Інформація щодо принципів протидії відмиванню коштів (AML) та фінансуванню тероризму (CTF)

1. Загальна інформація

Політика протидії відмиванню коштів та фінансуванню тероризму (далі – «Політика») спрямована на запобігання та мінімізацію потенційних ризиків залучення **Pilot Innovation** (далі – «Компанія») до будь-якої незаконної діяльності.

З метою дотримання як міжнародних, так і національних нормативно-правових вимог, Компанія впроваджує ефективні внутрішні процедури та механізми для запобігання відмиванню коштів, фінансуванню тероризму, незаконному обігу наркотиків та торгівлі людьми, розповсюдженню зброї масового знищення, корупції та хабарництву, а також для реагування на будь-які прояви підозрілої діяльності з боку Користувачів.

«Відмивання коштів (легалізація доходів, одержаних злочинним шляхом)» розуміється відповідно до статті 299 Кримінального кодексу Республіки Польща від 6 червня 1997 року.

«Фінансування тероризму» розуміється відповідно до статті 165 a Кримінального кодексу Республіки Польща від 6 червня 1997 року.

Ця Політика не повинна тлумачитися як вичерпний перелік усіх політик, процедур та контрольних заходів, що застосовуються Компанією з метою запобігання відмиванню коштів, фінансуванню тероризму та іншим незаконним діям.

2. Обов’язки Компанії

2.1. Зобов’язаний суб’єкт у Польщі

PILOT INNOVATION SP. Z O.O. є зобов’язаним суб’єктом відповідно до положень Закону Республіки Польща від 1 березня 2018 року «Про протидію відмиванню коштів та фінансуванню тероризму» (Dz.U. 2018, поз. 723 зі змінами), а також інших застосовних нормативно-правових актів.

Наглядовий орган

Компанія перебуває під наглядом **Генерального інспектора фінансової інформації (GIIF)**, який є компетентним органом у Польщі, відповідальним за моніторинг та запобігання фінансовим злочинам.

Обов’язки Компанії

Ідентифікація клієнтів та заходи фінансової безпеки (KYC/CDD):

- впровадження процедур «Know Your Customer» (KYC);
- оцінка ризику клієнтів відповідно до підходу, заснованого на ризиках (Risk-Based Approach, RBA);
- застосування посиленої перевірки (Enhanced Due Diligence, EDD) щодо клієнтів підвищеного ризику.

Звітність перед GIIF:

- звітування про транзакції на суму від 15 000 євро і більше;
- обов'язкове повідомлення про підозрілі транзакції, які можуть бути пов'язані з відмиванням коштів або фінансуванням тероризму;
- ведення належної документації та зберігання записів не менше ніж протягом 5 років.

Дотримання міжнародних стандартів AML/CTF

Компанія забезпечує відповідність міжнародним стандартам у сфері протидії відмиванню коштів та фінансуванню тероризму, включаючи:

- Директиву (ЄС) 2015/849 (Четверта директива AML);
- Регламент (ЄС) 2023/1113 Європейського Парламенту та Ради щодо інформації, що супроводжує перекази коштів та деяких криптоактивів, а також про внесення змін до Директиви (ЄС) 2015/849 («Transfer Regulation»);
- Рекомендації FATF (Financial Action Task Force) щодо протидії фінансовим злочинам.

3. Обов'язки щодо належної перевірки клієнтів (Customer Due Diligence, CDD)

Комплексна перевірка ідентичності клієнта (Customer Due Diligence – CDD) є обов'язковим заходом відповідно до Закону Республіки Польща від 1 березня 2018 року «Про протидію відмиванню коштів та фінансуванню тероризму» (Dz.U. 2023, поз. 1124).

Компанія зобов'язана збирати, перевіряти та оновлювати інформацію про клієнтів на всіх етапах співпраці.

Залежно від рівня ризику клієнта застосовуються різні рівні CDD:

- Стандартна перевірка (Standard Due Diligence, SDD) – застосовується до клієнтів із низьким рівнем ризику;
- Посилена перевірка (Enhanced Due Diligence, EDD) – застосовується у випадках підвищеного ризику та передбачає збір додаткової інформації.

