Información sobre los Principios de Prevención del Blanqueo de Capitales (AML) y Financiación del Terrorismo (CTF)

1. Información General

La Política de Prevención del Blanqueo de Capitales y Financiación del Terrorismo (en adelante, la "Política") tiene como objetivo prevenir y mitigar los riesgos potenciales de que Pilot Innovation (en adelante, la "Compañía") pueda verse involucrada en cualquier actividad ilegal.

Para cumplir tanto con la normativa internacional como con la nacional, la Compañía implementa procedimientos internos y mecanismos eficaces para prevenir el blanqueo de capitales, la financiación del terrorismo, el tráfico de drogas y de personas, la proliferación de armas de destrucción masiva, la corrupción y el soborno, así como para responder a cualquier forma de actividad sospechosa por parte de sus Usuarios.

El "Blanqueo de Capitales (legalización de los beneficios procedentes del delito)" se entenderá conforme al artículo 299 del Código Penal polaco de 6 de junio de 1997.
La "Financiación del Terrorismo" se entenderá conforme al artículo 165a del Código Penal polaco de 6 de junio de 1997.

Esta Política no debe interpretarse como un conjunto exhaustivo de todas las políticas, procedimientos y medidas de control aplicadas por la Compañía para prevenir el blanqueo de capitales, la financiación del terrorismo y otras actividades ilícitas.

2. Obligaciones de la Compañía

2.1 Sujeto obligado en Polonia

PILOT INNOVATION SP. Z O.O. es un sujeto obligado conforme a la Ley polaca de 1 de marzo de 2018 sobre la Prevención del Blanqueo de Capitales y la Financiación del Terrorismo (Diario Oficial de 2018, artículo 723, con sus modificaciones), así como a otros actos legales aplicables.

Autoridad Supervisora

La Compañía está sujeta a la supervisión del Inspector General de Información Financiera (GIIF), que es la autoridad competente en Polonia responsable de la supervisión y prevención de los delitos financieros.

Obligaciones de la Compañía

Identificación del Cliente y Medidas de Seguridad Financiera (KYC/CDD):

- Implementación de procedimientos “Know Your Customer” (KYC);
- Evaluación del riesgo del cliente conforme al enfoque basado en el riesgo (Risk-Based Approach – RBA);
- Aplicación de medidas reforzadas de diligencia debida (Enhanced Due Diligence – EDD) para clientes de mayor riesgo.

Obligaciones de reporte al GIIF:

- Reporte de transacciones con un valor igual o superior a 15.000 EUR;
- Reporte obligatorio de transacciones sospechosas potencialmente relacionadas con el blanqueo de capitales o la financiación del terrorismo;
- Mantenimiento de registros y documentación adecuados durante un período no inferior a 5 años.

Cumplimiento de los estándares internacionales AML/CTF

La Compañía garantiza el cumplimiento de los estándares internacionales de prevención del blanqueo de capitales y financiación del terrorismo, incluyendo:

- Directiva (UE) 2015/849 (4ª Directiva AML);
- Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo sobre la información que acompaña a las transferencias de fondos y determinados criptoactivos, y por el que se modifica la Directiva (UE) 2015/849 (“Transfer Regulation”);
- Recomendaciones del FATF (Financial Action Task Force) para la lucha contra la delincuencia financiera.

3. Obligaciones de Diligencia Debida del Cliente (CDD)

La verificación integral de la identidad del cliente (Customer Due Diligence – CDD) es una medida obligatoria conforme a la Ley polaca de 1 de marzo de 2018 sobre la Prevención del Blanqueo de Capitales y la Financiación del Terrorismo (Diario Oficial de 2023, artículo 1124). La Compañía está obligada a recopilar, verificar y actualizar la información del cliente en todas las etapas de la relación comercial.

Dependiendo del nivel de riesgo asignado al cliente, se aplican diferentes niveles de CDD:

- Standard Due Diligence (SDD) – aplicada a clientes de bajo riesgo;
- Enhanced Due Diligence (EDD) – aplicada cuando se identifica un mayor riesgo, requiriendo información adicional.

