

Информация о принципах противодействия отмыванию денежных средств (AML) и финансированию терроризма (CTF)

1. Общая информация

Политика противодействия отмыванию денежных средств и финансированию терроризма (далее — «Политика») направлена на предотвращение и минимизацию потенциальных рисков вовлечения Pilot Innovation (далее — «Компания») в любую незаконную деятельность.

Для соблюдения как международных, так и национальных требований Компания внедряет эффективные внутренние процедуры и механизмы для предотвращения отмывания денежных средств, финансирования терроризма, торговли наркотиками и людьми, распространения оружия массового уничтожения, коррупции и взяточничества, а также для реагирования на любые формы подозрительной активности со стороны Пользователей.

«Отмывание денежных средств (легализация доходов, полученных преступным путем)» понимается в соответствии со статьей 299 Уголовного кодекса Польши от 6 июня 1997 года.

«Финансирование терроризма» понимается в соответствии со статьей 165а Уголовного кодекса Польши от 6 июня 1997 года.

Настоящая Политика не должна толковаться как исчерпывающий перечень всех политик, процедур и контрольных мер, применяемых Компанией для предотвращения отмывания денежных средств, финансирования терроризма и иных незаконных действий.

2. Обязанности Компании

2.1 Обязанное лицо в Польше

PILOT INNOVATION SP. Z O.O. является обязанным субъектом в соответствии с Законом Польши от 1 марта 2018 года о противодействии отмыванию денежных средств и финансированию терроризма (Dz.U. 2018, поз. 723, с последующими изменениями), а также иными применимыми нормативными актами.

Надзорный орган

Компания находится под надзором Генерального инспектора финансовой информации (GIIF), который является компетентным органом в Польше, ответственным за мониторинг и предотвращение финансовых преступлений.

Обязанности Компании

Идентификация клиентов и меры финансовой безопасности (KYC/CDD):

- внедрение процедур «Know Your Customer» (KYC);
- оценка риска клиента в соответствии с риск-ориентированным подходом (Risk-Based Approach – RBA);
- применение усиленной проверки (Enhanced Due Diligence – EDD) для клиентов повышенного риска.

Обязанности по отчетности перед GIIF:

- отчетность по операциям на сумму 15 000 EUR и более;
- обязательное сообщение о подозрительных транзакциях, потенциально связанных с отмыванием денежных средств или финансированием терроризма;
- ведение надлежащих записей и документации в течение не менее 5 лет.

Соответствие международным стандартам AML/CTF

Компания обеспечивает соответствие международным стандартам противодействия отмыванию денежных средств и финансированию терроризма, включая:

- Директиву (ЕС) 2015/849 (4-я AML директива);
- Регламент (ЕС) 2023/1113 Европейского парламента и Совета об информации, сопровождающей переводы денежных средств и некоторых криптоактивов, и вносящий изменения в Директиву (ЕС) 2015/849 («Transfer Regulation»);
- Рекомендации FATF (Financial Action Task Force) по борьбе с финансовыми преступлениями.

3. Обязанности по надлежащей проверке клиента (CDD)

Комплексная проверка личности клиента (Customer Due Diligence – CDD) является обязательной мерой в соответствии с Законом Польши от 1 марта 2018 года о противодействии отмыванию денежных средств и финансированию терроризма (Dz.U. 2023, поз. 1124). Компания обязана собирать, проверять и обновлять информацию о клиентах на всех этапах сотрудничества.

В зависимости от уровня риска клиента применяются различные уровни CDD:

- Standard Due Diligence (SDD) — применяется к клиентам с низким уровнем риска;
- Enhanced Due Diligence (EDD) — применяется при выявлении повышенного риска и требует дополнительных данных.

3.1 Standard Due Diligence (SDD)

Для физических лиц требуются следующие документы и проверки:

- паспорт или национальное удостоверение личности;
- подтверждение адреса проживания (например, банковская выписка, счет за коммунальные услуги);
- биометрическая проверка (liveness check) при удаленной верификации.

Для корпоративных клиентов требуются:

- регистрационные документы компании;
- документы, удостоверяющие личность конечного бенефициарного владельца (UBO) и членов руководства;
- подтверждение адреса компании;
- выписка из Национального судебного реестра (KRS);
- подтверждение источника средств;
- список 5 основных деловых партнеров и договоры с ними;
- информация о веб-сайте компании и подтверждение владения доменом.

3.2 Enhanced Due Diligence (EDD)

Компания применяет меры усиленной проверки в следующих случаях:

- если данные клиента вызывают сомнения в их достоверности;
- если клиент является финансовым учреждением из третьей страны;
- если клиент является политически значимым лицом (PEP) или близким родственником/ассоциированным лицом;
- если клиент проживает или ведет деятельность в юрисдикции высокого риска.

