LIGNES DIRECTRICES CONCERNANT LA LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME

INTRODUCTION

L'objectif de ces lignes directrices relatives à la lutte contre le blanchiment d'argent, le financement du terrorisme et les sanctions est de veiller à ce que l'**UAB Criptomy** (la société) dispose de lignes directrices internes pour empêcher l'utilisation de ses activités à des fins de blanchiment d'argent et de financement du terrorisme, ainsi que de lignes directrices internes pour la mise en œuvre des sanctions internationales.

Ces lignes directrices ont été adoptées pour garantir que l'entreprise respecte les règles et réglementations définies dans la loi de la République de Lituanie sur la prévention du blanchiment d'argent et du financement du terrorisme (loi) et dans d'autres législations applicables, y compris les suivantes :

- Exigences techniques du processus d'identification des clients pour l'authentification de l'identification à distance via des dispositifs électroniques de transmission vidéo directe approuvées par le directeur du service d'enquête sur la criminalité financière relevant du ministère de l'Intérieur de la République de Lituanie le 30 novembre 2016 par la résolution n° V-314 " Exigences techniques du processus d'identification des clients pour l'authentification de l'identification à distance via des dispositifs électroniques de transmission vidéo directe " (ci-après - Exigences techniques).[1]
- Résolution n° V-240 du 5 décembre 2014 du directeur du service d'enquête sur la criminalité financière relevant du ministère de l'intérieur de la République de Lituanie "Sur l'approbation de la liste des critères d'identification du blanchiment d'argent et des opérations ou transactions monétaires suspectes ou inhabituelles".[2]
- Résolution No. V-5 du 5 janvier 10 de 2020 du directeur du service d'enquête sur les crimes financiers sous le ministère des affaires intérieures de la République de Lituanie "Sur l'approbation des lignes directrices pour les opérateurs de portefeuilles de monnaies virtuelles dépositaires et les opérateurs d'échange de monnaies virtuelles pour prévenir le blanchiment d'argent et / ou le financement du terrorisme".[3]
- Résolution n° V-273 du 20 octobre 2016 du directeur du service d'enquête sur les crimes financiers du ministère de l'Intérieur de la République de Lituanie "Sur l'approbation des lignes directrices pour la supervision des crimes financiers pour la mise en œuvre des sanctions financières internationales dans le domaine des règlements du ministère de l'Intérieur de la République de Lituanie".[4]
- Le ministre de l'Intérieur de la République de Lituanie, le 16 octobre 2017, par l'ordonnance no. 1V- 701 "Sur la suspension des transactions ou opérations monétaires suspectes et la soumission d'informations sur les transactions ou opérations monétaires suspectes au service d'enquête sur la criminalité financière en vertu de la description de la procédure du ministère de l'Intérieur de la République de Lituanie et les informations sur les transactions ou opérations en espèces égales ou supérieures à 15 000 euros ou la soumission du montant correspondant en devises étrangères...".

[1] https://www.e-tar.lt/portal/lt/legalAct/e45f4270b70011e6aae49c0b9525cbbb/asr
[2] https://www.e-tar.lt/portal/lt/legalAct/a664b2107ecd11e4bc68a1493830b8b9
[3] https://www.e-tar.lt/portal/lt/legalAct/570a231035e011ea829bc2bea81c1194
[4] https://www.e-tar.lt/portal/lt/legalAct/01d5d4e0974411e69ad4c8713b612d0f

monnaie au service d'enquête sur la criminalité financière sous l'approbation de la description de la procédure du ministère de l'intérieur de la République de Lituanie ".[5]

- Directeur du Service d'enquête sur la criminalité financière 2015 21 mai par ordre no. V-129 "Sur l'approbation des formulaires d'information, des schémas de soumission et des recommandations pour compléter les informations fournies conformément aux exigences de la loi sur la prévention du blanchiment d'argent et du financement du terrorisme de la République de Lituanie".[6]

Les présentes lignes directrices font l'objet d'un examen par le conseil d'administration au moins une fois par an. La proposition de révision et la révision des présentes lignes directrices peuvent être programmées plus fréquemment sur décision du Money Laundering Reporting Officer (MLRO) de la société ou du responsable du contrôle interne.

Les présentes lignes directrices sont acceptées et approuvées par une résolution du conseil d'administration de la société.

DÉFINITIONS

Le **bénéficiaire effectif est** une personne physique qui, profitant de son influence, effectue une transaction, un acte, une action, une opération ou une démarche ou exerce un contrôle d'une autre manière sur une transaction, un acte, une action, une opération ou une démarche ou sur une autre personne et dans l'intérêt ou au profit ou pour le compte de laquelle une transaction, un acte, une action, une opération ou une démarche est effectuée. Dans le cas d'une personne morale, le bénéficiaire effectif est une personne physique dont la participation directe ou indirecte, ou la somme de toutes les participations directes et indirectes dans la personne morale, dépasse 25 %, y compris les participations sous forme d'actions ou d'autres formes au porteur.

Relation d'affaires : une relation établie à la suite de la conclusion d'un contrat à long terme par l'entreprise dans le cadre d'activités économiques ou professionnelles en vue de la fourniture d'un service ou de sa distribution d'une autre manière, ou qui n'est pas fondée sur un contrat à long terme, mais dont on peut raisonnablement attendre une certaine durée au moment de l'établissement du contact et au cours de laquelle l'entreprise effectue de manière répétée des transactions distinctes dans le cadre d'activités économiques ou professionnelles tout en fournissant un service.

L'**entreprise** est une personne morale dont les données sont les suivantes :

- nom de l'entreprise : UAB Criptomy ;
- pays d'enregistrement : Lituanie ;
- numéro d'enregistrement : 306127858 ;
- adresse : Vilnius, Eišiškių Sodų 18-oji g. 11 ;
- Courriel : info@criptomy.exchange, contact@criptomy.exchange

Le **portefeuille de monnaie virtuelle du dépositaire** désigne la ou les adresses de monnaie virtuelle générées avec la clé publique[7] pour le stockage et la gestion des monnaies virtuelles confiées à la société, mais qui restent leur propriété.

[5] https://e-tar.lt/portal/lt/legalAct/143ad320b24011e7afdadfc0e4460de4
[6] https://www.e-tar.lt/portal/lt/legalAct/e1f42fa0006d11e588da8908dfa91cac

Le **portefeuille de monnaie virtuelle du dépositaire** désigne la ou les adresses de monnaie virtuelle générées avec la clé publique[7] pour le stockage et la gestion des monnaies virtuelles confiées à la société, mais qui restent leur propriété.

Le **client** est une personne physique ou morale qui entretient une relation d'affaires avec la société.

Employé : employé de l'entreprise et toute autre personne impliquée dans l'application des présentes lignes directrices au sein de l'entreprise.

Lignes directrices - le présent document, y compris toutes les annexes susmentionnées. Les lignes directrices comprennent notamment la procédure de contrôle interne de l'entreprise concernant les lignes directrices et la politique d'évaluation des risques de l'entreprise concernant l'approche fondée sur les risques pour les risques de blanchiment d'argent et de financement du terrorisme.

Par "conseil d'administration", on entend le conseil d'administration de l'entreprise. Si l'entreprise n'a pas de conseil d'administration, le directeur de l'entreprise est considéré comme le membre du conseil d'administration et il ou elle est responsable des fonctions du conseil d'administration dans le contexte des lignes directrices.

MLRO signifie Money Laundering Reporting Officer, qui est nommé au sein de l'entreprise en tant que personne responsable de la réception des divulgations internes et des rapports au Financial Crime Investigation Service (FCIS), ainsi que d'autres tâches telles que décrites ci-dessus.

Opération monétaire : tout paiement, transfert ou réception d'argent.

Le **blanchiment de capitaux** (BC) consiste à dissimuler l'origine de fonds illicites en les introduisant dans le système économique légal et en effectuant des transactions qui semblent légitimes. Le processus de blanchiment d'argent comporte trois étapes reconnues :

- le placement, qui consiste à placer les produits du crime dans le système financier ;
- la stratification, qui consiste à convertir les produits du crime sous une autre forme et à créer des couches complexes de transactions financières afin de dissimuler la piste d'audit ainsi que la source et la propriété des fonds ;
- l'intégration, qui consiste à réintégrer les produits blanchis dans l'économie afin de créer une perception de légitimité.

Transaction occasionnelle : transaction effectuée par la société dans le cadre d'activités économiques ou professionnelles en vue de fournir un service ou de vendre des biens ou de les distribuer d'une autre manière au client en dehors du cadre d'une relation commerciale établie.

On entend par **PPE** une personne physique qui exerce ou a exercé des fonctions publiques importantes et à l'égard de laquelle des risques subsistent.

Les **sanctions** sont un outil essentiel de la politique étrangère visant à soutenir le maintien ou le rétablissement de la paix, de la sécurité internationale, de la démocratie et de l'État de droit, ainsi que le respect des droits de l'homme.