3.1 Standard Due Diligence (SDD)

Para clientes individuales se requieren los siguientes documentos y verificaciones:

- Pasaporte o documento nacional de identidad;
- Comprobante de domicilio (por ejemplo, extracto bancario, factura de servicios);
- Verificación biométrica (liveness check) en caso de verificación remota.

Para clientes corporativos se requieren:

- Documentos de constitución de la empresa;
- Documentos de identificación del Beneficiario Final (UBO) y de los miembros del órgano de administración;
- Comprobante del domicilio de la empresa;
- Extracto del Registro Nacional Judicial (KRS);
- Prueba del origen de los fondos;
- Lista de los 5 principales socios comerciales y contratos con ellos;
- Información sobre el sitio web de la empresa y prueba de titularidad del dominio.

3.2 Enhanced Due Diligence (EDD)

La Compañía aplica medidas de diligencia debida reforzada en los siguientes casos:

- Cuando los datos del cliente generan dudas sobre su credibilidad;
- Cuando el cliente es una institución financiera de un tercer país;
- Cuando el cliente es una Persona Políticamente Expuesta (PEP) o un familiar/ asociado cercano;
- Cuando el cliente reside o opera desde una jurisdicción de alto riesgo.

En tales casos, la Compañía podrá:

- Solicitar documentos adicionales de verificación de identidad;
- Verificar el origen de los fondos y del patrimonio del cliente;
- Aumentar la frecuencia del monitoreo de transacciones;
- Realizar un análisis más profundo de la actividad comercial del cliente.

3.3 Verificación del Origen de los Fondos

La Compañía está obligada a garantizar que los fondos utilizados por el cliente provienen de una fuente legítima. Para este propósito, se podrá solicitar:

- Extractos bancarios;
- Documentos que confirmen ingresos e inversiones;
- Evidencia de venta de activos u otras transacciones legales.

4. Personas Políticamente Expuestas (PEP)

La Compañía determina si un cliente o su beneficiario final es una Persona Políticamente Expuesta (PEP), un miembro de su familia o un asociado cercano. Si un cliente es

identificado como PEP, se aplican automáticamente medidas reforzadas de diligencia debida (Enhanced Due Diligence – EDD).

5. Monitoreo continuo y actualización de datos

La Compañía implementa sistemas de monitoreo de transacciones de conformidad con la Ley polaca de 1 de marzo de 2018 sobre la prevención del blanqueo de capitales y la financiación del terrorismo (Diario Oficial 2018, artículo 723). El objetivo del monitoreo es detectar y prevenir operaciones financieras sospechosas que puedan estar relacionadas con el blanqueo de capitales (AML) o la financiación del terrorismo (CTF).

5.1 Procedimientos de monitoreo

El monitoreo de transacciones es continuo e incluye:

- análisis de los patrones de actividad transaccional del cliente;
- filtrado automatizado de transacciones mediante sistemas de análisis de datos;
- revisión manual de transacciones que cumplan criterios sospechosos;
- verificación de transacciones contra listas de sanciones y listas de jurisdicciones de alto riesgo;
- evaluación continua del riesgo del cliente y de su actividad transaccional.

La Compañía aplica un enfoque basado en el riesgo (Risk-Based Approach – RBA), en virtud del cual los clientes se clasifican en diferentes niveles de riesgo (bajo, medio, alto e inaceptable), y sus transacciones se revisan con el nivel de detalle apropiado según su clasificación de riesgo.

5.2 Identificación de transacciones sospechosas

La Compañía está obligada a mantener un registro de transacciones sospechosas y a reportarlas al Inspector General de Información Financiera (GIIF).

5.3 Evaluación de riesgos

La Compañía realiza una evaluación interna de riesgos de forma anual, teniendo en cuenta:

- factores geográficos (países con altos niveles de corrupción o supervisión financiera débil);
- tipo de cliente (PEP, instituciones financieras);
- instrumentos de pago utilizados (efectivo, pagos anónimos);
- naturaleza de la actividad del cliente (empresas que operan en sectores con mayor riesgo AML/CTF).

