Informações sobre os Princípios de Prevenção à Lavagem de Dinheiro (AML) e Combate ao Financiamento do Terrorismo (CTF)

1. Informações Gerais

A Política de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (doravante denominada “Política”) tem como objetivo prevenir e mitigar os potenciais riscos de que a Pilot Innovation (doravante denominada a “Empresa”) possa estar envolvida em quaisquer atividades ilegais.

Para cumprir tanto as regulamentações internacionais quanto as nacionais, a Empresa implementa procedimentos internos e mecanismos eficazes para prevenir a lavagem de dinheiro, o financiamento do terrorismo, o tráfico de drogas e de pessoas, a proliferação de armas de destruição em massa, a corrupção e o suborno, bem como para responder a qualquer forma de atividade suspeita por parte de seus Usuários.

“Lavagem de Dinheiro (legalização de produtos de crime)” deve ser entendida de acordo com o Artigo 299 do Código Penal Polonês de 6 de junho de 1997.
“Financiamento do Terrorismo” deve ser entendido de acordo com o Artigo 165a do Código Penal Polonês de 6 de junho de 1997.

Esta Política não deve ser interpretada como um conjunto abrangente de todas as políticas, procedimentos e medidas de controle aplicadas pela Empresa para prevenir a lavagem de dinheiro, o financiamento do terrorismo e outras atividades ilícitas.

2. Obrigações da Empresa

2.1 Entidade Obrigada na Polónia

A PILOT INNOVATION SP. Z O.O. é uma entidade obrigada nos termos da Lei polaca de 1 de março de 2018 sobre a Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (Diário Oficial de 2018, item 723, conforme alterado), bem como de outros atos legais aplicáveis.

Autoridade Supervisora

A Empresa está sujeita à supervisão do Inspetor-Geral de Informação Financeira (GIIF), que é a autoridade competente na Polónia responsável pela monitorização e prevenção de crimes financeiros.

Obrigações da Empresa

Identificação do Cliente e Medidas de Segurança Financeira (KYC/CDD):

- Implementação de procedimentos “Know Your Customer” (KYC);
- Avaliação de risco do cliente de acordo com a Abordagem Baseada em Risco (Risk-Based Approach – RBA);
- Aplicação de Due Diligence Reforçada (Enhanced Due Diligence – EDD) para clientes de maior risco.

Obrigações de Reporte ao GIIF:

- Reporte de transações com valor igual ou superior a EUR 15.000;
- Reporte obrigatório de transações suspeitas potencialmente relacionadas à lavagem de dinheiro ou financiamento do terrorismo;
- Manutenção de registos e documentação adequados por um período não inferior a 5 anos.

Conformidade com Normas Internacionais AML/CTF

A Empresa assegura conformidade com as normas internacionais de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo, incluindo:

- Diretiva (UE) 2015/849 (4ª Diretiva AML);
- Regulamento (UE) 2023/1113 do Parlamento Europeu e do Conselho relativo às informações que acompanham transferências de fundos e determinados criptoativos, e que altera a Diretiva (UE) 2015/849 (“Transfer Regulation”);
- Recomendações do FATF (Financial Action Task Force) para o combate à criminalidade financeira.

3. Obrigações de Diligência devida do Cliente (CDD)

A verificação abrangente da identidade do cliente (Customer Due Diligence – CDD) é uma medida obrigatória nos termos da Lei polaca de 1 de março de 2018 sobre a Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (Diário Oficial de 2023, item 1124). A Empresa é obrigada a recolher, verificar e atualizar as informações do cliente em todas as fases da relação comercial.

Dependendo do nível de risco atribuído ao cliente, diferentes níveis de CDD são aplicados:

- Standard Due Diligence (SDD) – aplicada a clientes de baixo risco;
- Enhanced Due Diligence (EDD) – aplicada quando é identificado risco mais elevado, exigindo dados adicionais.

