, provide assess for our services, and meet legal and regulatory obligations.

5.2.2. Government identifiers and supporting documents include but are not limited to: passport and ID numbers, national insurance/tax identifiers, passport scans, ID cards, utility bills, bank

statements, power of attorney/agent details. To verify identity and comply with AML/KYC and financial regulations.

5.2.3. Corporate client verification documents - for clients that are legal entities: incorporation documents, financial statements, business plans, and identification documents (passport/ID, utility bills) of directors, shareholders, and authorised persons. To verify the identity of the entity and its controllers and comply with AML/KYC obligations.

5.2.4. Account and access data: usernames, passwords, account credentials. To provide secure access to the Website and Services.

5.2.5. Contact details: address, email, phone number, messenger accounts. To communicate with you, provide updates, and verify identity.

5.2.6. Financial and background information include but are not limited to: bank account number, sort code, payment details, income, source of funds, source of wealth, assets, liabilities, employer details, job title. To process payments, assess suitability, and comply with AML and financial regulations.

5.2.7. Suitability and appropriateness information: trading knowledge, investment experience, financial circumstances, investment objectives, capacity for loss and risk tolerance. This information is collected to assess whether our products and services are appropriate for you and to comply with applicable legal and regulatory requirements.

5.2.8. KYC screening results: PEP checks, sanctions screening, adverse media checks. To comply with AML, counter-terrorist financing, and sanctions requirements.

5.2.9. Trading and transaction data: account history, trading activity, orders, demo accounts, simulators, transaction reporting references, etc. To execute orders and meet reporting obligations.

5.2.10. Technical and device data includes but is not limited to: IP address, device ID, phone type, operating system, browser type, GUID, Google 360 ID, IDFA, GAID. For fraud prevention, system performance, security, and marketing purposes.

5.2.11. Biometric data includes but is not limited to: facial images, advanced selfie, liveness verification. To verify identity during onboarding, and where required by law or necessary for compliance.

5.2.12. Geolocation information - to restrict access from prohibited jurisdictions and comply with licensing requirements.

5.2.13. Communication records, such as phone call recordings, chat transcripts, emails. Recorded and stored for customer service, verification, complaint handling, compliance monitoring, and dispute resolution; retained for the period necessary to meet regulatory and evidential requirements and protected through access controls and encryption, and may be disclosed to competent authorities where legally required.

5.2.14. Information required for regulatory reporting and compliance purposes, including transaction reporting information, account identifiers and other information required by applicable laws, regulations or competent authorities.

5.2.15. Cookies, analytics, and usage data: cookie ID, local storage data, web analytics, marketing tags (UTM/GCLID/FBCLID), platform and app usage. To optimize the Website, measure marketing effectiveness, analyse engagement, and improve the Services.

5.2.16. Information you voluntarily provide to us: feedback, suggestions, requests. To respond to you and improve the Services.

5.3. Sensitive and/or Special Category Data. We do not process Sensitive and/or Special Category Data except where permitted by law and strictly necessary for stated purposes, for example, biometric data for identity verification during onboarding. Where we ask you for such data, we will tell you why and how it will be used. In all cases we apply suitable safeguards: data minimisation, access controls, limited retention, and, where required, prior assessments and explicit consent.

6. Data Protection Principles

6.1. As Data Controller, the Company determines the purposes and means of processing and is responsible for complying with Relevant Legislation wherever it operates or wherever such laws apply to Users.

6.2. Whether a given data-protection law applies depends on the nature and context of processing: establishment in a territory, targeting or monitoring of individuals there, or extraterritorial effect of local law. Where it applies, we comply with it regardless of your location.

6.3. We ensure that Personal Data is:

(a) processed lawfully, fairly, transparently, and accountably;
(b) collected for specified, explicit, and legitimate purposes, and not further processed incompatibly with them;
(c) limited to what is necessary for those purposes;
(d) kept accurate and up to date; inaccuracies are rectified or erased without undue delay;
(e) retained in identifiable form no longer than necessary, then destroyed or anonymised;

(f) processed in accordance with Data Subjects' rights;
(g) protected by appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss, destruction, or damage;
(h) processed by third parties only under written agreements binding them to data-protection obligations.

6.4. Minors. The Services are not intended for anyone younger than eighteen (18) years, or below the age of legal majority in their jurisdiction, whichever is greater. We do not knowingly collect their Personal Data; if we discover we have, we delete it without undue delay. We may restrict access where we reasonably believe a User is under the applicable age.

