ROX PAY S.R.L.
POLITIQUE DE PRÉVENTION ET DE LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

1 - APERÇU

1.1 – RÉGLEMENTATIONS ET CONSEILS CLÉS

Ce document présente la politique de Rox Pay S.r.l. en matière de lutte contre le blanchiment d'argent, le financement du terrorisme et la violation des mesures restrictives.[1]et s'applique à Rox Pay S.r.l. et ses opérations.

Les normes doivent être considérées comme complémentaires et applicables car elles ne sont pas en conflit avec les dispositions émises par les autorités locales.

1.2 – DESTINATAIRES ET MODALITÉS DE MISE EN ŒUVRE

La Politique s'applique à Rox Pay S.r.l.

2 – PRINCIPES GÉNÉRAUX

2.1 CADRE RÉGLEMENTAIRE LBC-FT

Le blanchiment des produits d'activités illégales et criminelles est l'une des formes de criminalité les plus graves sur les marchés financiers et constitue un domaine d'intérêt particulier pour les activités criminelles organisées.

Le blanchiment d'argent a un impact négatif important sur l'ensemble de l'économie : le réinvestissement des produits illégaux dans des activités légales et la collusion entre des individus ou des institutions financières et des organisations criminelles affectent profondément les mécanismes de marché, compromettent l'efficacité et l'équité des activités financières et affaiblissent l'économie. Le financement d'activités terroristes peut impliquer l'utilisation de produits d'origine licite et/ou d'origine criminelle.

La nature changeante du blanchiment d'argent et du financement du terrorisme, également facilitée par l'évolution continue de la technologie, nécessite une adaptation constante des mesures de prévention et de lutte.

Le cadre réglementaire de lutte contre le blanchiment d'argent (AML) et le financement du terrorisme (CFT) repose sur un ensemble complet de sources réglementaires nationales, européennes et internationales.

Au niveau international, le Groupe d'action financière (GAFI), le principal organisme international actif dans la lutte contre le blanchiment d'argent, le financement du terrorisme et la prolifération des armes de destruction massive, a apporté une contribution essentielle à l'harmonisation de la réglementation.

1 Telles que définies dans les orientations de l'ABE (EBA/GL/2024/14) : « Les mesures restrictives de l'Union visées à l'article 2, point (1) de la directive (UE) 2024/1226 et les mesures restrictives nationales adoptées par les États membres conformément à leur ordre juridique national (dans la mesure où elles s'appliquent aux institutions financières).

Pour s'acquitter de ses responsabilités, le GAFI a établi un ensemble de normes internationales, les « 40 recommandations », auxquelles 9 autres recommandations spéciales ont été ajoutées en 2001 pour lutter contre le financement du terrorisme international. Le sujet a été entièrement revu en février 2012 avec l'adoption des normes internationales sur la lutte contre le blanchiment d'argent et le financement du terrorisme et de la prolifération, puis résumées dans les « 40 recommandations » susmentionnées.

Dans le cadre de la lutte contre la prolifération des armes de destruction massive, les Nations Unies ont préparé un ensemble de mesures pour lutter contre le financement des programmes de prolifération, y compris l'interdiction d'assister ou de financer toute personne impliquée dans de telles activités.

En mettant en œuvre les résolutions adoptées dans le cadre des Nations Unies, l'Union européenne a publié un ensemble de dispositions afin de mettre en œuvre des mesures restrictives telles que le gel des fonds et des ressources économiques des personnes ou entités impliquées dans le développement d'activités d'armes de destruction massive sensibles à la prolifération.

Le GAFI a élaboré des lignes directrices pour mettre en œuvre les sanctions financières adoptées par les Nations Unies.

Des mesures spécifiques visant à lutter contre la prolifération des armes de destruction massive ont récemment été incluses dans les recommandations, conformément aux résolutions du Conseil de sécurité des Nations Unies.

Les lignes directrices de l'UE sur la prévention de l'utilisation du système financier à des fins de blanchiment de capitaux et de financement du terrorisme sont contenues dans la directive européenne 2015/849.[2]du Parlement européen et du Conseil du 20 mai 2015 (Quatrième Directive anti-blanchiment d'argent), telle que modifiée par la Directive UE 2018/843 (Cinquième Directive anti-blanchiment d'argent) ainsi que dans les Règlements et Orientations émises respectivement par l'UE – Union européenne et par l'ABE – Autorité bancaire européenne.

Au niveau national, la prévention et la lutte contre le blanchiment d'argent et le financement du terrorisme sont régies par les lois primaires suivantes :

- **Décret législatif italien no. 109 du 22 juin 2007 et ses modifications et compléments ultérieurs qui prévoient des « Dispositions visant à prévenir, contrer et réprimer le financement du terrorisme et l'activité des pays qui menacent la paix et la sécurité internationale », mettant en œuvre la Directive 2015/849 telle que modifiée par la Directive UE 2018/843 ;**
- **Décret législatif italien no. 231 du 21 novembre 2007, et modifications et compléments ultérieurs mettant en œuvre la directive 2015/849/UE, qui modifie la directive 2009/138/CE et 2013/36/UE, modifiée par la directive 2018/843/UE relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme (ci-après également le décret).**

2 La directive UE 2024/1640 du Parlement européen et du Conseil du 31/05/2024 relative aux procédures à mettre en place par les États membres pour prévenir l'utilisation du système financier à des fins de blanchiment de capitaux ou de financement du terrorisme, à transposer d'ici le 10 juillet 2027, modifie la directive UE 2019/1937 et abroge la directive UE 2015/849.

Enfin, il existe également une législation dérivée au niveau national qui a été émise par la Banque d'Italie.
et la Cellule d'information financière (« CRF »), et elle est contenue dans les sources réglementaires suivantes :

- **Disposition du 26 mars 2019 fixant les dispositions d'application en matière d'organisation, de procédures et de contrôles internes visant à prévenir le recours à des intermédiaires financiers et à d'autres entités à des fins de blanchiment de capitaux et de financement du terrorisme, telle que modifiée par la disposition de la Banque d'Italie du 1er août 2023 ;**
- **Disposition du 28 mars 2019 fixant les instructions en matière de communication objective ;**
- **Disposition du 30 juillet 2019 fixant les dispositions d'application en matière de vigilance à l'égard de la clientèle, telle que modifiée par la Disposition de la Banque d'Italie du 13 juin 2023 ;**
- **Disposition du 24 mars 2020 fixant les dispositions d'application relatives à la conservation et à la disponibilité des documents, données et informations en matière de lutte contre le blanchiment et le financement du terrorisme ;**
- **Disposition du 25 août 2020 fixant les modalités de transmission des déclarations LBC agrégées ;**
- **Disposition du 12 mai 2023 relative aux indicateurs d'anomalies pour les intermédiaires afin de faciliter l'identification des opérations suspectes, applicable à compter du 1er janvier 2024.**

Rox Pay S.r.l. (ci-après « la Société ») met en œuvre la réglementation ci-dessus dans ses documents réglementaires internes.

D'une manière générale, la Société a adopté cette « Politique de lutte contre le blanchiment d'argent et le financement du terrorisme » (ci-après la « Politique ») comme expression de son engagement à lutter contre les phénomènes criminels susmentionnés sur le plan international, en accordant une attention particulière au contraste, dans la conscience que la recherche de rentabilité et d'efficacité doit être combinée avec le contrôle continu et efficace de l'intégrité des structures de l'entreprise.

La Politique appliquée au sein de la Société décrit la politique adoptée par Rox Pay S.r.l. conformément aux règles et principes dictés par les dispositions réglementaires nationales et européennes, dans le respect des normes internationales pertinentes et est mis en œuvre conjointement avec les procédures internes de lutte contre le blanchiment d'argent et le financement du terrorisme, le code d'éthique et les procédures internes qui mettent en œuvre la législation locale primaire et secondaire en vigueur précisant les processus, les rôles et les responsabilités.

La politique actuelle a été approuvée par le conseil d'administration de la société.

Les directives AML et CFT sont appliquées par Rox Pay S.r.l. en cohérence avec les lois applicables.

