Informations sur les Principes de Lutte contre le Blanchiment de Capitaux (AML) et le Financement du Terrorisme (CTF)

1. Informations générales

La Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (ci-après la « Politique ») vise à prévenir et atténuer les risques potentiels que Pilot Innovation (ci-après la « Société ») puisse être impliquée dans des activités illégales.

Afin de se conformer à la fois aux réglementations internationales et nationales, la Société met en œuvre des procédures internes et des mécanismes efficaces pour prévenir le blanchiment de capitaux, le financement du terrorisme, le trafic de drogue et d'êtres humains, la prolifération des armes de destruction massive, la corruption et la fraude, ainsi que pour répondre à toute forme d'activité suspecte de la part de ses Utilisateurs.

Le « Blanchiment de capitaux (légalisation des produits du crime) » doit être interprété conformément à l'article 299 du Code pénal polonais du 6 juin 1997.
Le « Financement du terrorisme » doit être interprété conformément à l'article 165a du Code pénal polonais du 6 juin 1997.

La présente Politique ne doit pas être interprétée comme un ensemble exhaustif de toutes les politiques, procédures et mesures de contrôle appliquées par la Société pour prévenir le blanchiment de capitaux, le financement du terrorisme et d'autres activités illicites.

2. Obligations de la Société

2.1 Entité assujettie en Pologne

PILOT INNOVATION SP. Z O.O. est une entité assujettie conformément à la loi polonaise du 1er mars 2018 relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme (Journal officiel 2018, position 723, telle que modifiée), ainsi qu'à d'autres actes juridiques applicables.

Autorité de supervision

La Société est soumise à la supervision de l'Inspecteur Général de l'Information Financière (GIIF), qui est l'autorité compétente en Pologne chargée du contrôle et de la prévention des crimes financiers.

Obligations de la Société

Identification du client et mesures de sécurité financière (KYC/CDD) :

- mise en œuvre des procédures « Know Your Customer » (KYC) ;
- évaluation du risque client conformément à l'approche fondée sur le risque (Risk-Based Approach – RBA) ;
- application de mesures de diligence renforcée (Enhanced Due Diligence – EDD) pour les clients à risque plus élevé.

Obligations de déclaration auprès du GIIF :

- déclaration des transactions d'un montant égal ou supérieur à 15 000 EUR ;
- déclaration obligatoire des transactions suspectes potentiellement liées au blanchiment de capitaux ou au financement du terrorisme ;
- conservation des registres et de la documentation appropriés pendant une durée minimale de 5 ans.

Conformité aux normes internationales AML/CTF

La Société assure la conformité avec les normes internationales de lutte contre le blanchiment de capitaux et le financement du terrorisme, notamment :

- Directive (UE) 2015/849 (4e directive AML) ;
- Règlement (UE) 2023/1113 du Parlement européen et du Conseil concernant les informations accompagnant les transferts de fonds et de certains crypto-actifs, et modifiant la directive (UE) 2015/849 (« Transfer Regulation ») ;
- Recommandations du GAFI (Financial Action Task Force) relatives à la lutte contre la criminalité financière.

3. Obligations de diligence raisonnable à l'égard de la clientèle (CDD)

La vérification complète de l'identité du client (Customer Due Diligence – CDD) constitue une mesure obligatoire en vertu de la loi polonaise du 1er mars 2018 relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme (Journal officiel 2023, position 1124). La Société est tenue de collecter, vérifier et mettre à jour les informations relatives aux clients à toutes les étapes de la relation d'affaires.

Selon le niveau de risque attribué au client, différents niveaux de CDD sont appliqués :

- Standard Due Diligence (SDD) – appliquée aux clients à faible risque ;
- Enhanced Due Diligence (EDD) – appliquée lorsqu'un risque plus élevé est identifié et nécessitant des informations supplémentaires.

3.1 Standard Due Diligence (SDD)

Pour les clients personnes physiques, les documents et contrôles suivants sont requis :

- passeport ou carte nationale d'identité ;
- justificatif de domicile (par exemple relevé bancaire, facture de services publics) ;

- vérification biométrique (liveness check) en cas de vérification à distance.