---

[7] La **clé publique** est un code de lettres, de chiffres et/ou de symboles destiné à identifier le client et à générer l'adresse de monnaie virtuelle du client.

Les sanctions ont pour but de protéger les droits de l'homme et le droit international ou d'atteindre d'autres objectifs de la Charte des Nations unies ou de la politique étrangère et de sécurité commune de l'Union européenne. Les sanctions comprennent :

- les sanctions internationales imposées à l'égard d'un État, d'un territoire, d'une unité territoriale, d'un régime, d'une organisation, d'une association, d'un groupe ou d'une personne par une résolution du Conseil de sécurité des Nations unies, une décision du Conseil de l'Union européenne ou toute autre législation imposant des obligations à la Lituanie ;
- Les sanctions du gouvernement de la République de Lituanie, qui sont un instrument de politique étrangère, peuvent être imposées en plus des objectifs spécifiés dans la clause précédente afin de protéger la sécurité ou les intérêts de la Lituanie.

Les sanctions internationales peuvent interdire l'entrée d'une personne faisant l'objet d'une sanction internationale dans l'État, restreindre le commerce international et les transactions internationales, et imposer d'autres interdictions ou obligations.

L'objet des sanctions est toute personne physique ou morale, entité ou organisme, désigné dans l'acte juridique imposant ou mettant en œuvre les sanctions, à l'égard duquel les sanctions s'appliquent.

Le **financement du terrorisme** (FT) désigne le financement et le soutien d'un acte de terrorisme et sa commission, ainsi que le financement et le soutien d'un voyage à des fins de terrorisme au sens de la législation applicable.

Pays tiers : un État qui n'est pas membre de l'Espace économique européen (EEE).

Monnaie virtuelle désigne une valeur représentée sous forme numérique, qui est numériquement transférable, conservable ou négociable et que des personnes physiques ou morales acceptent comme instrument de paiement, mais qui n'a pas cours légal dans un pays ou des fonds aux fins de l'article 4, paragraphe 25, de la directive (UE) 2015/2366 du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, pp 35-127) ou une opération de paiement aux fins de l'article 3, points k) et l), de la même directive.

L'adresse de la monnaie virtuelle désigne l'adresse/le compte généré(e) à partir de lettres, de chiffres et/ou de symboles dans la blockchain, par laquelle la blockchain attribue la monnaie virtuelle au propriétaire ou au destinataire.

PRINCIPES DE STRUCTURE ET DE GESTION DE L'ENTREPRISE

La structure organisationnelle de l'entreprise doit correspondre à sa taille ainsi qu'à la nature, à l'étendue et au niveau de complexité de ses activités et des services qu'elle fournit, y compris l'appétit pour le risque et les risques connexes, et doit être structurée conformément au principe des **trois lignes de défense.** La structure organisationnelle de l'entreprise doit correspondre à une compréhension complète des risques potentiels et de leur gestion. Les chaînes de reporting et de subordination de l'entreprise doivent être assurées de manière à ce que tous les employés connaissent leur place dans l'organigramme et leurs tâches.

Le conseil d'administration

Le conseil d'administration est le porteur de la culture de conformité aux exigences de la prévention du blanchiment d'argent et du financement du terrorisme, garantissant que les membres du conseil d'administration et les employés de la société opèrent dans un environnement où ils sont pleinement conscients des exigences de la prévention du blanchiment d'argent et du financement du terrorisme et des obligations associées à ces exigences, et que les considérations de risque pertinentes sont prises en compte dans une mesure appropriée dans les processus de prise de décision de la société.

Les membres du conseil d'administration sont responsables en dernier ressort des mesures prises pour empêcher l'utilisation des services de la société à des fins de blanchiment d'argent ou de financement du terrorisme. Ils assurent la surveillance et sont responsables de ce qui suit :

- établir et maintenir les processus, les procédures, les risques et les processus de contrôle de la lutte contre le blanchiment d'argent (AML) sur le site[8] ;
- l'adoption des présentes lignes directrices et d'autres lignes directrices et instructions internes ;
- déterminer les lignes directrices de l'entreprise en matière de lutte contre le blanchiment d'argent ;
- nommer un MLRO et s'assurer qu'il dispose des pouvoirs, des ressources et de l'expertise nécessaires à l'accomplissement de sa mission ;
- allouer des ressources suffisantes pour assurer la mise en œuvre effective des lignes directrices et des autres documents connexes et pour maintenir l'organisation ;
- veiller à ce que tous les employés concernés suivent une formation annuelle sur la lutte contre le blanchiment d'argent.

La première ligne de défense - les employés

La première ligne de défense a pour fonction d'appliquer les mesures de diligence raisonnable lors de la relation d'affaires et d'appliquer les mesures de diligence raisonnable pendant la relation d'affaires. La première ligne de défense comprend les unités structurelles et les employés de la société dont les activités comportent des risques et qui doivent identifier et évaluer ces risques, leurs caractéristiques spécifiques et leur portée, et qui gèrent ces risques dans le cadre de leurs activités ordinaires, principalement par l'application de mesures de diligence raisonnable. Les risques découlant des activités et de la prestation de services de la société appartiennent à la première ligne de défense. Ils sont les gestionnaires (propriétaires) de ces risques et en sont responsables.

[8] Afin de simplifier les présentes lignes directrices, le terme "AML" englobe également la prévention du financement du terrorisme et la mise en œuvre des sanctions.

Les employés de la société doivent agir avec la prévoyance et la compétence que l'on attend d'eux et conformément aux exigences fixées pour leur poste, en fonction des intérêts et des objectifs de la société, et veiller à ce que le système financier et l'espace économique du pays ne soient pas utilisés pour le blanchiment d'argent et le financement du terrorisme. La société prend des mesures pour évaluer l'aptitude des employés avant qu'ils ne commencent à travailler, en leur dispensant une formation appropriée.

Pour les raisons susmentionnées, les employés sont tenus de :

- respecter toutes les exigences énoncées dans les lignes directrices et autres documents connexes ;
- recueillir les informations requises sur les clients conformément à leur fonction et à leurs responsabilités ;
- signaler au MLRO les informations, situations, activités, transactions ou tentatives de transactions qui sont inhabituelles pour tout type de service ou de relation avec le client, quel qu'en soit le montant, que la transaction ait été effectuée sans délai ou non ;
- ne pas informer ou faire savoir d'une autre manière aux clients si le client ou d'autres clients font ou peuvent faire l'objet d'une déclaration ou si une déclaration a été ou peut être déposée ;
- suivre la formation appropriée en matière de lutte contre le blanchiment d'argent requise pour le poste occupé par l'employé.

La deuxième ligne de défense - Gestion des risques et conformité, MLRO

La deuxième ligne de défense est constituée des fonctions de gestion des risques et de conformité. Ces fonctions peuvent également être exercées par la même personne ou la même unité structurelle en fonction de la taille de l'entreprise et de la nature, de l'étendue et du niveau de complexité de leurs activités et des services fournis, y compris l'appétit pour le risque et les risques découlant des activités de l'entreprise.

L'objectif de la **fonction de conformité** est de garantir que l'entreprise respecte la législation, les lignes directrices et les autres documents en vigueur et d'évaluer l'effet possible de tout changement dans l'environnement juridique ou réglementaire sur les activités de l'entreprise et sur le cadre de conformité. La tâche de la conformité est d'aider la première ligne de défense, en tant que propriétaire des risques, à définir les endroits où les risques se manifestent (par exemple, l'analyse des transactions suspectes et inhabituelles, pour lesquelles les employés chargés de la conformité possèdent les compétences professionnelles et les qualités personnelles requises, etc. La deuxième ligne de défense ne prend pas de risques.

La politique de gestion des risques est mise en œuvre et le cadre de gestion des risques est contrôlé par la **fonction de gestion des risques**. Le responsable de la fonction de gestion des risques veille à ce que tous les risques soient identifiés, évalués, mesurés, surveillés et gérés, et il en informe les unités appropriées de la société. Aux fins de la lutte contre le blanchiment d'argent, la personne chargée de la fonction de gestion des risques supervise principalement le respect de l'appétit pour le risque, la tolérance au risque, l'identification des changements dans les risques, la vue d'ensemble des risques associés et d'autres tâches liées à la gestion des risques.

Le conseil d'administration a désigné un **MLRO** pour assurer les fonctions de la deuxième ligne de défense. Cette personne n'est pas impliquée sur le plan opérationnel dans les domaines que le MLRO contrôlera et vérifiera et est donc indépendante à cet égard.

Dans le cadre du dispositif actuel de lutte contre le blanchiment d'argent de l'entreprise, c'est le MLRO qui prend les décisions clés concernant les questions individuelles de lutte contre le blanchiment d'argent, telles que l'approbation des PPE, l'acceptation ou le refus des utilisateurs à haut risque, etc.