La Société s'engage à respecter ce cadre réglementaire ainsi que toutes dispositions d'application émises par la Banque d'Italie en matière de vigilance à l'égard de la clientèle, de conservation des données et informations, de l'organisation, des procédures, des contrôles et des contrôles renforcés contre le financement de programmes visant à la prolifération des armes de destruction massive.

La Société s'engage pleinement à garantir que l'organisation opérationnelle et le système de contrôle soient complets, adéquats, fonctionnels et fiables pour la supervision stratégique, à protéger la Société de la tolérance ou du mélange de formes d'illégalité qui peuvent nuire à sa réputation et affecter sa stabilité.

Pour ces raisons, Rox Pay S.r.l. a adopté des règles organisationnelles et comportementales et des systèmes de surveillance et de contrôle visant à assurer le respect de la législation en vigueur par les organes d'administration et de contrôle, le personnel, les collaborateurs et les consultants de la Société. Ces contrôles sont également conformes aux règles et procédures établies par le code de protection des données personnelles.

La Société s'appuie également sur des indicateurs d'anomalies et de modèles de comportements irréguliers dans l'environnement économique et financier, qui sont émis au fil du temps par la Cellule de renseignement financier (CRF) concernant d'éventuelles activités de blanchiment d'argent et de financement du terrorisme.

2.2 - LE CADRE RÉGLEMENTAIRE CONCERNANT LES MESURES RESTRICTIVES ET LES EMBARGO

Toutes les mesures restrictives mises en place pour lutter contre le financement du terrorisme et toutes les activités illicites ou suspectes qui menacent la paix et la sécurité internationales peuvent être soit commerciales, comme les restrictions à l'import/export depuis/vers un pays, soit financières, comme le blocage partiel ou total des transferts de fonds mais aussi les limitations opérationnelles et le gel des fonds.

Les mesures restrictives comprennent des sanctions financières internationales, également appelées embargos, mises en œuvre par l'État italien, des agences étrangères (par exemple OFAC, UKSL) et des organisations supranationales (ONU, UE) à travers une série d'obligations que la Société est tenue de respecter. Certaines mesures restrictives (sanctions) sont imposées à tous les États membres de l'ONU par le Conseil pour mettre en œuvre les résolutions adoptées par le Conseil de sécurité de l'ONU en vertu du Chapitre VII de la Charte des Nations Unies. En outre, des sanctions peuvent être adoptées ou décidées de manière autonome par l'Union européenne au moyen de règlements du Conseil, qui sont immédiatement exécutoires dans chaque État membre afin de garantir leur application rapide et simultanée.

Au niveau international, il existe des réglementations qui établissent des interdictions ou des restrictions spécifiques sur l'investissement dans certains secteurs industriels ou sur l'importation/exportation depuis/vers des « pays à risque élevé ou significatif ». Il s'agit en particulier des résolutions du Conseil de sécurité des Nations Unies (CSNU) au titre de l'article 41 du Chapitre VII de la Charte des Nations Unies, par lesquelles des mesures restrictives sont imposées à l'égard de personnes et/ou de pays.

En ce qui concerne la législation communautaire, les principales dispositions sont :

- le Règlement 2021/821 du Parlement européen et du Conseil du 20 mai 2021[3] **et les modifications ultérieures, par lesquelles un régime européen est établi afin de contrôler les exportations, le transfert, le courtage et le transit de biens à double usage ;**

3 qui a remplacé le règlement 428/2009/CE du Conseil du 5 mai 2009

- le Règlement (UE) 2023/1113 du Parlement européen et du Conseil du 31 mai 2023 relatif aux informations accompagnant les transferts de fonds et de certains crypto-actifs et modifiant la directive (UE) 2015/849 (refonte) ;
- le règlement (UE) 2024/886 du Parlement européen et du Conseil du 13 mars 2024 modifiant les règlements (UE) n° 260/2012 et (UE) 2021/1230 et les directives 98/26/CE et (UE) 2015/2366 en ce qui concerne les virements instantanés en euros ;
- la Directive (UE) 2024/1226 du Parlement européen et du Conseil du 24 avril 2024 relative à la définition des infractions pénales et aux sanctions en cas de violation des mesures restrictives de l'Union et modifiant la directive (UE) 2018/1673 transposée en droit italien par le décret législatif 211/2025.
- **Lignes directrices de l'Autorité bancaire européenne sur les politiques, procédures et contrôles internes visant à garantir la mise en œuvre des mesures restrictives de l'Union et nationales (EBA/GL/2024/14)**[4];
- **Lignes directrices de l'Autorité bancaire européenne concernant les politiques, procédures et contrôles internes visant à garantir la mise en œuvre des mesures restrictives de l'Union et nationales, conformément au règlement (UE) 2023/1113 (EBA/GL/2024/15) concernant les informations accompagnant les transferts de fonds et de certains crypto-actifs, et modifiant la directive (UE) 2015/849.**[5].

Enfin, au niveau national, les embargos sont réglementés comme suit :

- **Législation primaire :**
  - **Décret législatif n° 221/2017, qui a modifié et simplifié les procédures d'autorisation pour l'exportation de biens et de technologies à double usage et les sanctions en matière d'embargos commerciaux ainsi que tous les types d'opérations d'exportation de matériaux proliférants.**
- **Législation secondaire :**
  - **Banque d'Italie Disposition du 12 mai 2023 contenant des indicateurs d'anomalies pour les intermédiaires afin de faciliter l'identification des transactions suspectes.**

Enfin, toutes les réglementations émises par les autorités américaines sont pertinentes pour l'activité de la Société compte tenu des aspects de réputation et de la référence à ces réglementations dans les engagements contractuels impliquant l'application potentielle de sanctions à effet extraterritorial (dites « sanctions secondaires ») américaines. De telles dispositions réglementaires sont contenues dans le USA Patriot Act6 et dans les mesures relatives aux sanctions économiques et commerciales émises par le gouvernement américain par l'intermédiaire de l'Office of Foreign Assets Control (OFAC) du Département du Trésor.[6]

4 que la Banque d'Italie a déclaré son intention de respecter dans la note no. 48 du 8 avril 2025 et applicable à partir du 30 décembre 2025.

5 que la Banque d'Italie a déclaré son intention de respecter dans la note no. 52 du 19 mai 2025 et applicable à partir du 30 décembre 2025.

6 Loi fédérale américaine du 26 octobre 2001, officiellement intitulée « Uniting and Strengthening America by Provider Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ».

3 – MODÈLES ET MÉTHODOLOGIES DE GROUPE

3.1 – ASPECTS GÉNÉRAUX

Le cadre réglementaire national établi pour la prévention du blanchiment de capitaux, du financement du terrorisme et des violations des mesures restrictives repose sur une série d'obligations.

que les destinataires sont tenus de respecter :

- obligation d'adopter des structures organisationnelles, des procédures et des mesures de contrôle interne appropriées ;
- obligation d'adopter des procédures cohérentes pour l'analyse et l'évaluation des risques liés au blanchiment d'argent, au financement du terrorisme et à la violation des mesures restrictives ainsi que d'établir la surveillance, les contrôles et les procédures nécessaires pour atténuer et gérer ces risques ;
- obligation de diligence raisonnable à l'égard de la clientèle, par laquelle la Société acquiert et vérifie des informations sur l'identité d'un client et de tout bénéficiaire effectif, ainsi que sur l'objet et la nature envisagée de la relation ou de la transaction, tout en assurant un suivi constant de toutes les transactions entreprises par le client ;
- une approche basée sur les risques, dans laquelle les obligations de diligence raisonnable à l'égard de la clientèle sont divisées en différents degrés de diligence raisonnable en fonction du profil de risque du client ;
- obligation de conserver les documents, données et informations afin de permettre leur acquisition dans les délais, leur transparence, leur exhaustivité, leur inaltérabilité et leur intégrité, ainsi qu'une accessibilité globale et rapide ;
- obligation de déclaration des transactions suspectes ;
- obligation de s'abstenir d'entrer dans toute nouvelle relation client, de réaliser des transactions occasionnelles ou de maintenir une relation client existante lorsque la diligence raisonnable n'a pas été effectuée ou lorsqu'il est suspecté qu'il peut y avoir un lien avec le blanchiment d'argent ou le financement du terrorisme ;
- obligation de notifier au Ministère de l'Économie et des Finances les infractions visées aux articles 49 et 50 du décret législatif 231/07 et de respecter les limitations d'utilisation des espèces et des titres au porteur ;
- surveiller toutes les transactions avec des personnes physiques et morales et/ou avec des pays figurant sur les listes du Conseil de l'Union européenne (UE), sur la liste de l'Office of Foreign Assets Control (OFAC), sur la UK Sanctions List (UKSL)[7], dans la liste consolidée des sanctions du Conseil de sécurité des Nations Unies (ONU) dans les dispositions émises par les autorités nationales contenant des mesures restrictives spécifiques pour lutter contre le terrorisme ;
- surveiller les transactions conclues avec des pays considérés comme non coopératifs en matière de fiscalité, de contrôle financier et de lutte contre le blanchiment, généralement appelés « paradis fiscaux » ou « centres financiers offshore » ;
- adopter des programmes de formation du personnel appropriés pour assurer la mise en œuvre et la bonne application des lois et réglementations ;
- obligation de fournir à la CRF des « communications objectives » conformément à des des instructions concernant les méthodes et la fréquence des communications ;

