

ASTEO LUXEMBOURG S.A.

PRIVACY POLICY

Effective Date: 1 May 2025 | Version 1.0

Data Controller	ASTEO LUXEMBOURG S.A.
Registered Address	25B Boulevard Royal, L-2449 Luxembourg
CSSF Registration	P00000438
LEI Code	222100L7BX1XCBJHH958
Supervisory Authority	Commission de Surveillance du Secteur Financier (CSSF), Luxembourg
DPO Contact	dpo@asteo.eu
Legal Basis	GDPR (EU) 2016/679 Luxembourg Data Protection Law of 1 August 2018

1. Introduction

This Privacy Policy explains how ASTEO LUXEMBOURG S.A. ("Asteo", "we", "us", "our") collects, uses, stores, and protects your personal data when you access our website, register for an account, or use our investment services. Asteo is a regulated investment firm authorised and supervised by the Commission de Surveillance du Secteur Financier (CSSF) in Luxembourg under registration number P00000438.

We are committed to processing your personal data in full compliance with Regulation (EU) 2016/679 ("GDPR"), the Luxembourg Data Protection Law of 1 August 2018, and all applicable financial services legislation including MiFID II.

2. Scope of This Policy

This Policy applies to:

- Prospective clients who register or complete our onboarding forms
- Active and former clients using Asteo's trading platforms
- Visitors to our website and mobile applications
- Counterparties, agents, and service providers whose personal data we process

It covers personal data processed across all Asteo services including CFD trading, foreign exchange (forex), cryptocurrency instruments, portfolio management, and investment advisory services.

3. Data We Collect

3.1 Identity & Contact Data

- Full legal name, date of birth, nationality, country of residence
- Government-issued identification (passport, national ID card)
- Residential address and proof of address documentation
- Email address, telephone number

3.2 Financial & KYC Data

- Source of funds and source of wealth declarations
- Annual income, net worth, and financial standing information
- Bank account details and payment instrument information
- Tax identification numbers (TIN) and FATCA/CRS declarations
- Credit and solvency assessments (where applicable)

3.3 Trading & Account Data

- Trade history: orders, executions, positions, and transaction records for CFDs, forex pairs, and crypto assets
- Account balances, margin levels, profit and loss statements
- Trading preferences, risk appetite assessments, and suitability questionnaire responses
- Communications with our dealing desk, compliance, and support teams

3.4 Technical & Usage Data

- IP addresses, browser type and version, operating system, device identifiers
- Login timestamps, session duration, platform activity logs
- Cookies and tracking technologies (see Section 12)

3.5 Sensitive Data

We do not deliberately collect sensitive personal data (e.g. health, biometric, or political data) unless strictly required by applicable law (e.g. disability-related trading accommodations). Where such data is provided voluntarily, it will be processed under explicit consent.

4. Purposes and Legal Bases for Processing

Purpose	Legal Basis (GDPR Art.)
Client onboarding & KYC / AML verification	Art. 6(1)(c) – Legal obligation (AMLD, MiFID II)
Account management and order execution	Art. 6(1)(b) – Performance of contract
MiFID II suitability & appropriateness assessments	Art. 6(1)(c) – Legal obligation

Regulatory reporting (EMIR, MiFIR, FATCA/CRS)	Art. 6(1)(c) – Legal obligation
Risk management and margin monitoring	Art. 6(1)(b) – Performance of contract; Art. 6(1)(f) – Legitimate interest
Fraud prevention and security monitoring	Art. 6(1)(f) – Legitimate interest
Direct marketing and service communications	Art. 6(1)(a) – Consent (withdrawable at any time)
Legal claims and dispute resolution	Art. 6(1)(f) – Legitimate interest
Improving our platforms and services	Art. 6(1)(f) – Legitimate interest

5. Data Retention

We retain your personal data for the following minimum periods, in line with our regulatory obligations:

Data Category	Retention Period
Client identity & KYC documents	10 years from end of business relationship (AMLД)
Trade records and transaction data	7 years from transaction date (MiFID II / MiFIR)
Communications relating to client orders	5 years (MiFID II Art. 16)
EMIR trade repository data	10 years from trade date
Tax-related records (FATCA/CRS)	7 years
Marketing consent records	Until consent is withdrawn + 3 years
Website usage / technical logs	13 months

After applicable retention periods, data is securely deleted or anonymised. We may retain data for longer where required by a court order, regulatory investigation, or active litigation.

