ALPHA MAESTRO

Политика ПОД/ФТ

Версия 1.6

Оператор

Закрытое акционерное общество «Диджитал Эссет Инвестментс»
Лицензия №103 (Серия ВА №0118)
г. Бишкек

Политика противодействия легализации (отмыванию) преступных доходов и финансированию террористической деятельности (ПОД/ФТ)

Настоящая Политика раскрывает основные публичные правила Оператора в сфере противодействия финансированию террористической деятельности и легализации (отмыванию) преступных доходов (ПФТД/ЛПД, ПОД/ФТ) при оказании услуг оператора обмена виртуальных активов. Полная программа внутреннего контроля является внутренним документом ограниченного доступа.

1. Правовая основа

1.1. Оператор соблюдает законодательство Кыргызской Республики о противодействии финансированию террористической деятельности и легализации (отмыванию) преступных доходов, Закон КР «О виртуальных активах», а также требования уполномоченных органов, включая Финнадзор, применимые к лицензированным VASP.

1.2. Оператор применяет KYC, риск-ориентированный подход, мониторинг операций, хранение сведений и взаимодействие с Государственной службой финансовой разведки при Министерстве финансов КР (ГСФР).

1.3. Политика применяется ко всем Пользователям и операциям в Сервисе и читается совместно с Публичной офертой и Условиями использования.

2. Основные термины

• Идентификация — установление идентификационных данных Пользователя (и при необходимости бенефициарного владельца / представителя).
• Верификация (KYC) — проверка идентификационных данных и документов.
• Источник происхождения средств (SoF) — законный источник денежных средств и/или виртуальных активов, используемых в операции.
• ПДЛ (PEP) — публичное должностное лицо (национальное, иностранное, международной организации), а также близкие родственники и доверенные лица.
• Подозрительная операция — операция, в отношении которой имеются основания полагать о связи с легализацией преступных доходов, финансированием терроризма / экстремизма либо иными противоправными действиями.
• Комплаенс-офицер — уполномоченный сотрудник Оператора по ПОД/ФТ.
• Санкционный перечень — сводные перечни КР, СБ ООН и иные списки, применяемые Оператором по внутренним правилам (включая OFAC/ЕС при необходимости).

3. Надлежащая проверка клиента (KYC)

3.1. До оказания услуг и в течение отношений Оператор проводит идентификацию и верификацию. Сервис предназначен для обслуживания физических лиц, достигших 18 лет.

Отдельная процедура идентификации юридических лиц в Сервисе не применяется. Статус индивидуального предпринимателя (при наличии) указывается Пользователем в анкете ПОД/ФТ и учитывается при оценке риска; отдельный «пакет документов юрлица» при этом не формируется.

3.2. В отношении Пользователя устанавливаются, в частности: ФИО, дата рождения, гражданство, данные документа, удостоверяющего личность, адрес, контакты, статус ПДЛ, цель отношений и сведения об источнике средств.

3.3. Пользователь заполняет электронную анкету ПОД/ФТ и обязан предоставлять точные сведения. При недостоверности Оператор вправе запросить пояснения, приостановить операции или прекратить отношения.

3.4. Оператор привлекает независимого KYC-провайдера: Didit (Didit Identity Spain, S.L. / Didit Identity, Inc.; обработка сессий, как правило, в ЕС). Провайдер в рамках процедуры идентификации может запрашивать документы, удостоверяющие личность, в том числе:

• паспорт гражданина Кыргызской Республики / ID-карту гражданина КР;
• паспорт иностранного гражданина;
• вид на жительство в Кыргызской Республике — при необходимости.

Иной тип документа может быть запрошен / принят, если он допускается настройками процедуры Didit и достаточен для идентификации. Инициируя верификацию, Пользователь соглашается на передачу необходимых данных провайдеру, в том числе трансгранично.

3.5. Идентификация личности проводится дистанционно через Didit (Didit Identity Spain, S.L. / Didit Identity, Inc.). В рамках сессии, как правило, выполняются: получение изображений документа, удостоверяющего личность; сверка лица (face match); проверка liveness. Предоставление бумажного оригинала, нотариально заверенной копии или апостиля для прохождения стандартной KYC-сессии не требуется, если Оператор дополнительно не запросил иные документы в рамках усиленной проверки / SoF.

3.6. Оператор подтверждает принадлежность Расчётного счёта Пользователю. Платежи от третьих лиц не принимаются.

3.7. Оператор вправе запросить иные документы и сведения, необходимые для надлежащей проверки клиента (включая подтверждение адреса и документы об источнике средств в случаях, предусмотренных настоящей Политикой).

