

Политика ПФПД/ЛПД и ЗСК (Знай своего клиента) Платформы VexPay	AML/CFT and KYC Policy of the VexPay Platform
Дата вступления в силу: 5 августа 2026 года	Effective Date: August 5, 2026
«Ограничение ответственности»	Disclaimer
Настоящий документ определяет общие принципы и ключевые аспекты деятельности проекта VexPay в сфере соблюдения требований ПФПД/ЛПД и идентификации клиентов (комплаенс). Он не является исчерпывающим документом правового характера и не заменяет собой полный текст применимого законодательства или внутренних операционных инструкций. Дополнительные меры в сфере ПФПД/ЛПД и идентификации клиентов могут осуществляться третьими лицами — контрагентами, агентами или поставщиками услуг, привлекаемыми VexPay, в случае участия таких лиц в оказании услуг проекту VexPay или его клиентам. VexPay сохраняет за собой ответственность за обеспечение соблюдения любыми такими третьими лицами минимальных стандартов, установленных настоящей Политикой и применимым законодательством.	This document reflects the general framework and key aspects of the KYC/AML compliance activities of the VexPay project. It is not an exhaustive legal document and does not replace the full text of applicable laws or internal operational manuals. Additional KYC/AML measures may be carried out by third parties – counterparties, agents, or service providers engaged by VexPay – when such parties are involved in the provision of services to VexPay or its clients. VexPay remains responsible for ensuring that any such third parties comply with the minimum standards set forth in this Policy and applicable legislation.
1. Цель и сфера применения 1.1. Настоящая Политика разработана в соответствии с требованиями Закона Кыргызской Республики «О противодействии финансированию террористической деятельности и легализации (отмыванию) преступных доходов» № 87 от 6 августа 2018 года с соответствующими изменениями (далее — «Закон о ПФПД/ЛПД»), а также международными стандартами Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ). 1.2. Политика определяет внутренние процедуры, направленные на предотвращение использования Платформы VexPay (далее — «Платформа») в целях легализации (отмывания) доходов, полученных преступным путем, финансирования террористической и экстремистской деятельности, финансирования распространения оружия массового уничтожения, а также	1. Purpose and Scope 1.1. This Policy is developed in accordance with the requirements of the Law of the Kyrgyz Republic “On Combating the Financing of Criminal Activity and Legalization (Laundering) of Proceeds from Crime” No. 87 of 6 August 2018, as amended (hereinafter – the “AML Law”), as well as international standards of the Financial Action Task Force (FATF). 1.2. The Policy defines internal procedures aimed at preventing the use of the VexPay Platform (hereinafter – the “Platform”) for the purposes of legalization (laundering) of criminal proceeds, financing of terrorist and extremist activities, financing of the proliferation of weapons of mass destruction, and financing of organized groups or criminal communities. 1.3. This Policy is binding on all departments and employees of the Platform, as well as on counterparties (correspondent banks, payment

финансирования организованных групп или преступных сообществ. 1.3. Настоящая Политика является обязательной для исполнения всеми подразделениями и сотрудниками Платформы, а также контрагентами (банками-корреспондентами, платежными агентами, поставщиками услуг в сфере криптоактивов) в той мере, в какой это допускается договорами и применимым законодательством.	agents, crypto-asset service providers) to the extent permitted by contracts and applicable law.
2. Термины и определения 2.1. Термины и определения, используемые в настоящей Политике, применяются в значениях, установленных в Статье 1 Закона о ПФПД/ЛПД, включая, помимо прочего, следующие: • Виртуальный актив — цифровое выражение стоимости, которое может являться объектом гражданских прав, в том числе использоваться в качестве средства платежа, обмена, сбережения или инвестиционного актива. • Бенефициарный владелец — физическое лицо, которое в конечном счете (через цепочку владения или контроля) прямо или косвенно владеет клиентом или контролирует его, либо физическое лицо, от имени или в интересах которого совершается операция (сделка). • Публичное должностное лицо (ПДЛ) — иностранное ПДЛ, национальное ПДЛ и ПДЛ международных организаций в значениях, определенных Законом о ПОД/ФТ. • Страны высокого риска — государства и территории, которые не применяют или применяют в недостаточной степени международные стандарты ПФПД/ЛПД, а также оффшорные зоны. • Санкционный перечень — перечень физических и юридических лиц, групп и организаций, в отношении которых имеются сведения об их причастности к преступной деятельности, формируемый в соответствии со Статьей 12 Закона о ПФПД/ЛПД.	2. Definitions 2.1. Terms and definitions used in this Policy are as set forth in Article 1 of the AML Law, including but not limited to: • Virtual asset – a digital representation of value that may be the object of civil rights, including as a means of payment, exchange, savings or investment asset. • Beneficial owner – an individual who ultimately (through a chain of ownership or control) directly or indirectly owns or controls a client, or an individual on whose behalf a transaction is conducted. • Politically Exposed Person (PEP) – foreign PEP, domestic PEP, and PEP of international organizations as defined by the AML Law. • High-risk countries – states and territories that do not apply or insufficiently apply international AML/CFT standards, as well as offshore zones. • Sanctions List – the list of individuals, legal entities, groups and organizations against which there is information about involvement in criminal activity, formed under Article 12 of the AML Law.
3. Категории риска 3.1. Платформа применяет риск-ориентированный подход во всех процедурах ПФПД/ЛПД.	3. Risk Categories 3.1. The Platform implements a risk-based approach in all AML/CFT procedures.

