POLITIQUE DE PRÉVENTION DU BLANCHIMENT DE CAPITAUX ET DU FINANCEMENT DU TERRORISME D'AGEM

1. Introduction

AGEM (ci-après, « AGEM » ou la « Société »), pleinement consciente de l'importance de prévenir l'utilisation de la société comme instrument de canalisation de ressources d'origine illicite ou destinées à des fins criminelles, adopte par la présente **Politique d'Entreprise de Prévention du Blanchiment de Capitaux et du Financement du Terrorisme** (ci-après, la « Politique ») un engagement ferme et explicite de **tolérance zéro** face à toute pratique susceptible d'être liée, directement ou indirectement, à la commission d'infractions de blanchiment de capitaux ou de financement du terrorisme.

La prévention de tels comportements constitue un objectif prioritaire pour AGEM, non seulement en raison des responsabilités pénales, administratives et réputationnelles évidentes qui pourraient en découler pour la société et pour les personnes physiques qui la composent, mais également en raison de l'obligation éthique et sociale d'agir en toute circonstance avec la plus grande intégrité, diligence et transparence. L'implication de la Société dans des activités délictueuses de cette nature serait incompatible avec ses principes et valeurs d'entreprise, affecterait gravement la confiance des clients, fournisseurs et autorités, et mettrait en péril sa propre viabilité économique.

AGEM déclare donc expressément qu'elle ne tolérera aucune participation, directe ou indirecte, volontaire ou par omission, à quelque activité que ce soit pouvant donner lieu à un processus de blanchiment de capitaux, entendu comme le processus par lequel l'on tente de donner une apparence de légalité à des ressources économiques d'origine délictueuse, ni à des activités liées au financement du terrorisme, consistant à fournir, réunir ou utiliser des fonds dans le but de commettre des actes terroristes ou d'être utilisés, en tout ou partie, par des organisations terroristes.

La présente Politique est adoptée en application de la **Loi 10/2010, du 28 avril**, relative à la prévention du blanchiment de capitaux et du financement du terrorisme, de son Règlement d'application approuvé par le Décret royal 304/2014, du 5 mai, ainsi que des **Directives (UE) 2015/849 et 2018/843** et des Recommandations du Groupe d'action financière (GAFI/FATF). Elle s'aligne également sur les exigences de l'article 31 bis du Code pénal espagnol relatif à la responsabilité pénale des personnes morales et sur la **norme UNE 19601:2025** relative aux systèmes de management de la conformité pénale, constituant un élément essentiel du Système de Conformité Pénale d'AGEM.

L'Administrateur Unique d'AGEM, en tant qu'organe suprême de gouvernance de la société, assume la responsabilité ultime de l'approbation, de la mise en œuvre, du suivi et de l'amélioration continue de cette Politique, dont le respect sera obligatoire pour

l'ensemble des salariés, dirigeants, représentants et tiers agissant au nom ou pour le compte de la Société, ou dont la relation commerciale ou contractuelle pourrait l'exposer à des risques de blanchiment de capitaux ou de financement du terrorisme.

2. Objet et objectifs de la Politique

La présente Politique a pour objet d'établir un cadre normatif interne cohérent, uniforme et efficace, destiné à prévenir, détecter et, le cas échéant, signaler toute opération, relation ou comportement susceptible d'être lié au blanchiment de capitaux ou au financement du terrorisme.

En conformité avec la législation en vigueur et les normes internationales applicables, AGEM poursuit, à travers cette Politique, les objectifs fondamentaux suivants :

Premièrement, garantir que l'ensemble des opérations économiques, commerciales et financières auxquelles participe la Société se déroulent en toute transparence, avec traçabilité et dans le respect de la légalité, de sorte qu'elles ne puissent en aucun cas servir, même involontairement, à canaliser des ressources illicites ou destinées à des fins délictueuses.

Deuxièmement, établir des procédures internes de vigilance raisonnable pour l'identification et la connaissance adéquates des clients, fournisseurs, sous-traitants, intermédiaires et partenaires commerciaux, afin de vérifier leur honorabilité, leur réputation, leur capacité financière et, le cas échéant, la licéité de l'origine des fonds qu'ils gèrent ou transfèrent dans le cadre de leurs relations avec AGEM.