3.1 Standard Due Diligence (SDD)

Para clientes individuais, são exigidos os seguintes documentos e verificações:

- Passaporte ou documento de identidade nacional;
- Comprovativo de morada (ex.: extrato bancário, fatura de serviços públicos);
- Verificação biométrica (liveness check) em caso de verificação remota.

Para clientes corporativos, são exigidos:

- Documentos de constituição da empresa;
- Documentos de identificação do Beneficiário Efetivo (UBO) e dos membros da administração;
- Comprovativo do endereço da empresa;
- Extrato do Registo Nacional Judicial (KRS);
- Comprovativo da origem dos fundos;
- Lista dos 5 principais parceiros comerciais e respetivos contratos;
- Informações sobre o website da empresa e comprovativo da titularidade do domínio.
-

3.2 Enhanced Due Diligence (EDD)

A Empresa aplica medidas de EDD nos seguintes casos:

- Quando os dados do cliente levantam dúvidas quanto à sua credibilidade;
- Quando o cliente é uma instituição financeira de um país terceiro;
- Quando o cliente é uma Pessoa Politicamente Exposta (PEP) ou um familiar/ associado próximo;
- Quando o cliente reside ou opera a partir de uma jurisdição de alto risco.

Nestes casos, a Empresa poderá:

- Solicitar documentos adicionais de verificação de identidade;
- Verificar a origem dos fundos e do património do cliente;
- Aumentar a frequência da monitorização das transações;
- Realizar uma análise mais aprofundada da atividade comercial do cliente.

3.3 Verificação da Origem dos Fundos

A Empresa é obrigada a garantir que os fundos utilizados pelo cliente têm origem legítima. Para esse efeito, poderão ser solicitados:

- Extratos bancários;
- Documentos comprovativos de rendimentos e investimentos;
- Provas de venda de ativos ou outras transações legais.

4. Pessoas Politicamente Expostas (PEP)

A Empresa determina se um cliente ou o seu beneficiário efetivo é uma Pessoa Politicamente Exposta (PEP), um membro da família ou um associado próximo. Caso um cliente seja identificado como PEP, medidas de diligência reforçada (Enhanced Due Diligence – EDD) são automaticamente aplicadas.

5. Monitorização Contínua e Atualização de Dados

A Empresa implementa sistemas de monitorização de transações em conformidade com a Lei polaca de 1 de março de 2018 relativa à prevenção do branqueamento de capitais e do financiamento do terrorismo (Diário Oficial de 2018, item 723). O objetivo da monitorização é detetar e prevenir operações financeiras suspeitas que possam estar relacionadas com branqueamento de capitais (AML) ou financiamento do terrorismo (CTF).

5.1 Procedimentos de Monitorização

A monitorização das transações é contínua e inclui:

- análise dos padrões de atividade transacional do cliente;
- triagem automatizada de transações utilizando sistemas de análise de dados;
- revisão manual de transações que cumpram critérios suspeitos;
- verificação de transações contra listas de sanções e listas de jurisdições de alto risco;
- avaliação contínua do risco do cliente e da sua atividade transacional.

A Empresa aplica uma Abordagem Baseada no Risco (Risk-Based Approach – RBA), segundo a qual os clientes são classificados em diferentes níveis de risco (baixo, médio, alto e inaceitável), e as suas transações são analisadas com o nível de detalhe adequado dependendo da sua classificação de risco.

5.2 Identificação de Transações Suspeitas

A Empresa é obrigada a manter um registo de transações suspeitas e a reportá-las ao Inspetor-Geral de Informação Financeira (GIIF).

5.3 Avaliação de Risco

A Empresa realiza uma avaliação interna de risco anualmente, tendo em consideração:

- fatores geográficos (países com elevados níveis de corrupção ou supervisão financeira fraca);
- tipo de cliente (PEP, instituições financeiras);
- instrumentos de pagamento utilizados (numerário, pagamentos anónimos);
- natureza da atividade do cliente (empresas que operam em setores com risco elevado de AML/CTF).

