RATİN TEKNOLOJİ VE YÖNETİM DANIŞMANLIK HİZMETLERİ TİCARET LİMİTED ŞİRKETİ

Document Name: Internal AML & KYC Compliance Policy Manual Version: 1.0 (2026) Status: Strictly Confidential / Official Use Only

Section 1: Introduction and Mission Statement

1.1 Background RATİN TEKNOLOJİ VE YÖNETİM DANIŞMANLIK HİZMETLERİ TİCARET LİMİTED ŞİRKETİ (the “Company”), operating in the fields of digital marketing, influencer management, and YouTube revenue orchestration, recognizes the critical importance of preventing financial crimes. As the digital economy grows, we remain dedicated to ensuring our platform and services are not utilized for illicit activities.

1.2 Commitment to Compliance The Company is strictly committed to adhering to the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) laws of the Republic of Turkey, specifically the regulations governed by the **Financial Crimes Investigation Board (MASAK)**. Furthermore, our internal policies are aligned with the international standards and recommendations set by the **Financial Action Task Force (FATF)**.

1.3 Mission Statement Our mission is to provide a transparent and secure financial ecosystem for content creators and global brands. We maintain a **Zero Tolerance** policy toward money laundering, tax evasion, and the financing of terrorism. By implementing robust KYC (Know Your Customer) and KYB (Know Your Business) protocols, we protect our partners, our reputation, and the integrity of the international financial system.

1.4 Policy Review This policy is a dynamic document and is subject to annual review or updates whenever there is a significant change in local or international regulations.

Section 2: Governance and Compliance Officer

2.1 Compliance Leadership The Board of Directors of **RATİN TEKNOLOJİ** has the ultimate responsibility for overseeing the AML/CTF framework. To ensure daily operational adherence, the Board has appointed a **Dedicated Compliance Officer (DCO)** who acts as the primary liaison between the Company and regulatory bodies such as **MASAK**.

2.2 Role of the Compliance Officer The Dedicated Compliance Officer is empowered with the authority and resources necessary to manage the Company’s compliance program. The key responsibilities include:

- **Policy Development:** Creating, maintaining, and updating AML and KYC procedures in line with evolving Turkish and international laws.
- **Transaction Oversight:** Reviewing flagged transactions and conducting internal investigations into suspicious financial behavior.
- **Reporting:** Preparing and submitting **Suspicious Activity Reports (SARs)** to the Financial Crimes Investigation Board (MASAK) without delay.
- **Audit Coordination:** Acting as the main point of contact for external auditors and bank compliance teams during annual reviews.

2.3 Independence and Access To maintain integrity, the Compliance Officer operates with full independence and has unrestricted access to all customer files, transaction data, and company records. Any attempt to interfere with the Compliance Officer’s duties is strictly prohibited under the Company’s code of conduct.

2.4 Board Oversight The DCO provides quarterly reports to the Board of Directors, detailing:

- The number of new clients onboarded and their risk levels.
- Any identified "Red Flags" or blocked transactions.
- Updates on any changes in Turkish or global AML regulations.

Section 3: Customer Due Diligence (CDD) and KYC Procedures

3.1 Overview The Company implements a mandatory **Know Your Customer (KYC)** and **Know Your Business (KYB)** procedure for all new relationships. No transaction shall be processed, and no business relationship shall be established until the identity of the client is verified to the satisfaction of the Compliance Officer.