7 La liste OFSI (Office of Financial Sanctions Implementation HMT) a été clôturée le 28 janvier 2026 ; à partir de cette date, la liste des sanctions britanniques est la seule source officielle de toutes les désignations de sanctions britanniques.

- obligation de divulguer les manquements ou infractions qui pourraient être portés à la connaissance des organismes de contrôle dans l'exercice de leurs missions ;
- obligation d'adopter des procédures pour gérer les signalements internes des violations soumises par les salariés (Whistleblowing).

En ce qui concerne les activités de lutte contre le financement du terrorisme, la législation italienne impose aux parties obligées de procéder comme suit :

- gel des fonds et des ressources économiques de certaines personnes inscrites sur les listes de l'UE ;
- informer la Cellule de renseignement financier (CRF) des mesures appliquées pour le gel des fonds, ou l'Unité spéciale de police monétaire de la Guardia di Finanza (Police financière) en cas de ressources économiques ;
- informer la CRF des transactions suspectes, des relations d'affaires et de toute autre information disponible concernant les personnes inscrites sur les listes noires publiées par la CRF elle-même ;
- signaler les transactions suspectes qui, sur la base des informations disponibles, sont directement ou indirectement liées à des activités de financement du terrorisme.

En ce qui concerne les sanctions internationales (appelées embargos) et l'exposition à des mesures restrictives, la législation exige que certaines mesures soient prises, notamment :

- données personnelles et contrôles transactionnels sur les opérations liées aux importations et/ou exportations effectuées par les clients, visant à bloquer les importations/exportations depuis ou vers un pays, et réglementations correspondantes. L'interdiction peut être soit générale, touchant tous les types de marchandises, sauf autorisation expresse, soit limitée à certains types de marchandises, par ex. armements (voir code des douanes) ;
- des restrictions totales ou partielles sur les transferts financiers depuis/vers un pays ;
- obligation d'autorisation préalable pour effectuer des transferts ;
- obligation de notifier les virements (sortants ou entrants) ;
- interdiction de financer, de fournir une aide financière ou de mettre des prêts bonifiés à la disposition du gouvernement (directement ou dans certains cas indirectement via des sociétés affiliées ou une participation à des institutions financières internationales) ;
- interdiction de financer des clients opérant avec des pays sanctionnés ;
- mise en œuvre de mesures restrictives contre les sujets russes et biélorusses ;
- la traçabilité des contrôles effectués sur les opérations en provenance ou à destination des pays, personnes et entités soumis à des restrictions.

3.2 - DILIGENCE CLIENT

3.2.1 – Aspects généraux

La Société prend toutes les mesures de diligence raisonnable à l'égard de sa clientèle lorsque :

- établir des relations d'affaires;
- effectuer des transactions occasionnelles, organisées par les clients, telles que des

virements électroniques ou d'autres transactions égales ou supérieures au seuil désigné applicable, que la transaction soit réalisée en une seule opération ou en plusieurs opérations liées ou qu'elle consiste en un transfert de fonds dépassant les limites légales ;

- il existe une suspicion de blanchiment de capitaux ou de financement du terrorisme, indépendamment de toute dérogation, exemption ou seuil désigné pouvant s'appliquer ;
- il existe des doutes sur l'exhaustivité, la fiabilité et la véracité des informations ou documents préalablement acquis aux fins d'identification d'un Client.

Obligations de diligence raisonnable :

- sont remplis :
  - envers de nouveaux clients avant l'établissement d'une relation continue ou la réalisation d'une transaction occasionnelle ;
  - envers les clients existants, chaque fois qu'une diligence raisonnable est appropriée à la lumière d'un changement dans le niveau de risque de blanchiment d'argent ou de financement du terrorisme associé au client ou lorsqu'il existe des soupçons ou des doutes quant à l'exactitude ou à l'adéquation des informations précédemment obtenues auprès du client ;

- et comprend les activités suivantes :
  - identifier le Client, le bénéficiaire effectif et l'exécuteur testamentaire et vérifier leur identité sur la base de documents, données ou informations obtenus auprès d'une source fiable et indépendante ;
  - obtenir et évaluer des informations sur l'objet et la nature envisagée de la relation commerciale ;
  - effectuer un suivi continu pendant toute la durée de la relation client.

A cette fin, la Société - par l'intermédiaire de ses employés et/ou par l'intermédiaire d'agents/conseillers financiers autorisés à faire des offres hors établissement et qui entrent en contact direct avec le Client - obtient les informations requises par la réglementation et collecte toute autre documentation pertinente comme spécifié dans la présente Politique et dans les documents de procédure de la Société.

La Société applique des mesures de vigilance ordinaires, simplifiées ou renforcées selon l'approche par les risques appliquée aux clients.

3.2.2 - Intégration client à distance

Dans les cas où la Société utilise des méthodes d'identification à distance autorisées par le décret législatif n. 231/07, article 19, paragraphe 1, point a), points 2 et 5, elle adopte des procédures particulières pour s'acquitter de ses obligations de diligence, compte tenu également du risque de fraude lié à l'usurpation d'identité. Dans ce cas, l'identification repose sur l'acquisition du certificat de signature électronique qualifié, qui est généré après un processus d'identification effectué à travers :

- l'utilisation du système public d'identité numérique (SPID) ou de la carte d'identité électronique ;
- au moyen de techniques et de procédures d'identification électronique sécurisées et réglementées, autorisées ou reconnues par l'Agence pour l'Italie Numérique.

Dans tous les cas, le processus d'identification à distance implique la collecte sous forme électronique des données d'identification du client et de tout exécuteur testamentaire, ainsi

que la réalisation de vérifications et de contrôles de l'authenticité des données, en plus de celles prévues pour l'identification physique, selon une approche basée sur les risques, y compris par un contact téléphonique sur un numéro certifié (appel de bienvenue) ou par un transfert d'argent effectué par le client via un intermédiaire bancaire et financier basé en Italie.

Afin de limiter l'exposition aux risques potentiels de blanchiment d'argent et/ou de fraude, il n'est pas permis d'établir des relations bancaires à distance avec des personnes morales ou des personnes physiques agissant pour le compte d'une personne morale, sauf si elles ont été identifiées personnellement (face à face).

L'établissement de relations bancaires à distance avec des clients qui ne résident pas en Italie n'est pas autorisé.

3.2.3 – Évaluation préalable à la mise en œuvre et surveillance continue des processus d'ouverture de relations à distance.