В таких случаях Компания может:

- запросить дополнительные документы для подтверждения личности;
- проверить источник средств и благосостояния клиента;
- увеличить частоту мониторинга транзакций;
- провести более глубокий анализ деловой деятельности клиента.

3.3 Проверка источника средств

Компания обязана убедиться, что средства, используемые клиентом, имеют законное происхождение. Для этой цели могут быть запрошены:

- банковские выписки;
- документы, подтверждающие доходы и инвестиции;
- доказательства продажи активов или иных законных операций.

4. Политически значимые лица (PEP)

Компания определяет, является ли клиент или его бенефициарный владелец политически значимым лицом (PEP), членом семьи такого лица или близким деловым партнером. Если клиент идентифицирован как PEP, автоматически применяются меры усиленной проверки (Enhanced Due Diligence – EDD).

5. Постоянный мониторинг и обновление данных

Компания внедряет системы мониторинга транзакций в соответствии с Законом Польши от 1 марта 2018 года о противодействии отмыванию денежных средств и финансированию терроризма (Dz.U. 2018, поз. 723). Цель мониторинга — выявление и предотвращение подозрительных финансовых операций, которые могут быть связаны с отмыванием денежных средств (AML) или финансированием терроризма (CTF).

5.1 Процедуры мониторинга

Мониторинг транзакций осуществляется на постоянной основе и включает:

- анализ моделей транзакционной активности клиента;
- автоматический скрининг транзакций с использованием систем анализа данных;
- ручную проверку транзакций, соответствующих подозрительным критериям;
- проверку транзакций по санкционным спискам и спискам юрисдикций высокого риска;
- постоянную оценку риска клиента и его транзакционной активности.

Компания применяет риск-ориентированный подход (Risk-Based Approach – RBA), в рамках которого клиенты классифицируются по различным уровням риска (низкий, средний, высокий и недопустимый), а их транзакции анализируются с соответствующим уровнем детализации в зависимости от присвоенной категории риска.

5.2 Выявление подозрительных транзакций

Компания обязана вести реестр подозрительных транзакций и сообщать о них Генеральному инспектору финансовой информации (GIIF).

5.3 Оценка рисков

Компания ежегодно проводит внутреннюю оценку рисков с учетом следующих факторов:

- географические факторы (страны с высоким уровнем коррупции или слабым финансовым надзором);
- тип клиента (PEP, финансовые учреждения);
- используемые платежные инструменты (наличные, анонимные платежи);

- характер деятельности клиента (компании, работающие в секторах повышенного риска AML/CTF).

На основании данной оценки разрабатываются корректирующие меры для минимизации рисков и улучшения процессов мониторинга.

5.4 Использование технологий в мониторинге

Компания применяет современные технологии для анализа транзакционных данных, включая:

- автоматизированные системы мониторинга с алгоритмами машинного обучения;
- инструменты аналитики блокчейна для отслеживания операций с криптовалютами;
- базы данных санкционных списков, политически значимых лиц (PEP) и негативных медиа;
- инструменты анализа поведенческих данных клиентов.

Данные технологии повышают точность выявления подозрительных транзакций и уменьшают количество ложных срабатываний.

6. Ответственное лицо (RO)

Ответственное лицо Компании (Responsible Officer – RO) контролирует соблюдение Политики AML/CTF и обеспечивает соответствие требованиям законодательства Республики Польша и международным стандартам.

Ключевые обязанности включают:

- надзор за применением процедур AML/CTF и мониторингом транзакций;
- взаимодействие с GIIF и подачу отчетов о подозрительных транзакциях;
- разработку и обновление внутренних процедур AML/CTF;
- обучение сотрудников и проведение внутренних аудитов;
- оценку рисков и внедрение корректирующих мер.

Ответственное лицо выступает основным контактным лицом для регуляторов и обеспечивает эффективность системы внутреннего контроля Компании.

7. Отказ в предоставлении услуг

Недопустимые клиенты

Компания не устанавливает деловые отношения с клиентами, которые:

- отказываются предоставить необходимую информацию и документы для верификации;
- являются «Shell Banks» (банки без физического присутствия в регулируемой юрисдикции);
- проживают или ведут деятельность в странах, находящихся под международными санкциями или запрещенных внутренней политикой Компании;
- вызывают обоснованные подозрения возможного участия в отмытии денежных средств, финансировании терроризма или иной незаконной деятельности.

