OFFICIAL PUBLIC POLICY

Global Privacy Notice

Document information	Details
Status	OFFICIAL PUBLIC POLICY
Effective date	25 August 2026
Version	1.0
Legal entity	Ergenso Ltd
Registration and licence	Company No. HV00726497 | Mwali Licence No. BFX2026056

This document is issued by Ergenso Ltd and applies from the effective date above. Where it refers to the Client Portal, a Current Schedule or a product-specific disclosure, the version provided for the relevant account, product and jurisdiction applies.

Q.1 Controller

Ergenso Ltd is responsible for the personal data described in this notice when it determines why and how the data is used. Country-specific notices may identify an additional local entity, representative or data protection contact. The current privacy contact channel is published on the website and Client Portal.

Q.2 Data collected

- Identity, age, nationality, tax residence, address, contact details, government identifiers and verification documents.
- Employment, business, income, assets, liabilities, source of funds and wealth, objectives, knowledge, experience and risk profile.
- Account, order, position, payment, bank, card-token, wallet, device, IP, location, cookie, authentication and security data.
- Calls, chats, emails, support, advice, complaint, consent and marketing records.
- Sanctions, PEP, adverse-media, fraud and legally obtained public or third-party information.

Q.3 Purposes and legal bases

We use data to assess and onboard clients; provide accounts, execution, payments and advice; verify identity; prevent financial crime; manage risk; communicate; improve and secure services; handle complaints; keep records; enforce agreements; and comply with legal obligations. Depending on the jurisdiction, the legal basis may be contract, legal obligation, legitimate interests, public-interest financial-crime prevention, consent or another lawful basis.

Q.4 Recipients

Data may be shared on a need-to-know basis with group entities, banks, payment processors, identity and screening providers, trading platforms, liquidity or execution providers, cloud and communications providers, professional advisers, auditors, insurers, regulators, courts, law enforcement, fraud-prevention networks and a purchaser in a legitimate business transaction. We do not sell personal data in the ordinary meaning of selling client lists for money.

Q.5 International transfers

Because Ergenso operates internationally, data may be processed outside the country where it was collected. Where transfer restrictions apply, Ergenso will use a lawful mechanism and supplementary safeguards appropriate to the data and destination, such as adequacy decisions, approved contractual clauses, binding arrangements or consent where valid. Clients may request information about the applicable safeguard where the law provides that right.

Q.6 Retention

Data is kept only as long as needed for the stated purposes, legal limitation periods, disputes, security and regulatory obligations. Core KYC and transaction records are normally retained for at least five years after the relationship or transaction and longer where law, litigation hold or regulatory direction requires. Data is then deleted, anonymised or securely archived.

Q.7 Rights

Depending on location, a person may request access, correction, deletion, restriction, objection, portability, withdrawal of consent, information about transfers, review of certain automated decisions, or complaint to a privacy authority. Rights are subject to legal exceptions, including AML confidentiality, legal privilege, fraud prevention and record-retention duties. Identity may be verified before a request is fulfilled.

Q.8 Automated processing and profiling

Ergenso may use automated indicators to assess fraud, sanctions, onboarding, product access, risk, marketing relevance and account security. Material decisions should include human review where required. Ergenso will provide additional information and a challenge route where applicable law grants that right.

Q.9 Security and breaches

Ergenso uses administrative, technical and physical controls proportionate to the risk, including access control, authentication, encryption where appropriate, logging, vendor oversight, backup and incident response. No system is completely secure. We will notify affected persons and authorities of a breach where required by law.

Q.10 Children

Services are not intended for minors or persons below the applicable legal age. If such data is identified, Ergenso may close the application and delete it unless retention is legally required.

Q.11 Regional addendum

Ergenso applies country-specific privacy terms where required by the EU GDPR, UK GDPR and PECR, Brazil LGPD, Australia Privacy Act and APPs, Canada federal and provincial privacy laws, Japan APPI, Singapore PDPA, Hong Kong PDPO and other applicable laws. Cookie and direct-marketing controls follow local consent requirements.