De même, la Politique vise à définir des mécanismes clairs et efficaces de détection et de signalement des opérations suspectes, de sorte que tout salarié, dirigeant ou tiers lié à la Société dispose de canaux internes sûrs, confidentiels et protégés pour alerter immédiatement en cas de faits ou d'indices pouvant être contraires à la réglementation applicable.

Enfin, la présente Politique vise à promouvoir une culture d'entreprise de prévention et de conformité en matière de blanchiment de capitaux et de financement du terrorisme, en garantissant que tous les membres d'AGEM reçoivent une formation adéquate, connaissent leurs obligations légales et internes, et agissent avec la plus grande diligence dans l'exercice de leurs fonctions.

3. Champ d'application et personnes assujetties

La Politique est d'application obligatoire pour AGEM en tant que société mère, pour l'ensemble de ses filiales et délégations, tant en Espagne qu'à l'étranger, pour l'Administrateur Unique, le Compliance Officer, l'ensemble des salariés, dirigeants et représentants de la Société, ainsi que pour tous les tiers — fournisseurs, sous-traitants, intermédiaires, agents commerciaux, partenaires stratégiques — dont les activités, de

par leur nature ou leur volume, pourraient exposer AGEM à des risques de blanchiment de capitaux ou de financement du terrorisme.

L'ensemble de ces personnes devront agir dans le cadre de cette Politique avec diligence, intégrité et transparence, en assumant expressément l'obligation de coopérer à l'application des procédures internes de vigilance raisonnable, de détection des risques, de formation et de signalement des opérations suspectes qui y sont prévues.

4. Principes directeurs

L'action d'AGEM en matière de prévention du blanchiment de capitaux et du financement du terrorisme s'inspire d'un ensemble de principes directeurs qui constituent le fondement éthique, juridique et opérationnel de cette Politique, garantissant sa correcte application à tous les niveaux de l'organisation et dans toutes les juridictions où la Société exerce son activité.

En premier lieu, le **principe de légalité** impose l'obligation de respecter strictement l'ensemble des dispositions de la Loi 10/2010, de son Règlement d'application et des Directives européennes applicables, ainsi que les recommandations des organismes internationaux compétents, tels que le Groupe d'action financière (GAFI), le Fonds monétaire international ou la Banque centrale européenne, dans la mesure où ceux-ci peuvent affecter les opérations, produits ou services de la Société.

Le **principe de vigilance raisonnable** exige l'application de contrôles proportionnés au risque, fondés sur une identification, une vérification et un suivi adéquats des clients, fournisseurs et partenaires commerciaux, en particulier dans les cas où des facteurs accroissent l'exposition à des opérations potentiellement illicites, tels que la présence dans des juridictions à haut risque, la complexité financière de l'opération ou l'utilisation d'espèces en montants significatifs.

Le **principe de prévention**, quant à lui, oblige la Société à adopter des mesures organisationnelles, formatives et technologiques destinées à éviter, avant qu'elles ne se matérialisent, toute opération susceptible d'être utilisée à des fins de blanchiment ou de financement du terrorisme, garantissant une réponse précoce et efficace face à la détection des risques.

Le **principe de transparence et de traçabilité** implique que l'ensemble des opérations économiques, financières et commerciales auxquelles participe AGEM doivent être enregistrées, documentées et conservées conformément à la réglementation en vigueur, de sorte qu'elles puissent faire l'objet d'une vérification, d'un audit et, le cas échéant, d'une communication aux autorités compétentes sans retard injustifié.

Le **principe de coopération active** consacre l'obligation d'AGEM de coopérer de manière loyale et diligente avec les autorités judiciaires, policières et administratives, en particulier avec le Service Exécutif de la Commission de Prévention du Blanchiment de Capitaux et des Infractions Monétaires (SEPBLAC), en facilitant le signalement immédiat des opérations suspectes et la fourniture des informations et documents qui lui seraient demandés dans l'exercice de ses fonctions légales.