Запрещённые страны и территории

Компания не осуществляет онбординг клиентов из следующих стран и территорий: Афганистан; Американское Самоа; Беларусь; Бурунди; Камбоджа; Камерун; Центральноафриканская Республика; Чад; Куба; Корейская Народно-Демократическая Республика (Северная Корея); Демократическая Республика Конго; Эритрея; Эфиопия; Гаити; Иран; Ирак; Казахстан; Кыргызстан; Ливан; Ливия; Мали; Мозамбик; Мьянма (Бирма); Никарагуа; Пакистан; Палестина; Россия; Сенегал; Сьерра-Леоне; Сомали; Южный Судан; Судан; Сирия; Таджикистан; Приднестровье; Туркменистан; Уганда; Украина — территории, не контролируемые правительством (Крым, Донецкая, Херсонская, Луганская, Запорожская области); Узбекистан; Венесуэла; Йемен; Зимбабве.

Клиенты или бенефициарные владельцы, связанные с указанными странами, автоматически классифицируются как «Отклонённые / Запрещённые».

Страны третьих государств высокого риска

Следующие юрисдикции классифицируются как страны высокого риска в соответствии с Делегированным регламентом ЕС (EU) 2024/594, публичными заявлениями FATF и Законом Польши о ПОД/ФТ (ст. 2 (2)(13)). Клиенты или контрагенты, связанные с этими странами, могут быть приняты только при применении усиленной проверки (EDD), одобрении MLRO и документированной проверке источника средств и благосостояния (SoF/SoW).

Албания; Барбадос; Буркина-Фасо; Камерун; Каймановы острова; Гибралтар; Ямайка; Иордания; Нигерия; Панама; Филиппины; Южная Африка; Танзания; Тринидад и Тобаго; Уганда; Объединённые Арабские Эмираты (ОАЭ); Вьетнам; а также любая другая юрисдикция, признанная FATF или Европейской комиссией как высокорисковая на момент онбординга или периодического пересмотра.

Страны среднего риска

Юрисдикции с частично эффективным надзором AML/CFT, повышенным уровнем коррупции или проблемами налоговой прозрачности, но в целом сотрудничающие. Рекомендуется применение EDD для транзакций большого объема или операций с криптоактивами.

Список стран среднего риска:

Андорра; Ангола; Аргентина; Армения; Азербайджан; Багамы; Бахрейн; Бангладеш; Босния и Герцеговина; Ботсвана; Бразилия; Бруней; Чили; Китай (КНР); Колумбия; Коста-Рика; Хорватия; Чехия; Доминиканская Республика; Эквадор; Египет; Сальвадор; Грузия; Гана; Греция; Гватемала; Гондурас; Гонконг; Венгрия; Индия; Индонезия; Израиль; Кения; Кувейт; Лаос; Латвия; Литва; Малайзия; Мальдивы; Мальта; Маврикий; Мексика; Молдова; Монголия; Черногория; Марокко; Намибия; Непал; Северная Македония; Оман; Папуа — Новая Гвинея; Парагвай; Перу; Польша; Катар; Румыния; Саудовская Аравия; Сербия; Сингапур; Словакия; Словения; Шри-Ланка; Суринам; Тайвань; Таиланд; Тунис; Турция; Украина (территория, контролируемая правительством); Уругвай.

Страны низкого риска

Страны с устойчивыми режимами AML/CFT, высоким уровнем управления, низким уровнем восприятия коррупции и полной соответствием стандартам ЕС/ОЭСР/FATF. В случаях, когда это допускается законодательством, может применяться стандартная проверка (SDD).

Список стран низкого риска:

Австрия; Австралия; Бельгия; Болгария; Канада; Хорватия; Кипр; Дания; Эстония; Финляндия; Франция; Германия; Исландия; Ирландия; Италия; Япония; Лихтенштейн; Люксембург; Монако; Нидерланды; Новая Зеландия; Норвегия; Португалия; Сан-Марино; Южная Корея; Испания; Швеция; Швейцария; Великобритания.

Запрещённые виды деятельности

Компания не вступает и не поддерживает деловые отношения с лицами или организациями, вовлечёнными или связанными с:

- незаконным игорным бизнесом или букмекерской деятельностью без лицензии;
- торговлей оружием или деятельностью, связанной с оборонной сферой (включая посредников, товары двойного назначения, боеприпасы, химическое или биологическое оружие, кассетные боеприпасы);
- наркотическими средствами, прекурсорами или незаконными фармацевтическими продуктами;
- торговлей людьми, современным рабством или эксплуатацией детей;
- shell-банками или учреждениями без физического присутствия и эффективного надзора;
- контентом для взрослых (порнография, вебкам-сервисы, стриминг для взрослых, контент с участием детей или животных, материалы, связанные с насилием или изнасилованием);

- нарушением прав интеллектуальной собственности или авторских прав, контрафактными товарами;
- нелицензированными финансовыми учреждениями, операторами денежных переводов или провайдерами виртуальных активов;
- криптовалютами с повышенной анонимностью (например, Monero, Zcash, Dash);
- схемами Понци, финансовыми пирамидами или инвестициями с высокой доходностью;
- бинарными опционами, нерегулируемыми торговыми платформами или размещением токенов ICO/ITO;
- клиентами, выпускающими или владеющими акциями на предъявителя или иными инструментами владения, не поддающимися отслеживанию.