3.1. Стандартна перевірка (SDD)

Для фізичних осіб вимагаються:

- паспорт або національний документ, що посвідчує особу;
- підтвердження адреси проживання (наприклад, банківська виписка або рахунок за комунальні послуги);
- біометрична верифікація (liveness check) у разі дистанційної перевірки.

Для юридичних осіб вимагаються:

- установчі документи;
- документи, що посвідчують особу кінцевого бенефіціарного власника (UBO) та членів органів управління;
- підтвердження адреси компанії;
- витяг з Національного судового реєстру (KRS);
- підтвердження джерела походження коштів;
- перелік топ-5 бізнес-партнерів та договори з ними;
- інформація про вебсайт компанії та підтвердження права власності на домен.

3.2. Посилена перевірка (EDD)

Компанія застосовує заходи EDD у таких випадках:
- якщо дані клієнта викликають сумніви щодо їх достовірності;
- якщо клієнт є фінансовою установою з третьої країни;
- якщо клієнт є політично значущою особою (PEP), членом її сім'ї або пов'язаною особою;
- якщо клієнт проживає або здійснює діяльність у юрисдикції підвищеного ризику.

У таких випадках Компанія може:
- вимагати додаткові документи для підтвердження особи;
- перевіряти джерела походження коштів та статків клієнта;
- підвищувати частоту моніторингу транзакцій;
- проводити поглиблений аналіз бізнес-діяльності клієнта.

3.3. Перевірка джерела походження коштів (Source of Funds)

Компанія зобов'язана забезпечити перевірку законного походження коштів клієнта
З цією метою можуть бути запитані:
- банківські виписки;
- документи, що підтверджують доходи та інвестиції;
- підтвердження продажу активів або інших законних операцій.

4. Політично значущі особи (PEP)

Компанія визначає, чи є клієнт або його кінцевий бенефіціарний власник політично значущою особою (PEP), членом її сім'ї або пов'язаною з нею особою.
У разі ідентифікації клієнта як PEP автоматично застосовуються заходи посиленої перевірки (EDD).

5. Постійний моніторинг та оновлення даних

Компанія впроваджує системи моніторингу транзакцій відповідно до Закону Республіки Польща від 1 березня 2018 року «Про протидію відмиванню коштів та фінансуванню тероризму» (Dz.U. 2018, поз. 723).
Метою такого моніторингу є виявлення та запобігання підозрілим фінансовим операціям, які можуть бути пов'язані з відмиванням коштів (AML) або фінансуванням тероризму (CTF).

5.1. Процедури моніторингу

Моніторинг транзакцій здійснюється на постійній основі та включає:

- аналіз моделей транзакційної активності клієнтів;
- автоматизований скринінг транзакцій із використанням систем аналізу даних;
- ручну перевірку транзакцій, що відповідають критеріям підозрілості;
- перевірку транзакцій за санкційними списками та списками юрисдикцій підвищеного ризику;
- постійну оцінку ризику клієнта та його транзакційної діяльності.

Компанія застосовує підхід, заснований на оцінці ризиків (Risk-Based Approach, RBA), відповідно до якого клієнти класифікуються за рівнями ризику (низький, середній, високий та неприйнятний), а їхні транзакції перевіряються з відповідним рівнем деталізації залежно від такої класифікації.

5.2. Виявлення підозрілих транзакцій

Компанія зобов'язана вести реєстр підозрілих транзакцій та повідомляти про них Генерального інспектора фінансової інформації (GIIF).

5.3. Оцінка ризиків

Компанія проводить внутрішню оцінку ризиків щонайменше раз на рік із урахуванням таких факторів:

- географічні фактори (країни з високим рівнем корупції або слабким фінансовим наглядом);
- тип клієнта (наприклад, PEP або фінансові установи);
- використовувані платіжні інструменти (зокрема готівкові розрахунки та інші способи з підвищеним рівнем анонімності);
- характер діяльності клієнта (компанії, що працюють у секторах із підвищеним AML/CTF ризиком).