Enfin, le **principe de confidentialité et de protection du lanceur d'alerte** garantit que toute communication interne relative à des opérations suspectes ou à des manquements à cette Politique sera traitée avec la plus grande confidentialité et sécurité, toute forme de représailles, sanction ou traitement discriminatoire à l'encontre de ceux qui effectuent de telles communications de bonne foi étant expressément interdite, conformément aux dispositions de la Loi 2/2023 et de la Directive (UE) 2019/1937 relative à la protection des personnes signalant des violations du droit de l'Union.

5. Mesures de vigilance raisonnable et de contrôle interne

AGEM mettra en place un **Système de Vigilance Raisonnable** comprenant l'identification, la vérification et le suivi continu de l'ensemble des clients, fournisseurs, sous-traitants, intermédiaires et partenaires commerciaux avec lesquels la Société établit des relations commerciales ou professionnelles impliquant des opérations économiques ou financières significatives.

L'identification formelle des personnes physiques et morales avec lesquelles AGEM entretient des relations comprendra, au minimum, l'obtention et la vérification de leur nom, dénomination sociale, domicile, activité, bénéficiaire effectif, structure sociétaire et, le cas échéant, l'existence de personnes politiquement exposées (PPE) directement ou indirectement liées à l'opération ou à la relation commerciale.

Le respect du principe « connaître son client » (KYC) impliquera l'obligation d'obtenir des informations suffisantes et fiables sur la nature de l'activité professionnelle ou commerciale du client ou du fournisseur, l'origine licite des fonds, la finalité et la nature de la relation commerciale, ainsi que toute autre donnée pertinente pour évaluer le risque de blanchiment ou de financement du terrorisme associé à l'opération ou à la relation contractuelle.

Dans les cas où concourent des facteurs de risque aggravant, tels que des opérations transfrontalières complexes, l'utilisation de structures fiduciaires, la présence dans des juridictions non coopératives, des montants d'une valeur anormalement élevée ou l'implication de personnes politiquement exposées, AGEM appliquera des mesures renforcées de vigilance raisonnable, incluant des vérifications documentaires supplémentaires, des demandes d'informations complémentaires, des autorisations préalables de l'Administrateur Unique et un suivi spécifique par le Compliance Officer.

Toutes les opérations feront l'objet d'un **suivi continu**, afin de détecter des schémas inhabituels, des transactions atypiques ou des comportements s'écartant de l'activité ordinaire du client, du fournisseur ou du partenaire commercial. Ce suivi s'appuiera sur des outils technologiques et sur la révision périodique des informations disponibles, garantissant leur mise à jour constante et leur cohérence avec l'évolution de la relation commerciale ou contractuelle.

6. Procédures d'identification, de signalement et de coopération avec les autorités

Lorsque tout salarié, dirigeant ou tiers lié à AGEM dispose d'indices, de soupçons ou de connaissances qu'une opération, relation commerciale ou transaction pourrait être liée au blanchiment de capitaux ou au financement du terrorisme, il aura l'obligation immédiate de le signaler de manière confidentielle et sécurisée au Compliance Officer, par les canaux internes prévus à cet effet.

Le Compliance Officer, après réception du signalement, évaluera en urgence l'opération ou la transaction suspecte, pouvant demander des informations complémentaires aux domaines concernés et adoptant, le cas échéant, des mesures conservatoires telles que la suspension temporaire de l'opération jusqu'à l'achèvement de l'examen interne.

Si, de l'avis du Compliance Officer et de l'Administrateur Unique, l'opération présente des indices raisonnables d'être liée au blanchiment de capitaux ou au financement du terrorisme, AGEM procédera à son signalement immédiat au SEPBLAC, conformément aux dispositions de la Loi 10/2010 et de sa réglementation d'application, en fournissant l'ensemble de la documentation et des informations disponibles et en coopérant de manière loyale et diligente avec cet organisme ainsi qu'avec les autorités judiciaires ou policières susceptibles de mener l'enquête.

En aucun cas le signalement interne ou externe d'opérations suspectes ne pourra constituer un manquement au devoir de confidentialité protégeant le lanceur d'alerte, ni donner lieu à des représailles professionnelles, contractuelles ou de travail à l'encontre de la personne ayant effectué le signalement de bonne foi, même si les faits signalés ne se trouvent finalement pas confirmés.