3.2. Для Клиентов устанавливаются следующие уровни риска:

Уровень риска	Критерии
Высокий	– Клиенты, являющиеся ПДЛ, члены их семей и близкие соратники; – Клиенты, являющиеся резидентами или зарегистрированными в Странах высокого риска; – Клиенты, использующие технологии анонимизации (миксеры, тумблеры, конфиденциальные криптовалюты); – Клиенты, осуществляющие перевод средств на/с нерегулируемых криптобирж или онлайн-казино; – Юридические лица со сложной структурой собственности (номинальные акционеры, трасты).
Стандартный	– Физические лица, осуществляющие переводы с очевидной законной целью, не являющиеся ПДЛ и не происходящие из юрисдикций высокого риска; – Юридические лица, зарегистрированные в юрисдикциях с надлежащим контролем в сфере ПОД/ФТ и прозрачной структурой собственности.
Низкий	– Регулируемые финансовые организации (банки, брокеры) из стран с сопоставимыми стандартами ПОД/ФТ; – Публичные компании, акции которых торгуются на бирже, подпадающие под требования о раскрытии информации; – Государственные корпорации.

3.2. The following risk levels are established for Clients:

Risk Level	Criteria
High	– Clients who are PEPs, their family members and close associates; – Clients resident or registered in High-risk countries; – Clients using anonymizing technologies (mixers, tumblers, privacy coins); – Clients transferring funds to/from unregulated crypto exchanges or online casinos; – Legal entities with complex ownership structures (nominee shareholders, trusts).
Standard	– Individuals conducting transfers with a clear legitimate purpose, not PEPs, not from high-risk jurisdictions; – Legal entities registered in jurisdictions with adequate AML/CFT controls and transparent ownership.
Low	- Regulated financial institutions (banks, brokers) from countries with comparable AML/CFT standards; – Publicly traded companies subject to disclosure requirements; – Government-owned corporations.

4. Идентификация и верификация Клиентов (KYC)

4.1. Идентификация и верификация Клиента должны быть завершены до установления деловых отношений (приема на обслуживание).

4.2. Минимальный перечень данных для идентификации физического лица:

- Полное имя (ФИО);
- Дата и место рождения;
- Гражданство;
- Документ, удостоверяющий личность (паспорт, ID-карта);
- Адрес регистрации (фактического проживания);
- Номер телефона, адрес электронной почты.

4.3. Минимальный перечень данных для идентификации юридического лица:

4. Client Identification and Verification (KYC)

4.1. Identification and verification of the Client must be completed **before** establishing a business relationship (onboarding).

4.2. Minimum data for identification of an individual:

- Full name;
- Date and place of birth;
- Nationality;
- Identity document (passport, ID card);
- Registered address (actual residence);
- Phone number, email address.

4.3. Minimum data for identification of a legal entity:

- Full name, registration number, country of incorporation;
- Founding documents (Charter, certificate of incorporation);

• Полное наименование, регистрационный номер, страна инкорпорации; • Учредительные документы (Устав, свидетельство о регистрации); • Зарегистрированный адрес (юридический и фактический); • Сведения о бенефициарных владельцах; • Сведения о руководителе и лицах, уполномоченных подписывать финансовые документы. 4.4. Процедуры верификации: • Установление подлинности предоставленных документов; • Верификация адреса электронной почты и номера телефона; • Сверка данных с официальными реестрами (при их наличии); • Биометрическая верификация (с согласия Клиента).	• Registered address (legal and actual); • Information on beneficial owners; • Information on the director and persons authorized to sign financial documents. 4.4. Verification procedures: • Authentication of documents provided; • Verification of email address and phone number; • Cross-checking against official registers (where available); • Biometric verification (with Client consent).
5. Верификация бенефициарного владельца 5.1. Платформа принимает разумные и доступные меры для идентификации и верификации конечного бенефициарного владельца каждого Клиента, являющегося юридическим лицом. 5.2. Критерии определения бенефициарного владельца: любое физическое лицо, которое прямо или косвенно владеет более чем 25% акций (долей участия) либо иным образом осуществляет контроль над юридическим лицом. 5.3. В отношении Клиентов высокого уровня риска, а также в случае возникновения сомнений в достоверности предоставленных сведений, Платформа вправе запросить дополнительные документы, подтверждающие структуру собственности и источник происхождения средств.	5. Beneficial Owner (UBO) Verification 5.1. The Platform takes reasonable measures to identify and verify the ultimate beneficial owner (UBO) of each Client that is a legal entity. 5.2. UBO criteria – any individual who directly or indirectly owns more than 25% of shares/units or otherwise controls the legal entity. 5.3. For high-risk Clients, or where doubts arise about the accuracy of information, the Platform may request additional documents proving ownership structure and source of funds.

