AML & CTF
POLICY

Version Control

Document Owner: **EyeFG Ltd**

Version No.	Approval Date:	Revisions/Changes:
1.0	*2025*	*Creation of Policy*

Table of Contents

Contents

1. Introduction

This Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy outlines EyeFG Ltd's commitment to preventing financial crime, ensuring alignment with the applicable AML/CFT framework of the Republic of Cyprus, and maintaining the integrity of its platform.

Although EyeFG Ltd does not engage in financial services, investment activities, or fund management, it acknowledges the potential risks associated with payment processing, fraud, and identity misuse. This policy establishes our framework for risk mitigation, monitoring, and compliance in line with Cypriot standards and applicable international best practice (including FATF recommendations).

2. Regulatory Context

EyeFG Ltd is a Cyprus-based e-commerce education company incorporated in the Republic of Cyprus (company registration number: HE481186). While EyeFG Ltd is not licensed as a financial institution, and may not in all cases fall within the statutory definition of an "obliged entity" under Cypriot AML legislation, it voluntarily implements AML/CTF measures that are consistent with the Cyprus AML/CFT framework. Where EyeFG Ltd does fall within the scope of the relevant legislation, it will comply with all binding obligations in full.

Our approach is aligned with, and where applicable subject to:

- **Prevention and Suppression of Money Laundering Activities Law of 2007, as amended (Law 188(I)/2007), including relevant subsidiary legislation and the implementation of EU Anti-Money Laundering Directives.**
- **Relevant EU Regulations and UN Security Council sanctions (restrictive measures) as implemented and enforced in the Republic of Cyprus.**
- **Guidance, circulars and expectations issued by competent authorities, including the Unit for Combating Money Laundering (MOKAS – Cyprus FIU) and, where applicable, supervisory authorities depending on the nature of the Company's activities.**
- **Regulation (EU) 2016/679 (GDPR) and Cyprus Law 125(I)/2018, and guidance issued by the Office of the Commissioner for Personal Data Protection.**
- The competent authority for receiving and analysing Suspicious Transaction Reports (STRs) in Cyprus is MOKAS (Cyprus FIU).

3. Risk Assessment & Mitigation

3.1 Business Risk Profile

Given the nature of EyeFG Ltd's business as an e-commerce education platform, the primary financial crime risks include:

- **Fraudulent Transactions** – Potential misuse of stolen or unauthorised payment methods or false identities for purchasing services.
- **Money Laundering via Refund Abuse** – Attempts to exploit the refund process to layer or integrate illicit funds.
- **Affiliate and Referral Fraud** – Abuse of partnerships, influencers, or referral incentives for illegitimate gains or to disguise beneficial ownership of funds.

3.2 Risk Mitigation Measures

To address these risks, EyeFG Ltd applies a risk-based approach consistent with Law 188(I)/2007/Law 188(I)/2007 principles, including:

- **Customer Due Diligence (CDD)** – Identification and, where applicable, verification of customers and partners based on risk.
- **Payment Screening** – Monitoring transactions for unusual patterns (e.g. multiple purchases with different cards, IP mismatches, high-risk jurisdictions).
- **Refund Policy Controls** – Clear and strictly enforced refund rules to prevent abuse; refunds are generally returned to the original payment method where possible.
- **Transaction Monitoring** – Periodic reviews of payments and other activity for red flags indicating potential money laundering, terrorist financing, fraud, or sanctions breaches.

4. Know Your Customer (KYC) & Customer Due Diligence (CDD)

4.1 Identification & Verification

While EyeFG Ltd does not directly operate as a bank or investment firm, it recognises the importance of KYC/CDD. Consistent with Law 188(I)/2007/Law 188(I)/2007 concepts of CDD and Enhanced Due Diligence (EDD), EyeFG Ltd applies proportionate checks, in particular to:

- **High-value or high-risk customers** (e.g. bulk purchases, unusual payment patterns, customers from higher-risk jurisdictions).

- **Introducing partners, affiliates and influencers** who promote EyeFG Ltd's services and may receive commission or revenue share.
- **Customers requesting excessive, repeated, or unusual refunds** relative to their profile.

Depending on the risk, EyeFG Ltd may request:

- Full name, contact details and country of residence.
- Copies of a valid government-issued ID and, where relevant, proof of address.
- Additional information on **source of funds** and **source of wealth** for higher-risk relationships.

4.2 Third-Party Verification

Payment transactions are processed through PCI-compliant third-party providers and payment service providers (PSPs) that maintain their own AML/CFT, fraud detection, and security controls, including:

- AI-driven or rules-based fraud prevention tools.
- Strong customer authentication (e.g. 3-D Secure or similar).
- Geolocation, IP, device fingerprinting, and velocity checks.

EyeFG Ltd conducts due diligence on key PSPs and service providers, and where appropriate relies on their controls, consistent with the concepts of reliance on third parties under Law 188(I)/2007/Law 188(I)/2007, without abdicating its own responsibility.

5. Monitoring & Reporting Suspicious Activity

5.1 Internal Monitoring

EyeFG Ltd monitors transactions and user activity for indicators that may suggest money laundering, terrorist financing, or fraud, such as:

- Multiple purchases using different payment methods, identities, or devices that appear linked.
- Frequent chargebacks, disputes, or refund requests inconsistent with normal customer behaviour.
- Affiliate or referral activity with sudden, unexplained spikes or patterns that do not match typical marketing performance.
- Use of high-risk jurisdictions or sanctioned countries, where identified through PSP screening or internal checks.