Le responsable de la lutte contre le blanchiment d'argent désigné par l'entreprise est le cadre supérieur de l'entreprise et une personne qui possède toutes les connaissances et l'expérience professionnelle nécessaires.

Le MLRO est responsable des activités suivantes :

- produire et, le cas échéant, mettre à jour les lignes directrices de l'entreprise ;
- contrôler et vérifier en permanence que l'entreprise respecte les exigences prescrites par les présentes lignes directrices et les documents connexes, ainsi que les lois et réglementations externes ;
- fournir au personnel de l'entreprise et aux membres du conseil d'administration des conseils et un soutien concernant les règles relatives au blanchiment d'argent et au financement du terrorisme ;
- informer et former les membres du conseil d'administration et les personnes concernées sur les règles relatives au blanchiment de capitaux et au financement du terrorisme ;
- examiner et enregistrer des données suffisantes sur les notifications internes reçues et décider si l'activité peut être justifiée ou si elle est suspecte ;
- déposer les rapports pertinents auprès des autorités réglementaires appropriées conformément à la législation en vigueur ;
- vérifier et évaluer régulièrement si les procédures et les lignes directrices de l'entreprise visant à empêcher l'utilisation de l'entreprise à des fins de blanchiment de capitaux ou de financement du terrorisme sont adaptées à l'objectif visé et efficaces.

Le MLRO fait rapport au conseil d'administration tous les trimestres. Ce rapport doit être établi par écrit et comprendre au moins les éléments suivants :

- nombre de clients dans toutes les catégories de risques
- nombre d'occurrences de personnes en relation avec les listes de sanctions et les mesures appliquées ;
- le nombre de clients ou de représentants de clients identifiés comme étant des PPE ou des personnes ayant un lien avec une PPE ;
- le nombre de notifications internes sur des activités ou des transactions suspectes ;
- nombre de rapports pertinents transmis au Service d'enquête sur la criminalité financière (FCIS) ;
- le nombre et le contenu d'une demande d'information au FCIS dans le cadre d'une enquête ;
- la confirmation que l'évaluation des risques de l'entreprise en matière de blanchiment de capitaux et de financement du terrorisme est à jour ;
- la confirmation que ces lignes directrices et autres documents connexes sont à jour ;
- la confirmation que le personnel chargé des mesures de lutte contre le blanchiment d'argent est suffisant ;
- toutes les insuffisances (le cas échéant) identifiées par la fonction de contrôle ont été traitées.

La troisième ligne de défense - L'audit interne

La troisième ligne de défense est constituée par une fonction d'audit interne indépendante et efficace. La fonction d'audit interne peut être exercée par un responsable du contrôle interne. Il peut s'agir d'un ou de plusieurs employés, de l'unité structurelle de la société ayant les fonctions concernées ou d'un tiers qui fournit le service concerné à la société. Le responsable du contrôle interne n'est pas autorisé à occuper le poste de MLRO et/ou de membre du conseil d'administration de la société ou tout autre poste dont les fonctions incluent la rédaction et/ou l'édition des règlements et lignes directrices internes de la société en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.

Les employés, l'unité structurelle de l'entreprise ou un tiers qui exerce la fonction d'audit interne doivent disposer des compétences, des outils et de l'accès aux informations pertinentes dans toutes les unités structurelles de l'entreprise. Les méthodes d'audit interne doivent être adaptées à la taille de l'entreprise, à la nature, à la portée et au niveau de complexité des activités et des services fournis, y compris l'appétit pour le risque et les risques découlant des activités de l'entreprise.

La décision d'effectuer un audit interne est prise par une résolution du conseil d'administration. Le conseil d'administration doit évaluer la nécessité d'effectuer un audit interne au moins une fois par an.

PRINCIPES DES MESURES DE VIGILANCE À L'ÉGARD DE LA CLIENTÈLE MISE EN ŒUVRE

Les mesures de vigilance à l'égard de la clientèle (CDD) sont nécessaires pour vérifier l'identité d'un nouveau client ou d'un client existant, dans le cadre d'un contrôle permanent de la relation d'affaires avec le client, fondé sur le risque. Les mesures de vigilance à l'égard de la clientèle comprennent trois niveaux, dont les mesures de vigilance simplifiées et renforcées, comme indiqué ci-dessous.

Les grands principes

Les mesures CDD sont prises et exécutées dans la mesure nécessaire compte tenu du profil de risque du client et d'autres circonstances dans les cas suivants :

- lors de l'établissement de la relation d'affaires et au cours du suivi de la relation d'affaires ;
- lors de l'exécution ou de la médiation de transactions occasionnelles en dehors de la relation d'affaires, lorsque la valeur de la ou des transactions s'élève à 700 euros ou plus (ou un montant équivalent dans d'autres actifs) dans un délai de 24 heures ;
- lors de l'exécution ou de la médiation de transactions occasionnelles en dehors de la relation d'affaires, lorsque la valeur de la ou des transactions s'élève à 10 000 euros ou plus (ou un montant équivalent dans d'autres actifs) au cours d'un mois ;
- lors de la vérification des informations recueillies dans le cadre de l'application des mesures de diligence raisonnable ou, en cas de doute sur la suffisance ou la véracité des documents ou données recueillis précédemment, lors de la mise à jour des données pertinentes ;
- en cas de soupçon de blanchiment de capitaux ou de financement du terrorisme, indépendamment des dérogations, exceptions ou limites prévues par les présentes lignes directrices et la législation applicable.

L'entreprise n'établit pas ou ne maintient pas la relation d'affaires et n'effectue pas la transaction si :

- l'entreprise n'est pas en mesure de prendre et d'appliquer les mesures CDD requises ;
- l'entreprise a des soupçons que les services ou les transactions de l'entreprise seront utilisés pour le blanchiment d'argent ou le financement du terrorisme ;
- le niveau de risque du client ou de la transaction n'est pas conforme à l'appétit pour le risque de la société.

Si l'entreprise reçoit des informations dans des langues étrangères dans le cadre de la mise en œuvre de la CDD, elle peut demander à ce que les documents soient traduits dans une autre langue qu'elle peut utiliser. L'utilisation de traductions doit être évitée dans les situations où les documents originaux sont préparés dans une langue applicable à l'entreprise.

La réalisation du CDD est un processus qui commence par la mise en œuvre de mesures de CDD. À l'issue de ce processus, le client se voit attribuer un niveau de risque individuel documenté qui servira de base aux mesures de suivi, et qui fera l'objet d'un suivi et d'une mise à jour si nécessaire.

L'entreprise a appliqué les mesures de diligence raisonnable de manière adéquate si elle a l'intime conviction qu'elle s'est conformée à l'obligation d'appliquer les mesures de diligence raisonnable. Le principe du caractère raisonnable est observé dans l'examen de l'intime conviction. Cela signifie que l'entreprise doit, lors de l'application des mesures de CDD, acquérir la connaissance, la compréhension et l'affirmation qu'elle a recueilli suffisamment d'informations sur le client, les activités du client, l'objet de la relation d'affaires et des transactions effectuées dans le cadre de la relation d'affaires, l'origine des fonds, etc., afin de comprendre le client et ses activités (commerciales), en tenant compte du niveau de risque du client, du risque associé à la relation d'affaires et de la nature de cette relation. Ce niveau d'affirmation doit permettre d'identifier les transactions compliquées, de grande valeur et inhabituelles, ainsi que les schémas de transactions qui n'ont pas d'objectif économique ou légitime raisonnable ou évident ou qui ne sont pas caractéristiques des spécificités de l'activité en question.

La société doit appliquer la CDD non seulement aux clients personnes physiques mais aussi aux personnes morales. Toutes les contreparties et tous les partenaires de l'entreprise sont vérifiés manuellement par le responsable MLRO à l'aide de sources fiables et indépendantes.

Les services fournis

La principale activité économique de la Société est la fourniture de services de monnaies virtuelles. C'est pourquoi elle propose à ses clients les types de transactions suivants :

- fournir un service d'opérateur de change de monnaies virtuelles, qui permet au client d'échanger, d'acheter et de vendre des monnaies virtuelles.

L'entreprise ne fournit les services susmentionnés que dans le cadre d'une relation commerciale établie.

La vérification des informations utilisées pour l'identification du client

La vérification des informations relatives à l'identification du client consiste à utiliser des données provenant d'une source fiable et indépendante pour confirmer que ces données sont exactes et correctes, et à confirmer également, si nécessaire, que les données directement liées au client sont exactes et correctes. Cela signifie, entre autres, que l'objectif de la vérification des informations est d'obtenir l'assurance que le client, qui souhaite établir une relation d'affaires, est bien la personne qu'il prétend être.