3.2 Tiered Identification Levels

- **Level 1: Natural Persons (Individual Clients & Influencers)** For individual content creators and freelancers, the Company collects:
    - **Identity Verification:** A high-resolution color scan of a valid Passport or National ID card.
    - **Proof of Residence:** A utility bill (electricity, water, or gas) or bank statement issued within the last 3 months.
    - **Liveness Check:** Where applicable, a digital "selfie" or video verification to ensure the document belongs to the applicant.
- **Level 2: Legal Entities (Corporate Clients & Agencies)** For brands, marketing agencies, and corporate partners, the Company collects:
    - **Certificate of Incorporation:** Official registration documents from the relevant Trade Registry.
    - **Articles of Association:** The company's governing documents.
    - **Proof of Business Address:** Lease agreement or utility bill in the company's name.
    - **Authorized Signatory List:** Documents (such as the *İmza Sirküleri* in Turkey) identifying the individuals authorized to sign on behalf of the company.
    - **Tax Identity:** Valid Tax Certificate (Vergi Levhası) or VAT registration.
- **Level 3: Ultimate Beneficial Ownership (UBO)** In accordance with international transparency standards, the Company must identify the natural person(s) who ultimately own or control the legal entity.
    - The Company requires a shareholding structure chart for any corporate client.
    - Identification and verification are mandatory for any individual holding **25% or more** of the shares or voting rights, directly or indirectly.

3.3 Ongoing Due Diligence The Company does not only verify clients at the time of onboarding. We perform "Ongoing Monitoring" to ensure that the transactions and activities are consistent with the client's stated business profile and source of funds.

3.4 Refusal of Relationship The Company will refuse to open an account or will terminate an existing relationship if:

- The applicant provides false or suspicious documentation.
- The identity of the UBO cannot be clearly established.
- The applicant is found on any global sanctions or high-risk watchlists.

Section 4: Risk-Based Approach (RBA)

4.1 Policy Overview The Company applies a Risk-Based Approach (RBA) to ensure that AML and CTF efforts are commensurate with the risks identified. This allows the Company to allocate resources more effectively by focusing on high-risk areas.

4.2 Customer Risk Categorization Every client is assigned a risk rating during the onboarding process, which is reviewed periodically:

- **Low Risk:**
  - Publicly traded companies on recognized stock exchanges.
  - Regulated financial institutions.
  - Clients with long-term, transparent business histories in low-risk jurisdictions.
  - *Procedure:* Simplified Due Diligence (SDD).
- **Medium Risk:**
  - Standard corporate clients and established digital marketing agencies.
  - Influencers with stable and consistent revenue streams from verified platforms (e.g., Google/YouTube).
  - *Procedure:* Standard Customer Due Diligence (CDD).
- **High Risk:**
  - **Politically Exposed Persons (PEPs):** Individuals holding prominent public positions and their immediate family members.
  - Clients from jurisdictions identified by the FATF as having strategic AML/CTF deficiencies.
  - Complex corporate structures with no clear commercial rationale.
  - Businesses involving high-volume cash-intensive activities.
  - *Procedure:* **Enhanced Due Diligence (EDD)**.

4.3 Enhanced Due Diligence (EDD) Measures For clients categorized as High Risk, the Company applies stricter oversight, including:

- Obtaining additional information on the **Source of Wealth** and **Source of Funds**.
- Requiring senior management approval (CEO level) to establish or continue the business relationship.
- More frequent monitoring of transactions and regular updates of KYC documentation (e.g., every 6 months instead of annually).

4.4 Jurisdictional Risk The Company maintains a list of "High-Risk Jurisdictions" based on the FATF Grey/Black lists and internal assessments. Any transaction or client originating from these regions undergoes immediate manual review by the Compliance Officer.

Section 5: Sanctions Screening

5.1 Sanctions Compliance Policy The Company maintains a zero-tolerance policy regarding transactions involving individuals, entities, or jurisdictions subject to international sanctions. Screening is performed at the time of onboarding and is continuously repeated against updated global databases.

5.2 Global Screening Lists All clients, authorized signatories, and Ultimate Beneficial Owners (UBOs) are screened against the following primary lists:

- **United Nations Security Council Sanctions (UNSC):** The consolidated list of individuals and entities subject to sanctions measures imposed by the UN.
- **OFAC (Office of Foreign Assets Control):** The United States' Specially Designated Nationals (SDN) and Blocked Persons lists.
- **EU Consolidated List:** Financial sanctions imposed by the European Union.
- **UK HM Treasury List:** Consolidated list of financial sanctions targets in the UK.

- **Local MASAK Lists:** Domestic lists provided by the Turkish Financial Crimes Investigation Board.