Where red flags are identified, EyeFG Ltd may:

- Delay or decline transactions.
- Request additional information or documentation from the customer.
- Restrict or terminate access to services.
- Escalate the case internally to the designated compliance function.

5.2 Reporting Obligations

Where EyeFG Ltd is, or becomes, a "reporting person" under Law 188(I)/2007, it will comply with all statutory reporting and record-keeping obligations, including:

- **Internal escalation** of suspicious activity to the designated **Money Laundering Reporting Officer (MLRO)** or Chief Compliance Officer (CCO).
- **Assessment of suspicion** – the MLRO/CCO assesses internal reports to determine whether there are reasonable grounds to suspect money laundering, terrorist financing, or proliferation financing.
- **External reporting to MOKAS – where suspicion is confirmed, submission of a Suspicious Transaction Report (STR) or other report as required, to the Unit for Combating Money Laundering (MOKAS) in Cyprus, in the manner and within the time limits prescribed by law.**
- **Cooperation with authorities – Eye FG Ltd will cooperate with the MOKAS and any other competent authorities (e.g. law enforcement, regulators) in lawful investigations, subject to data protection requirements and legal privilege where applicable.**

Where performing full CDD may risk tipping-off a customer, EyeFG Ltd will follow the approach envisaged in Law 188(I)/2007 Regulations (e.g. filing an STR without completing CDD, where appropriate). (Fium Cyprus)

6. Data Protection & Record Keeping

EyeFG Ltd recognises that AML/CFT compliance must be balanced with data protection obligations under the Data Protection Act 2017 (GDPR and Cyprus Law 125(I)/2018) and, where applicable, the EU GDPR.

6.1 Record Keeping

Subject to its status under Law 188(I)/2007, EyeFG Ltd aims to apply the standards of record retention specified for reporting persons in Cypriot legislation, including:

Maintaining books and records with respect to customers and transactions for **at least seven (7) years** after the business relationship ends.

- Keeping records for individual transactions (domestic and international) for **at least seven (7) years** after completion of the transaction.

- Retaining copies of suspicious transaction reports and supporting documentation for **at least seven (7) years** from the date of reporting.

Records may include:

- Identification and verification documents.
- Transaction logs and payment records.
- Internal alerts, investigations and decisions.
- Training records related to AML/CFT.

6.2 Data Protection

- Personal data collected for AML/CFT purposes is **limited to what is necessary**, processed lawfully, and retained no longer than required for legal or legitimate business purposes.
- Data is stored securely, with access restricted to authorised personnel only (e.g. compliance, finance, designated management).
- Appropriate technical and organisational measures (e.g. encryption, access controls, secure transmission) are implemented to protect personal data against loss, unauthorised access, or misuse.

7. Training & Compliance Oversight

- All relevant employees (including customer support, finance, marketing/affiliate management, and management) receive **AML/CTF awareness training**, tailored to their role and the risk profile of the company.
- Training covers, at a minimum:
    - Basic concepts of money laundering and terrorist financing.
    - Internal red flags and typologies relevant to e-commerce and online education.
    - Procedures for escalating suspicious activity to the MLRO/CCO.
    - Confidentiality and anti–tipping-off requirements.
- Training is refreshed **at least annually** or more frequently where required by changes in law, guidance, or risk exposure.

The Compliance / Legal function is responsible for:

- Maintaining and updating this Policy.
- Ensuring staff are trained and aware of their responsibilities.
- Monitoring the effectiveness of AML/CFT controls.

The Policy is reviewed at least once a year, or more frequently in response to changes in the Cypriot legal framework, MOKAS/CySEC (where applicable)/Central Bank of Cyprus (where applicable) guidance, or EyeFG Ltd’s business model.

8. Governance & Responsibility

8.1 Board and Senior Management

The Board of Directors and senior management of EyeFG Ltd have ultimate responsibility for ensuring that:

- EyeFG Ltd identifies, assesses, and mitigates its money laundering, terrorist financing and fraud risks.
- Adequate policies, procedures, systems and controls are established and maintained.
- Sufficient resources (including qualified staff and technology) are allocated to AML/CFT compliance.

8.2 Chief Compliance Officer (CCO) / Money Laundering Reporting Officer (MLRO)

EyeFG Ltd appoints a designated senior person (CCO and/or MLRO) to:

- Oversee implementation of this Policy and related procedures.
- Receive and review internal reports of suspicious activity.
- Decide whether an STR should be filed with the MOKAS and ensure that any such reporting is done in compliance with Law 188(I)/2007 and Law 188(I)/2007 Regulations.
- Act as the primary contact point with regulators and competent authorities in Cyprus on AML/CFT matters.

8.3 Operational Teams

- **Customer Support & Finance Teams:**
  - Monitor customer interactions and transactions.
  - Flag and escalate unusual or suspicious activity according to internal procedures.
  - Ensure refund practices are consistent with AML/CFT controls.
- **Marketing & Affiliate Management:**
  - Conduct basic due diligence on affiliates and partners, especially those in higher-risk markets.
  - Monitor affiliate performance for anomalies or potential misuse.

9. Conclusion

While EyeFG Ltd is not a traditional financial institution, it is committed to maintaining a safe, transparent, and compliant business environment in line with the AML/CFT framework of the Republic of Cyprus.

Through risk-based controls, proportionate KYC/CDD, transaction monitoring, record keeping and cooperation with the Cypriot Financial Intelligence Unit and other competent authorities where required, EyeFG Ltd seeks to proactively mitigate risks associated with fraud, money laundering, terrorist financing, and other financial crime.

This Policy will be reviewed at least annually and updated as necessary to remain effective and aligned with evolving Cypriot legislation, regulatory expectations, and industry best practice.