7. Obligation individuelle de contrôle et de vérification préalable des opérations

Outre le système général de prévention, de supervision et de contrôle établi dans cette Politique et les fonctions attribuées à l'Administrateur Unique et au Compliance Officer, tout salarié ou dirigeant d'AGEM recevant, traitant, autorisant ou exécutant des paiements, virements ou opérations économiques ou financières de toute nature est soumis à l'**obligation individuelle de vérification préalable et diligente** de chaque transaction avant son traitement ou son enregistrement comptable.

Cette obligation vise à établir un premier niveau de contrôle décentralisé, au point le plus proche de l'opération concrète, de sorte qu'aucun paiement ou virement ne puisse être exécuté sans que la personne directement responsable de son traitement n'ait vérifié, sous sa responsabilité professionnelle, l'absence d'éléments objectifs susceptibles de faire suspecter son origine illicite, son absence de justification économique ou son éventuel lien avec des activités délictueuses ou avec le financement du terrorisme.

La vérification individuelle comprendra, au minimum, la vérification :

- De l'identité du donneur d'ordre et du bénéficiaire, en confrontant leur cohérence avec les informations contractuelles ou commerciales disponibles.
- De la cohérence du montant et de l'objet de l'opération avec la nature et les antécédents de la relation commerciale existante.
- De la cohérence et de la suffisance de la documentation justificative, y compris les factures, contrats, ordres de paiement et tout autre support probant.
- De l'absence d'indices d'irrégularité, tels que des paiements à destination ou en provenance de juridictions à risque, des structures sociétaires opaques, l'utilisation d'espèces en montants inhabituels ou le fractionnement injustifié d'opérations.

Si, au cours de cette vérification individuelle, la personne responsable détecte une anomalie, une incohérence ou un indice suspect, elle sera tenue de suspendre l'opération à titre conservatoire et de signaler l'incident de manière immédiate et confidentielle au Compliance Officer par le canal prévu à cet effet, en s'abstenant de procéder à son exécution jusqu'à réception d'instructions expresses contraires.

L'omission de cette vérification préalable, le traitement d'opérations sans la diligence requise ou l'absence de signalement d'indices suspects constitueront un **manquement grave** à la présente Politique, pouvant donner lieu à l'adoption de mesures disciplinaires ou contractuelles, sans préjudice des éventuelles responsabilités administratives ou pénales encourues en cas de commission d'infractions.

Toutes les opérations vérifiées devront être documentées et enregistrées dans les systèmes internes d'AGEM, en conservant la trace expresse de l'identité de la personne ayant effectué la vérification, de la date et de l'heure de celle-ci, des incidents détectés et, le cas échéant, des signalements effectués au Compliance Officer ou aux autorités compétentes.

Grâce à ce mécanisme, AGEM renforce de manière effective son engagement en faveur de la prévention active du blanchiment de capitaux et du financement du terrorisme, en veillant à ce que la vigilance raisonnable ne se limite pas à une supervision centralisée, mais imprègne l'ensemble des étapes et des niveaux de l'activité opérationnelle et financière de la Société.

8. Formation et sensibilisation du personnel

L'efficacité du système de prévention du blanchiment de capitaux et du financement du terrorisme dépend en grande partie du niveau de connaissance, de sensibilisation et de formation de l'ensemble des personnes composant AGEM. C'est pourquoi la Société mettra en œuvre un **programme de formation continue** destiné à l'ensemble de ses salariés, dirigeants et collaborateurs, adapté à la nature de leurs fonctions, à leur niveau de responsabilité et à l'exposition au risque inhérente à leur poste.

La formation portera non seulement sur les aspects juridiques et réglementaires de la prévention du blanchiment de capitaux et du financement du terrorisme, mais également sur l'application pratique des procédures internes, notamment l'identification des opérations suspectes, l'utilisation du canal de signalement prévu, la documentation requise et les obligations de confidentialité et de coopération avec les autorités compétentes.

Le Compliance Officer sera chargé de concevoir et de coordonner les programmes de formation, en assurant leur mise à jour périodique en fonction de l'évolution réglementaire, des directives des organismes de supervision et des enseignements tirés des audits, inspections ou enquêtes internes.