5.3 Screening Frequency and Automation

- **Pre-Onboarding:** No client is approved without a successful screening result.
- **Ongoing Monitoring:** The Company utilizes automated screening tools to re-scan the existing client database whenever international sanction lists are updated.
- **Manual Intervention:** Any "Potential Match" or "False Positive" is manually reviewed by the Compliance Officer to confirm identity before any funds are moved.

5.4 Target Jurisdictions and Prohibited Regions The Company does not establish business relationships or facilitate transactions originating from or destined for high-risk jurisdictions currently under comprehensive sanctions (e.g., North Korea, Iran, etc.) or regions identified as having significant strategic deficiencies in their AML/CTF frameworks by the FATF.

5.5 Handling Sanction Matches In the event of a confirmed sanctions match (True Match):

- The business relationship is immediately terminated or the onboarding application is rejected.
- Any existing funds or assets related to the match are frozen in accordance with legal requirements.
- A report is filed with **MASAK** and other relevant authorities within 24 hours.

Section 6: Transaction Monitoring

6.1 Continuous Monitoring Strategy The Company performs ongoing monitoring of all business relationships and transactions to ensure they are consistent with the client's known business profile, risk level, and source of funds. Monitoring is conducted through a combination of automated systems and manual oversight.

6.2 Identifying Unusual Activity (Red Flags) The Compliance Officer and relevant department heads are trained to identify "Red Flags" specific to the digital marketing and influencer industry, including:

- **Inconsistent Volume:** Sudden, large transfers that do not align with the historical revenue of a YouTube channel or marketing campaign.
- **Structuring (Smurfing):** Multiple small transactions conducted just below reporting thresholds to avoid detection.
- **Third-Party Payments:** Funds originating from or being sent to individuals or entities that have no clear contractual relationship with the client.
- **High-Risk Jurisdictions:** Transactions involving banks or partners in countries known for high levels of financial crime or lack of AML oversight.
- **Rapid Pass-Through:** Funds that are deposited and immediately withdrawn or transferred to another party without any clear commercial or service-based reason.

6.3 Investigation Process When a transaction is flagged as unusual:

1. **Holding Period:** The transaction may be temporarily placed on hold for further review.

2. **Request for Information (RFI):** The Company will request supporting documentation from the client, such as invoices, service agreements, or screenshots of YouTube analytics/dashboards to verify the legitimacy of the revenue.
3. **Determination:** If the client provides a valid commercial explanation and supporting evidence, the transaction is cleared. If the activity remains suspicious, it is escalated for potential reporting.

6.4 Post-Transaction Review On a quarterly basis, the Compliance Officer conducts a retrospective review of a sample of transactions to identify any long-term trends or systemic risks that may require updates to the Company's risk-based approach.

Section 7: Suspicious Activity Reporting (SAR)

7.1 Reporting Obligation In accordance with Law No. 5549 on Prevention of Laundering Proceeds of Crime, the Company is legally obligated to report any transaction or attempt to conduct a transaction that is suspected to be related to money laundering, terrorist financing, or other criminal activities.

7.2 Internal Reporting Process

- **Identification:** If any employee identifies a transaction or behavior that matches the "Red Flags" mentioned in Section 6, they must immediately notify the **Compliance Officer** via an internal memo.
- **Confidentiality:** Employees are strictly prohibited from "tipping off" the client. The client must not be informed that their activity is being investigated or reported.

7.3 Evaluation by the Compliance Officer The Compliance Officer will investigate the internal report by:

- Reviewing the client’s KYC profile and transaction history.
- Analyzing the source of funds and the purpose of the transaction.
- Determining whether the suspicion is grounded in fact.

7.4 Filing a SAR with MASAK If the Compliance Officer determines that a transaction is suspicious, a **Suspicious Activity Report (SAR)** will be filed through the official MASAK online reporting system (EMIS.ONLINE) or via the prescribed legal forms.

- **Timeline:** Reports must be submitted immediately, and in any case, within **10 working days** from the date the suspicion arose.
- **No Immunity for Failure to Report:** The Company recognizes that failure to report suspicious activities can lead to severe administrative and criminal penalties for both the individuals involved and the Company.