6. Мониторинг операций и направление сообщений о подозрительных операциях 6.1. Платформа осуществляет постоянный мониторинг всех операций Клиентов. 6.2. Сообщение о подозрительной операции (СПО) подлежит обязательному направлению в орган финансовой разведки Кыргызской Республики. Сотрудникам Платформы строго запрещается информировать Клиента или любых третьих лиц о факте направления такого сообщения (запрет на разглашение информации / tipping-off).	6. Transaction Monitoring and Suspicious Activity Reporting 6.1. The Platform continuously monitors all Client transactions. 6.2. Suspicious Transaction Report (STR) must be submitted to the Financial Intelligence Unit (FIU) of the Kyrgyz Republic. Employees of the Platform are strictly prohibited from informing the Client or any third party about the fact of such reporting (tipping-off).
7. Санкционный скрининг (проверка по санкционным перечням) 7.1. Платформа осуществляет проверку всех Клиентов и их контрагентов на предмет наличия в следующих перечнях: • Сводный санкционный перечень Кыргызской Республики (формируемый органом финансовой разведки); • Сводный санкционный перечень Совета Безопасности ООН. 7.2. В случае выявления совпадения (положительного результата проверки) с Санкционным перечнем Платформа обязана: • Незамедлительно заморозить все операции и активы такого лица; • Направить сообщение в орган финансовой разведки; • Запретить прямое или косвенное предоставление любых денежных средств, имущества или услуг такому лицу. 7.3. Управление и хранение замороженных активов осуществляются в соответствии с порядком, установленным Кабинетом Министров Кыргызской Республики. Размораживание активов возможно исключительно после исключения лица из Санкционного перечня либо на основании судебного решения.	7. Sanctions Screening 7.1. The Platform screens all Clients and their counterparties against: • The Consolidated Sanctions List of the Kyrgyz Republic (maintained by the FIU); • The UN Security Council Consolidated Sanctions List. 7.2. Upon a positive match with a Sanctions List, the Platform must: • Immediately freeze all transactions and assets of such person; • Report to the FIU; • Prohibit directly or indirectly providing any funds or services to such person. 7.3. Frozen assets shall be managed and held in accordance with procedures set by the Cabinet of Ministers of the Kyrgyz Republic. Unfreezing is only possible upon removal from the Sanctions List or by court decision.

8. Публичные должностные лица (ПДЛ) 8.1. В отношении ПДЛ, членов их семей и близких соратников применяются усиленные меры надлежащей проверки (УМНП): • Получение письменного разрешения высшего руководства до установления деловых отношений; • Установление источника происхождения состояния (богатства) и источника происхождения денежных средств (SoW/SoF); • Проведение усиленного постоянного мониторинга в течение всего периода деловых отношений. 8.2. Если ПДЛ не предоставляет сведения об источнике происхождения денежных средств или в случае выявления высокого уровня риска, Платформа оставляет за собой право отказать в установлении деловых отношений либо прекратить их.	8. Politically Exposed Persons (PEPs) 8.1. Enhanced Due Diligence (EDD) applies to PEPs, their family members, and close associates: • Obtain written approval from senior management before establishing business relations; • Establish the source of wealth and source of funds (SoW/SoF); • Conduct enhanced ongoing monitoring throughout the business relationship. 8.2. If a PEP fails to provide information on source of funds, or if high risk is identified, the Platform reserves the right to refuse or terminate business relations.
9. Хранение документов и сведений 9.1. Все данные, полученные в ходе процедур КУС/НПК (идентификации, верификации, анкетирования), а также записи об операциях и аналитические отчеты подлежат хранению в течение не менее 5 лет после прекращения деловых отношений или совершения операции. 9.2. Документы и сведения хранятся в защищенной электронной базе данных, обеспечивающей их конфиденциальность, целостность и доступность для проверки надзорными органами и органом финансовой разведки по законному запросу.	9. Record Keeping 9.1. All data obtained during KYC/CDD procedures (identification, verification, questionnaires), as well as transaction records and analytical reports, shall be retained for at least 5 years after the termination of business relations or completion of the transaction. 9.2. Records are stored in a secure electronic database ensuring confidentiality, integrity, and availability for inspection by supervisory authorities and the FIU upon lawful request.
10. Программа внутреннего контроля 10.1. Платформа утверждает и поддерживает в актуальном состоянии Программу внутреннего контроля, включая привлечение квалифицированных сторонних поставщиков решений (сервисов) в сфере КУС/ ПФПД/ЛПД.	10. Internal Control Program 10.1. The Platform adopts and maintains an Internal Control Program, including engagement of qualified third-party KYC/AML decision' providers.