Pour les clients entreprises, les éléments suivants sont requis :

- documents constitutifs de la société ;
- documents d'identification du bénéficiaire effectif (UBO) et des membres de la direction ;
- justificatif d'adresse de la société ;
- extrait du Registre National Judiciaire (KRS) ;
- preuve de l'origine des fonds ;
- liste des 5 principaux partenaires commerciaux et contrats correspondants ;
- informations sur le site internet de la société et preuve de propriété du domaine.

3.2 Enhanced Due Diligence (EDD)

La Société applique des mesures EDD dans les cas suivants :

- lorsque les données du client suscitent des doutes quant à leur crédibilité ;
- lorsque le client est une institution financière d'un pays tiers ;
- lorsque le client est une personne politiquement exposée (PEP) ou un membre de sa famille / associé proche ;
- lorsque le client réside ou opère depuis une juridiction à haut risque.

Dans ces cas, la Société peut :

- demander des documents supplémentaires de vérification d'identité ;
- vérifier l'origine des fonds et du patrimoine du client ;
- augmenter la fréquence du contrôle des transactions ;
- effectuer une analyse plus approfondie de l'activité commerciale du client.

3.3 Vérification de l'origine des fonds

La Société est tenue de s'assurer que les fonds utilisés par le client proviennent d'une source légitime. À cette fin, les éléments suivants peuvent être demandés :

- relevés bancaires ;
- documents confirmant les revenus et les investissements ;
- preuves de vente d'actifs ou d'autres transactions licites.

4. Personnes Politiquement Exposées (PEP)

La Société détermine si un client ou son bénéficiaire effectif est une Personne Politiquement Exposée (PEP), un membre de sa famille ou un proche associé. Lorsqu'un client est identifié comme PEP, des mesures de diligence renforcée (Enhanced Due Diligence – EDD) sont automatiquement appliquées.

5. Surveillance continue et mise à jour des données

La Société met en œuvre des systèmes de surveillance des transactions conformément à la loi polonaise du 1er mars 2018 relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme (Journal officiel 2018, position 723). L'objectif de la surveillance est de détecter et de prévenir les opérations financières suspectes pouvant être liées au blanchiment de capitaux (AML) ou au financement du terrorisme (CTF).

5.1 Procédures de surveillance

La surveillance des transactions est continue et comprend :

- l'analyse des schémas d'activité transactionnelle des clients ;
- le filtrage automatisé des transactions à l'aide de systèmes d'analyse de données ;
- l'examen manuel des transactions répondant à des critères suspects ;
- le filtrage des transactions par rapport aux listes de sanctions et aux listes de juridictions à haut risque ;
- l'évaluation continue du risque du client et de son activité transactionnelle.

La Société applique une approche fondée sur le risque (Risk-Based Approach – RBA), selon laquelle les clients sont classés dans différents niveaux de risque (faible, moyen, élevé et inacceptable), et leurs transactions sont examinées avec un niveau de détail approprié en fonction de leur classification de risque.

5.2 Identification des transactions suspectes

La Société est tenue de maintenir un registre des transactions suspectes et de les signaler à l'Inspecteur Général de l'Information Financière (GIIF).

5.3 Évaluation des risques

La Société effectue une évaluation interne des risques chaque année, en tenant compte des éléments suivants :

- facteurs géographiques (pays présentant des niveaux élevés de corruption ou une supervision financière faible) ;
- type de client (PEP, institutions financières) ;
- instruments de paiement utilisés (espèces, paiements anonymes) ;
- nature de l'activité du client (sociétés opérant dans des secteurs présentant un risque AML/CTF élevé).

Sur la base de cette évaluation, des actions correctives sont élaborées afin de minimiser les risques et d'améliorer les processus de surveillance.