Les processus d'identification et d'onboarding des clients à distance sont formalisés et détaillés dans le règlement intérieur. Le modèle de supervision de ces processus comprend :

I. l'évaluation préliminaire de la solution d'onboarding à distance (appelée Pre-Implementation Assessment)[8]) visant à :
   (i) évaluer l'adéquation de la solution en termes d'exhaustivité et d'exactitude des données et documents à collecter, ainsi que de fiabilité et d'indépendance des sources d'informations utilisées ;
   (ii) évaluer l'impact de l'utilisation de la solution sur les risques commerciaux, y compris les risques opérationnels, de réputation et juridiques grâce à l'implication des fonctions techniques et spécialisées concernées ;
   (iii) identifier les mesures d'atténuation et les actions correctives pour chaque risque identifié ;
   (iv) définir des tests ex ante pour évaluer les risques TIC et de fraude ainsi que des tests de bout en bout sur le fonctionnement de la solution.

II. surveillance continue de la solution d'intégration adoptée au moyen de contrôles périodiques et événementiels pour garantir son bon fonctionnement dans le temps (ce que l'on appelle la surveillance continue).

III. l'examen de l'évaluation préliminaire de la solution d'intégration à distance (dite évaluation préalable à la mise en œuvre) lorsque des changements structurels dans la solution adoptée ou certains événements surviennent tels que :
   (i) l'évolution de l'exposition aux risques en matière de lutte contre le blanchiment d'argent et le financement du terrorisme, ainsi que les embargos ;
   ii) les lacunes détectées pour que notre solution fonctionne ;
   iii) une augmentation des tentatives de fraude ;
   (iv) les changements dans la législation.

3.2.4 – Obligations de diligence raisonnable simplifiées

De manière générale, la Société utilise une approche basée sur les risques pour identifier les types de clients auxquels des mesures de diligence raisonnable simplifiées peuvent être appliquées. Cela inclut les cas où des « indicateurs de risque faible » sont présents, comme indiqué à l'annexe 1 de la disposition de la Banque d'Italie sur le devoir de vigilance à l'égard de la clientèle du 30 juillet 2019 (ci-après « la disposition »).

8 Note n° 32 du 13 juin 2023 par laquelle la Banque d'Italie a déclaré son intention de se conformer aux lignes directrices de l'ABE (EBA/GL/2022/15) sur l'utilisation de solutions d'intégration des clients à distance.

Les « indicateurs de risque faible » pertinents pour appliquer une procédure de due diligence simplifiée sont basés sur le type de client, d'exécuteur ou de bénéficiaire effectif, la zone géographique de résidence ou dans laquelle le siège social est établi, un produit, un service ou un canal de distribution spécifique.

Plus précisément, les types de clients considérés comme présentant un faible risque de blanchiment d'argent, auxquels la diligence raisonnable simplifiée peut s'appliquer, comprennent :

- Administrations publiques, institutions ou organismes exerçant des fonctions publiques, conformément au droit de l'Union européenne ;
- Sociétés cotées sur un marché réglementé et soumises à des exigences de divulgation, notamment en garantissant une transparence adéquate sur la propriété effective ultime ;
- les établissements de crédit et financiers de la Communauté européenne énumérés à l'article 3 (2) du décret anti-blanchiment - à l'exception de ceux aux lettres i), o), s), v)[9]— et les établissements de crédit et financiers résidant dans des États membres ou des pays tiers dotés de systèmes efficaces de blanchiment de capitaux et de financement du terrorisme;
- Clients, exécuteurs testamentaires ou ayants droit économiques résidant ou établis dans des zones géographiques à faible risque de blanchiment.

La Société n'applique pas de mesures simplifiées de vigilance à l'égard de la clientèle lorsque :

- des doutes, des incertitudes ou des incohérences surviennent concernant les données d'identification et les informations recueillies lors de l'identification du client, de l'exécuteur testamentaire ou du bénéficiaire effectif ;
- les conditions d'une vigilance simplifiée à l'égard de la clientèle ne sont plus remplies sur la base des indicateurs de risque prévus par le décret anti-blanchiment et la réglementation dérivée y relative ;
- le suivi de l'ensemble des opérations réalisées par le client et des informations recueillies tout au long de la relation exclut un type de risque faible ;
- le suspect de blanchiment d'argent ou de financement du terrorisme se pose toujours.

La Fonction Anti-Blanchiment a la responsabilité exclusive de l'évaluation et de l'autorisation des mesures simplifiées de vigilance à l'égard de la clientèle, réalisées en suivant toutes les étapes requises pour le processus ordinaire de vigilance à l'égard de la clientèle - y compris l'obligation d'identifier et de vérifier l'identité du client, de l'exécuteur testamentaire et du bénéficiaire effectif, et d'acquérir toutes les données et documents nécessaires à leur enregistrement complet (par exemple, nom, statut juridique, siège social et, le cas échéant, code fiscal) - bien qu'en réduisant leur niveau de profondeur, leur portée et leur fréquence.

3.2.5 – Des obligations de diligence raisonnable renforcées

La Société applique des mesures de vigilance renforcées à l'égard de sa clientèle en présence de clients ou de situations présentant un risque plus élevé de blanchiment d'argent ou de financement du terrorisme et dans tous les cas visés à l'article 24 du décret. Ces mesures renforcées incluent, entre autres, l'implication de rôles de responsabilité proportionnés au niveau de risque identifié par rapport au client.

9 i) les courtiers en valeurs mobilières mentionnés à l'article 201 du TUF ; o) les intermédiaires d'assurance visés à l'article 109, alinéa 2, lettres a), b) et d), de la CAP, exerçant dans les branches d'activité visées à l'article 2, alinéa 1, de la CAP ; s) les sociétés fiduciaires inscrites au registre établi conformément à l'article 106 du TUB ; v) les conseillers financiers mentionnés à l'article 18-bis du TUF et les cabinets de conseils financiers mentionnés à l'article 18-ter du TUF.

Concernant les clients de la banque privée, la Société évalue les facteurs de risques spécifiques inhérents à la nature de leur activité et applique des mesures de vigilance renforcées sur la base de l'ensemble des informations disponibles et des évaluations réalisées.

L'intervention de la Fonction Anti-Blanchiment est requise dans les cas suivants :

- les personnes physiques et morales inscrites sur les listes des personnes ou entités soumises à des mesures de gel des fonds en vertu des règlements ou décrets européens en vertu du décret législatif 109/07, ainsi que celles qui leur sont étroitement liées ;
- une relation de correspondant bancaire transfrontalier établie avec une banque ou un établissement situé dans un pays tiers, sur la base de facteurs géographiques à haut risque (comme indiqué dans l'annexe 2 des dispositions de la Banque d'Italie sur la diligence raisonnable en matière de clientèle) ;
- relations ou transactions dans lesquelles le client ou le bénéficiaire effectif ultime est une personne politiquement exposée[10];
- les situations comportant des éléments de risque qui nécessitent l'application de mesures de confidentialité spécifiques ;
- situation présentant un risque plus élevé de blanchiment d'argent ou de financement du terrorisme en raison de contingences objectives, environnementales ou subjectives ;
- les clients classés comme « Trust », les services de transfert d'argent et les échanges de devises virtuelles ;
- les sociétés de fiducie, sauf dans les cas prévus au paragraphe 3.4 ;

Par ailleurs, avant d'entrer, de poursuivre ou d'entretenir une relation continue avec des Personnes Politiquement Exposées ou des Entités Correspondantes de pays tiers, il est nécessaire d'obtenir l'autorisation appropriée du Directeur Général ou de son délégué, après avoir obtenu l'avis de la Fonction Anti-Blanchiment. Dans le cas de délégués conformément à l'article 25 du décret législatif 231/07 appartenant à la fonction anti-blanchiment d'argent, cette autorisation est incluse dans le processus de diligence renforcée.

Dans tous les autres cas, l'application de mesures renforcées est proportionnelle au niveau de risque imputé au client. Si le risque est considéré comme moyen/élevé, ou si certains facteurs de risque sont présents quelle que soit la note attribuée, l'implication du responsable de l'unité commerciale responsable de la gestion commerciale du client est requise.

Des exemples de tels cas sont :

- les clients personnes morales ayant un Exécuteur identifié comme PEP ou PEP indirecte, quel que soit le profil de risque ;
- services offerts par l'intermédiaire de réseaux d'agents financiers, de conseillers financiers, d'entrepreneurs et d'agents ;
- les clients classés en Fondation/Organisations à but non lucratif ;
- les clients personnes morales pendant la phase d'intégration ;
- les clients ayant reçu des nouvelles négatives lors de la phase d'intégration (« Nouvelles indésirables ») ;

10 Personnes Politiquement Exposées (PPE) : telles qu'énumérées par l'art. 1, paragraphe 2, lettre dd) Décret législatif 231/07.