La source fiable et indépendante (doit exister cumulativement) est la vérification des informations obtenues au cours de l'identification :

- qui provient de deux sources différentes ;
- qui a été émise par (documents d'identité) ou reçue d'un tiers ou d'un lieu qui n'a aucun intérêt ou lien avec le client ou la société, c'est-à-dire qui est neutre (par exemple, les informations obtenues sur Internet ne sont pas de telles informations, car elles proviennent souvent du client lui-même ou leur fiabilité et leur indépendance ne peuvent pas être vérifiées) ;
- dont la fiabilité et l'indépendance peuvent être déterminées sans obstacles objectifs et dont la fiabilité et l'indépendance sont également compréhensibles pour un tiers non impliqué dans la relation d'affaires ; et
- les données qui y figurent ou qui sont obtenues par ce biais sont à jour et pertinentes, et l'entreprise peut obtenir des garanties à ce sujet (dans certains cas, ces garanties peuvent également être obtenues sur la base des deux clauses précédentes).

Application des mesures simplifiées de diligence raisonnable (niveau 1)

Des mesures de diligence simplifiée sont appliquées lorsque le profil de risque du client indique un faible niveau de risque de blanchiment d'argent et de financement du terrorisme.

Lors de l'application des mesures de DTS, la société ne doit obtenir que[9] les données suivantes du client qui est une personne physique :

- nom(s) et prénom(s) ;
- numéro personnel ;[10] ou

dans le cas du client, qui est une personne morale, les données suivantes :

- le nom ou la raison sociale de l'entreprise ;
- forme juridique ;
- le numéro d'enregistrement, s'il a été délivré ;
- le siège social (adresse) et l'adresse de l'exploitation effective ;
- le(s) nom(s), prénom(s) et numéro personnel ou date de naissance du représentant du client ; et

veiller à ce que le premier paiement soit effectué sur un compte ouvert auprès d'un établissement de crédit, lorsque cet établissement est enregistré dans l'EEE ou dans un pays tiers qui impose des exigences équivalentes à celles prévues par la législation applicable et qui est contrôlé par les autorités compétentes en ce qui concerne le respect de ces exigences.

Les mesures de DTS ne peuvent être mises en œuvre que lorsque le suivi permanent de la relation d'affaires avec le client est effectué conformément aux lignes directrices et qu'il est possible d'identifier des opérations et des transactions monétaires suspectes.

Les mesures de DTS ne doivent pas être mises en œuvre dans les circonstances où des mesures de diligence raisonnable renforcées (telles que décrites ci-dessous) doivent être mises en œuvre.

---

[9] Lorsque le client est une institution ou une agence nationale ou municipale ou la Banque de Lituanie, l'entreprise peut, dans le cadre de l'application des mesures de DTS, collecter uniquement les données personnelles de ces entités et de leurs représentants.

[10] dans le cas d'un étranger - la date de naissance (le cas échéant - le numéro personnel ou toute autre séquence unique de symboles attribuée à cette personne, destinée à son identification personnelle).

Lorsque, dans le cadre de la surveillance continue des relations d'affaires du client, il est établi que le risque de blanchiment d'argent et/ou de financement du terrorisme n'est plus faible, l'entreprise doit appliquer le niveau approprié de mesures de vigilance à l'égard de la clientèle.

Application des mesures standard de diligence raisonnable (niveau 2)

Les mesures de vigilance standard sont appliquées à tous les clients pour lesquels des mesures de vigilance doivent être appliquées conformément aux lignes directrices. Les mesures de vigilance standard suivantes doivent être appliquées :

- l'identification du client et la vérification des informations fournies sur la base d'informations obtenues auprès d'une source fiable et indépendante ;
- l'identification et la vérification d'un représentant du client et de son droit de représentation ;
- l'identification du bénéficiaire effectif et, aux fins de la vérification de son identité, la prise de mesures permettant à la société de s'assurer qu'elle sait qui est le bénéficiaire effectif et qu'elle comprend la structure de propriété et de contrôle du client ;
- la compréhension de la relation d'affaires, de la transaction ou de l'opération et, le cas échéant, la collecte d'informations à ce sujet ;
- recueillir des informations pour savoir si le client est un PPE, un membre de sa famille ou une personne connue pour être un proche ;
- le suivi de la relation d'affaires.

Les mesures de diligence raisonnable spécifiées ci-dessus doivent être appliquées avant d'établir la relation d'affaires ou d'effectuer la transaction. Les instructions précises concernant l'application des mesures de diligence raisonnable standard sont fournies dans les lignes directrices.

Application de mesures de diligence raisonnable renforcées (niveau 3)

Outre les mesures de diligence normale, l'entreprise applique des mesures de diligence renforcée afin de gérer et d'atténuer un risque établi de blanchiment de capitaux et de financement du terrorisme lorsque ce risque s'avère plus élevé que d'habitude.

L'entreprise applique toujours des mesures de CED, lorsque :

- le profil de risque du client indique un niveau de risque élevé de blanchiment d'argent ou de financement du terrorisme ;
- après identification du client ou vérification des informations fournies, il existe des doutes quant à la véracité des données fournies, à l'authenticité des documents ou à l'identification du bénéficiaire effectif ;
- lorsque des relations de correspondance transfrontalière sont établies avec le client, qui est une institution financière d'un pays tiers ;
- dans le cas de l'exécution d'une transaction ou d'une relation d'affaires avec le PEP, le membre de la famille du PEP ou une personne connue pour être un proche collaborateur du PEP ;
- lorsque la transaction ou la relation d'affaires est effectuée avec des personnes physiques résidant ou des personnes morales établies dans des pays tiers à haut risque tels qu'identifiés par la Commission européenne ;

- le client est originaire d'un tel pays ou territoire ou son lieu de résidence ou son siège ou le siège du prestataire de services de paiement du bénéficiaire se trouve dans un pays ou territoire qui, selon des sources crédibles telles que des évaluations mutuelles, des rapports ou des rapports de suivi publiés, n'a pas mis en place de systèmes efficaces de lutte contre le blanchiment de capitaux et le financement du terrorisme conformes aux recommandations du GAFI.

Avant d'appliquer les mesures de CED, l'employé de la société s'assure que la relation d'affaires ou la transaction présente un risque élevé et qu'un taux de risque élevé peut être attribué à cette relation d'affaires ou à cette transaction. Avant tout, l'employé évalue, avant d'appliquer les mesures de discernement, si les caractéristiques décrites ci-dessus sont présentes et les applique en tant que motifs indépendants (c'est-à-dire que chacun des facteurs identifiés permet l'application des mesures de discernement à l'égard du client).

Lors de l'application des mesures de DPE lorsque des relations de correspondance transfrontalières sont établies avec le client, qui est une institution financière d'un pays tiers, la société doit appliquer les mesures suivantes :

- recueillir suffisamment d'informations sur le client pour comprendre pleinement la nature de ses activités et déterminer, à partir d'informations accessibles au public, la réputation du client et la qualité du contrôle ;
- évaluer les mécanismes de contrôle de la lutte contre le blanchiment d'argent du client et de l'entité qui reçoit les fonds ;
- obtenir l'approbation du membre du conseil d'administration avant d'établir de nouvelles relations avec des correspondants ;
- documenter les responsabilités respectives du client ;
- s'assurer que le client a fait preuve d'une diligence raisonnable (y compris la vérification de l'identité des clients ayant un accès direct aux comptes du client et l'exécution d'autres mesures de diligence raisonnable à l'égard du client) et qu'il est en mesure de fournir à la société, à sa demande, les données d'identification du client pertinentes.

Lors de l'application des mesures de CED, lorsque des transactions ou des relations d'affaires sont effectuées avec la PPE, un membre de la famille de la PPE ou une personne connue pour être un proche collaborateur de la PPE, l'entreprise doit appliquer les mesures suivantes :

- obtenir l'approbation du membre du conseil d'administration avant d'établir une relation d'affaires avec ce client ou de poursuivre la relation d'affaires avec le client lorsqu'il devient une PPE ;
- prendre des mesures adéquates pour établir l'origine des richesses et des fonds impliqués dans la relation d'affaires ou la transaction ;
- effectuer un suivi continu de la relation commerciale avec le client en augmentant le nombre et le calendrier des contrôles appliqués et en sélectionnant les types de transactions qui nécessitent un examen plus approfondi.

Lors de l'application des mesures de CED lorsque la transaction ou la relation d'affaires est effectuée avec des personnes physiques résidant ou des personnes morales établies dans des pays tiers à haut risque tels qu'identifiés par la Commission européenne, l'entreprise doit appliquer les mesures suivantes :

- obtenir des informations sur l'origine des fonds et la source de la richesse du client et de son bénéficiaire effectif ;
- obtenir des informations sur les raisons des transactions envisagées ou effectuées ;
- obtenir l'approbation du membre du conseil d'administration pour établir des relations d'affaires avec le client ou poursuivre des relations d'affaires avec lui ;
- effectuer un suivi continu de la relation commerciale avec le client en augmentant le nombre et le calendrier des contrôles appliqués et en sélectionnant les types de transactions qui nécessitent un examen plus approfondi ;
- veiller à ce que le premier paiement soit effectué sur un compte ouvert au nom du client auprès d'un établissement de crédit, lorsque cet établissement est enregistré dans l'EEE ou dans un pays tiers qui impose des exigences équivalentes à celles prévues par la législation applicable et qui est contrôlé par les autorités compétentes en ce qui concerne le respect de ces exigences.