Con base en esta evaluación, se desarrollan acciones correctivas para minimizar los riesgos y mejorar los procesos de monitoreo.

5.4 Uso de tecnología en el monitoreo

La Compañía emplea tecnologías avanzadas para el análisis de datos transaccionales, incluyendo:

- sistemas automatizados de monitoreo con algoritmos de aprendizaje automático;
- análisis de blockchain para rastrear operaciones con criptomonedas;
- bases de datos de listas de sanciones, Personas Políticamente Expuestas (PEP) y noticias adversas;
- herramientas de análisis del comportamiento de los clientes.

Estas tecnologías mejoran la precisión en la detección de transacciones sospechosas y reducen el número de falsos positivos.

6. Responsable designado (RO)

El Responsable designado de la Compañía (Responsible Officer – RO) supervisa el cumplimiento de la Política AML/CTF y garantiza la adhesión a los requisitos legales de la República de Polonia y a los estándares internacionales.

Las responsabilidades clave incluyen:

- supervisar la aplicación de los procedimientos AML/CTF y el monitoreo de transacciones;
- cooperar con el GIIF y presentar reportes de transacciones sospechosas;
- desarrollar y actualizar procedimientos internos AML/CTF;
- capacitar a los empleados y realizar auditorías internas;
- evaluar riesgos e implementar medidas correctivas.

El Responsable designado actúa como el principal punto de contacto con los reguladores y garantiza la eficacia del marco de control interno de la Compañía.

7. Rechazo del servicio

Clientes no aceptables

La Compañía no establece relaciones comerciales con clientes que:

- se nieguen a proporcionar la información y los documentos requeridos para la verificación;
- sean “Shell Banks” (bancos sin presencia física en una jurisdicción regulada);
- residan u operen en países sujetos a sanciones internacionales o prohibidos por la política interna de la Compañía;

- generen sospechas justificadas de posible participación en blanqueo de capitales, financiación del terrorismo u otras actividades ilegales.

Países y territorios prohibidos

La Compañía no incorpora clientes de los siguientes países y territorios:
Afganistán; Samoa Americana; Bielorrusia; Burundi; Camboya; Camerún; República Centroafricana; Chad; Cuba; República Popular Democrática de Corea (Corea del Norte); República Democrática del Congo; Eritrea; Etiopía; Haití; Irán; Irak; Kazajistán; Kirguistán; Líbano; Libia; Mali; Mozambique; Myanmar (Birmania); Nicaragua; Pakistán; Palestina; Rusia; Senegal; Sierra Leona; Somalia; Sudán del Sur; Sudán; Siria; Tayikistán; Transnistria; Turkmenistán; Uganda; Ucrania – territorios no controlados por el gobierno (Crimea, Donetsk, Kherson, Luhansk, Zaporizhzhia); Uzbekistán; Venezuela; Yemen; Zimbabue.

Los clientes o beneficiarios finales vinculados a estos países se clasifican automáticamente como “Rechazados / Prohibidos”.

Países terceros de alto riesgo

Las siguientes jurisdicciones se clasifican como de alto riesgo de conformidad con el Reglamento Delegado (UE) 2024/594, las declaraciones públicas del FATF y la Ley AML polaca (art. 2 (2)(13)). Los clientes o contrapartes vinculados con estos países solo podrán ser aceptados bajo medidas reforzadas de diligencia debida (EDD), aprobación del MLRO y verificación documentada del origen de fondos y patrimonio (SoF/SoW).

Albania; Barbados; Burkina Faso; Camerún; Islas Caimán; Gibraltar; Jamaica; Jordania; Nigeria; Panamá; Filipinas; Sudáfrica; Tanzania; Trinidad y Tobago; Uganda; Emiratos Árabes Unidos (EAU); Vietnam; y cualquier otra jurisdicción designada como de alto riesgo por el FATF o la Comisión Europea en el momento del onboarding o revisión periódica.

Países de riesgo medio

Jurisdicciones con supervisión AML/CFT parcialmente efectiva, mayor nivel de corrupción o preocupaciones de transparencia fiscal, pero con marcos generalmente cooperativos. Se recomienda aplicar EDD para transacciones de gran volumen o exposición a criptoactivos.