6.5. Additional rights or obligations may apply depending on your jurisdiction.

6.6. Certain Personal Data is mandatory for legal and regulatory compliance (including KYC/AML/Verification Checks) and for establishing a client relationship. If you do not provide it, we may be unable to provide the Services.

7. Purposes of Processing

7.1. We process Personal Data, in compliance with Relevant Legislation, in order to:

7.1.1. Business operations - meet our contractual commitments to partners, contractors, and service providers, including the reporting, integrations, and operational support those relationships involve.

7.1.2. Communications - send you service notices, security alerts, and updates, and, where the law permits, marketing and promotional content, which you may object to, or withdraw Consent from at any time. Marketing may reach you by email, telephone, SMS, push notification, or, where the Company uses them, messaging apps such as Telegram, WhatsApp, etc.

7.1.3. Compliance analytics, security and fraud prevention - run monitoring and analytics that flag abuse, suspicious activity, or other misuse of the Services, going no further than is necessary and proportionate, and keep the Services secure and intact.

7.1.4. Customer relationship administration - maintain the client relationship day to day: handling complaints, evidencing our position in disputes, recovering sums payable, and resolving queries.

7.1.5. Internal purposes - train our staff, raise the quality of customer service, and study how the Services are used so we can make them perform better.

7.1.6. Legal claims and proceedings - establish and enforce our legal rights, defend claims brought against us, and honour court orders or lawful directions from competent authorities.

7.1.7. Onboarding and account management - review your registration application, confirm who you are, run KYC/AML/Verification Checks, open and administer your account, and validate the instructions you give us.

7.1.8. Payment processing and chargebacks - monitor payment transactions for irregularities, handle chargebacks, and prevent payment methods from being misused.

7.1.9. Provision of services - deliver the Services and products you request: giving you access to the Website and platforms, executing your orders, providing you additional information, supporting you, and answering your inquiries.

7.1.10. Risk and compliance - assess risk, keep suitability under review, satisfy our legal and regulatory obligations — transaction reporting, tax, and licensing among them — and cooperate with competent authorities, such as, the Financial Services Commission, the Financial Intelligence Unit, law enforcement agencies and other competent authorities where required by law or regulation.

7.1.11. Service diagnostics: gather and analyse technical logs and telemetry to track uptime, tune performance, investigate errors, and keep the Services reliable.

7.1.12. Suitability and appropriateness assessments: carry out the suitability and appropriateness tests, and risk assessments that applicable requirements demand.

7.1.13. Client categorization: recognise, and where necessary make allowance for, circumstances or characteristics suggesting vulnerability, so that you are treated fairly, protected appropriately, and receive outcomes consistent with Relevant Legislation.

7.2. Restrictions. We will not use Personal Data to any purpose incompatible with those above, unless the law requires it or you have given your Consent.

7.3. We may also contact you regarding important changes affecting your account, trading platform, client agreements, legal obligations, security matters or regulatory requirements.

8. Your Rights and Controls

8.1. Under Relevant Legislation you may, as a Data Subject, be entitled to request:

8.1.1. Inquire information regarding your personal data handling : request confirmation of whether we process your Personal Data, and details of the categories, methods, and purposes of processing.

8.1.2. Data correction: amendment of Personal Data that is inaccurate, incomplete, or outdated.

8.1.3. Deletion: deletion of your Personal Data, where the law permits.

8.1.4. Restriction of Data usage: suspension of processing, in whole or in part, in circumstances the law permits as well as to withdrawal of any Consent previously given. Withdrawal does not affect the lawfulness of prior processing, we will cease processing unless continued processing is permitted under Relevant Legislation (e.g., AML obligations).

8.1.5. Objection / opt-out of processing of Your Personal Data : objection to processing of your Personal Data based on legitimate interests or public interest, including direct marketing and related profiling.

8.1.6. Complaint: file a complaint to the Data Protection Authority of Mauritius or, where applicable, the competent authority in your jurisdiction.

8.2. In order to exercise your rights, contact us at support@metritax.com. We respond within the timeframes Relevant Legislation requires and may ask for additional information to confirm your identity first. Some rights apply only in certain territories or circumstances. Rights may be restricted or limited by law. We will explain any limitation when we respond.

8.2.1. While you may exercise your privacy rights, certain information must be retained by the Company where required by applicable financial services, anti-money laundering, tax or other regulatory obligations.

8.3. Verification; fees. For access, deletion, or correction requests we may require account-linked details to verify identity. If you do not provide these details, we may be unable to link the request to prior interactions and therefore unable to act on it. We may charge a reasonable fee, or decline to act, where a request is manifestly unfounded, excessive, or repetitive, in accordance with Relevant Legislation.