Lors de l'application des mesures de DPE lorsque le client est originaire d'un pays ou d'un territoire ou que son lieu de résidence ou son siège ou le siège du prestataire de services de paiement du bénéficiaire se trouve dans un pays ou un territoire qui, selon des sources crédibles telles que des évaluations mutuelles, des rapports ou des rapports de suivi publiés, n'a pas mis en place des systèmes efficaces de LBC/FT conformes aux recommandations du GAFI, la société doit appliquer les mesures suivantes :

- obtenir l'approbation du membre du conseil d'administration pour établir des relations d'affaires avec le client ou poursuivre des relations d'affaires avec lui ;
- obtenir des informations sur l'origine des fonds et la source de la richesse du client et de son bénéficiaire effectif ;
- effectuer un suivi continu de la relation commerciale avec le client en augmentant le nombre et le calendrier des contrôles appliqués et en sélectionnant les types de transactions qui nécessitent un examen plus approfondi ;

Dans tous les autres cas où des mesures de DED doivent être appliquées, l'ampleur des mesures de DED et leur portée sont déterminées par l'employé qui applique ces mesures. Les mesures de diligence raisonnable supplémentaires et pertinentes suivantes peuvent être appliquées :

- la vérification des informations supplémentaires soumises lors de l'identification du client sur la base de documents, de données ou d'informations supplémentaires provenant d'une source crédible et indépendante ;
- recueillir des informations supplémentaires sur l'objet et la nature de la relation d'affaires ou de la transaction et vérifier les informations fournies sur la base de documents, de données ou d'informations supplémentaires provenant d'une source fiable et indépendante ;
- la collecte d'informations et de documents supplémentaires concernant l'exécution réelle des transactions effectuées dans le cadre de la relation d'affaires, afin d'exclure l'ostensibilité des transactions ;
- la collecte d'informations et de documents supplémentaires dans le but d'identifier la source et l'origine des fonds utilisés dans une transaction effectuée dans le cadre de la relation d'affaires, afin d'exclure l'ostensibilité des transactions ;

- l'application de mesures CDD à l'égard du client ou de son représentant en se trouvant au même endroit que le client ou son représentant ;
- la collecte d'informations supplémentaires sur le client et son bénéficiaire effectif, y compris l'identification de tous les propriétaires du client, y compris ceux dont la participation est inférieure à 25 % ;
- recueillir des informations sur l'origine des fonds et du patrimoine du client et de son bénéficiaire effectif ;
- améliorer le suivi de la relation d'affaires en augmentant le nombre et la fréquence des mesures de contrôle appliquées et en choisissant des indicateurs de transaction ou des modèles de transaction qui font l'objet d'une vérification supplémentaire ;
- obtenir l'approbation du membre du conseil d'administration pour effectuer des transactions ou établir des relations d'affaires avec des clients nouveaux ou existants ;

Dans certains cas, la société est tenue de prendre des mesures raisonnables pour établir l'origine des fonds et la source de la richesse des clients. L'origine des fonds peut être vérifiée en se référant, *entre autres,* aux éléments suivants

- une déclaration fiscale annuelle ;
- l'original ou une copie certifiée conforme d'une fiche de paie récente ;
- une confirmation écrite du salaire annuel signée par l'employeur ;
- un original ou une copie certifiée conforme du contrat de vente du bien immobilier et un extrait original d'une institution financière attestant la réception des fonds provenant de la vente du bien immobilier, s'il est disponible ;
- l'original ou la copie certifiée conforme d'un testament ou d'un document équivalent attestant de l'héritage ;
- l'original ou une copie certifiée conforme d'un accord de donation (soit sous une forme écrite simple, soit certifiée par un notaire public dans le cas où la loi exige un accord notarié) ;
- l'original ou une copie certifiée conforme d'un contrat de prêt (sous forme écrite simple ou certifiée par un notaire public si la forme notariée du contrat est exigée par la loi) et un extrait d'une institution financière attestant la réception ou l'envoi de fonds liés à l'obtention du prêt ou au remboursement d'un prêt accordé ; ou un billet à ordre (sous forme écrite simple ou certifiée par un notaire public si la forme notariée du contrat est exigée par la loi) ;
- une recherche sur Internet dans le registre des entreprises pour confirmer la vente d'une entreprise ;
- l'original ou une copie certifiée conforme du contrat de dépôt ;
- livre de caisse ou registre des opérations de caisse (pour les personnes morales) ;
- d'autres informations.

L'employé doit notifier les mesures d'EDD appliquées dans les deux jours ouvrables suivant le début de l'application des mesures d'EDD en envoyant la notification correspondante au MLRO.

En cas d'application de mesures de CED, la société réévalue le profil de risque du client au plus tard tous les six mois.

MESURES DE VIGILANCE À L'ÉGARD DES CLIENTS

Identification du client - personne physique

La Société identifie le Client qui est une personne physique et, le cas échéant, son représentant et conserve les données suivantes sur le Client :

- nom(s) et prénom(s) ;
- numéro personnel ;[11]
- la citoyenneté ;[12]
- photographie ;
- signature.[13]

Les documents d'identité suivants, en cours de validité et contenant les données précisées ci-dessus, peuvent servir de base à l'identification d'une personne physique :

- un document d'identité de la République de Lituanie, à l'exception du permis de séjour de la République de Lituanie ;
- un document d'identité d'un État étranger ;

Le client, qui est une personne physique, ne peut pas faire appel à un représentant dans le cadre de sa relation d'affaires avec la société.

Identification du client - personne morale

La Société identifie le Client qui est une personne morale et son représentant et conserve les données suivantes sur le Client :

- le nom ou la raison sociale de l'entreprise ;
- forme juridique ;
- le numéro d'enregistrement, s'il a été délivré ;
- nom(s) et prénom(s), numéro personnel (dans le cas d'un étranger - date de naissance ou, le cas échéant, numéro personnel ou toute autre séquence unique de symboles accordée à l'étranger)

[11] dans le cas d'un étranger - la date de naissance (le cas échéant - le numéro personnel ou toute autre séquence unique de symboles attribuée à cette personne, destinée à son identification personnelle) ;

[12] lorsqu'un document d'identité ne contient pas de données sur la citoyenneté du client, les institutions financières et autres entités obligées doivent, lorsqu'elles identifient le client qui est une personne physique en sa présence physique, demander au client de fournir les données sur sa citoyenneté.

[13] sauf dans les cas où elle est facultative dans le document d'identité ;

cette personne, destinée à l'identification personnelle) et la citoyenneté du (des) directeur(s) ou membre(s) du conseil d'administration ou membre(s) d'un autre organe équivalent, ainsi que leurs pouvoirs dans la représentation du client ;

- un extrait d'enregistrement et sa date de délivrance ;
- siège social (adresse) et adresse de l'exploitation effective
- Les documents suivants, délivrés par une autorité ou un organisme compétent au plus tôt six mois avant leur utilisation, peuvent être utilisés pour l'identification du client :
    - la carte d'immatriculation du registre concerné ; ou
    - le certificat d'enregistrement du registre concerné ; ou
    - un document équivalent aux documents susmentionnés ou aux documents d'établissement pertinents du client.

La Société vérifie l'exactitude des données du Client spécifiées ci-dessus, en utilisant à cette fin des informations provenant d'une source crédible et indépendante. Lorsque la société a accès au registre des personnes morales, il n'est pas nécessaire d'exiger du client qu'il fournisse les documents susmentionnés.L'identité de l'entité juridique et le droit de représentation de l'entité juridique peuvent être vérifiés sur la base d'un document spécifié ci-dessus, qui a été authentifié par un notaire ou certifié par un notaire ou officiellement, ou sur la base d'autres informations provenant d'une source crédible et indépendante, y compris les moyens d'identification électronique et les services de confiance pour les transactions électroniques, en utilisant ainsi au moins deux sources différentes pour la vérification des données dans un tel cas.

l'identification du représentant du client et son droit de représentation

Le représentant du client doit être identifié comme étant le client, qui est une personne physique conformément aux présentes lignes directrices. La société doit également identifier et vérifier la nature et l'étendue du droit de représentation du client. Le nom, la date d'émission et le nom de l'émetteur du document qui sert de base au droit de représentation doivent être déterminés et conservés, sauf dans le cas où le droit de représentation a été vérifié à l'aide d'informations provenant du registre pertinent.La société doit respecter les conditions du droit de représentation accordé aux représentants de la personne morale et ne fournir des services que dans le cadre du droit de représentation.

L'autorisation doit être conforme aux exigences du code civil lituanien. L'autorisation délivrée à l'étranger doit être légalisée ou porter une apostille. Si le droit de représentation du client (personne morale) ressort clairement de l'extrait de registre, des statuts ou de documents équivalents attestant de l'identité du client (personne morale), un document d'autorisation distinct (par exemple, une procuration) n'est pas nécessaire.