4. Порог запроса документов об источнике происхождения средств

4.1. Оператор запрашивает документы и/или сведения, подтверждающие источник происхождения денежных средств и/или виртуальных активов, если выполняется хотя бы одно из условий:

• сумма одной операции (Заявки) равна или превышает 2 700 000 (два миллиона семьсот тысяч) кыргызских сомов либо эквивалент 32 000 (тридцати двух тысяч) долларов США или евро — по курсу / котировке, применяемой Оператором на момент оценки;
• совокупный объём операций Пользователя за календарный месяц равен или превышает указанный порог;
• Пользователь относится к категории повышенного риска (в том числе ПДЛ) — независимо от суммы;
• имеются признаки необычности / подозрительности, дробления сумм, несоответствия профилю либо иные индикаторы программы внутреннего контроля.

4.2. До получения и удовлетворительной проверки документов SoF Оператор вправе приостановить исполнение, ограничить лимиты либо отказать в операции.

4.3. Оператор вправе запросить SoF и ниже порога п. 4.1 при необходимости управления

рисками.

4.4. Порог может быть изменён при изменении закона, требований регулятора или внутренней оценки рисков. Актуальная редакция публикуется в Сервисе.

5. Документы, подтверждающие источник средств

В качестве подтверждения могут запрашиваться, в частности:

• выписка по банковскому счёту / карте;
• справка о доходах / заработной плате, трудовой договор;
• налоговая декларация, документы о предпринимательской деятельности;
• договор купли-продажи имущества, дарения, наследственные документы;
• документы о движении виртуальных активов на иных платформах;
• иные документы, позволяющие установить законность происхождения средств.

Документы на иностранном языке по требованию Оператора предоставляются с переводом. Непредоставление либо недостаточность документов — основание для отказа в операции и/или прекращения отношений.

6. Риск-ориентированный подход

6.1. Оператор присваивает уровень риска и применяет меры пропорционально риску.

6.2. К повышенному риску относятся, в частности: ПДЛ и связанные лица; клиенты из высокорискованных юрисдикций; уклонение от предоставления сведений; операции, не соответствующие профилю.

6.3. К клиентам повышенного риска применяются усиленные меры: обязательный SoF, расширенный мониторинг, согласование существенных операций комплаенс-офицером / руководством.

7. Мониторинг операций

7.1. Операции проверяются по программе внутреннего контроля, в том числе с использованием автоматизированных / ручных методов и при необходимости внешних AML/KYT-инструментов.

7.2. Признаки подозрительности включают, в частности: несоответствие профилю; дробление сумм; отказ от идентификации / ложные сведения; использование миксеров / анонимных инструментов / высокорискованных адресов; совпадения по санкционным перечням.

7.3. При выявлении признаков комплаенс-офицер фиксирует сведения, вправе приостановить операцию и инициирует взаимодействие с ГСФР.

8. Санкции, приостановление и отказ

8.1. Оператор безотлагательно замораживает операции и/или средства лиц из применимых санкционных перечней — в случаях и порядке, установленных законом, без предварительного уведомления, если иное не предусмотрено обязательными нормами.

8.2. Оператор приостанавливает подозрительные операции до завершения проверки и вправе запросить подтверждающие документы.

8.3. Отказ в отношениях / операции либо приостановление по основаниям ПОД/ФТ не являются нарушением обязательств Оператора перед Пользователем.

9. Запрещённые операции

Не принимаются / подлежат отказу, в частности:

• платежи и поступления от третьих лиц;
• операции со средствами незаконного происхождения;
• операции в интересах лиц из санкционных перечней либо связанные с запрещённой деятельностью;
• обход идентификации, использование подставных лиц, заведомо ложные сведения.

10. Взаимодействие с ГСФР

10.1. При выявлении подозрительной операции Оператор через комплаенс-офицера направляет сообщение в ГСФР безотлагательно, но не позднее одного рабочего дня с момента выявления подозрительной операции или обстоятельства, подлежащего обязательному контролю, — в порядке и по формам, установленным законодательством КР.

10.2. Сведения о подозрительных операциях конфиденциальны и не разглашаются Пользователю и третьим лицам иначе как в случаях, прямо предусмотренных законом.

11. Хранение и обучение

11.1. Сведения и документы по идентификации, анкетам, операциям и проверкам хранятся не менее 5 лет с даты прекращения отношений либо последней операции — в зависимости от того, какой срок наступает позднее, если закон не устанавливает более длительный срок.

11.2. Оператор обеспечивает защиту сведений и актуализацию внутренних правил.

11.3. Сотрудники, участвующие в мерах ПОД/ФТ, проходят обучение с периодичностью, установленной внутренними правилами (не реже одного раза в год — если иное не предусмотрено законом).

12. Контакты

Комплаенс: compliance@alphamaestro.io.

Актуальная редакция Политики размещается в Сервисе.