8.4. Appeals. If we reject a request, you may appeal our decision where Relevant Legislation provides for it, using the procedures applicable in Your jurisdiction.

9. Disclosure of Personal Data

9.1. Where needed to deliver the Services, meet legal obligations, or pursue legitimate interests, the Company may share Personal Data with:

9.1.1. Advertising, marketing, and authentication providers - selected partners that help us personalise promotions, measure marketing campaigns results, or authenticate you through third-party platforms such as Google or Apple, etc.; with Consent where the law requires it.

9.1.2. Business transfers - parties to a merger, acquisition, restructuring, or asset sale, under confidentiality obligations.

9.1.3. Professional advisers - legal, financial, and regulatory advisers, and credit reference or verification agencies, for professional services and handling disputes.

9.1.4. Publicly shared data : when the Services offer community or social features, details such as usernames, avatars, trading activity, or performance metrics may be visible to other Users. Only what the feature requires is shown, and you are told what will be visible.

9.1.5. Regulators, authorities, auditors, courts, legal representatives and other relevant parties - regulators, courts, law enforcement, tax authorities, auditors, trade repositories, and other competent bodies, in connection with laws, investigations, reporting, or enforcement, including lawful requests from public authorities even where disclosure is not compelled, and disclosures mandated under credit-reporting or other laws or by court order, or where necessary to protect the rights, property, or safety of the Company, Users, or others.

9.1.6. Service providers and business partners - validated and trusted third parties that support our operations: IT hosting and cloud infrastructure, payment providers, banks, other financial institutions, identity verification and AML/KYC screening, customer support platforms, analytics and search engines, and marketing partners. Each acts solely on our instructions and under contractual confidentiality and data-protection duties.

9.1.7. Where the Company outsources operational, technology, compliance or support functions, Personal Data may be shared with approved service providers strictly to the extent necessary for them to perform the services requested. Such service providers are required to maintain appropriate confidentiality and data protection standards.

9.1.8. Third parties you authorise or consent to - anyone you have explicitly Consented to our sharing with, or authorised to obtain your data from us.

9.2. Every Data recipient must be bound by confidentiality and data-protection obligations consistent with Relevant Legislation, and we take reasonable steps to check their safeguards. We do not sell Personal Data. Sharing happens only as this Policy and Relevant Legislation allow.

9.3. Analytics and advertising data. Device identifiers (including Google Advertising ID and Apple IDFA), cookie IDs, and clickstream data may be processed for analytics, campaign measurement, and interest-based advertising. This can involve sharing pseudonymised data with advertising and analytics partners, within the bounds of Relevant Legislation.

10. Data Retention

10.1. We keep Personal Data only as long as the purposes it was collected for, and our statutory, regulatory, contractual, and business obligations, require.

10.2. Personal Data from KYC/AML/Verification procedures, trades, and transactions is kept for at least seven (7) years after the client relationship ends or the transaction completes, as Section 17F of the Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA) requires, or longer where Relevant Legislation demands. Your right to request erasure does not override these statutory duties: where they apply, we keep the data solely for compliance and securely delete or anonymise it once the retention period ends. Data needed to defend legal claims may be kept until the applicable limitation period expires.

10.2.1. Records relating to complaints, communications, transactions, suitability assessments and client due diligence may also be retained for periods required under applicable financial services and regulatory requirements.

10.3. Data linked to your account is kept while the account is active, and for a limited period after closure to allow account recovery, resolve disputes, and meet record-keeping obligations.

10.4. If you apply for an account but no client relationship is established, we keep your data for up to one hundred eighty (180) days from submission. For demo accounts, webinar registrations, and other leads: we keep your data for up to ninety (90) days. Renewed interest within these periods - a login, a re-submitted application, extends retention by thirty (30) days from that activity, and extensions can repeat during the initial period.

10.5. Marketing data is kept until you withdraw Consent or opt out. After that, we may keep minimal data (such as an email address or phone number) on a suppression list, solely to record your preference and make sure no further marketing reaches you.

10.6. Where a client is subject to an investigation, we retain the relevant records as the investigating authority instructs. We maintain records so that they can be retrieved without undue delay and produced to competent authorities on request.

10.7. Data held in encrypted disaster-recovery backups follows our internal retention schedules and is automatically overwritten or deleted within twelve (12) months at most, unless emergency restoration is needed.