L'identification du bénéficiaire effectif du client

La société doit identifier le bénéficiaire effectif du client, c'est-à-dire la personne qui, en dernier ressort, possède ou contrôle le client ou pour le compte de laquelle une transaction est effectuée. La société doit également prendre des mesures pour vérifier l'identité du bénéficiaire effectif dans la mesure où cela lui permet de s'assurer qu'elle sait qui est le bénéficiaire effectif. L'entreprise ne peut pas supposer que les particuliers eux-mêmes sont lesbénéficiaires effectifs du client et doit toujours commencer par obtenir du client des informations sur l'identité du bénéficiaire effectif. L'identification du bénéficiaire effectif signifie l'identification d'une personne physique ou d'un groupe de personnes physiques. L'identification du BO signifie l'identification d'une personne physique ou d'un groupe de personnes physiques.

La société recueille les données suivantes concernant le(s) bénéficiaire(s) effectif(s) du client :

- nom(s) et prénom(s) ;
- numéro personnel ;[14]
- la citoyenneté.[15]

La compagnie demande au client des informations sur le bénéficiaire effectif du client (par exemple, en donnant au client la possibilité de préciser son bénéficiaire effectif lors de la collecte des données le concernant).

L'entreprise n'établit pas la relation d'affaires si le client, qui est une personne physique, a un bénéficiaire effectif qui n'est pas la même personne que le client.

L'identification du bénéficiaire effectif d'une entité juridique s'effectue par étapes, l'entité obligée passant à chaque étape suivante si le bénéficiaire effectif de l'entité juridique ne peut être déterminé à l'étape précédente. Les étapes sont les suivantes :

- est-il possible d'identifier, en ce qui concerne le client qui est une entité juridique ou une personne participant à la transaction, la ou les personnes physiques qui contrôlent effectivement en dernier ressort l'entité juridique ou qui exercent une influence ou un contrôle sur elle de toute autre manière, quelle que soit l'importance des actions, des droits de vote ou des droits de propriété ou leur nature directe ou indirecte ;
- si le client qui est une personne morale ou la personne qui participe à la transaction a une ou plusieurs personnes physiques qui possèdent ou contrôlent la personne morale par le biais d'une participation directe[16] ou indirecte[17] . Les liens familiaux et contractuels doivent également être pris en compte ;
- qui est la personne physique occupant un poste de direction[18] , qui doit être définie comme le bénéficiaire effectif, en raison de l'exécution des deux étapes précédentes qui n'ont pas permis à l'entité obligée d'identifier le bénéficiaire effectif.

Le cadre supérieur du client ne doit être indiqué en tant que bénéficiaire effectif que dans des cas exceptionnels où la société déploie tous les efforts raisonnables pour déterminer le bénéficiaire effectif et à condition qu'il n'y ait aucune raison de soupçonner que l'identité du bénéficiaire effectif est dissimulée. Dans ce cas, le cadre supérieur doit être compris comme le chef (par exemple, le PDG),

---

[14] dans le cas d'un étranger - la date de naissance (le cas échéant - le numéro personnel ou toute autre séquence unique de symboles attribuée à cette personne, destinée à son identification personnelle) ;

[15] lorsqu'un document d'identité ne contient pas de données sur la citoyenneté du client, les institutions financières et autres entités obligées doivent, lorsqu'elles identifient le client qui est une personne physique en sa présence physique, demander au client de fournir les données sur sa citoyenneté.

[16] **la propriété directe** est une manière d'exercer le contrôle par laquelle la personne physique détient une participation de 25 % plus une action ou un droit de propriété de plus de 25 % dans l'entreprise

[17] **La propriété indirecte** est un mode d'exercice du contrôle par lequel une participation de 25 % plus une action ou un droit de propriété de plus de 25 % dans la société est détenue par une société contrôlée par une personne physique ou par plusieurs sociétés contrôlées par la même personne physique.

[18] un **membre de la** direction générale est une personne qui prend les décisions stratégiques qui affectent fondamentalement les activités et/ou les pratiques commerciales et/ou les tendances générales (commerciales) de l'entreprise ou qui, en son absence, exerce des fonctions de gestion quotidienne ou régulière de l'entreprise dans le cadre du pouvoir exécutif (par exemple, directeur général (CEO), directeur financier (CFO), directeur ou président, etc.)

Les documents utilisés pour l'identification de l'entité légale ou les autres documents soumis ne sont pas des documents d'identité.

La Société appliquera des mesures raisonnables pour vérifier l'exactitude des informations établies sur la base de déclarations ou d'un document manuscrit (par exemple en effectuant des recherches dans les registres pertinents), en exigeant la présentation du rapport annuel de l'entité juridique ou d'un autre document pertinent. Si la société a des doutes sur l'exactitude ou l'exhaustivité des informations pertinentes, elle vérifiera les informations fournies à partir de sources accessibles au public et, si nécessaire, demandera des informations supplémentaires au client.

Difficultés rencontrées lors de l'identification du bénéficiaire effectif

La société doit être consciente que les informations relatives à la propriété effective peuvent être masquées par l'utilisation de sociétés écrans, de structures de propriété et de contrôle complexes impliquant de nombreuses couches d'actions enregistrées au nom d'autres personnes morales, d'actionnaires et d'administrateurs désignés, tels que des associés proches et des membres de la famille, et par d'autres moyens.

Dans de nombreux cas, le rôle des administrateurs et des actionnaires désignés est de protéger ou de dissimuler l'identité de l'administrateur et du contrôleur d'une société ou d'un actif. Un prête-nom peut aider à surmonter les contrôles juridictionnels sur la propriété d'une société et à contourner les interdictions d'exercer des fonctions d'administrateur imposées par les tribunaux et les autorités gouvernementales. La société doit donc être particulièrement attentive aux structures de sociétés qui favorisent la complexité et augmentent la difficulté d'obtenir des informations précises sur les bénéficiaires effectifs. En outre, la société doit être consciente de la possibilité qu'il existe des accords de prête-nom dans lesquels des amis, des membres de la famille ou des associés prétendent être les administrateurs de personnes morales, de constructions juridiques ou d'autres entreprises.

Par conséquent, l'entreprise doit prendre des mesures appropriées et adéquates pour déterminer les véritables bénéficiaires effectifs et identifier les situations dans lesquelles la propriété effective est occultée.

Pour déterminer la BO, la compagnie doit collecter des données sur la structure de propriété du client et les vérifier sur la base de documents, de données ou d'informations obtenus auprès d'une source fiable et indépendante. Dans le cas d'une propriété à plusieurs niveaux, le schéma de la structure de propriété doit être rédigé par le client ou obtenu de lui.

La Société doit également s'assurer qu'elle comprend la structure de propriété et de contrôle du Client, en particulier si la structure de propriété et de contrôle est complexe (par exemple, les actionnaires proviennent de plusieurs juridictions différentes ; les actionnaires sont de différents types d'entités juridiques / d'arrangements juridiques, il y a des trusts et des véhicules d'investissement privés dans la structure de propriété et de contrôle, le Client a émis des actions au porteur). La Compagnie doit évaluer si la structure de propriété et de contrôle est logique d'un point de vue commercial, économique ou juridique.

Utilisation du système d'information des entités juridiques Participants

Lors de l'identification d'un bénéficiaire effectif, la société doit également utiliser le système d'information des participants aux entités juridiques (JADIS), qui permet d'obtenir des données sur les bénéficiaires effectifs de la société.

Le client et a le droit d'utiliser d'autres systèmes d'information et registres de l'État dans lesquels des données sur les participants des personnes morales sont accumulées.

JADIS est accessible par l'intermédiaire du Centre des registres de l'entreprise d'État lituanienne (SECR) via l'application correspondante. La demande peut être soumise :

- par voie électronique via le système de libre-service du Centre des registres ;
- par e-mail info@registrucentras.lt qui doit être signé par e-signature ;
- auprès du service clientèle du Centre des registres en présentant l'original.

Les extraits JADIS préparés et les copies de documents peuvent être :

- téléchargée à partir du libre-service du Centre des registres (uniquement si la demande a été déposée par l'intermédiaire du libre-service du Centre des registres) ;
- auprès des bureaux de service à la clientèle du Centre des registres ;
- par courrier à l'adresse indiquée par le client.

Lorsqu'ils constatent une divergence entre les informations sur les bénéficiaires effectifs du client qui est une personne morale, disponibles dans JADIS, et les informations sur les bénéficiaires effectifs du même client dont ils disposent, ils en informent le client et proposent de fournir des informations exactes sur ses bénéficiaires effectifs au responsable du traitement des données de JADIS.