- les clients résidant ou basés dans des pays tiers à haut risque ou dans le cas de relations continues, de services professionnels et d'opérations impliquant des pays à haut risque ;
- les sociétés qui ont émis des actions au porteur ou qui ont une société émettant des actions au porteur au sein de leur structure de chaîne de contrôle ;
- relations ou transactions dans lesquelles le client et le bénéficiaire effectif ultime exercent une fonction publique autre que celles énumérées pour les personnes politiquement exposées[11];
- sociétés détenues par des fiducies, des sociétés de fiducie, des fondations, des sociétés par actions à travers plusieurs niveaux de participation ou des participations croisées ;
- les clients exerçant un type d'activité économique particulièrement exposé au risque de blanchiment ou dans des secteurs d'activité « controversés »[12]ou des activités commerciales à forte intensité de liquidités, telles que l'argent contre de l'or, le change, les jeux d'argent/paris, y compris en ligne, l'industrie de l'armement, l'exploitation minière, la collecte et l'élimination des déchets, la production d'énergie renouvelable, les entreprises opérant dans le secteur des crypto-actifs, la construction, l'achat d'instruments pharmaceutiques ;
- les clients participant à des marchés publics ou bénéficiant de financements publics (santé, construction, collecte et élimination des déchets, production d'énergie renouvelable, exploitation minière, fourniture d'instruments pharmaceutiques) ;
- dans le cas de clients qui ont acquis la citoyenneté d'un État membre ou obtenu des droits de séjour dans un État membre (UE) grâce à un programme de citoyenneté par investissement ou de résidence par investissement ;
- dans le cas de clients personnes morales résidant dans un pays de l'UE, où les droits de propriété de la société sont détenus - directement ou indirectement - à plus de 40 % par une personne morale, une organisation ou un organisme établi en Russie, ou par une personne physique résidant ou citoyen russe.

L'implication du responsable de la business unit en charge de la gestion commerciale du client est également requise en cas d'erreurs informatiques susceptibles d'empêcher le calcul en temps réel du risque de blanchiment du client.

Les mesures de vigilance renforcées comprennent l'acquisition d'informations complémentaires sur le client, l'exécuteur testamentaire et le bénéficiaire effectif, l'enquête sur l'objet et la nature de la relation et l'augmentation de la fréquence des procédures visant à assurer un contrôle continu tout au long de la relation en cours.

En pleine conformité avec la législation en vigueur et les dispositions des procédures internes de lutte contre le blanchiment d'argent et le financement du terrorisme et conformément au Code d'éthique de la Société, la Société ne soutient pas de transactions avec des clients opérant dans des secteurs controversés qui
(i) ne sont pas conformes à la législation nationale en vigueur et (ii) ne sont pas, le cas échéant, autorisés au préalable par les autorités nationales italiennes compétentes, notamment :

- la production, le transit et/ou la commercialisation de matériels d'armement ;
- la production et la vente de marijuana légère, les lieux de divertissement pour adultes ;

11 Fonctions publiques autres que celles exercées par des personnes politiquement exposées (PPE) telles que visées à la note 1), s'appliquant à toutes les personnes exerçant des fonctions dans, mais sans s'y limiter, des organismes publics, des consortiums, des associations à caractère public tels que énumérés à la section A 8) de l'annexe 2 de la disposition.
12 un secteur économique est « controversé » si les biens/services fabriqués/offerts et/ou les manières dont ils sont produits/offerts contrastent avec les valeurs largement partagées d'éthique et de durabilité, même lorsque les services ou activités sont licites et donc non contraires aux obligations légales.

- activités commerciales à forte intensité de liquidités autres que celles énumérées ci-dessus, telles que les organisations caritatives et les ONG non réglementées, la production de métaux et de pierres précieux, les envois de fonds.

En outre, la Société accorde une attention particulière au respect des mesures restrictives mises en place par l'État italien, des organismes étrangers (par exemple OFAC, UKSL) et/ou des organismes supranationaux (ONU, UE). Ces mesures peuvent être de nature commerciale (par exemple, blocage des importations/exportations) ou de nature financière, comme le blocage partiel/total des transferts d'argent depuis ou vers un pays spécifique ou des limitations des opérations et/ou le gel des fonds détenus auprès d'intermédiaires financiers.

Afin de respecter les obligations énoncées dans le décret législatif italien 109/07 - visant à prévenir et combattre le financement du terrorisme et les activités des pays menaçant la paix et la sécurité internationales, à travers l'application de mesures restrictives visant à "geler" les fonds et les ressources économiques détenus par des personnes physiques et morales, des groupes et des entités spécifiquement identifiés par les Nations Unies et l'Union européenne ("sujets désignés") - et les obligations de diligence raisonnable renforcées énoncées dans le décret législatif italien 231/07, la Société a adopté un contrôle automatique. procédures. Ces procédures sont capables de vérifier la cohérence entre les données d'identification des clients obtenues dans le cadre du processus de due diligence et celles contenues dans les listes élaborées par l'UE et d'autres institutions et organismes internationaux, tels que :

- les personnes physiques chargées d'une fonction publique importante ou qui ont cessé d'exercer ces fonctions depuis moins d'un an (PEP), les membres de leur famille et ceux ayant des liens étroits avec elles selon la définition de l'art. 1 c. 2 lettre dd du décret législatif 231/07 (PPE résidentes et non-résidentes) ;
- les personnes résidant en Italie et exerçant des fonctions publiques, qui n'entrent pas dans la définition des PPE, mais sont néanmoins exposées à un risque important de corruption et de blanchiment d'argent ;
- les personnes physiques et morales opérant, même partiellement, dans des États qui n'imposent pas de mesures et réglementations équivalentes, selon les lignes directrices de la Banque d'Italie ou d'autres institutions nationales ou supranationales engagées dans la prévention du crime ;
- personnes physiques et morales soumises à des mesures d'embargo ou au gel de fonds/ressources économiques et d'avoirs financiers (Listes de sanctions ONU, UE, UKSL, OFAC).

3.3 - PROFILAGE CLIENT

La Société adopte des procédures appropriées visant à définir le profil de risque de blanchiment d'argent et de financement du terrorisme (RP) attribuable à chaque client, sur la base des informations acquises et des analyses effectuées, en référence à la fois aux éléments d'évaluation indiqués dans la Disposition et à d'autres éléments qui peuvent être adoptés par la Société elle-même au fil du temps (ce que l'on appelle le profilage).

Sur la base du profilage des clients, également réalisé périodiquement, la Société applique des mesures standards ou renforcées, qui incluent l'implication de rôles de responsabilité proportionnés au niveau de risque identifié du client. L'avis préalable de la Fonction Anti-Blanchiment est requis conformément aux responsabilités définies dans le document interne «

Procédures Internes de Lutte contre le Blanchiment et le Financement du Terrorisme ».

Le classement des clients en due diligence simplifiée est autorisé par la Fonction Anti-Blanchiment, à la demande du Responsable de la Business Unit Opérationnelle.

Dans un tel cas, la portée et la fréquence des exigences sont réduites, la vérification expirant au bout de 8 ans quel que soit le score de risque, à moins que les conditions d'application des diligences simplifiées ne soient plus remplies.