11. Data Security and International Data Transfers

11.1. The Company applies technical and organisational measures, appropriate to the nature of the data we hold, to protect Personal Data against unauthorised access, disclosure, alteration, or destruction.

11.2. We test and assess these measures regularly to keep our processing systems secure, confidential, and resilient.

11.3. Data Security measures may include:

11.3.1. encrypted, documented, backups and disaster recovery procedures;

11.3.2. encryption of Personal Data in transit and, wherever appropriate, at rest;

11.3.3. firewalls and secure server infrastructure protecting our databases and cloud storage;

11.3.4. incident response procedures and logging of administrative access;

11.3.5. need-to-know role base access: rights differentiated by job responsibility, with authentication and monitoring of system access;

11.3.6. staff training and confidentiality undertakings, with disciplinary consequences for breach;

11.3.7. vendor due diligence and contracts requiring service providers to maintain equivalent safeguards.

11.4. We take reasonable steps to protect Personal Data, but no system or transmission can be guaranteed fully secure. We maintain processes to detect and respond to security incidents in line with Relevant Legislation. If a breach occurs, we act as Relevant Legislation requires, including, where required, notifying competent authorities and affected Users within the applicable timeframes.

International transfers safeguards

11.5. Our operations are global, so Personal Data may be transferred to and processed in countries other than yours by Company entities, subcontractors, and trusted partners, as this Policy describes.

11.6. Every international transfer complies with Relevant Legislation: we verify that the recipient country or organisation ensures adequate protection, or add safeguards where required.

11.7. Depending on the transfer, we may also segregate operational and backup storage, apply minimisation and pseudonymisation before transfer where appropriate, and review government access requests.

Data Protection Officer

11.8. Inquiries. All inquiries about this Policy or the processing of Personal Data must be submitted to the Company's support team, which forwards them to the Data Protection Officer for review under our established procedure.

11.9. Data Protection Officer. In accordance with local regulations, the Company has appointed a Data Protection Officer whose duties include:

11.9.1. monitoring compliance with our data-protection policies and with applicable data protection laws;

11.9.2. acting as the contact point for the Data Protection Commissioner of Mauritius on processing matters - consultations, investigations, audits, and anything else the Commissioner requires under data protection law;

11.9.3. serving as the focal point for Data Subject complaints and maintaining adequate mechanisms for handling disputes;

11.9.4. support awareness and training initiatives and provide guidance to employees regarding data protection obligations.

Cybersecurity Incident Management

11.10. The Company maintains procedures for identifying, investigating, managing and responding to cybersecurity incidents and data breaches. Where required by law, the Company may notify regulators, affected individuals and other relevant parties.

12. General Provisions

12.1. Automated decision-making and profiling. No decision producing legal or similarly significant effects for you is made by automated means alone. Profiling and automated analysis operate under human oversight and Relevant Legislation, and you retain the right not to be subject to a solely automated decision, including profiling, with such effects.

12.2. Changes to this Policy. We may update this Policy as our operations, legal requirements, or guidance change. The current version and its last-updated date live on the Website. For changes materially affecting your rights or our processing, we may give prominent advance notice and,

where the law requires, seek renewed Consent. Using the Services after the effective date signifies acknowledgement of the update, except where Consent is required.

12.3. Consent at onboarding. We obtain your Consent to this Policy when the business relationship is established, before providing any Services; it may be given electronically. Where the law requires Consent for a specific processing activity or disclosure, we obtain it separately, in the form the law prescribes.

12.4. Cookies and tracking. We use cookies and similar technologies to improve your experience, analyse usage, and personalise content and advertising. The types, purposes, and your preference controls are set out in the Cookie Policy on the Website.

12.5. Governing law. This Policy is governed by the laws applicable to the Company, without prejudice to mandatory data-protection rights you hold under Relevant Legislation in your jurisdiction.

12.6. Prevailing language. Translations that may be available are for convenience only; if one conflicts with the English version, English prevails.

12.7. Severability. If any provision proves invalid, illegal, or unenforceable, the rest stays in full force.

12.8. Third-party websites. The Website and Services may contain links to websites, applications, or services operated by others, e.g. payment provider pages, app stores, or social media. We do not control these third parties and are not responsible for their privacy practices, content, or security. Check their privacy policies before sharing any Personal Data with them.

12.9. Contact. Questions about this Policy or our processing of Personal Data may be sent to:

(a) Email: support@metritax.com
(b) Registered and business address: 4th Floor, Standard Chartered, 19 Bank Street, Cybercity, Ebene 72201, Mauritius.