eurotrader

LEGAL DOCUMENTS / MAURITIUS AND SOUTH AFRICA

Privacy Policy

November 2026

Eurotrade International Ltd
Eurotrade SA (Pty) Ltd

Mauritius and South Africa / English

Privacy Policy

Eurotrade International Ltd and Eurotrade SA (Pty) Ltd

This policy explains how personal information is handled for the Eurotrader website, applications and brokerage and intermediary services. It covers prospective, current and former clients, authorised representatives, beneficial owners and people who contact us. It does not require you to publish private account information or to consent to every use of information.

1 Responsible companies and contact

1.1 Eurotrade International Ltd, registration 197389 GBC, FSC licence GB22201125, is at 3 Emerald Park, Trianon, Quatre Bornes 72257, Republic of Mauritius. It is responsible for processing undertaken for its trading, investment and related account services under applicable Mauritius law, including the Data Protection Act 2017.

1.2 Eurotrade SA (Pty) Ltd, registration K2017223774, FSP 44351, is at 74 Walmer Street, Sydenham, Johannesburg, 2192, South Africa. It is the responsible party for processing undertaken for its South African intermediary service under applicable law, including the Protection of Personal Information Act (POPIA).

1.3 Each company determines the purposes and lawful grounds for processing within its role. A common brand does not make all processing joint or permit unrestricted sharing. Eurotrade SA acts as intermediary for Eurotrade International Ltd; necessary information passes between them for that arrangement subject to the safeguards below.

1.4 Send a privacy enquiry or rights request to compliance@eurotrader.com or support@eurotrader.com, identifying the company and writing Privacy in the subject, or write to its address. The enquiry is directed to the responsible privacy function, including the South African Information Officer or Mauritius data protection contact as applicable. You need not send a password or authentication code.

2 Information we process and its sources

2.1 Information can include identity, date of birth, nationality, contact and residential details, identification documents, tax residence and identifiers, occupation, financial circumstances, source of funds or wealth, beneficial ownership, authority, knowledge and experience, risk information and legal eligibility.

2.2 Account and transaction information can include applications, accepted terms, payment details, account and wallet references, instructions, positions, holdings, confirmations, settlements, balances, correspondence, complaints, security events and verification results. We process only information relevant to the purpose and legal duty concerned.

2.3 Website and device information can include IP address, browser and device characteristics, access times, logs, security identifiers and cookie choices. Optional analytics or marketing tracking follows the cookie controls and applicable consent rules. A device identifier or pseudonymous record can still be personal information.

2.4 Information usually comes from you or your authorised representative. Where lawful and necessary, it can also come from the other contracting company, identity and fraud-check providers, payment or execution providers, custodians, lawful public records, sanctions and public-function screening sources, introducers and regulators. We assess relevance and reliability rather than assuming that a third-party result is correct.

2.5 Special categories, special personal information, criminal-record or biometric information receive the additional protection required by applicable law. We do not treat an ordinary contract acceptance as permission for unrestricted use of such information. Any additional condition or consent needed for a particular verification process must be addressed before that processing.

3 Purposes and lawful grounds

3.1 We process information to assess applications and authority, verify identity and beneficial ownership, perform due diligence, prevent financial crime and meet tax, regulatory, recordkeeping and lawful reporting obligations. The relevant ground is the applicable legal obligation or other lawful condition permitted for the specific processing.

3.2 Necessary processing for an application you request and an accepted contract includes opening and administering accounts, transmitting and executing instructions within each company's role, arranging payments, custody and settlement, providing support, statements and service notices, and handling closure or transfer.

3.3 Where permitted, legitimate interests can support proportionate security, fraud prevention, dispute handling, service quality and management. We consider necessity, your reasonable expectations and the effect on your rights; a commercial interest alone does not justify any use of information. Applicable objection rights remain available.

3.4 Consent is used where required, including relevant optional electronic marketing, non-essential tracking or specific additional processing. Consent must be sufficiently informed, specific and

voluntary. You can withdraw it for the future without affecting the lawfulness of processing already undertaken or a separate legal duty.

3.5 We may need information to establish, exercise or defend legal claims, protect vital interests in an applicable emergency, or comply with a lawful official request. We do not rely on every listed ground for every activity. Ask us to explain the ground and purpose for processing that concerns you.

3.6 Required application or compliance information must be distinguished from optional information. If necessary information is not provided or cannot be verified, we may be unable to open, maintain or service the account. Refusing optional marketing does not itself prevent access to the core service.