5.4 Utilisation de la technologie dans la surveillance

La Société utilise des technologies avancées pour l'analyse des données transactionnelles, notamment :

- des systèmes de surveillance automatisés avec des algorithmes d'apprentissage automatique ;
- des outils d'analyse blockchain pour tracer les opérations en crypto-actifs ;
- des bases de données de listes de sanctions, de personnes politiquement exposées (PEP) et de médias négatifs ;
- des outils d'analyse comportementale des clients.

Ces technologies améliorent la précision de la détection des transactions suspectes et réduisent le nombre de faux positifs.

6. Responsable désigné (RO)

Le Responsable désigné (Responsible Officer – RO) de la Société supervise la conformité avec la Politique AML/CTF et assure le respect des exigences légales de la République de Pologne ainsi que des normes internationales.

Les principales responsabilités comprennent :

- la supervision de l'application des procédures AML/CTF et de la surveillance des transactions ;
- la coopération avec le GIIF et la soumission de déclarations de transactions suspectes ;
- l'élaboration et la mise à jour des procédures internes AML/CTF ;
- la formation des employés et la réalisation d'audits internes ;
- l'évaluation des risques et la mise en œuvre de mesures correctives.

Le Responsable désigné agit en tant que principal point de contact avec les autorités de régulation et assure l'efficacité du cadre de contrôle interne de la Société.

7. Refus de service

Clients inacceptables

La Société n'établit pas de relations d'affaires avec des clients qui :

- refusent de fournir les informations et documents requis pour la vérification ;
- sont des « Shell Banks » (banques sans présence physique dans une juridiction réglementée) ;
- résident ou opèrent dans des pays soumis à des sanctions internationales ou interdits par la politique interne de la Société ;

- suscitent des soupçons raisonnables d'implication potentielle dans le blanchiment de capitaux, le financement du terrorisme ou d'autres activités illégales.

Pays et territoires interdits

La Société n'accepte pas l'onboarding de clients provenant des pays et territoires suivants : Afghanistan ; Samoa américaines ; Biélorussie ; Burundi ; Cambodge ; Cameroun ; République centrafricaine ; Tchad ; Cuba ; République populaire démocratique de Corée (Corée du Nord) ; République démocratique du Congo ; Érythrée ; Éthiopie ; Haïti ; Iran ; Irak ; Kazakhstan ; Kirghizistan ; Liban ; Libye ; Mali ; Mozambique ; Myanmar (Birmanie) ; Nicaragua ; Pakistan ; Palestine ; Russie ; Sénégal ; Sierra Leone ; Somalie ; Soudan du Sud ; Soudan ; Syrie ; Tadjikistan ; Transnistrie ; Turkménistan ; Ouganda ; Ukraine – territoires non contrôlés par le gouvernement (oblasts de Crimée, Donetsk, Kherson, Louhansk, Zaporijjia) ; Ouzbékistan ; Venezuela ; Yémen ; Zimbabwe.

Les clients ou bénéficiaires effectifs liés à ces pays sont automatiquement classés comme « Rejetés / Interdits ».

Pays tiers à haut risque

Les juridictions suivantes sont classées à haut risque conformément au Règlement délégué (UE) 2024/594, aux déclarations publiques du GAFI (FATF) et à la loi AML polonaise (art. 2 (2)(13)). Les clients ou contreparties liés à ces pays ne peuvent être acceptés que sous réserve de l'application de mesures de vigilance renforcée (EDD), de l'approbation du MLRO et d'une vérification documentée de l'origine des fonds et du patrimoine (SoF/SoW).

Albanie ; Barbade ; Burkina Faso ; Cameroun ; Îles Caïmans ; Gibraltar ; Jamaïque ; Jordanie ; Nigeria ; Panama ; Philippines ; Afrique du Sud ; Tanzanie ; Trinité-et-Tobago ; Ouganda ; Émirats arabes unis (EAU) ; Vietnam ; ainsi que toute autre juridiction désignée comme à haut risque par le GAFI ou la Commission européenne au moment de l'onboarding ou de la revue périodique.

Pays à risque moyen

Juridictions présentant une supervision AML/CFT partiellement efficace, des niveaux élevés de corruption ou des préoccupations en matière de transparence fiscale, mais disposant généralement de cadres coopératifs. L'EDD est recommandée pour les transactions de volume élevé ou présentant une exposition aux crypto-actifs.