Com base nesta avaliação, são desenvolvidas ações corretivas para minimizar os riscos e melhorar os processos de monitorização.

5.4 Utilização de Tecnologia na Monitorização

A Empresa utiliza tecnologias avançadas para a análise de dados transacionais, incluindo:

- sistemas automatizados de monitorização com algoritmos de aprendizagem automática;
- análise de blockchain para rastrear operações com criptomoedas;
- bases de dados de listas de sanções, Pessoas Politicamente Expostas (PEP) e notícias adversas;
- ferramentas de análise comportamental dos clientes.

Estas tecnologias aumentam a precisão na deteção de transações suspeitas e reduzem o número de falsos positivos.

6. Responsável Designado (RO)

O Responsável Designado da Empresa (Responsible Officer – RO) supervisiona a conformidade com a Política AML/CTF e assegura o cumprimento dos requisitos legais da República da Polónia e dos padrões internacionais.

As principais responsabilidades incluem:

- supervisionar a aplicação dos procedimentos AML/CTF e a monitorização de transações;
- cooperar com o GIIF e submeter relatórios de transações suspeitas;
- desenvolver e atualizar procedimentos internos AML/CTF;
- formar colaboradores e realizar auditorias internas;
- avaliar riscos e implementar medidas corretivas.

O Responsável Designado atua como principal ponto de contacto com os reguladores e assegura a eficácia do sistema de controlo interno da Empresa.

7. Recusa de Prestação de Serviços

Clientes Inaceitáveis

A Empresa não estabelece relações comerciais com clientes que:

- se recusem a fornecer as informações e documentos necessários para verificação;
- sejam “Shell Banks” (bancos sem presença física numa jurisdição regulamentada);
- residam ou operem em países sujeitos a sanções internacionais ou proibidos pela política interna da Empresa;

- levantem suspeitas justificadas de potencial envolvimento em branqueamento de capitais, financiamento do terrorismo ou outras atividades ilegais.

Países e Territórios Proibidos

A Empresa não realiza o onboarding de clientes provenientes dos seguintes países e territórios:
Afeganistão; Samoa Americana; Bielorrússia; Burundi; Camboja; Camarões; República Centro-Africana; Chade; Cuba; República Popular Democrática da Coreia (Coreia do Norte); República Democrática do Congo; Eritreia; Etiópia; Haiti; Irã; Iraque; Cazaquistão; Quirguistão; Líbano; Líbia; Mali; Moçambique; Myanmar (Birmânia); Nicarágua; Paquistão; Palestina; Rússia; Senegal; Serra Leoa; Somália; Sudão do Sul; Sudão; Síria; Tajiquistão; Transnístria; Turquemenistão; Uganda; Ucrânia – territórios não controlados pelo governo (Crimeia, Donetsk, Kherson, Luhansk, Zaporizhzhia); Uzbequistão; Venezuela; Iêmen; Zimbábue.

Clientes ou beneficiários efetivos vinculados a esses países são automaticamente classificados como “Rejeitados / Proibidos”.

Países terceiros de alto risco

As seguintes jurisdições são classificadas como de alto risco de acordo com o Regulamento Delegado (UE) 2024/594, declarações públicas do FATF e a Lei AML polaca (Art. 2 (2)(13)). Clientes ou contrapartes conectados a esses países podem ser aceites apenas mediante aplicação de Due Diligence Reforçada (EDD), aprovação do MLRO e verificação documentada da origem dos fundos e da riqueza (SoF/SoW).

Albânia; Barbados; Burkina Faso; Camarões; Ilhas Cayman; Gibraltar; Jamaica; Jordânia; Nigéria; Panamá; Filipinas; África do Sul; Tanzânia; Trinidad e Tobago; Uganda; Emirados Árabes Unidos (EAU); Vietname; e qualquer outra jurisdição designada como de alto risco pelo FATF ou pela Comissão Europeia no momento do onboarding ou revisão periódica.