На основі цієї оцінки розробляються коригувальні заходи з метою мінімізації ризиків та вдосконалення процесів моніторингу.

5.4. Використання технологій у моніторингу

Компанія застосовує сучасні технології для аналізу транзакційних даних, зокрема:

- автоматизовані системи моніторингу з використанням алгоритмів машинного навчання;
- інструменти блокчейн-аналітики для відстеження операцій із криптоактивами;
- бази даних санкційних списків, політично значущих осіб (PEP) та негативних медіа (adverse media);
- інструменти аналізу поведінкових даних клієнтів.

Застосування цих технологій підвищує точність виявлення підозрілих транзакцій та зменшує кількість хибнопозитивних спрацьовувань.

6. Відповідальна особа (Responsible Officer, RO)

Відповідальна особа Компанії (RO) здійснює нагляд за дотриманням Політики AML/CTF та забезпечує відповідність законодавству Республіки Польща та міжнародним стандартам.

Основні обов’язки:

- контроль за застосуванням процедур AML/CTF та моніторингом транзакцій;
- взаємодія з GIIF та подання звітів про підозрілі транзакції;
- розробка та оновлення внутрішніх процедур AML/CTF;
- навчання працівників та проведення внутрішніх аудитів;
- оцінка ризиків та впровадження коригувальних заходів.

Відповідальна особа є основною контактною особою для регуляторних органів та забезпечує ефективність внутрішньої системи контролю Компанії.

7. Відмова у наданні послуг

Неприйнятні клієнти

Компанія не встановлює ділові відносини з клієнтами, які:

- відмовляються надавати необхідну інформацію та документи для верифікації;
- є так званими «shell banks» (банки без фізичної присутності у регульованій юрисдикції);
- проживають або здійснюють діяльність у країнах, що підпадають під міжнародні санкції або заборонені внутрішньою політикою Компанії;
- викликають обґрунтовані підозри щодо можливого залучення до відмивання коштів, фінансування тероризму або іншої незаконної діяльності.

Заборонені країни та території

Компанія не здійснює онбординг клієнтів з наступних країн та територій:

Afghanistan; American Samoa; Belarus; Burundi; Cambodia; Cameroon; Central African Republic; Chad; Cuba; Democratic People's Republic of Korea (North Korea); Democratic Republic of the Congo; Eritrea; Ethiopia; Haiti; Iran; Iraq; Kazakhstan; Kyrgyzstan; Lebanon; Libya; Mali; Mozambique; Myanmar (Burma); Nicaragua; Pakistan; Palestine; Russia; Senegal; Sierra Leone; Somalia; South Sudan; Sudan; Syria; Tajikistan; Transnistria; Turkmenistan; Uganda; Україна – території, що не контролюються урядом (Крим, Донецька, Херсонська, Луганська, Запорізька області); Uzbekistan; Venezuela; Yemen; Zimbabwe.

Клієнти або кінцеві бенефіціарні власники, пов'язані з цими країнами, автоматично класифікуються як **«Відхилені / Заборонені»**.

Країни підвищеного ризику (High-Risk Third Countries)

Наступні юрисдикції класифікуються як високоризикові відповідно до Делегованого регламенту ЄС (EU) 2024/594, публічних заяв FATF та Закону Польщі про AML (ст. 2 (2) (13)).

Клієнти або контрагенти, пов'язані з цими країнами, можуть бути прийняті лише за умови:

- застосування посиленої перевірки (EDD);
- схвалення з боку MLRO;
- документально підтвердженої перевірки джерела коштів (SoF) та джерела статків (SoW).

Перелік:

Albania; Barbados; Burkina Faso; Cameroon; Cayman Islands; Gibraltar; Jamaica; Jordan; Nigeria; Panama; Philippines; South Africa; Tanzania; Trinidad and Tobago; Uganda; United Arab Emirates (UAE); Vietnam; а також будь-яка інша юрисдикція, визначена FATF або Європейською Комісією як високоризикова на момент онбордингу або періодичного перегляду.