11. Запрещенная деятельность 11.1. Платформа строго запрещает следующее: • Использование неидентифицированных (анонимных) кошельков или предоплаченных карт для совершения любых операций; • Открытие или ведение анонимных счетов либо счетов на вымышленные имена; • Установление корреспондентских отношений с банками-ширмами; • Проведение операций с физическими или юридическими лицами, включенными в санкционные перечни.	11. Prohibited Activities 11.1. The Platform strictly prohibits: • Use of unidentified (anonymous) wallets or pre-paid cards for any transaction; • Opening or maintaining anonymous accounts or accounts under fictitious names; • Establishing correspondent relations with shell banks; • Conducting transactions with individuals or entities on Sanctions Lists.
12. Ответственность и освобождение от ответственности 12.1. Платформа и её сотрудники несут ответственность за неправомерное разглашение сведений о направлении сообщения о подозрительной операции Клиенту или третьим лицам (нарушение запрета на разглашение информации / tipping-off). 12.2. Платформа не несет гражданско-правовой или иной ответственности за ущерб, причиненный Клиенту в результате: • Замораживания активов / приостановления операций во исполнение требований законодательства в сфере ПФПД/ЛПД; • Отказа в установлении или прекращения деловых отношений; • Отказа в выполнении, приостановления или задержки проведения операции; • Действий, совершенных добросовестно во исполнение требований Закона о ПФПД/ЛПД.	12. Liability and Safe Harbor 12.1. The Platform and its employees shall be liable for unlawful disclosure of a suspicious transaction report to the Client or third parties (tipping-off). 12.2. The Platform shall not bear civil or other liability for damage caused to a Client as a result of: • Freezing of assets/transactions in compliance with AML/CFT requirements; • Refusal to establish or termination of business relations; • Refusal to execute, suspension, or delay of a transaction; • Actions taken in good faith reliance on the AML Law.
13. Привлечение третьих лиц 13.1. VexPay может привлекать сторонних поставщиков услуг, контрагентов, агентов или партнеров (например, банки-корреспонденты, платежные процессоры, кастодианы криптоактивов, поставщики услуг по	13. Third-Party Involvement 13.1. VexPay may engage third-party service providers, counterparties, agents, or partners (e.g., correspondent banks, payment processors, crypto-asset custodians, identity verification

верификации личности) для выполнения определенных функций в сфере КҮС/ПФПД/ЛПД либо для содействия в оказании услуг Клиентам. 13.2. В случае привлечения таких третьих лиц ими могут осуществляться дополнительные меры в сфере КҮС/ ПФПД/ЛПД, включая, помимо прочего, верификацию личности, санкционный скрининг, мониторинг операций и направление сообщений о подозрительных операциях. 13.3. VexPay сохраняет за собой ответственность за обеспечение того, чтобы любое третье лицо, действующее от его имени или оказывающее услуги под брендом VexPay либо по его поручению, соблюдало стандарты, которые являются как минимум такими же строгими, как стандарты, установленные настоящей Политикой, а также соблюдало применимое законодательство и нормативные правовые акты в сфере ПФПД/ЛПД. 13.4. VexPay включает в договоры положения, обязывающие такие третьи лица соблюдать конфиденциальность, оказывать содействие при проведении аудита, а также незамедлительно сообщать о любой подозрительной деятельности или выявленных совпадениях с Санкционными перечнями.	vendors) to perform certain KYC/AML functions or to facilitate the provision of services to Clients. 13.2. When such third parties are involved, additional KYC/AML measures may be carried out by them, including but not limited to identity verification, sanctions screening, transaction monitoring, and suspicious activity reporting. 13.3. VexPay remains responsible for ensuring that any third party acting on its behalf or providing services under VexPay’s brand or instructions adheres to standards at least as stringent as those set forth in this Policy and complies with applicable AML/CFT laws and regulations. 13.4. VexPay shall include contractual provisions requiring such third parties to maintain confidentiality, cooperate with audits, and promptly report any suspicious activities or matches with Sanctions Lists.
--	---