Países de risco médio

Jurisdições com supervisão AML/CFT parcialmente eficaz, níveis elevados de corrupção ou preocupações de transparência fiscal, mas com estruturas geralmente cooperativas. Recomenda-se EDD para transações de grande volume ou exposição a criptoativos.

Lista de risco médio:
Andorra; Angola; Argentina; Arménia; Azerbaijão; Bahamas; Bahrein; Bangladesh; Bósnia e Herzegovina; Botsuana; Brasil; Brunei; Chile; China (RPC); Colômbia; Costa Rica; Croácia; República Checa; República Dominicana; Equador; Egito; El Salvador; Geórgia; Gana; Grécia; Guatemala; Honduras; Hong Kong RAE; Hungria; Índia; Indonésia; Israel; Quénia; Kuwait; Laos; Letónia; Lituânia; Malásia; Maldivas; Malta; Maurício; México; Moldávia; Mongólia; Montenegro; Marrocos; Namíbia; Nepal; Macedónia do Norte; Omã; Papua-Nova

Guiné; Paraguai; Peru; Polónia; Qatar; Roménia; Arábia Saudita; Sérvia; Singapura; Eslováquia; Eslovénia; Sri Lanka; Suriname; Taiwan; Tailândia; Tunísia; Turquia; Ucrânia (território controlado pelo governo); Uruguai.

Países de baixo risco

Países com regimes AML/CFT robustos, forte governação, baixa perceção de corrupção e plena conformidade com UE/OCDE/FATF. O SDD pode ser aplicado quando legalmente permitido.

Lista de baixo risco:
Áustria; Austrália; Bélgica; Bulgária; Canadá; Croácia; Chipre; Dinamarca; Estónia; Finlândia; França; Alemanha; Islândia; Irlanda; Itália; Japão; Liechtenstein; Luxemburgo; Mónaco; Países Baixos; Nova Zelândia; Noruega; Portugal; San Marino; Coreia do Sul; Espanha; Suécia; Suíça; Reino Unido.

Atividades proibidas

A Empresa não estabelecerá nem manterá relações comerciais com indivíduos ou entidades envolvidos ou ligados a:

- jogos de azar ilegais ou apostas sem licença;
- comércio de armas ou atividades relacionadas com defesa (incluindo intermediários, bens de dupla utilização, munições, armas químicas ou biológicas, munições cluster);
- narcóticos, precursores ou produtos farmacêuticos ilegais;
- tráfico de seres humanos, escravidão moderna ou exploração infantil;
- shell banks ou instituições sem presença física ou supervisão eficaz;
- conteúdo adulto (pornografia, serviços webcam, streaming adulto, conteúdo infantil ou bestialidade, material relacionado com violência ou violação);
- violação de propriedade intelectual ou direitos de autor, bens contrafeitos;
- instituições financeiras não licenciadas, transmissores de dinheiro ou fornecedores de ativos virtuais não licenciados;
- criptomoedas de privacidade ou com anonimato reforçado (ex.: Monero, Zcash, Dash);
- esquemas Ponzi, piramidais ou investimentos de alto rendimento;
- opções binárias, plataformas de negociação não regulamentadas ou colocações de tokens ICO/ITO;
- clientes que emitam ou detenham ações ao portador ou instrumentos equivalentes não rastreáveis.

Ações ao portador referem-se a instrumentos negociáveis que representam a propriedade de uma entidade jurídica, em que o controlo pertence exclusivamente ao detentor físico e não pode ser verificado pela Empresa. Ações nominativas ou desmaterializadas são aceitáveis.

A Empresa reserva-se o direito de rejeitar, suspender ou encerrar qualquer relação comercial ou transação que esteja fora do seu apetite de risco ou apresente risco AML/CFT não gerenciável.