6. Third-Party Sharing

6.1 Regulated Disclosures

We are legally required to share your data with:

- CSSF (Luxembourg) and, where applicable, Consob (Italy) under cross-border passporting obligations

- Financial intelligence units and law enforcement in connection with AML/CFT obligations
- EMIR trade repositories and MiFIR transaction reporting systems
- Tax authorities under FATCA and CRS automatic exchange of information frameworks

6.2 Service Providers (Data Processors)

We engage trusted third parties who process data strictly on our behalf under GDPR-compliant Data Processing Agreements:

- Technology and platform providers (trading system infrastructure)
- KYC/AML identity verification providers
- Payment processors and banking partners
- Cloud hosting and data storage providers
- Cybersecurity and fraud monitoring services
- Legal, audit, and compliance advisors

6.3 No Sale of Data

Asteo does not sell, rent, or trade your personal data to third parties for their own marketing purposes.

7. International Data Transfers

Asteo is headquartered in Luxembourg (EEA). Where we transfer personal data outside the EEA, we implement appropriate safeguards as required by GDPR Chapter V, including:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Transfers to countries benefiting from an EU adequacy decision
- Binding Corporate Rules where applicable

A list of third countries to which we transfer data and the applicable safeguards is available upon request from our DPO.

8. Your Rights

Under GDPR, you have the following rights in respect of your personal data:

Right	Description
Access (Art. 15)	Request a copy of the personal data we hold about you
Rectification (Art. 16)	Request correction of inaccurate or incomplete data
Erasure (Art. 17)	Request deletion (subject to legal retention obligations)
Restriction (Art. 18)	Request restriction of processing in specific circumstances
Data Portability (Art. 20)	Receive your data in a structured, machine-readable format
Objection (Art. 21)	Object to processing based on legitimate interests or for direct marketing

Withdraw Consent	Withdraw any consent given at any time, without affecting prior processing
-------------------------	--

To exercise any of these rights, contact our Data Protection Officer at dpo@asteo.eu or in writing to our registered address. We will respond within 30 days. You also have the right to lodge a complaint with the CSSF or the Commission Nationale pour la Protection des Données (CNPDP) in Luxembourg at www.cnpdp.lu.

9. Data Security

Asteo implements appropriate technical and organisational measures to protect your personal data, including:

- AES-256 encryption at rest and TLS 1.3 in transit for all data transfers
- Role-based access controls and least-privilege principles
- Multi-factor authentication for all staff system access
- Regular penetration testing and vulnerability assessments
- ISO 27001-aligned information security management practices
- Incident response procedures compliant with GDPR Art. 33-34 (72-hour breach notification)

In the event of a personal data breach that is likely to result in risk to your rights and freedoms, we will notify you promptly and without undue delay.

10. Children

Our services are exclusively available to persons aged 18 years or over. We do not knowingly collect personal data from minors. If we become aware that data has been collected from a person under 18, we will delete it immediately. If you believe we hold data relating to a child, please contact dpo@asteo.eu.

11. Automated Decision-Making and Profiling

Asteo may use automated systems for:

- AML/KYC risk scoring during onboarding (subject to human review for significant outcomes)
- Suitability and appropriateness scoring under MiFID II (with human oversight)
- Margin call calculations and automated risk management

Where automated decisions produce legal or similarly significant effects, you have the right to request human review. Contact compliance@asteo.eu to exercise this right.

12. Cookies and Tracking Technologies

Our website and trading platform use cookies and similar technologies. Categories include:

Cookie Type	Purpose / Legal Basis
-------------	-----------------------

Strictly Necessary	Session management, security, platform function — no consent required
Performance / Analytics	Platform improvement and usage analytics — consent required
Functional	Remembering user preferences — consent required
Marketing / Tracking	Personalised content (not used for third-party ad targeting) — consent required

You may manage cookie preferences through our Cookie Consent Manager available on our website. Withdrawing consent for non-essential cookies does not affect platform functionality. For full details, see our Cookie Policy.

13. Cryptocurrency and Blockchain Considerations

Where you trade crypto asset instruments through Asteo's platform, please note:

- Blockchain transactions are inherently pseudonymous and, depending on the instrument structure, certain transaction data may be permanently recorded on public ledgers
- On-chain data associated with your wallet addresses may not be erasable due to the immutable nature of blockchain technology; this limitation will be explained prior to trading
- Asteo complies with the Travel Rule under FATF/EU TFR Regulation for applicable crypto transfers

14. Updates to This Policy

We may update this Privacy Policy from time to time to reflect changes in law, regulatory requirements, or our business practices. We will notify you of material changes via email or a prominent notice on our platform at least 30 days before the changes take effect. The current version is always available on our website. Continued use of our services after the effective date constitutes acceptance of the revised policy.

15. Contact Us

For all privacy-related enquiries, requests, or complaints:

Data Protection Officer	dpo@asteo.eu
Compliance Department	compliance@asteo.eu
Postal Address	ASTEIO LUXEMBOURG S.A., 25B Boulevard Royal, L-2449 Luxembourg
Supervisory Authority	CNPD Luxembourg — www.cnpd.lu
Italian Supervisory Authority	Garante per la protezione dei dati personali — www.garanteprivacy.it