Par ailleurs, la Société a mis en place une procédure informatique permettant d'évaluer le profil de risque du client et de définir de manière cohérente un délai de réévaluation adapté au niveau de risque calculé ; la fréquence de réévaluation dépend du processus identifié lors de la dernière évaluation réalisée ou, en l'absence de questionnaire KYC, du profil de risque du client, comme précisé ci-dessous :

Classe de risque (RP)	Score	Processus de diligence raisonnable	Rôle de validation	Fréquence de réévaluation
Clients classés comme soumis aux diligences simplifiées	NA	Simplifié	Réception automatique/Business Manager (*)	8 ans
Immatériel	<=5	Norme	Acceptation automatique	8 ans
Faible	>=6 et <=12			6 ans
Moyen	>=13 et <=24	Amélioré	Responsable d'unité commerciale (**)	2 ans
Élevé	>=25			1 an
En cas d'éléments de risque spécifiques (***)		Amélioré	Fonction de validation AML	1 an

(*) à préciser si le score de risque calculé ou résultant du KYC réalisé est au moins moyen. (**) fourni même en présence d'éléments de risque définis qui maintiennent le profil de risque en dessous de moyen.
(***) à condition même en présence d'entités juridiques avec RP >39, si elles exercent des activités commerciales liées à l'achat d'or, aux jeux et paris et à la collecte et à l'élimination des déchets (codes ATECO à haut risque) et/ou si elles sont soumises à des audits/enquêtes.

3.4 - OUTILS POUR SOUTENIR LA DILIGENCE DÛE

La Société a mis en œuvre des outils technologiquement avancés pour soutenir les processus de lutte contre le blanchiment d'argent, aux côtés des applications traditionnelles déjà utilisées :

- Robotic Process Automation (RPA) appliqué aux activités de collecte de données dans les domaines de la due diligence client et du reporting des transactions suspectes ;
- Moteur d'intelligence artificielle, basé sur des composants statistiques et des indicateurs prédictifs (Predict Index AML, Reputational Index et Criminal Infiltration Index) construits avec des techniques d'analyse de données, appliqués au processus régulier d'évaluation des clients ;
- Plateforme de renseignement Cogito, une application utilisée pour collecter des actualités, des documents et des informations textuelles afin de rechercher des nouvelles défavorables concernant les clients soumis à une diligence raisonnable ;
- Rozes, un outil de data intelligence qui, en analysant les états financiers en temps réel, permet d'identifier les entreprises dont le bilan et les indicateurs financiers sont

similaires à ceux des entreprises victimes d'infiltration criminelle.

De plus, dans le cadre des outils avancés mentionnés ci-dessus, certains « événements déclencheurs » ont été identifiés, visant à intercepter des événements concernant le client et/ou les relations associées, déterminant une variation de la date d'expiration de l'« Évaluation Client - KYC », par exemple :

- en cas de modification des données du registre du bénéficiaire effectif et du représentant légal ;
- en cas de modification du Profil de Risque en raison de la présence de certains facteurs de risque élevés parmi ceux prévus par la Disposition ;
- en cas de prise en charge par un bénéficiaire effectif de la fonction de PEP, ou d'enregistrement d'un nouveau bénéficiaire effectif de PEP ;
- en cas de délégation à une personne physique de la relation client donnée à une personne classée PPE ;
- en cas de divergence entre le bénéficiaire effectif inscrit au registre et les preuves recueillies à partir des extraits de la Chambre de Commerce ;
- en cas de contrôles de deuxième niveau par la Fonction LBC.

La responsabilité du processus de diligence raisonnable d'un client incombe à l'unité de gestion des relations clients, qui gère généralement l'établissement de nouvelles relations continues, exécute toutes les transactions occasionnelles, réévalue périodiquement les clients existants et assure un suivi continu de la relation client.

3.5 - OBLIGATIONS D'ABSTENTION

La Société s'abstient d'établir, d'exécuter ou de poursuivre la relation, les opérations et les services professionnels (ce que l'on appelle l'obligation d'abstention) en cas d'impossibilité objective d'exercer une diligence raisonnable à l'égard de la clientèle, en évaluant l'opportunité de déclarer une transaction suspecte à la CRF.

Dans les cas où l'abstention n'est pas possible, car il existe une obligation légale d'exécuter l'opération qui ne peut être différée ou si son refus pourrait entraver l'enquête, la Société est néanmoins tenue de déclarer immédiatement l'opération suspecte.

Par ailleurs, si après une évaluation plus approfondie ou en aval du processus de due diligence renforcée, des éléments de risque élevé apparaissent qui pourraient affecter le profil juridique et/ou réputationnel de la Société, la Société se réserve le droit de limiter ou de mettre fin à la relation commerciale avec le client. Ces limitations peuvent concerner par exemple l'accès des clients à certains types de produits ou entraîner l'interruption des services proposés par la Société en relation avec le compte/la relation.

Les mesures de vigilance à l'égard de la clientèle adoptées par la Société n'empêchent cependant pas/refusent l'accès aux services financiers aux clients ou à des catégories entières de clients à haut risque qui y auraient droit en vertu de la législation en vigueur, sauf dans les cas expressément prévus par le décret législatif 231/07, concernant l'interdiction d'entretenir des relations avec certains types d'entités.

La Société n'entre pas de relation de correspondant avec une banque fictive et s'abstient d'entrer en relation avec des entités qui permettent d'accéder à des relations de correspondant avec une banque fictive. Elle ne peut nouer de relations d'affaires avec des entités dont la structure de propriété (corporative, fiscale et financière) se caractérise par un degré élevé d'opacité qui empêche l'identification claire du bénéficiaire effectif ou de la nature et de l'objet de la structure.

A cette fin, la Société prend toutes les mesures pour s'assurer qu'elle ne collabore pas délibérément et sciemment avec des institutions financières qui opèrent elles-mêmes avec des banques fictives.

Par ailleurs, la Société s'interdit d'entrer ou de poursuivre des relations d'affaires avec des personnes particulièrement exposées au risque de blanchiment/financement du terrorisme, telles que :

- Les sociétés de fiducie ayant leur siège social dans un pays indiqué par le GAFI comme présentant un risque de blanchiment d'argent plus élevé ou qui n'adoptent pas de mesures conformes aux obligations imposées par le décret législatif 231/07 ou les directives européennes ;
- Les fiducies pour lesquelles des informations appropriées, exactes et à jour sur la propriété effective de la fiducie, sa nature et son objet ne sont pas disponibles ;
- Les sociétés de paris, y compris les opérateurs de jeux en ligne, de casinos et de bingo, pour lesquels les autorisations et/ou licences requises par la législation italienne et internationale n'ont pas été délivrées et/ou vérifiées ;
- Entités affiliées et agents de prestataires de services de paiement (visés dans la définition de l'art.1 c. 2 lettre nn) et établissements de monnaie électronique qui ne respectent pas les dispositions du chapitre V du décret législatif 231/07 aux articles 43 et suivants ;
- Sociétés à responsabilité limitée ou sociétés contrôlées par actions au porteur, dont le siège social est situé dans des pays à haut risque ;
- Clients opérant dans la production et la vente de marijuana légère ou dans des lieux de divertissement pour adultes, s'ils ne sont pas en mesure de vérifier les autorisations requises par la loi.

La Société utilise toutes les informations acquises lors du processus de due diligence concernant ses clients et leurs transactions pour déterminer si une transaction ou une relation commerciale est, directement ou indirectement, liée à des personnes ou entités impliquées dans le blanchiment d'argent, le financement du terrorisme ou dans le développement d'armes de destruction massive, et ne soutient en aucun cas des transactions impliquant des armes controversées et/ou interdites par les traités internationaux,
par ex. armes nucléaires, biologiques et chimiques, bombes à fragmentation, armes contenant de l'uranium appauvri, mines terrestres antipersonnel.

En ce qui concerne la production, le transit et/ou la commercialisation de matériels d'armement autres que ceux mentionnés ci-dessus, la Société pourra soutenir des transactions dûment autorisées par les autorités compétentes et conformes à la législation applicable et en vigueur.

3.6 – DÉCLARATION DE TRANSACTIONS SUSPECTES

Chaque fois que la Société soupçonne ou a des motifs raisonnables de soupçonner qu'une opération de blanchiment d'argent ou de financement du terrorisme a été ou est en cours de réalisation ou de tentative :

- elle soumet une déclaration de transaction suspecte à la Cellule de renseignement financier (CRF), si la transaction est basée en Italie ;

- si la transaction est basée dans un autre pays, elle respecte les dispositions de la législation locale et, lorsque celle-ci prévoit l'application de mesures équivalentes à celles prévues par le droit de l'UE, elle en informe sans délai le responsable de la lutte contre le blanchiment d'argent, en prenant toutes les précautions nécessaires pour protéger l'identité des personnes déclarant la transaction suspecte.