Les cours, ateliers et sessions de formation seront documentés au moyen de registres de présence et d'évaluations des acquis, afin de pouvoir démontrer, en cas d'inspections ou de procédures judiciaires, qu'AGEM a rempli son obligation légale de former adéquatement son personnel en la matière.

La formation sera obligatoire pour l'ensemble du personnel, et sera également incluse dans le processus d'accueil des nouveaux salariés et dans la contractualisation avec des tiers dont l'activité pourrait comporter des risques en matière de prévention du blanchiment de capitaux ou du financement du terrorisme.

9. Régime disciplinaire et conséquences du non-respect

Le non-respect des obligations découlant de la présente Politique, de la Loi 10/2010 et de sa réglementation d'application sera considéré comme un **manquement grave** aux règles internes d'AGEM et pourra donner lieu à l'adoption de mesures disciplinaires, contractuelles ou légales, selon la nature, la gravité et la portée du comportement détecté.

Pour les salariés et dirigeants de la Société, les manquements seront sanctionnés conformément à la législation du travail en vigueur, à la convention collective applicable et au régime disciplinaire interne d'AGEM, pouvant consister en des avertissements écrits, des suspensions d'emploi et de salaire ou, dans les cas les plus graves, la rupture de la relation de travail, sans préjudice de l'éventuelle responsabilité civile ou pénale que pourrait encourir le contrevenant.

En ce qui concerne les tiers sous-traitants, fournisseurs ou partenaires commerciaux, le non-respect de cette Politique constituera un motif de **résiliation immédiate** de la relation contractuelle, indépendamment des actions légales qu'AGEM pourrait engager pour réclamer des dommages et intérêts, ainsi que de l'obligation de signaler aux autorités compétentes en cas d'indices de commission d'infractions pénales.

Toutes les mesures disciplinaires et contractuelles adoptées respecteront les principes de **proportionnalité, de légalité et de respect des droits fondamentaux**, en garantissant toujours le droit du présumé contrevenant à être entendu et à se défendre, ainsi que la documentation écrite de l'ensemble de la procédure disciplinaire.

10. Supervision, suivi et contrôle interne

Le Compliance Officer, sous la supervision directe de l'Administrateur Unique, sera responsable de la vérification de la bonne mise en œuvre et du respect de cette Politique, ainsi que de l'évaluation périodique de l'efficacité des procédures internes de prévention du blanchiment de capitaux et du financement du terrorisme.

À cette fin, il élaborera un **Plan Annuel de Supervision et d'Audit** comprenant des révisions périodiques de la Cartographie des Risques, des vérifications de l'adéquation des procédures internes, des analyses d'opérations inhabituelles ou suspectes, ainsi que des évaluations du niveau de formation et de sensibilisation du personnel.

Les résultats des audits internes, ainsi que les signalements reçus par le canal prévu à cet effet, les mesures adoptées et les éventuels incidents détectés, seront compilés dans des rapports périodiques que le Compliance Officer présentera à l'Administrateur Unique, lequel adoptera les décisions nécessaires pour renforcer le système de prévention et garantir son amélioration continue.

De même, chaque fois que surviennent des changements réglementaires pertinents, des modifications de la structure sociétaire, l'ouverture de nouvelles filiales dans des juridictions à risque ou des incidents significatifs en matière de prévention du blanchiment de capitaux ou du financement du terrorisme, le Compliance Officer proposera la révision immédiate de la Politique, garantissant son adéquation permanente à la législation applicable et aux meilleures pratiques internationales.

11. Approbation, entrée en vigueur et mise à jour

La présente Politique sera formellement approuvée par l'Administrateur Unique d'AGEM, qui assume la responsabilité ultime de sa mise en œuvre effective, de l'allocation des ressources humaines, technologiques et financières nécessaires à son respect, ainsi que de la supervision du système de prévention du blanchiment de capitaux et du financement du terrorisme.

Une fois approuvée, la Politique entrera en vigueur à la date indiquée dans l'accord d'approbation et sera d'application obligatoire pour l'ensemble des salariés, dirigeants, représentants et tiers liés à la Société, sans exception.

La Politique fera l'objet d'une révision périodique au moins une fois par an, ou plus fréquemment lorsque des changements législatifs, des recommandations des autorités compétentes, des modifications de la structure ou de l'activité d'AGEM, ou la détection de lacunes dans son application pratique l'exigeront.