Liste des pays à risque moyen :
Andorre ; Angola ; Argentine ; Arménie ; Azerbaïdjan ; Bahamas ; Bahreïn ; Bangladesh ; Bosnie-Herzégovine ; Botswana ; Brésil ; Brunei ; Chili ; Chine (RPC) ; Colombie ; Costa Rica ; Croatie ; République tchèque ; République dominicaine ; Équateur ; Égypte ; Salvador ; Géorgie ; Ghana ; Grèce ; Guatemala ; Honduras ; Hong Kong RAS ; Hongrie ; Inde ; Indonésie ; Israël ; Kenya ; Koweït ; Laos ; Lettonie ; Lituanie ; Malaisie ; Maldives ; Malte ;

Maurice ; Mexique ; Moldavie ; Mongolie ; Monténégro ; Maroc ; Namibie ; Népal ; Macédoine du Nord ; Oman ; Papouasie-Nouvelle-Guinée ; Paraguay ; Pérou ; Pologne ; Qatar ; Roumanie ; Arabie saoudite ; Serbie ; Singapour ; Slovaquie ; Slovénie ; Sri Lanka ; Suriname ; Taïwan ; Thaïlande ; Tunisie ; Turquie ; Ukraine (territoire contrôlé par le gouvernement) ; Uruguay.

Pays à faible risque

Pays disposant de régimes AML/CFT robustes, d'une gouvernance solide, d'une faible perception de la corruption et d'une conformité complète aux normes UE/OCDE/FATF. La SDD peut être appliquée lorsque cela est légalement autorisé.

Liste des pays à faible risque :
Autriche ; Australie ; Belgique ; Bulgarie ; Canada ; Croatie ; Chypre ; Danemark ; Estonie ; Finlande ; France ; Allemagne ; Islande ; Irlande ; Italie ; Japon ; Liechtenstein ; Luxembourg ; Monaco ; Pays-Bas ; Nouvelle-Zélande ; Norvège ; Portugal ; Saint-Marin ; Corée du Sud ; Espagne ; Suède ; Suisse ; Royaume-Uni.

Activités interdites

La Société ne conclura ni ne maintiendra sciemment de relations d'affaires avec des personnes ou entités impliquées dans :

- les jeux d'argent illégaux ou les activités de paris non autorisées ;
- le commerce d'armes ou les activités liées à la défense (y compris intermédiaires, biens à double usage, munitions, armes chimiques ou biologiques, munitions à sous-munitions) ;
- les stupéfiants, précurseurs ou produits pharmaceutiques illégaux ;
- la traite des êtres humains, l'esclavage moderne ou l'exploitation des enfants ;
- les shell banks ou institutions sans présence physique ni supervision efficace ;
- les contenus pour adultes (pornographie, services webcam, streaming pour adultes, contenu impliquant des mineurs ou la bestialité, matériel lié à la violence ou au viol) ;
- la violation des droits de propriété intellectuelle ou du droit d'auteur, produits contrefaits ;
- les institutions financières non agréées, services de transfert de fonds ou fournisseurs d'actifs virtuels non autorisés ;
- les cryptomonnaies axées sur la confidentialité ou renforçant l'anonymat (par ex. Monero, Zcash, Dash) ;
- les systèmes de Ponzi, pyramidaux ou investissements à rendement élevé ;
- les options binaires, plateformes de trading non réglementées ou placements de tokens ICO/ITO ;
- les clients émettant ou détenant des actions au porteur ou des instruments de propriété équivalents non traçables.

Les actions au porteur désignent des instruments négociables représentant la propriété d'une entité juridique, dont le contrôle appartient uniquement au détenteur physique et ne

peut être vérifié par la Société. Les actions nominatives ou dématérialisées sont acceptables.

La Société se réserve le droit de rejeter, suspendre ou mettre fin à toute relation d'affaires ou transaction sortant de son appétence au risque ou présentant un risque AML/CFT non maîtrisable.