La Société a mis en place des procédures et des processus pour surveiller, identifier et signaler les activités suspectes conformément au calendrier et aux méthodes requis par la loi applicable.

Les employés signalent sans délai toute connaissance ou suspicion de blanchiment d'argent, de financement du terrorisme ou d'autres activités criminelles, ou de produits d'activités criminelles, quelle que soit leur taille, conformément au modèle organisationnel mis à jour et aux modes de fonctionnement prévus dans le règlement interne de référence. Jusqu'à ce que le processus de déclaration soit terminé, la Société s'abstient d'exécuter l'opération, sauf si cela est impossible en raison d'une obligation légale d'accepter l'acte ou si l'exécution de l'opération ne peut être reportée en raison de la conduite normale des affaires ou si elle pourrait entraver les enquêtes. Dans ces cas, le rapport est soumis immédiatement après l'exécution de la transaction.

Les motifs de suspicion comprennent les caractéristiques, l'ampleur et la nature de la transaction, la tentative de scission de la transaction et toute autre circonstance dont les employés ont connaissance dans le cadre de leurs fonctions, en tenant également compte de l'ampleur financière et de la nature de l'activité exercée par la personne concernée, sur la base des éléments acquis conformément à la législation anti-blanchiment (par exemple lors d'une due diligence).

Afin de limiter le risque d'implication de la Société – même involontaire – dans les activités illégales mentionnées ci-dessus, un processus de due diligence renforcé est activé dans les accords de transfert de fonds où les acteurs impliqués dans ce type de transaction (initiateur, bénéficiaire, banques impliquées dans le transfert de fonds) peuvent conduire à des soupçons de blanchiment d'argent, de financement du terrorisme ou de violations des restrictions internationales applicables sur certains biens, personnes ou entités.

En aval du processus de reporting, la Société peut limiter et/ou interrompre la relation commerciale avec les clients, notamment lorsque cette relation peut constituer un risque juridique ou de réputation important pour Rox Pay S.r.l.

3.7 – CONSERVATION DES DONNÉES

La Société conserve tous les documents et enregistre toutes les données obtenues dans le cadre du processus de diligence raisonnable envers la clientèle, garantissant ainsi la traçabilité des transactions des clients afin de faciliter les fonctions de contrôle de la Banque d'Italie et de la CRF, y compris les inspections.

À cette fin, Rox Pay S.r.l., en tant qu'intermédiaire financier basé en Italie, a mis en place une Archive électronique unique (Archivio Unico Informatico ou AUI) qui lui permet de fournir des informations à la Banque d'Italie et à la CRF selon les normes techniques spécifiées à l'annexe 2 des Dispositions sur la conservation des données. Ces archives stockent électroniquement toutes les données d'identification et autres informations liées aux relations commerciales en cours et aux transactions clients, comme l'exige la loi applicable.

A cet égard, en réponse aux récentes mises à jour introduites par les « Dispositions sur la conservation des données et l'accès aux documents, données et informations » et les « Dispositions sur la transmission des données agrégées », la Société a décidé d'adopter certains principes d'exonération des obligations d'enregistrement tels qu'expressément prévus. En particulier, les données et informations concernant les opérations conclues par les intermédiaires bancaires et financiers, qui relèvent des cas prévus à l'article

8 des dispositions sur la conservation des données et l'article 3 des dispositions sur les données agrégées ne sont pas enregistrés dans l'archive électronique unique.

Concernant les exigences de vigilance à l'égard de la clientèle, la Société conserve des copies ou des enregistrements de tous les documents requis pendant une durée de dix ans après la fin de la relation commerciale.

En ce qui concerne les transactions et les relations commerciales en cours, toutes les pièces justificatives et documents, par exemple les documents originaux ou les copies admissibles en justice, sont conservés pendant une durée de dix ans après l'exécution de la transaction ou après la fin de la relation commerciale.

3.8 – PRÉVENTION REGARGIN MESURES RESTRICTIVES

Compte tenu de la nature, de la taille et de la complexité de son activité, ainsi que de la gamme et du type de services fournis, la Société est exposée au risque de violation des mesures restrictives.

Afin de maintenir un système organisationnel et procédural visant à garantir le respect des mesures restrictives internationales européennes et nationales, le risque de violation des mesures restrictives est évalué par la fonction anti-blanchiment d'argent sur la base de facteurs géographiques, de clients, de produits/services et de canaux de distribution, assurant un contrôle constant de l'efficacité du système, également garanti par la réalisation périodique d'un exercice d'auto-évaluation, qui permet d'identifier d'éventuelles actions correctives en réponse à la détection de problèmes critiques existants et/ou l'adoption de mesures appropriées de prévention et d'atténuation des risques.

La Société a établi des procédures et des processus pour surveiller, identifier et signaler les activités qui enfreignent les mesures restrictives, avec des délais et des méthodes conformes aux exigences légales.

Les contrôles existants sur les personnes/entités et les transactions sont effectués au moyen d'un processus de filtrage automatisé, effectué quotidiennement et pendant la phase d'intégration, à l'aide de listes spécifiques – mises à jour deux fois par jour – concernant les clients, les contreparties, les pays et les transactions.

Des processus sont en place pour contrôler les flux entrants ou sortants avec les pays et/ou entités soumis à des sanctions financières internationales, avec des responsabilités définies entre les services compétents.

Le personnel est assuré d'être correctement formé et sensibilisé aux politiques, procédures et contrôles afin de se conformer aux mesures restrictives.

4 – LISTE DES PROCESSUS CLÉS

4.1 – GESTION DES RISQUES DE BLANCHIMENT D'ARGENT ET DE FINANCEMENT DU TERRORISME

Le processus « Gestion des risques de blanchiment d'argent et de financement du terrorisme » est le processus par lequel les activités suivantes sont menées au sein de la Société afin

d’atténuer le risque de non-conformité aux exigences en matière de lutte contre le blanchiment d’argent et le financement du terrorisme :

- Identifier le risque de non-conformité aux exigences de LBC-FT grâce à une surveillance continue des modifications de la législation et à l'évaluation des impacts sur les processus et procédures commerciales ainsi qu'à l'identification et à l'évaluation des risques de LBC-FT en utilisant une approche basée sur les risques ;

- Gestion et atténuation du risque de blanchiment d'argent et de financement du terrorisme par la mise en œuvre et le suivi des actions d'atténuation des risques de non-conformité prévues dans le Plan Annuel (Plan AML) ou identifiées par la Gouvernance de la Société telles qu'appliquées par toutes les fonctions commerciales concernées dans la mise en œuvre des procédures (règlement intérieur, applications informatiques, processus opérationnels, contrôles) ;
- Contrôles de conformité (ex-ante et ex-post) dans les domaines réglementaires assignés par la propriété en définissant et en suivant des indicateurs de risques et leur évolution dans le temps. L'objectif est de détecter d'éventuelles situations de non-conformité ainsi que d'effectuer les activités de contrôle ex ante et ex post ;
- Fournir des conseils et un soutien sur les questions de LBC/FT, en participant à des équipes de travail interfonctionnelles et en fournissant un soutien soit aux structures de l'entreprise, soit aux organes de direction supérieure dans les questions et processus commerciaux où le risque de blanchiment d'argent et de financement du terrorisme est pertinent, en effectuant les accomplissements prévus par les réglementations de surveillance et en effectuant une évaluation préliminaire de conformité dans ce domaine lors de l'offre de nouveaux produits/services ;
- Surveillance et contrôle des risques de LBC/FT en analysant les flux d'informations reçus du niveau I et d'autres fonctions de contrôle liées aux exigences opérationnelles en matière de lutte contre le blanchiment d'argent et en mettant en œuvre des contrôles de surveillance des risques et en vérifiant constamment leur adéquation ;
- Réaliser une auto-évaluation AML en effectuant les activités préliminaires nécessaires pour compléter les questionnaires dits « Système » et « Opérationnel » ainsi que pour déterminer le risque résiduel ;
- Rendre compte aux plus hauts organes sociaux et aux autorités de contrôle, se préparer plus spécifiquement à rendre compte annuellement aux organes sociaux et au Conseil de Surveillance ainsi qu'à préparer un rapport périodique sur les activités réalisées et toute demande spécifique des Autorités de Contrôle ;
- Proposer des formations spécifiques en matière de LBC/FT en organisant un plan de formation adéquat en collaboration avec les autres fonctions de l'entreprise chargées de la formation. L'objectif est de parvenir à une formation continue des salariés et des collaborateurs.