Toute modification ou mise à jour de la Politique sera également approuvée par l'Administrateur Unique et communiquée immédiatement à l'ensemble des destinataires, en garantissant sa pleine accessibilité via l'intranet de l'entreprise, le site Internet d'AGEM et les processus de formation interne correspondants.

Annexe I – Procédure Opérationnelle de Prévention du Blanchiment de Capitaux et du Financement du Terrorisme

Afin de garantir la bonne application et l'opérationnalité de la Politique de Prévention du Blanchiment de Capitaux et du Financement du Terrorisme (LCB/FT) d'AGEM, la procédure interne obligatoire suivante est mise en œuvre, établissant les responsabilités, mesures et contrôles spécifiques à respecter dans le développement des relations et opérations avec les clients, fournisseurs, intermédiaires et partenaires commerciaux.

1. Identification et Vérification des Clients et Tiers (KYC/KYB)

1.1. Obligation d'Identification

Avant de formaliser toute opération ou relation commerciale pertinente, l'identité complète de la personne physique ou morale devra être vérifiée par l'obtention de la documentation minimale suivante :

- Personnes morales : Acte constitutif, données d'immatriculation, statuts à jour, numéro d'identification fiscale, structure sociétaire, identification des bénéficiaires effectifs et déclaration d'activité.
- Personnes physiques : Document d'identité valide (carte d'identité, titre de séjour ou passeport), domicile et activité professionnelle ou commerciale.

1.2. Vérification du Bénéficiaire Effectif

Dans toute relation avec des sociétés, fondations ou autres structures juridiques, il sera obligatoire de vérifier l'identité des personnes physiques contrôlant directement ou indirectement plus de 25 % du capital ou des droits de vote, ou exerçant un contrôle par d'autres moyens.

1.3. Vérification des Antécédents

Une vérification de base des antécédents réputationnels, disciplinaires et de propriété de l'entité sera effectuée dans des bases de données publiques et des listes de sanctions (par exemple, listes de l'UE, de l'ONU ou du GAFI), y compris l'identification des Personnes Politiquement Exposées (PPE).

2. Classification du Risque des Tiers

La classification adéquate du risque associé aux clients, fournisseurs, intermédiaires financiers et partenaires commerciaux constitue un outil essentiel pour prévenir les situations susceptibles d'impliquer AGEM dans des activités de blanchiment de capitaux ou de financement du terrorisme. Cette évaluation reposera sur une approche fondée sur le risque (« risk-based approach »), tenant compte des caractéristiques intrinsèques du tiers ainsi que de l'opération et de l'environnement géographique.

2.1. Facteurs d'évaluation du risque

a) Risque inhérent au client ou au tiers

- Nature juridique : entreprises présentant des structures sociétaires complexes ou récentes, sans antécédent opérationnel ou avec un objet social vaste ou ambigu.
- Activité économique exercée : secteurs à risque tels que le commerce extérieur, le conseil financier, l'import/export, les fondations, l'immobilier, etc.
- Structure sociétaire opaque : recours à des fiducies, trusts, comptes fiduciaires ou bénéficiaires inconnus.
- Antécédents réputationnels : présence dans des bases de données de sanctions, apparition dans les médias en lien avec des scandales financiers, déclarations d'insolvabilité ou de faillite.

b) Risque associé à la relation commerciale

- Volume et nature des opérations : contrats portant sur des montants significatifs, opérations inhabituelles ou paiement par des instruments non traçables.
- Durée et fréquence : les contacts occasionnels ou intermittents présentent un risque plus élevé que les relations continues, dotées d'un historique transparent.
- Mode de paiement : l'utilisation d'espèces, de cryptomonnaies, de chèques au porteur ou de comptes dans des juridictions opaques accroît le niveau de risque.

c) Risque géographique

- Pays figurant sur les listes noires ou grises du GAFI, présentant des niveaux élevés de corruption, ou où opèrent des organisations criminelles ou terroristes.

- Juridictions sanctionnées par les Nations Unies ou l'Union européenne.