Lignes directrices EBA / Rapports AMLRO

Conformément aux lignes directrices EBA/GL/2022/05 du 14 juin 2022 et à la position KNF sur l'AMLRO du 1er décembre 2022, la Société indique que, dans le cadre des informations de gestion périodiques (ou ad hoc) et du rapport annuel d'activité établi par l'employé désigné (AMLRO), les données suivantes sont notamment requises :

- risques ML/TF et conformité AML/CFT ;
- coopération avec les autorités compétentes ;
- conclusions des autorités de supervision et de renseignement financier ;
- problèmes matériels AML/CFT et mesures correctives ;
- résumé de l'évaluation du risque ML/TF ;
- changements dans la méthodologie d'évaluation du risque client ;
- classification des clients par catégories de risque ;
- nombre de dossiers clients par catégorie ;
- application des mesures de diligence raisonnable ;
- statistiques relatives aux transactions suspectes ;
- relations refusées ou résiliées ;
- demandes des autorités ;
- structure organisationnelle AML/CFT ;
- ressources humaines et techniques AML/CFT ;
- mécanismes d'atténuation des risques ;
- activités de surveillance de la conformité ;
- formation du personnel ;
- activités planifiées de l'AMLRO ;
- conclusions du contrôle interne ;
- changements réglementaires et impact AML/CFT

Personnes Politiquement Exposées (PEP)

PEP nationaux (Pologne / juridiction locale)

Personnes exerçant ou ayant exercé des fonctions publiques importantes :

- Chef d'État ou de gouvernement

- Ministres, vice-ministres, secrétaires d'État
- Membres du Parlement
- Membres d'organes de partis politiques
- Membres de la Cour suprême ou du Tribunal constitutionnel
- Membres de la Cour des comptes ou de la Banque nationale de Pologne
- Ambassadeurs
- Hauts gradés militaires
- Membres d'organes d'entreprises publiques
- Dirigeants d'organisations internationales

Remarque : les fonctions locales ne sont pas considérées comme PEP sauf influence nationale.

PEP étrangers

- Chefs d'État ou de gouvernement
- Ministres
- Membres de parlements
- Cours suprêmes
- Banques centrales
- Ambassadeurs
- Dirigeants d'entreprises publiques
- Dirigeants d'organisations internationales

PEP organisations internationales

ONU, FMI, Banque mondiale, UE, OTAN, OSCE, etc.

Membres de la famille des PEP

- Conjoint
- Enfants
- Parents

Associés proches

- copropriété avec un PEP
- relations commerciales étroites
- bénéficiaires de structures liées à un PEP

Clause d'exclusion

Ne sont pas considérés comme PEP :

- représentants locaux
- fonctionnaires sans pouvoir décisionnel national

- fonctions techniques ou consultatives

Documents d’identification acceptés

1. Objet et champ d’application

Cette annexe établit la liste des documents acceptés par Pilot Innovation Sp. z o.o. (« la Société ») aux fins des procédures CDD et KYC conformément à :

- loi AML polonaise
- directive UE 2015/849
- recommandations du GAFI
- lignes directrices EBA/GL/2022/05

2. Règles générales

1. Documents valides et lisibles.
2. Doivent contenir :
- nom complet
- date de naissance ou constitution
- nationalité ou juridiction
- numéro d’identification
- photo
- dates d’émission et d’expiration
3. Copies couleur requises.
4. Traduction certifiée si nécessaire.
5. Documents de juridictions interdites non acceptés.
6. La Société peut demander des documents supplémentaires dans le cadre de l’EDD.

8. Coopération et échange d’informations

La Société coopère activement avec les autorités réglementaires et les forces de l’ordre afin de prévenir le blanchiment de capitaux et le financement du terrorisme. PayPilot fournit les informations nécessaires sur demande officielle conformément à la législation applicable et aux obligations internationales.

Pour toute question relative à la coopération et à l’échange d’informations, la Société peut être contactée à l’adresse suivante :
aml@paypilot.org