L'entreprise ne noue pas de relation d'affaires et n'exécute pas de transaction (à l'exception des opérations monétaires ou des transactions conclues et/ou exécutées dans le cadre d'une relation d'affaires) lorsque les informations sur les bénéficiaires effectifs du client qui est une personne morale ne sont pas fournies dans JADIS ou lorsque les informations sur les bénéficiaires effectifs du client qui est une personne morale, fournies dans JADIS, sont inexactes.

Identification de la personne politiquement exposée

La société prend des mesures pour vérifier si le client, le bénéficiaire effectif du client ou le représentant de ce client est une PPE, un membre de sa famille[19] ou un proche[20] ou si le client est devenu une telle personne.

La Société demandera au client des informations permettant d'identifier si le client est un PPE, un membre de sa famille ou un proche (par exemple, en donnant au client la possibilité de préciser les informations pertinentes lors de la collecte des données le concernant).

La société vérifie les données reçues du client en interrogeant les bases de données pertinentes ou les bases de données publiques, en interrogeant ou en vérifiant les données sur les sites web des autorités de contrôle ou des institutions compétentes du pays dans lequel le client a son lieu de résidence ou son siège. Le PPE doit être vérifié en outre à l'aide d'un moteur de recherche international (par exemple Google) et du moteur de recherche local du pays d'origine du client, le cas échéant, en saisissant le nom du client en alphabet latin et en alphabet local, ainsi que sa date de naissance.

En outre, le contrôle du statut PEP est mis en œuvre et réalisé par la solution AML automatisée Sum & Substance. Cette solution permet d'examiner en permanence le statut des PPE et d'identifier les membres de leur famille et leurs proches collaborateurs.

Au moins les personnes suivantes sont considérées comme des PPE :

- le chef de l'Etat, le chef du gouvernement, un ministre, un vice-ministre ou un ministre adjoint, un secrétaire d'Etat, un chancelier du parlement, du gouvernement ou d'un ministère ;
- un membre du parlement ;
- un membre de la Cour suprême, de la Cour constitutionnelle ou de toute autre autorité judiciaire suprême dont les décisions ne sont pas susceptibles de recours ;
- un maire de la municipalité, un chef de l'administration municipale ;
- un membre de l'organe de direction de l'institution suprême d'audit ou de contrôle de l'État, ou un président, un vice-président ou un membre du conseil d'administration de la banque centrale ;
- les ambassadeurs d'États étrangers, un chargé d'affaires ad interim, le chef des forces armées lituaniennes, le commandant des forces et unités armées, le chef de l'état-major de la défense ou un officier supérieur des forces armées étrangères ;
- un membre de l'organe de gestion ou de surveillance d'une entreprise publique, d'une société anonyme ou d'une société à responsabilité limitée dont les actions ou une partie des actions, représentant plus de la moitié du total des voix à l'assemblée générale des actionnaires de ces sociétés, sont détenues par l'État ;

[19] **membre de la famille** : le conjoint, la personne avec laquelle le partenariat a été enregistré (c'est-à-dire le cohabitant), les parents, les frères, les sœurs, les enfants et les conjoints des enfants,
les cohabitants des enfants

[20] **proche associé** : une personne physique qui, avec le PEP, est membre de la même entité juridique ou d'un organisme sans personnalité juridique ou entretient d'autres relations d'affaires ; ou une personne physique qui est le seul bénéficiaire effectif de l'entité juridique ou d'un organisme sans personnalité juridique créé ou fonctionnant de facto dans le but d'acquérir des biens ou d'autres avantages personnels pour le PEP.

- un membre de l'organe de gestion ou de surveillance d'une entreprise municipale, d'une société anonyme ou d'une société à responsabilité limitée dont les actions ou une partie des actions, représentant plus de la moitié du total des voix à l'assemblée générale des actionnaires de ces sociétés, sont détenues par l'État et qui sont considérées comme de grandes entreprises au sens de la loi sur les états financiers des entités de la République de Lituanie ;
- un directeur, un directeur adjoint ou un membre de l'organe de direction ou de surveillance d'une organisation internationale intergouvernementale ;
- un dirigeant, un vice-président ou un membre de l'organe de direction d'un parti politique.

L'entreprise n'identifie les associés proches et les membres de la famille des PPE que si leur lien avec les PPE est connu du public ou si l'entreprise a des raisons de penser qu'un tel lien existe.

Lorsqu'un PPE n'est plus chargé d'une fonction publique éminente, la société doit, dans un délai de 12 mois à compter de la date de démission du PPE des fonctions publiques, prendre en compte les risques qui demeurent liés au client. Après une période de 12 mois à compter de la date de démission du PPE des fonctions publiques, l'entreprise est tenue de réévaluer les risques liés à ce client.

Identification de l'objet et de la nature de la relation d'affaires ou de la transaction

La société doit comprendre l'objet et la nature de l'établissement de la relation d'affaires ou de l'exécution de la transaction. En ce qui concerne les services fournis, la société peut demander au client les informations suivantes afin de comprendre l'objectif et la nature de la relation d'affaires ou de la transaction :

- si le client utilisera les services de la société pour ses propres besoins ou s'il représentera les intérêts d'une autre personne ;
- informations de contact ;
- les informations relatives à l'adresse enregistrée et à l'adresse de résidence effective du client ;
- le chiffre d'affaires estimé des transactions avec l'entreprise par année civile ;
- la source estimée des fonds utilisés dans la relation d'affaires ou la transaction ;
- si la relation d'affaires ou la transaction est liée à l'exercice d'activités économiques ou professionnelles par le client et de quelles activités il s'agit ;
- des informations sur la source des fonds liés à la relation d'affaires ou à la transaction, si le montant des transactions (y compris le montant prévu) dépasse la limite fixée.

L'entreprise applique des mesures supplémentaires et recueille des informations supplémentaires afin d'identifier l'objet et la nature de la relation d'affaires dans les cas suivants :

- il y a une situation qui se réfère à une valeur élevée ou qui est inhabituelle et/ou
- lorsque le risque et/ou le profil de risque associé au client et la nature de la relation d'affaires justifient la mise en œuvre d'actions supplémentaires afin de pouvoir assurer un suivi approprié de la relation d'affaires.

Si le client est une personne morale, en plus de ce qui précède, la société identifiera le **domaine d'activité du client**, où la société comprendra ce que le client traite et a l'intention de traiter dans le cadre de la relation d'affaires et comment cela correspond à l'objectif et à la nature de la relation d'affaires en général et si c'est raisonnable, compréhensible et plausible.

Le domaine d'activité doit correspondre au profil d'expérience du représentant du client (ou des personnes clés) et/ou du bénéficiaire effectif. Ainsi, la société doit déterminer d'où proviennent les capacités, aptitudes, compétences et connaissances (expérience en général) du représentant et/ou du bénéficiaire effectif pour opérer dans ce domaine d'activité, avec ces volumes d'affaires et avec ces principaux partenaires commerciaux.

Suivi de la relation d'affaires

L'entreprise surveille les relations d'affaires établies lorsque les mesures de diligence raisonnable permanente (périodiquement) suivantes sont mises en œuvre :

- veiller à ce que les documents, données ou informations collectés dans le cadre de l'application des mesures de diligence raisonnable soient mis à jour régulièrement et en cas d'événements déclencheurs, c'est-à-dire principalement les données concernant le client, son représentant (y compris le droit de représentation) et le bénéficiaire effectif, ainsi que l'objet et la nature de la relation d'affaires ;
- un suivi permanent de la relation d'affaires, qui couvre les transactions effectuées dans le cadre de la relation d'affaires afin de s'assurer que les transactions correspondent à la connaissance qu'a l'entreprise du client, de ses activités et de son profil de risque ;
- l'identification de la source et de l'origine des fonds utilisés dans la (les) transaction(s).

La Société **vérifie et met à jour** régulièrement les **documents, données et informations** collectés dans le cadre de la mise en œuvre des mesures CDD et met à jour le profil de risque du Client. La régularité des vérifications et des mises à jour doit être basée sur le profil de risque du client et les vérifications doivent avoir lieu au moins une fois par an :

- une fois par semestre pour les clients à profil de risque élevé ;
- une fois par an pour les clients présentant un profil de risque moyen ;
- une fois tous les deux ans pour le client à faible risque.

La société a mis en place un système de stockage, de systématisation et de contrôle des documents des clients. Le système informe automatiquement l'employé responsable de la nécessité de demander un document actualisé en fonction du profil de risque du client. Le système comprend également un contrôle de la date d'expiration et envoie une notification si la date d'expiration du document d'identité ou du justificatif de domicile du client est proche.

Les documents, données et informations collectés doivent également être vérifiés si un événement s'est produit qui indique la nécessité de mettre à jour les documents, données et informations collectés.

Dans le cadre de la **surveillance continue de la relation d'affaires**, la société surveille les transactions conclues au cours de la relation d'affaires de manière à pouvoir déterminer si les transactions à conclure correspondent aux informations précédemment connues sur le client (c'est-à-dire ce que le client a déclaré lors de l'établissement de la relation d'affaires ou ce qui a été connu au cours de la relation d'affaires).