Les règles et responsabilités spécifiques de la Société concernant ce processus sont détaillées dans le règlement intérieur
document « Procédures internes de lutte contre le blanchiment d'argent et le financement du terrorisme ».

4.2 – GESTION DES RELATIONS AVEC LES AUTORITÉS DE CONTRÔLE POUR LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

Le processus de gestion des relations réglementaires LAB/CFT est le processus par lequel les activités sont menées au sein de la Société pour gérer, analyser, diriger et surveiller toutes les communications avec les régulateurs sur les questions liées à la lutte contre le blanchiment d'argent et le financement du terrorisme. L'objectif est de superviser ces activités, y compris l'archivage des documents dans un référentiel unique.

Les activités suivantes sont réalisées dans le cadre de ce processus :

- Gestion des relations avec les Autorités de Contrôle (Anti-Blanchiment d'Argent),

gestion, analyse et traitement des communications et des demandes des Autorités de Contrôle concernant la conformité dans le domaine ;

- Gestion des rapports de surveillance anti-blanchiment, en préparant le flux et l'envoi des rapports de surveillance anti-blanchiment ;

- Gestion des procédures administratives liées à la lutte contre le blanchiment d'argent à travers l'examen des demandes reconventionnelles relatives aux procédures administratives notifiées à la Société par les autorités compétentes (GdF et CRF) ainsi que la représentation de la Société devant le MEF, en étant responsable du recensement des procédures dans l'application concernée et de l'affectation à la Provision pour Risques et Charges et des éventuels paiements de sanctions, en coordination avec la Fonction Budgétaire.

Les règles et responsabilités spécifiques de la Société concernant ce processus sont détaillées dans le document interne « Procédures internes de lutte contre le blanchiment d'argent et le financement du terrorisme ».

4.3 – GESTION DES BESOINS OPÉRATIONNELS POUR LUTTER CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

Le processus de gestion des exigences opérationnelles LAB/CFT est le processus par lequel les activités suivantes sont menées au sein de la Société afin de se conformer aux exigences réglementaires :

- limiter l'utilisation d'espèces et de titres au porteur, en appliquant les exigences réglementaires concernant les limitations à l'utilisation d'espèces et d'obligations/titres au porteur ;
- gérer les obligations adéquates de vigilance à l'égard de la clientèle, en exécutant les activités de vigilance à l'égard de la clientèle (ou de diligence renforcée) dans les cas établis par la loi italienne (Décret législatif 231/07 et modifications ultérieures) en fonction du profil de risque des clients, en soutenant le Réseau de la Société dans le respect des obligations requises par les lois et réglementations en vigueur, et en apportant un soutien aux structures de la Société gérant les relations avec les clients et les contreparties bancaires et financières afin de permettre l'établissement et le maintien des relations ;
- gérer les obligations de déclaration des transactions suspectes, en effectuant les activités de déclaration des transactions suspectes en exécutant les délégations de pouvoir du Conseil d'administration (ex art. 36 du décret législatif 231/07) et en surveillant les demandes reçues de la CRF ;
- gérer les obligations en matière de lutte contre le financement du terrorisme, en définissant la méthodologie de contrôle visant à garantir la mise en œuvre des mesures restrictives de l'Union et nationales, en vérifiant la transposition des mises à jour de la liste des sanctions ainsi qu'en rendant compte aux autorités compétentes (nationales et de surveillance) des mesures restrictives (CRF, MAECI et MEF) sur les mesures de gel des capitaux (ex-décret législatif 109/07) et en effectuant les exigences opérationnelles nécessaires ;
- gérer les obligations de conservation des données, en vérifiant la fiabilité du système d'information en mettant à jour l'Archivio Unico Informatico (AUI), en effectuant d'éventuelles révisions, en envoyant périodiquement des données agrégées à la CRF et en transmettant à la CRF et à la Banque d'Italie les notifications requises par la réglementation ;
- surveiller la bonne mise en œuvre des sanctions financières internationales (embargos financiers) ;
- surveillance continue des clients les plus exposés au risque de blanchiment d'argent et de financement du terrorisme, suivi des demandes d'enquêtes complémentaires

concernant les clients qui exposent potentiellement la Société à des risques élevés de blanchiment d'argent, activation, si nécessaire, du processus d'évaluation des transactions suspectes et du processus de sélection des clients qui exposent potentiellement la Société à des risques élevés de blanchiment d'argent.

Les règles et responsabilités spécifiques de la Société concernant ce processus sont détaillées dans le règlement intérieur

document « Procédures internes de lutte contre le blanchiment d'argent et le financement du terrorisme ».

5 - CADRES ORGANISATIONNELS ET ORGANES DE CONTRÔLE

Pour gérer efficacement le risque de blanchiment d'argent et de financement du terrorisme, ainsi que de violation des mesures restrictives, la Société a identifié les fonctions organisationnelles, les ressources et les procédures qui sont cohérentes et proportionnées au type et à la taille de l'activité exercée, à la complexité organisationnelle ainsi qu'aux caractéristiques opérationnelles.

La surveillance des risques liés au blanchiment de capitaux et au financement du terrorisme est assurée :

- par la Fonction Anti-Blanchiment d'Argent de Rox Pay S.r.l., dont la responsabilité est confiée au Chef de la Fonction AML qui rapporte directement au Directeur Général.
- Par le membre de l'organe de direction responsable de la lutte contre le blanchiment d'argent, avec responsabilité confiée au PDG, qui est le principal point de contact entre le responsable de la fonction anti-blanchiment d'argent et le conseil d'administration et veille à ce que le conseil d'administration dispose des informations nécessaires pour comprendre pleinement l'importance des risques de blanchiment d'argent pour lesquels Rox Pay S.r.l. est exposé.

Le suivi des risques liés à la violation des Mesures Restrictives :

- est assurée par le cadre supérieur responsable des mesures restrictives, dont la responsabilité est confiée au chef du département LBC, qui supervise l'adéquation et l'efficacité des politiques, des procédures internes et des contrôles relatifs à la gestion des mesures restrictives, des sanctions et des embargos. Le Cadre propose, en collaboration avec les fonctions concernées de l'entreprise, les changements organisationnels et procéduraux nécessaires et/ou appropriés pour assurer un suivi adéquat des risques de violation des mesures restrictives, des sanctions et des embargos.

Conformément à la réglementation en vigueur, la Société a établi sa structure organisationnelle et sa gouvernance d'entreprise de manière à protéger les intérêts de la Société tout en assurant une gestion saine et prudente et en évitant les risques, même involontaires.
- de toute implication directe dans des actes de blanchiment d'argent et/ou de financement du terrorisme.

À cette fin, conformément au système de contrôle interne adopté par la Société, le Conseil d'administration et les commissaires aux comptes sont impliqués dans l'atténuation des risques ci-dessus à travers des tâches et des responsabilités clairement définies.

Par ailleurs, la Société a mis en place une unité centralisée pour la gestion du système de reporting interne des violations, chargée de superviser les activités de réception, d'analyse et d'évaluation des alertes transmises par les salariés via la procédure d'alerte.

6 – RÉVISION ET MISE À JOUR DE LA POLITIQUE

La Fonction Anti-Blanchiment révise la politique au moins une fois par an, la met à jour si nécessaire et prépare le texte pour approbation par le Conseil d'Administration sur proposition du Directeur Général.

Toute modification à la politique approuvée par le conseil d'administration de Rox Pay S.r.l. sont ensuite mises en œuvre dans toute la Société par résolution de la haute direction, alignant les responsabilités, les processus et les règles internes.