Країни середнього ризику (Medium-Risk Countries)

Юрисдикції з частково ефективним AML/CFT наглядом, підвищеним рівнем корупції або ризиками податкової прозорості, але загалом із кооперативною регуляторною системою.

Для операцій значного обсягу або криптоактивності рекомендується застосування EDD.

Перелік:

Andorra; Angola; Argentina; Armenia; Azerbaijan; Bahamas; Bahrain; Bangladesh; Bosnia and Herzegovina; Botswana; Brazil; Brunei; Chile; China (PRC); Colombia; Costa Rica; Croatia; Czech Republic; Dominican Republic; Ecuador; Egypt; El Salvador; Georgia; Ghana; Greece; Guatemala; Honduras; Hong Kong SAR; Hungary; India; Indonesia; Israel; Kenya; Kuwait; Laos; Latvia; Lithuania; Malaysia; Maldives; Malta; Mauritius; Mexico; Moldova; Mongolia; Montenegro; Morocco; Namibia; Nepal; North Macedonia; Oman; Papua New Guinea; Paraguay; Peru; Poland; Qatar; Romania; Saudi Arabia; Serbia; Singapore; Slovakia; Slovenia; Sri Lanka; Suriname; Taiwan; Thailand; Tunisia; Turkey; Україна (території, що контролюються урядом); Uruguay.

Країни низького ризику (Low-Risk Countries)

Країни з розвиненими AML/CFT режимами, ефективним державним управлінням, низьким рівнем корупції та повною відповідністю стандартам ЄС / OECD / FATF.

У таких випадках може застосовуватися спрощена перевірка (SDD), якщо це дозволено законодавством.

Перелік:

Austria; Australia; Belgium; Bulgaria; Canada; Croatia; Cyprus; Denmark; Estonia; Finland; France; Germany; Iceland; Ireland; Italy; Japan; Liechtenstein; Luxembourg; Monaco; Netherlands; New Zealand; Norway; Portugal; San Marino; South Korea; Spain; Sweden; Switzerland; United Kingdom.

Заборонені види діяльності

Компанія не вступає у ділові відносини з фізичними або юридичними особами, які прямо або опосередковано пов’язані з:

- незаконними азартними іграми або неліцензованими беттінг-платформами;
- торгівлею зброєю або діяльністю, пов’язаною з оборонною сферою (включаючи посередництво, товари подвійного призначення, боєприпаси, хімічну чи біологічну зброю, касетні боєприпаси);
- наркотичними засобами, прекурсорами або незаконними фармацевтичними препаратами;
- торгівлею людьми, сучасним рабством або експлуатацією дітей;
- так званими «shell banks» або установами без фізичної присутності чи належного нагляду;

- дорослим контентом (порнографія, вебкам-сервіси, стримінг, матеріали із насильством або за участю неповнолітніх чи тварин);
- порушенням прав інтелектуальної власності або торгівлею контрафактною продукцією;
- неліцензованими фінансовими установами, платіжними посередниками або провайдерами віртуальних активів;
- криптовалютами з підвищеною анонімністю (наприклад Monero, Zcash, Dash);
- шахрайськими інвестиційними схемами (Ponzi, піраміди, high-yield investment schemes);
- бінарними опціонами, нерегульованими торговими платформами або ICO/ITO розміщеннями;
- компаніями, що випускають або володіють акціями на пред'явника (bearer shares) або аналогічними інструментами з непрозорою структурою власності.

Акції на пред'явника (Bearer shares) — це інструменти, що підтверджують право власності на юридичну особу, де контроль належить виключно фізичному власнику документа та не може бути належним чином перевірений Компанією. Іменні або дематеріалізовані акції є допустимими.

Компанія залишає за собою право відмовити, призупинити або припинити будь-які ділові відносини або транзакції, які не відповідають її рівню ризик-апетиту або створюють неприйнятний ризик у сфері AML/CFT.