Diretrizes EBA / Relatórios AMLRO

Com base nas Diretrizes EBA/GL/2022/05 de 14 de junho de 2022 e na posição KNF sobre AMLRO de 1 de dezembro de 2022, a Empresa indica que, no âmbito das informações periódicas (ou ad hoc) de gestão e do relatório anual elaborado pelo Funcionário Designado (AMLRO), são considerados necessários, em particular, os seguintes dados e informações:

- riscos ML/TF e conformidade com disposições AML/CFT;
- cooperação com autoridades competentes e correspondência relacionada;
- conclusões e ações das autoridades de supervisão e inteligência financeira;
- problemas materiais AML/CFT e medidas corretivas;
- resumo da avaliação institucional de risco ML/TF;
- alterações na metodologia de avaliação de risco do cliente;
- classificação de clientes por categorias de risco;
- número de ficheiros de clientes por categoria de risco;
- aplicação de medidas de due diligence;
- estatísticas sobre transações suspeitas;
- relações recusadas ou encerradas;
- pedidos de FIU, tribunais ou autoridades;
- estrutura organizacional AML/CFT;
- recursos humanos e técnicos AML/CFT;
- mecanismos de mitigação de risco;
- atividades de monitorização de conformidade;
- formação de colaboradores;
- atividades planeadas do AMLRO;
- resultados de controlo interno;
- alterações regulatórias e impacto AML/CFT.

Pessoas Politicamente Expostas (PEP)

PEP domésticos (Polónia / jurisdição local)

Indivíduos que exercem ou exerceram funções públicas proeminentes:

- Chefe de Estado ou de Governo
- Ministros, Vice-Ministros, Secretários de Estado
- Membros do Parlamento
- Órgãos de partidos políticos
- Tribunal Supremo ou Tribunal Constitucional
- Tribunal de Contas ou Banco Nacional da Polónia
- Embaixadores
- Altos oficiais militares

- Órgãos de empresas estatais
- Diretores de organizações internacionais

Nota: funções locais não são PEP salvo influência nacional.

PEP estrangeiros

- Chefes de Estado ou Governo
- Ministros
- Parlamentares
- Tribunais supremos
- Bancos centrais
- Embaixadores
- Executivos de empresas estatais
- Diretores de organizações internacionais

PEP organizações internacionais

ONU, FMI, Banco Mundial, UE, NATO, OSCE, etc.

Familiares de PEP

- Cônjuge
- Filhos
- Pais

Associados próximos

- copropriedade com PEP
- relações comerciais próximas
- beneficiários de estruturas criadas para PEP

Cláusula de exclusão

Não são PEP:

- autoridades locais
- funcionários sem poder decisório
- funções técnicas ou consultivas

Documentos de identificação aceites

1. Objetivo e âmbito

Este Anexo estabelece a lista de documentos aceites pela Pilot Innovation Sp. z o.o. (“a Empresa”) para CDD e KYC conforme:

- Lei AML polaca
- Diretiva UE 2015/849
- Recomendações FATF
- Diretrizes EBA/GL/2022/05

2. Regras gerais

1. Documentos válidos e legíveis.
2. Devem conter:
- nome completo
- data de nascimento ou constituição
- nacionalidade ou jurisdição
- número de identificação
- fotografia
- datas de emissão e validade
3. Cópias a cores.
4. Tradução certificada quando necessário.
5. Documentos de jurisdições proibidas não são aceites.
6. A Empresa pode solicitar documentos adicionais sob EDD.

8. Cooperação e intercâmbio de informações

A Empresa coopera ativamente com autoridades reguladoras e forças de aplicação da lei para prevenir branqueamento de capitais e financiamento do terrorismo. A PayPilot fornece as informações necessárias mediante pedido oficial, de acordo com a legislação aplicável e obrigações internacionais.

Para questões relacionadas com cooperação e intercâmbio de informações, a Empresa pode ser contactada em:
aml@paypilot.org