4 Recipients and confidentiality

4.1 Relevant recipients can include the other company involved in your account, authorised representatives, banks and payment processors, verification and financial-crime providers, execution and custody providers, technology and hosting processors, professional advisers, auditors, regulators and competent authorities. Disclosure is limited to the purpose, authority and information needed.

4.2 Service providers processing on a company's instructions must be subject to appropriate confidentiality, security and processing requirements. A provider independently deciding its own purposes may have separate legal duties and privacy information. Account disclosures identify the actual service arrangement where required.

4.3 Group affiliation, an introducer relationship or a request from a third party does not by itself authorise disclosure. We verify representative authority and assess legal requests. A proposed business transfer requires lawful grounds, appropriate safeguards and any notice required; it does not permit unrelated exploitation of account information.

5 International transfers

5.1 The South Africa to Mauritius intermediary arrangement and international providers can require transfers or remote access across borders. The receiving country may have different privacy laws. We assess the transfer and use a condition permitted by applicable law, such as adequate protection, binding contractual safeguards, a necessary contractual transfer or valid consent where that is the appropriate ground.

5.2 Transfers of South African personal information must satisfy POPIA section 72 and other applicable conditions. Transfers under Mauritius law must satisfy the Data Protection Act's international-transfer requirements. Routine service sharing is not justified solely by a general acceptance checkbox.

5.3 You may request information about the recipients, destinations and safeguards relevant to your information, subject to lawful confidentiality and security limits. We do not publish private provider agreements or other clients' information to answer such a request.

6 Security and retention

6.1 Appropriate technical and organisational measures are used in light of the nature, purpose and risks of processing. Access is limited by role and need. No electronic service is entirely risk-free. Protect credentials, use available security controls and report suspected compromise promptly.

6.2 We assess suspected security incidents, take appropriate mitigation and notify the relevant authority and affected persons when the applicable legal conditions require it. There is no universal notification deadline imposed by this policy across all jurisdictions and incidents.

6.3 Information is retained only for as long as needed for the purpose and applicable legal, regulatory, tax, financial-crime or dispute requirements. Periods vary by record and company; some duties continue after account closure. Retention is not unlimited merely because information may be useful. At the end of the applicable period, records are deleted, securely destroyed or irreversibly anonymised as appropriate.

6.4 A legal hold or mandatory retention duty can limit deletion. Where lawful, we explain the basis and restrict further processing to what is necessary. Backups and archives follow controlled retention and access arrangements rather than immediate deletion from every copy.

7 Your rights and automated processing

7.1 Depending on the law and circumstances, you may request confirmation and access, correction, deletion, restriction or cessation, object to particular processing, withdraw consent and exercise any applicable portability or automated-decision rights. These rights can be subject to lawful exceptions, competing rights and verification.

7.2 We may request proportionate evidence of identity or authority before disclosing or changing a record. We respond within applicable legal periods, explain a refusal or limitation where required, and identify available complaint routes. Any lawful charge must be explained before it applies; a privacy request is not an opportunity to impose an undisclosed brokerage fee.

7.3 Electronic screening and risk tools can assist verification, security and eligibility. Where a decision with significant effects is made solely by automated means, the applicable legal conditions and safeguards must be met. You may ask about such a decision and seek human review or challenge where the law provides that right. Accepting this policy is not a blanket waiver of those safeguards.

7.4 Keep material information current and tell us if a record appears inaccurate. Requests concerning records held independently by a bank or other provider may also need to be directed to that provider. We assist with identifying the relevant responsibility within our service.

8 Marketing cookies and external services

8.1 Optional direct marketing is handled according to applicable law and your preferences, separately from necessary account notices. Use an unsubscribe facility or contact us to object or withdraw relevant consent. A withdrawal does not prevent essential security, transaction or legal communications.

8.2 The Cookie Policy explains website storage, categories and choices. Changing a legal-page company view does not provide tracking consent. External websites and independently operated services have their own policies; check them before supplying information.

8.3 Our services are intended for eligible adults. If we learn that information about a child has been supplied without a lawful basis, we assess the appropriate restriction, verification and deletion or legally required retention. We do not use it to market trading to children.

9 Complaints and changes

9.1 Contact the relevant company first where practicable so that we can investigate. You may also complain to the Mauritius Data Protection Office at https://dataprotection.govmu.org/ or the South African Information Regulator at https://inforegulator.org.za/complaints/, according to the processing and jurisdiction involved. A company complaint is not a waiver of your right to approach an authority.

9.2 Material changes to processing are communicated as required by law. The published version and date identify this notice; website publication alone does not create consent for a new incompatible purpose. Ask us for clarification or a copy of the notice relevant to your account.