Lista de riesgo medio:
Andorra; Angola; Argentina; Armenia; Azerbaiyán; Bahamas; Bahréin; Bangladesh; Bosnia y Herzegovina; Botsuana; Brasil; Brunéi; Chile; China (RPC); Colombia; Costa Rica; Croacia; República Checa; República Dominicana; Ecuador; Egipto; El Salvador; Georgia; Ghana; Grecia; Guatemala; Honduras; Hong Kong RAE; Hungría; India; Indonesia; Israel; Kenia; Kuwait; Laos; Letonia; Lituania; Malasia; Maldivas; Malta; Mauricio; México; Moldavia; Mongolia; Montenegro; Marruecos; Namibia; Nepal; Macedonia del Norte; Omán; Papúa Nueva Guinea; Paraguay; Perú; Polonia; Qatar; Rumanía; Arabia Saudita; Serbia; Singapur;

Eslovaquia; Eslovenia; Sri Lanka; Surinam; Taiwán; Tailandia; Túnez; Turquía; Ucrania (territorio controlado por el gobierno); Uruguay.

Países de bajo riesgo

Países con regímenes AML/CFT sólidos, buena gobernanza, baja percepción de corrupción y pleno cumplimiento con UE/OCDE/FATF. Puede aplicarse SDD cuando esté legalmente permitido.

Lista de bajo riesgo:
Austria; Australia; Bélgica; Bulgaria; Canadá; Croacia; Chipre; Dinamarca; Estonia; Finlandia; Francia; Alemania; Islandia; Irlanda; Italia; Japón; Liechtenstein; Luxemburgo; Mónaco; Países Bajos; Nueva Zelanda; Noruega; Portugal; San Marino; Corea del Sur; España; Suecia; Suiza; Reino Unido.

Actividades prohibidas

La Compañía no establecerá ni mantendrá relaciones comerciales con personas o entidades involucradas o relacionadas con:

- juegos de azar ilegales o apuestas sin licencia;
- comercio de armas o actividades relacionadas con defensa (incluyendo intermediarios, bienes de doble uso, municiones, armas químicas o biológicas, municiones en racimo);
- narcóticos, precursores o productos farmacéuticos ilegales;
- trata de personas, esclavitud moderna o explotación infantil;
- bancos shell o instituciones sin presencia física o supervisión efectiva;
- contenido para adultos (pornografía, servicios webcam, streaming adulto, contenido infantil o con animales, material relacionado con violencia o violación);
- infracción de propiedad intelectual o derechos de autor, productos falsificados;
- instituciones financieras sin licencia, transmisores de dinero o proveedores de activos virtuales no autorizados;
- criptomonedas de privacidad o con anonimato reforzado (por ejemplo, Monero, Zcash, Dash);
- esquemas Ponzi, piramidales o inversiones de alto rendimiento;
- opciones binarias, plataformas de trading no reguladas o colocaciones de tokens ICO/ITO;
- clientes que emitan o posean acciones al portador u otros instrumentos de propiedad no rastreables.

Las acciones al portador se refieren a instrumentos negociables que representan la propiedad de una entidad jurídica, donde el control recae únicamente en el poseedor físico y no puede ser verificado por la Compañía. Las acciones nominativas o desmaterializadas son aceptables.

La Compañía se reserva el derecho de rechazar, suspender o terminar cualquier relación comercial o transacción que quede fuera de su apetito de riesgo o presente un riesgo AML/CFT no gestionable.

