Политика противодействия отмыванию денег (AML) и финансированию терроризма (CTF)

1. Общие положения

Компания **PLAYMAG FZCO**, зарегистрированная в **IFZA** (International Free Zone Authority) с регистрационным номером DSO-FZCO-26329 под надзором **Dubai Silicon Oasis Authority**, предоставляет услуги юридическим лицам, включая прием платежей от физических лиц в счет оплаты товаров и услуг.

Политика направлена на:

- Предотвращение использования услуг компании для отмывания денег, финансирования терроризма или уклонения от санкционных режимов.
- Соблюдение законодательства РФ, стран СНГ и ОАЭ в области AML/CTF.
- Защиту репутации компании и ее клиентов.

2. Законодательная основа

В Российской Федерации:

- Федеральный закон № 115-ФЗ "О противодействии легализации доходов, полученных преступным путем, и финансированию терроризма".
- Постановление Правительства РФ № 667 "О предоставлении информации о клиентах финансовым учреждениям".
- Процедуры внутреннего финансового мониторинга банков-партнеров.

В странах СНГ:

- Национальные законы об AML/CTF в странах присутствия клиентов, например, Казахстан, Беларусь и другие.

В ОАЭ:

- Федеральный закон № 20 от 2018 года "О противодействии отмыванию денег".
- Руководство Dubai Silicon Oasis Authority по AML/CTF.
- Рекомендации FATF.

3. Ответственность руководства и Compliance Officer

3.1. Роль руководства Высшее руководство компании:

- Утверждает внутренние регламенты по AML/CTF.
- Назначает Compliance Officer и контролирует его деятельность.
- Определяет стратегию управления рисками.

3.2. Обязанности Compliance Officer

- Внедрение процедур идентификации клиентов и мониторинга транзакций.
- Анализ и обработка подозрительных операций.
- Взаимодействие с отделом финансового мониторинга банка-партнера в РФ и FIU в ОАЭ.

4. Процедуры идентификации клиентов (KYC) и проверки операций

4.1. Идентификация клиентов Компания обязана собирать и проверять данные юридических лиц, включая:

- Учредительные документы, адрес регистрации, данные о бенефициарах.
- Информацию о назначении платежей от физических лиц.

4.2. Проверка данных

- Проверка клиентов на соответствие международным санкционным спискам (OFAC, EU Sanctions List).
- Использование автоматизированных систем для анализа рисков.

4.3. Классификация рисков клиентов Клиенты классифицируются по уровням риска:

- Низкий риск: стабильные и прозрачные юридические лица.
- Средний риск: компании, оперирующие в странах с умеренным риском.
- Высокий риск: нерезиденты, клиенты из высокорисковых юрисдикций.

5. Мониторинг транзакций

5.1. Автоматизированный мониторинг Компания использует системы для анализа транзакций, включая:

- Мониторинг платежей физических лиц на соответствие профилю клиента.
- Идентификацию необычных операций (например, нестандартно крупные платежи).

5.2. Риск-ориентированный подход Транзакции оцениваются с учетом:

- Страны происхождения средств.
- Суммы и частоты платежей.
- Типа клиента (юридическое или физическое лицо).

6. Обработка подозрительных операций

6.1. Взаимодействие с отделом финансового мониторинга банка-партнера (РФ) При выявлении подозрительных операций компания направляет данные в отдел финансового мониторинга банка-партнера, который оценивает риски и принимает решение о дальнейших действиях.

6.2. Сообщение в регулирующие органы

- В РФ: подозрительные операции передаются через банк-партнер.
- В ОАЭ: информация направляется в FIU (Financial Intelligence Unit).

7. Санкционная политика

Компания обязана:

- Проводить мониторинг клиентов и транзакций по санкционным спискам.
- Отклонять операции, связанные с санкционными лицами или юрисдикциями.

8. Обучение сотрудников

- Новые сотрудники проходят обучение в течение 30 дней с момента найма.
- Ежегодные курсы по AML/CTF проводятся для всего персонала.
- Особое внимание уделяется работе с банком-партнером и международным законодательством.

9. Хранение данных

- Документы клиентов и транзакции хранятся не менее 5 лет после завершения деловых отношений.
- Хранение данных соответствует стандартам безопасности и конфиденциальности.

10. Аудит и внутренние проверки

- Ежегодно проводится внутренний аудит системы AML/CTF.
- Compliance Officer готовит отчет для руководства и регуляторов.