Відповідно до Керівних принципів European Banking Authority (EBA/GL/2022/05 від 14 червня 2022 року) та позиції Komisja Nadzoru Finansowego (KNF) щодо AMLRO від 1 грудня 2022 року, Компанія зазначає, що в межах необхідного обсягу періодичної (або позапланової) управлінської звітності та щорічного звіту про діяльність, підготовленого Визначеним працівником (AMLRO), зокрема, вважаються обов'язковими такі дані та інформація:

- ризики ML/TF та відповідність Компанії вимогам AML/CFT;
- взаємодія Компанії з компетентними державними органами та відповідна кореспонденція;
- усі висновки та заходи органів фінансової розвідки та наглядових органів (включаючи аналітичні та інспекційні заходи), адресовані Компанії, зокрема інформація про застосовані заходи або накладені санкції, листування з Компанією, подані звіти, виявлені порушення та застосовані санкції, а також стан і спосіб виконання рекомендацій;
- будь-які суттєві проблеми та порушення у сфері AML/CFT, надані рекомендації та вжиті заходи щодо їх усунення;
- узагальнення основних висновків оцінки ризиків ML/TF на рівні всієї установи;
- опис змін у методології оцінки індивідуального ризикового профілю клієнта;
- класифікація клієнтів за категоріями ризику, включаючи зміни порівняно з попереднім звітним періодом та основні причини таких змін;
- кількість клієнтських досьє (за категоріями ризику), включаючи ті, для яких ще не проведено перегляд або оновлення оцінки ризику;
- застосування заходів належної перевірки клієнтів, у тому числі щодо разових транзакцій та клієнтів із підвищеним рівнем ризику;
- інформація та статистика щодо кількості:
    - виявлених та проаналізованих нетипових транзакцій;

    - повідомлень про підозрілі транзакції або інших заходів, поданих до підрозділу фінансової розвідки та органів прокуратури;
    - відмов у встановленні або припинення ділових відносин із клієнтами у зв'язку з неможливістю застосування заходів належної перевірки;
    - запитів, отриманих від підрозділів фінансової розвідки, судів або правоохоронних органів;
- опис організаційної структури у сфері AML/CFT та будь-яких суттєвих змін разом із їх обґрунтуванням;
- опис людських та технічних ресурсів, доступних підрозділу AML/CFT; у випадку аутсорсингу — перелік переданих функцій AML/CFT та результати їх моніторингу;
- у сфері оцінки ризиків — впроваджені механізми зниження ризиків та прийняті процедури, разом із описом проблем, недоліків і порушень, а також висновками, рекомендаціями та внесеними змінами;
- опис заходів комплаєнс-моніторингу щодо оцінки впровадження політик AML/CFT, внутрішніх контролів і процедур, а також оцінка їх ефективності;
- виконання обов'язку щодо навчання персоналу;
- заплановані дії Визначеного працівника (AMLRO);
- результати внутрішнього контролю та стан виконання наданих рекомендацій;
- опис змін у правовому середовищі, що застосовується до Компанії, та їх вплив на процеси AML/CFT.

Політично значущі особи (PEPs)

Компанія класифікує наступні категорії осіб як політично значущі особи (**PEPs**):

Внутрішні PEP (Польща / локальна юрисдикція)

Особи, які обіймають або обіймали важливі державні посади на національному рівні, зокрема:

- Глава держави або глава уряду;
- міністри, заступники міністрів, державні секретарі;
- члени парламенту (Сейм і Сенат);
- члени керівних органів політичних партій;
- судді Верховного Суду, Конституційного трибуналу або інших вищих судових органів, рішення яких не підлягають подальшому оскарженню;
- члени Рахункової палати або правління Національного банку Польщі;
- посли, повірені у справах;
- вищі офіцери збройних сил (рівень генерала/адмірала);
- члени органів управління, наглядових або адміністративних органів державних підприємств;
- директори, заступники директорів та члени керівних органів міжнародних організацій.

Примітка:
Особи, які обіймають місцеві або регіональні посади (наприклад, мери, депутати місцевих рад, представники органів місцевого самоврядування), не вважаються PEP,

якщо вони не мають впливу на рішення на національному рівні або на розподіл державних ресурсів.