Directrices EBA / Informes AMLRO

De conformidad con las Directrices EBA/GL/2022/05 de 14 de junio de 2022 y la Posición de la KNF sobre AMLRO de 1 de diciembre de 2022, la Compañía indica que, dentro del alcance necesario de la información periódica (o ad hoc) de gestión y del informe anual de actividad elaborado por el Empleado Designado (AMLRO), se consideran necesarios, en particular, los siguientes datos e información:

- riesgos ML/TF y cumplimiento de la Compañía con las disposiciones AML/CFT;
- cooperación con autoridades estatales competentes y correspondencia relacionada;
- conclusiones y acciones de autoridades de inteligencia financiera y supervisión;
- problemas materiales o incumplimientos AML/CFT y acciones correctivas;
- resumen de la evaluación de riesgo ML/TF a nivel institucional;
- cambios en el método de evaluación del perfil de riesgo del cliente;
- clasificación de clientes por categorías de riesgo;
- número de expedientes de clientes por categoría de riesgo;
- aplicación de medidas de diligencia debida;
- estadísticas sobre transacciones inusuales y sospechosas;
- relaciones rechazadas o terminadas;
- solicitudes de FIU, tribunales o autoridades;
- estructura organizativa AML/CFT;
- recursos humanos y técnicos AML/CFT;
- mecanismos de mitigación de riesgos;
- actividades de monitoreo de cumplimiento;
- formación del personal;
- actividades planificadas del AMLRO;
- resultados de control interno;
- cambios regulatorios y su impacto AML/CFT.

Personas Políticamente Expuestas (PEP)

PEP nacionales (Polonia / jurisdicción local)

Personas que desempeñan o han desempeñado funciones públicas destacadas a nivel nacional, incluyendo:

- Jefe de Estado o de Gobierno
- Ministros, Viceministros, Secretarios de Estado
- Miembros del Parlamento (Sejm y Senado)
- Miembros de órganos de partidos políticos
- Miembros del Tribunal Supremo o Tribunal Constitucional
- Miembros del Tribunal de Cuentas o del Banco Nacional de Polonia

- Embajadores
- Altos mandos de las fuerzas armadas
- Miembros de órganos de empresas estatales
- Directores de organizaciones internacionales

Nota:
Las funciones locales o regionales no se consideran PEP salvo influencia nacional.

PEP extranjeros

Personas con funciones públicas destacadas en un país extranjero:

- Jefes de Estado o Gobierno
- Ministros
- Parlamentarios
- Tribunales supremos
- Bancos centrales
- Embajadores
- Ejecutivos de empresas estatales
- Directivos de organizaciones internacionales

PEP de organizaciones internacionales

Personas con altos cargos en:
ONU, FMI, Banco Mundial, UE, OTAN, OSCE, etc.

Familiares de PEP

Se consideran relacionados:

- Cónyuge o equivalente
- Hijos y sus parejas
- Padres

Asociados cercanos de PEP

Personas que:

- comparten titularidad con un PEP
- mantienen relaciones comerciales estrechas
- son beneficiarios de estructuras creadas para PEP

Cláusula de exclusión

No se clasifican como PEP:

- autoridades locales

- funcionarios sin poder decisorio nacional
- personal técnico o asesor

Documentos de identificación aceptados

1. Objeto y alcance

Este Anexo establece la lista de documentos aceptados por Pilot Innovation Sp. z o.o. (“la Compañía”) para CDD y KYC conforme a:

- Ley AML polaca de 2018
- Directiva UE 2015/849
- Recomendaciones FATF
- Directrices EBA/GL/2022/05

Aplica al onboarding y verificación continua de personas físicas, jurídicas y beneficiarios finales.

2. Reglas generales

1. Los documentos deben ser válidos, legibles y emitidos por autoridad competente.
2. Deben contener como mínimo:
- nombre completo
- fecha de nacimiento o constitución
- nacionalidad o jurisdicción
- número identificativo
- fotografía (personas físicas)
- fechas de emisión y expiración
3. Copias en color y calidad suficiente.
4. Documentos no en español o inglés requieren traducción certificada.
5. Documentos de jurisdicciones prohibidas o de alto riesgo no son aceptados.
6. La Compañía puede solicitar documentación adicional bajo EDD.

8. Cooperación e intercambio de información

La Compañía coopera activamente con autoridades regulatorias y fuerzas del orden para prevenir el blanqueo de capitales y la financiación del terrorismo. PayPilot proporciona la información necesaria previa solicitud oficial conforme a la legislación aplicable y obligaciones internacionales.

Para cuestiones relativas a cooperación e intercambio de información, la Compañía puede ser contactada en:
aml@paypilot.org