11. Особенности работы с юридическими лицами и физическими лицами в роли плательщиков

- Прием платежей осуществляется только от физических лиц, использующих законные источники средств.
- Для юридических лиц проводится расширенная проверка структуры собственности и назначения платежей.

12. Обновление политики

Политика пересматривается ежегодно с учетом изменений в законодательстве РФ, стран СНГ и ОАЭ.

Дата утверждения: 23 декабря 2024 года. Дубай, ОАЭ.

ANTI-MONEY LAUNDERING (AML) AND COUNTER-TERRORIST FINANCING (CTF) POLICY

1. General Provisions

The company **PLAYMAG FZCO**, registered with **IFZA** (International Free Zone Authority) with registration number DSO-FZCO-26329 under the supervision of **Dubai Silicon Oasis Authority**, provides services to legal entities, including accepting payments from individuals for goods and services.

The policy aims to:

- Prevent the use of the company's services for money laundering, terrorist financing, or evasion of sanctions regimes.
- Ensure compliance with the legislation of the Russian Federation, CIS countries, and the UAE.

2. Legislative Framework

In the Russian Federation:

- Federal Law No. 115-FZ "On Counteracting the Legalization of Criminal Proceeds and the Financing of Terrorism."
- Government Resolution No. 667 "On Providing Information About Clients to Financial Institutions."
- Procedures for internal financial monitoring by partner banks.

In the CIS countries:

- National AML/CTF laws in countries where clients are present, such as Kazakhstan, Belarus, etc.

In the UAE:

- Federal Law No. 20 of 2018 "On Anti-Money Laundering and Combatting the Financing of Terrorism."
- Guidelines from Dubai Silicon Oasis Authority on AML/CTF.
- FATF recommendations.

3. Responsibilities of Management and Compliance Officer

3.1. Role of Management Senior management of the company:

- Approves internal regulations on AML/CTF.
- Appoints the Compliance Officer and oversees their activities.
- Defines risk management strategy.

3.2. Responsibilities of the Compliance Officer

- Implementing customer identification and transaction monitoring procedures.
- Analyzing and processing suspicious transactions.
- Interacting with the financial monitoring department of the partner bank in Russia and FIU in the UAE.

4. Customer Identification (KYC) and Transaction Verification Procedures

4.1. Customer Identification The company must collect and verify data from legal entities, including:

- Founding documents, registration address, and beneficiary information.
- Information on the purpose of payments from individuals.

4.2. Data Verification

- Clients are checked against international sanctions lists (OFAC, EU Sanctions List).
- Automated systems are used for risk analysis.

4.3. Client Risk Classification Clients are classified by risk levels:

- Low risk: stable and transparent legal entities.
- Medium risk: companies operating in countries with moderate risk.
- High risk: non-residents, clients from high-risk jurisdictions.

5. Transaction Monitoring

5.1. Automated Monitoring The company uses systems to analyze transactions, including:

- Monitoring payments from individuals to ensure they match the client's profile.
- Identifying unusual transactions (e.g., unusually large payments).

5.2. Risk-Based Approach Transactions are assessed considering:

- The country of origin of funds.
- The amount and frequency of payments.
- The type of client (legal or individual).

6. Handling Suspicious Transactions

6.1. Interaction with the financial monitoring department of the partner bank (Russia) Upon detecting suspicious transactions, the company forwards the data to the financial monitoring department of the partner bank, which assesses the risks and decides on further actions.

6.2. Reporting to Regulatory Authorities

- In Russia: suspicious transactions are passed through the partner bank.
- In the UAE: information is submitted to the FIU (Financial Intelligence Unit).

7. Sanctions Policy

The company is required to:

- Monitor clients and transactions against sanctions lists.
- Reject transactions involving sanctioned persons or jurisdictions.

8. Staff Training

- New staff undergo training within 30 days of employment.
- Annual AML/CTF courses are conducted for all staff.
- Special focus on working with the partner bank and international legislation.

9. Data Retention

- Client documents and transaction records are retained for at least 5 years after the end of business relationships.
- Data storage complies with security and confidentiality standards.

10. Audit and Internal Controls

- An internal audit of the AML/CTF system is conducted annually.
- The Compliance Officer prepares reports for management and regulators.

11. Specifics of Working with Legal Entities and Individuals as Payers

- Payments are accepted only from individuals using lawful sources of funds.
- Legal entities undergo enhanced checks for ownership structure and payment purposes.

12. Policy Updates

The policy is reviewed annually, taking into account changes in the legislation of Russia, CIS countries, and the UAE.

Approval date: December 23, 2024. Dubai, UAE.