7.5 Cooperation with Authorities The Company maintains a policy of full cooperation with MASAK, the Turkish Ministry of Treasury and Finance, and law enforcement agencies. This includes responding to information requests and providing access to requested transaction logs or customer files during official investigations.

Section 8: Record Keeping and Data Retention

8.1 Legal Obligation for Retention In accordance with Turkish AML/CTF regulations and Law No. 5549, **RATİN TEKNOLOJİ** maintains a comprehensive record-keeping system. All documents related to customer identification and transactions are retained for a minimum period of **10 years** from the date of the transaction or the termination of the business relationship.

8.2 Types of Records Retained The Company ensures the archiving of the following:

- **KYC/CDD Records:** Copies of passports, national IDs, trade registry gazettes, tax certificates, and UBO declaration forms.
- **Transaction Records:** Invoices, service agreements (specifically for influencer and YouTube services), bank transfer confirmations, and payment receipts.
- **Compliance Records:** Internal investigation files, screening logs (Sanctions/PEPs), and copies of any Suspicious Activity Reports (SARs) filed.
- **Communication Records:** Official correspondence with clients and regulatory authorities regarding compliance matters.

8.3 Format and Security of Records Records are maintained in both digital and, where necessary, physical formats:

- **Digital Archiving:** Records are stored in secure, encrypted cloud environments with restricted access to authorized compliance personnel only.
- **Data Integrity:** Regular backups are performed to ensure that records are protected against loss, damage, or unauthorized alteration.

8.4 Accessibility for Authorities The Company ensures that all records are organized and indexed in a manner that allows for timely retrieval. Upon an official request from **MASAK**, judicial authorities, or our banking partners (during audit/review), the Company is committed to providing the requested documents within the legally prescribed timeframe.

8.5 Data Privacy Compliance While maintaining these records for AML purposes, the Company also adheres to the **Law on the Protection of Personal Data (KVKK)** in Turkey. Records are used strictly for legal and regulatory compliance and are not shared with third parties for commercial purposes.

Section 9: Employee Training and Awareness

9.1 Importance of Training The Company recognizes that the effectiveness of its AML/CTF framework depends on the awareness and expertise of its staff. Therefore, we implement a mandatory and ongoing training program for all employees, especially those in "front-line" roles such as Sales, Finance, and Client Onboarding.

9.2 Training Objectives The primary goals of our training sessions are to ensure that employees:

- Understand the legal requirements under Turkish Law No. 5549 (**MASAK**).
- Can identify potential **"Red Flags"** and suspicious behavior in the digital marketing and influencer industry.
- Know the internal procedures for reporting suspicious activities to the Compliance Officer.
- Understand the legal consequences of non-compliance and "Tipping-Off."

9.3 Frequency of Training

- **Induction Training:** All new hires must complete an AML/KYC orientation within their first month of employment.
- **Annual Refresher:** Existing staff undergo a mandatory annual refresher course to stay updated on new money laundering methods and changes in international sanction lists.
- **Ad-hoc Updates:** If there is a major change in regulations (e.g., new FATF guidelines), a special training brief is provided to all relevant personnel.

9.4 Training Content Our curriculum includes, but is not limited to:

- **The Definition of Money Laundering:** Exploring the stages of placement, layering, and integration.
- **KYC/KYB Best Practices:** How to verify documents and spot forged IDs.
- **Digital Risks:** Specific risks associated with crypto-assets, digital wallets, and cross-border influencer payments.
- **Confidentiality:** Maintaining the secrecy of SAR filings and protecting customer data.

9.5 Record of Training The Company maintains a log of all completed training sessions, including the dates, names of participants, and test results (if applicable). These records are made available to banking partners and regulatory auditors upon request to demonstrate our "Culture of Compliance."

Final Approval & Execution

*This Internal AML Policy has been reviewed and approved by the Board of Directors of **RATİN TEKNOLOJİ VE YÖNETİM DANIŞMANLIK HİZMETLERİ TİCARET LİMİTED ŞİRKETİ**.*

Authorized Signatory:
Erkan Aygun CEO / Director
Date: February 23, 2026