2.2. Catégories de risque

Sur la base de l'évaluation précédente, le tiers sera classé dans l'une des catégories suivantes :

- Risque Faible : entités publiques, fournisseurs récurrents, entreprises aux pratiques établies, vérifications documentaires complètes et activité justifiée.
- Risque Moyen : nouveaux tiers sans antécédent avec AGEM, opérations uniques significatives ou clients ayant une activité transnationale justifiable.
- Risque Élevé : personnes situées dans des pays à haut risque, PPE, opérations impliquant des structures de propriété complexes ou des paiements en espèces ou opaques.

Pour les tiers classés à risque élevé, des mesures renforcées et des autorisations échelonnées seront appliquées.

3. Mesures de Vigilance Raisonnable

La vigilance raisonnable vise à vérifier l'identité et l'activité du tiers, à garantir la licéité de l'origine des fonds et de l'opération, et à détecter d'éventuels risques de blanchiment de capitaux ou de financement du terrorisme avant la formalisation de la relation commerciale.

3.1. Vigilance Raisonnable Standard

Applicable aux tiers présentant un profil de risque faible ou moyen. Elle comprendra :

- Vérification documentaire complète.
- Vérification initiale par rapport aux listes de sanctions.
- Confirmation de l'objet et du volume attendu de la relation commerciale.
- Évaluation des données fiscales et comptables disponibles.
- Vérification de la cohérence entre l'opération envisagée et l'activité habituelle du tiers.

3.2. Vigilance Raisonnable Renforcée

Obligatoire pour les tiers classés à risque élevé ou en présence de facteurs aggravants (opérations supérieures à 50 000 €, structures fiduciaires, paiements en espèces).

Documentation Complémentaire Obligatoire

- Attestations bancaires relatives à l'origine des fonds.
- Déclarations relatives au bénéficiaire effectif et aux bénéficiaires finaux.

- Vérification notariale ou bancaire pour les structures fiduciaires.

Autorisation et Supervision Renforcées

- Révision complète préalable de l'ensemble de la documentation par le Compliance Officer.
- Approbation préalable de l'Administrateur Unique.
- Intégration de clauses de contrôle et de conformité supplémentaires dans les contrats.

Contrôles Complémentaires

- Suivi périodique trimestriel du volume et de la nature de la relation.
- Surveillance continue des opérations exécutées et des changements de circonstances.
- Demande de mise à jour documentaire annuelle.

3.3. Exemption des Obligations de Vigilance

Peut s'appliquer dans des cas justifiés, notamment les relations avec :

- Les administrations publiques ou entités financières soumises à une réglementation de supervision.
- Les entreprises cotées dont les informations sont accessibles au public et vérifiées.

4. Suivi Continu des Opérations

- Toutes les transactions devront être examinées afin de détecter des indices d'irrégularité.
- Les opérations d'un montant supérieur à 50 000 € ou impliquant des comptes bancaires de tiers situés dans des pays à haut risque devront faire l'objet d'une attention particulière.
- Tout écart par rapport à l'activité prévue devra être documenté et signalé au Compliance Officer.

5. Signalement des Opérations Suspectes

- Tout salarié constatant des indices de blanchiment ou de financement du terrorisme devra en informer immédiatement et de manière confidentielle le Compliance Officer via le canal éthique.
- Le Compliance Officer évaluera le cas et, le cas échéant, signalera l'opération au SEPBLAC.
- Il est interdit de révéler au client ou au tiers l'existence d'une enquête interne ou d'un signalement externe (« interdiction de tipping-off »).

6. Obligation de Formation

AGEM garantira une formation initiale, annuelle et à chaque modification réglementaire pour ses salariés en matière de prévention du blanchiment de capitaux et du financement du terrorisme, en mettant l'accent sur les domaines les plus exposés (administration, achats, ventes, contrats internationaux, finances).

7. Conservation de la Documentation

Toute documentation obtenue en application de cette procédure devra être conservée pendant une durée minimale de 10 ans, conformément à la Loi 10/2010 et au Décret royal 304/2014.

8. Révision de la Procédure

La présente Annexe sera révisée tous les 12 mois par le Compliance Officer, ou plus tôt en cas de modifications de la législation applicable, de recommandations des organismes de supervision, ou d'incidents opérationnels.