Акции на предъявителя представляют собой оборотные инструменты, подтверждающие право собственности на юридическое лицо, где контроль принадлежит исключительно физическому держателю и не может быть проверен Компанией. Именные или дематериализованные акции допускаются.

Компания оставляет за собой право отклонить, приостановить или прекратить любые деловые отношения или транзакции, выходящие за рамки её риск-аппетита или представляющие неуправляемый риск AML/CFT.

Руководящие принципы ЕВА / Отчётность AMLRO

В соответствии с Руководящими принципами ЕВА/GL/2022/05 от 14 июня 2022 года и позицией KNF по AMLRO от 1 декабря 2022 года, Компания указывает, что в рамках периодической (или внеплановой) управленческой информации и годового отчёта, подготовленного назначенным сотрудником (AMLRO), в частности, требуются следующие данные и информация:

- риски ML/TF и соблюдение требований AML/CFT;
- сотрудничество с компетентными государственными органами и соответствующая переписка;
- выводы и действия органов финансовой разведки и надзора;
- существенные проблемы и нарушения в области AML/CFT и корректирующие меры;
- сводка оценки рисков ML/TF на уровне всей организации;
- изменения в методологии оценки индивидуального риска клиента;
- классификация клиентов по категориям риска;
- количество клиентских досье по категориям риска;
- применение мер должной осмотрительности;
- статистика необычных и подозрительных транзакций;
- отклонённые или прекращённые деловые отношения;
- запросы от FIU, судов или правоохранительных органов;
- описание организационной структуры AML/CFT;
- описание человеческих и технических ресурсов AML/CFT;
- механизмы снижения риска и процедуры;
- мероприятия по мониторингу комплаенса;

- выполнение требований по обучению;
- планируемые действия AMLRO;
- результаты внутреннего контроля;
- изменения нормативной среды и их влияние на процессы AML/CFT.

Политически значимые лица (PEP)

Национальные PEP (Польша / локальная юрисдикция)

Лица, занимающие или занимавшие значимые государственные должности:

- Глава государства или правительства
- Министры, заместители министров, государственные секретари
- Члены парламента
- Члены руководящих органов политических партий
- Члены Верховного суда или Конституционного трибунала
- Члены Счётной палаты или Совета Национального банка Польши
- Послы
- Высшие офицеры вооружённых сил
- Члены органов управления государственных компаний
- Руководители международных организаций

Примечание: местные должности не считаются PEP, если нет национального влияния.

Иностранные PEP

- главы государств или правительств
- министры
- парламентарии
- высшие судебные органы
- центральные банки
- послы
- руководители государственных компаний
- руководство международных организаций

PEP международных организаций

ООН, МВФ, Всемирный банк, ЕС, НАТО, ОБСЕ и др.

Члены семьи PEP

- супруг/супруга
- дети
- родители

Близкие партнёры

- совместное бенефициарное владение
- тесные деловые отношения
- структуры, созданные в интересах PEP

Исключения

Не считаются PEP:

- представители местных органов власти
- госслужащие без национальных полномочий
- технические или консультативные должности

Допустимые идентификационные документы

1. Цель и область применения

Настоящее Приложение устанавливает перечень документов, принимаемых Pilot Innovation Sp. z o.o. для процедур CDD и KYC в соответствии с:

- Законом Польши AML 2018
- Директивой ЕС 2015/849
- Рекомендациями FATF
- Руководством EBA/GL/2022/05

2. Общие правила

1. Документы должны быть действительными и читаемыми.
2. Должны содержать:
 - полное имя
 - дату рождения или регистрации
 - гражданство или юрисдикцию
 - идентификационный номер
 - фотографию
 - дату выдачи и срок действия
3. Копии должны быть цветными.
4. Требуется заверенный перевод при необходимости.
5. Документы из запрещённых юрисдикций не принимаются.
6. Компания может запросить дополнительные документы в рамках EDD.

8. Сотрудничество и обмен информацией

Компания активно сотрудничает с регулирующими органами и правоохранительными органами для предотвращения отмывания денежных средств и финансирования терроризма. PayPilot предоставляет необходимую информацию по официальному запросу в соответствии с применимым законодательством и международными обязательствами.

По вопросам сотрудничества и обмена информацией можно связаться по адресу:
aml@paypilot.org