Іноземні PEP

Особи, яким іноземною державою довірено виконання важливих державних функцій, зокрема:

- глави держав або урядів;
- міністри, заступники міністрів або помічники міністрів;
- члени національних парламентів;
- члени керівних органів політичних партій;
- судді верховних або конституційних судів;
- члени рахункових палат або правління центральних банків;
- посли, повірені у справах або високопосадові військові;
- керівники державних підприємств;
- директори, заступники директорів та члени керівництва міжнародних організацій.

PEP міжнародних організацій (International Organization PEPs)

До цієї категорії належать особи, які обіймають або обіймали керівні посади в міжнародних організаціях, зокрема:

- директори, заступники директорів або члени правління;
- старші керівники, еквівалентні зазначеним рівням.

Приклади: ООН, МВФ, Світовий банк, інституції ЄС, НАТО, ОБСЄ тощо.

Члени сім’ї PEP

До осіб, пов’язаних із PEP, також належать:

- чоловік/дружина або особа, яка прирівнюється до подружжя;
- діти та їхні чоловіки/дружини або партнери;
- батьки PEP.

Близькі асоційовані особи PEP

Будь-яка особа, щодо якої відомо, що вона:

- має спільне бенефіціарне володіння юридичними особами або правовими структурами разом із PEP;
- має тісні ділові відносини з PEP;
- є єдиним бенефіціарним власником юридичної особи або правової структури, яка, як відомо, була створена в інтересах PEP.

Виключення

Наступні категорії осіб не вважаються PEP, якщо не доведено інше:

- депутати або члени рад органів місцевого самоврядування (наприклад, міських або регіональних рад);
- державні службовці та працівники місцевих адміністрацій, які не мають повноважень щодо прийняття рішень на національному рівні;
- особи, що працюють у державних установах на технічних або консультативних посадах.

Прийнятні документи для ідентифікації

1. Мета та сфера застосування

Цей Додаток визначає перелік документів, прийнятних для ідентифікації, що використовуються **Pilot Innovation Sp. z o.o.** (далі – «Компанія») для цілей належної перевірки клієнтів (**CDD**) та процедур «Know Your Customer» (**KYC**) відповідно до:

- Закону Республіки Польща від 1 березня 2018 року «Про протидію відмиванню коштів та фінансуванню тероризму» («AML Act»);
- Директиви ЄС (EU) 2015/849 (AMLD IV) зі змінами;
- Рекомендацій FATF;
- Керівних принципів EBA (EBA/GL/2022/05).

Цей перелік застосовується як на етапі онбордингу, так і під час подальшої верифікації фізичних осіб, юридичних осіб та кінцевих бенефіціарних власників, незалежно від того, чи здійснюється ідентифікація безпосередньо Компанією або через автоматизовану систему **KYCAid**.

2. Загальні вимоги

1. Усі документи повинні бути чинними, чіткими для прочитання та виданими компетентним державним органом.
2. Документи повинні містити щонайменше:

    - повне ім’я;
    - дату народження або дату реєстрації;
    - громадянство або країну реєстрації;
    - ідентифікаційний номер (персональний або компанії);
    - фотографію (для фізичних осіб);
    - дату видачі та дату закінчення строку дії (за наявності).
3. Копії або скан-копії документів повинні бути кольоровими та достатньої якості для перевірки їх автентичності.
4. Документи, складені мовою, відмінною від польської або англійської, повинні супроводжуватися сертифікованим перекладом.
5. Документи, видані в заборонених або високоризикових юрисдикціях (як визначено в Додатку №1), не приймаються.
6. Компанія залишає за собою право вимагати додаткові документи або здійснювати додаткову перевірку у випадках, коли індикатори ризику потребують застосування посиленої перевірки (**EDD**).

8. Співпраця та обмін інформацією

Компанія активно співпрацює з регуляторними органами та правоохоронними органами з метою запобігання відмиванню коштів та фінансуванню тероризму.

PayPilot надає необхідну інформацію на підставі офіційних запитів відповідно до застосовного законодавства та міжнародних зобов’язань.

З питань співпраці та обміну інформацією з Компанією можна зв’язатися за адресою: **aml@paypilot.org**