L'Entreprise surveille également la Relation d'Affaires pour vérifier les activités du Client ou les faits qui indiquent des activités criminelles, le blanchiment d'argent ou le financement du terrorisme ou dont la relation avec le blanchiment d'argent ou le financement du terrorisme est probable, y compris les transactions compliquées, de grande valeur et inhabituelles et les modèles de transactions qui n'ont pas d'objectif économique ou légitime raisonnable ou évident ou qui ne sont pas caractéristiques des spécificités de l'activité en question. Dans le cadre de la relation d'affaires, l'entreprise évalue en permanence les éléments suivants
les changements dans les activités du client et évaluer si ces changements peuvent augmenter le niveau de risque associé au client et à la relation d'affaires, donnant lieu à la nécessité d'appliquer des mesures de CED.

Dans le cadre du contrôle permanent de la relation d'affaires, l'entreprise applique les mesures suivantes :

- c'est-à-dire le suivi des transactions en temps réel ;
- le suivi, c'est-à-dire l'analyse ultérieure des

transactions. L'objectif du **screening** est

d'identifier :

- les transactions suspectes et inhabituelles et les schémas de transaction ;
- les transactions dépassant les seuils prévus ;
- les personnes politiquement exposées et les circonstances concernant les sanctions.

Le contrôle des transactions est effectué automatiquement et comprend les mesures suivantes :

- des seuils établis pour les transactions du client, en fonction du profil de risque du client et de l'estimation du chiffre d'affaires des transactions déclarées par le client ;
- la notation des portefeuilles de monnaie virtuelle où la monnaie virtuelle sera envoyée conformément à la commande du client ;
- la notation des portefeuilles de monnaie virtuelle à partir desquels la monnaie virtuelle est reçue.

Si le client donne l'ordre d'effectuer une transaction qui dépasse le seuil fixé ou une transaction vers un portefeuille de monnaie virtuelle présentant un score de risque élevé (par exemple, des portefeuilles liés à la fraude, à la criminalité, etc.), la transaction est approuvée manuellement par l'employé, qui évalue, avant l'approbation, la nécessité d'appliquer des mesures CDD supplémentaires (par exemple, appliquer des mesures EDD, demander la source et l'origine des fonds ou demander des informations supplémentaires concernant la transaction).

Lors du **contrôle des transactions**, l'employé évalue les transactions en vue de détecter les activités et les transactions qui :

- s'écarter de ce que l'on est en droit d'attendre sur la base des mesures CDD mises en œuvre, des services fournis, des informations communiquées par le client et d'autres circonstances (par exemple, dépassement du chiffre d'affaires estimé, envoi de monnaie virtuelle à chaque fois vers un nouveau portefeuille de monnaie virtuelle, volume de transactions dépassant la limite) ;
- sans déroger à la clause précédente, peut être considéré comme faisant partie d'uneopération de blanchiment de capitaux ou de financement du terrorisme ;
- peut affecter le score du profil de risque du client.

Dans le cas où le fait susmentionné est détecté, l'employé doit en informer le MLRO et reporter toute transaction du client jusqu'à ce que le MLRO prenne une décision à ce sujet.
En plus de ce qui précède, le MLRO examine régulièrement (au moins une fois par semaine) les transactions de l'entreprise afin de s'assurer que

- les employés de la société ont correctement exécuté les obligations susmentionnées ;
- il n'y a pas de transactions ou de schémas de transactions compliqués, de grande valeur et inhabituels, qui n'ont pas d'objectif économique ou légitime raisonnable ou évident, ou qui ne sont pas caractéristiques des spécificités.

La Société **identifie la source[21] et l'origine[22] des fonds** utilisés dans la (les) transaction(s) si nécessaire. La nécessité d'identifier la source et l'origine des fonds dépend des activités antérieures du client ainsi que d'autres informations connues. L'identification de la source et de l'origine des fonds utilisés dans la transaction sera effectuée dans les cas suivants :

- les transactions dépassent les limites fixées par l'entreprise ;
- les transactions ne correspondent pas aux informations précédemment connues sur le client ;
- l'entreprise souhaite ou devrait raisonnablement considérer qu'il est nécessaire d'évaluer si les transactions correspondent aux informations précédemment connues sur le client ;
- l'entreprise soupçonne que les transactions sont le signe d'activités criminelles, de blanchiment de capitaux ou de financement du terrorisme, ou que le lien entre les transactions et le blanchiment de capitaux ou le financement du terrorisme est probable, y compris les transactions compliquées, de grande valeur et inhabituelles et les modèles de transactions qui n'ont pas d'objectif économique ou légitime raisonnable ou évident, ou qui ne sont pas caractéristiques des spécificités de l'activité en question.

MISE EN ŒUVRE DES SANCTIONS

Dès l'entrée en vigueur, la modification ou la levée des sanctions, la Société vérifie si le Client, son Bénéficiaire effectif ou une personne qui envisage d'avoir une Relation d'affaires ou une transaction avec lui fait l'objet de sanctions. Si l'Entreprise identifie une personne faisant l'objet de sanctions ou si la transaction envisagée ou effectuée par cette personne est en violation des sanctions, l'Entreprise applique les sanctions et en informe le FCIS dans un délai de 3 heures.

Procédure d'identification de la personne faisant l'objet de sanctions et d'une transaction violant les sanctions

La société utilise au moins les sources (bases de données) suivantes pour vérifier la relation du client avec les sanctions :

- Une liste consolidée des sanctions de l'UE ;
- Liste récapitulative des sanctions imposées par les Nations unies
- Office of Foreign Assets Control (OFAC).

Outre les sources susmentionnées, l'entreprise peut utiliser d'autres sources sur décision de l'employé qui applique les mesures de CDD.

[21] **la source des fonds** utilisés dans la transaction est la raison, l'explication et la base (relation juridique et son contenu) pour laquelle les fonds ont été transférés

[22] l'origine des fonds utilisés dans la transaction est l'activité par laquelle les fonds ont été gagnés ou reçus

Pour vérifier que les noms des personnes résultant de l'enquête sont les mêmes que les personnes énumérées dans une notification contenant une ou des sanctions, on utilise leurs données personnelles, dont les principales caractéristiques sont, pour une personne morale, son nom ou sa marque, son code de registre ou sa date d'enregistrement, et pour une personne physique, son nom et son identification personnelle ou sa date de naissance.

Afin d'établir l'identité des personnes spécifiées dans l'acte juridique ou l'avis pertinent et celles identifiées à la suite de l'interrogation des bases de données, l'entreprise doit analyser les noms des personnes trouvées à la suite de l'interrogation en fonction de l'effet possible des facteurs de distorsion des données à caractère personnel (par exemple, transcription de noms étrangers, ordre différent des mots, substitution de signes diacritiques ou de lettres doubles, etc.)

La société effectue les vérifications susmentionnées de manière continue dans le cadre d'une relation d'affaires établie. La fréquence des vérifications en cours dépend du profil de risque du client :

- une fois par semaine pour le client à haut risque ;
- une fois par mois pour le client à risque moyen ;
- une fois par trimestre pour le client à faible risque.

Si l'employé a des doutes sur le fait qu'une personne fait l'objet de sanctions, il en informe immédiatement le MLRO ou le membre du conseil d'administration. Dans ce cas, le MLRO ou le membre du conseil d'administration décide soit de demander ou d'obtenir des données supplémentaires de la personne, soit d'informer immédiatement le FCIS de ses soupçons.

L'entreprise doit en premier lieu acquérir par elle-même des informations supplémentaires sur la personne qui entretient une relation d'affaires ou effectue une transaction avec elle, ainsi que sur la personne qui a l'intention d'établir une relation d'affaires, d'effectuer une transaction ou un acte avec elle, en privilégiant les informations provenant d'une source crédible et indépendante. Si, pour une raison quelconque, ces informations ne sont pas disponibles, l'entreprise demande à la personne qui est en relation d'affaires ou qui effectue une transaction ou un acte avec elle, ainsi qu'à la personne qui a l'intention d'établir une relation d'affaires, d'effectuer une transaction ou un acte avec elle, si les informations proviennent d'une source crédible et indépendante, et elle évalue la réponse.

Actions en cas d'identification d'une personne visée par des sanctions ou d'une transaction violant des sanctions

Si l'employé de la société apprend que le client qui est en relation d'affaires ou qui effectue une transaction avec la société, ainsi qu'une personne qui a l'intention d'établir une relation d'affaires ou d'effectuer une transaction avec la société, fait l'objet de sanctions, il informe immédiatement le MLRO ou le membre du conseil d'administration de l'identification de la personne faisant l'objet de sanctions, des doutes qu'elle suscite et des mesures qu'elle a prises.

Le MLRO ou le membre du conseil d'administration refuse de conclure une transaction ou une procédure, prend les mesures prévues dans l'acte relatif à l'imposition ou à la mise en œuvre des sanctions et informe immédiatement le FCIS de ses doutes et des mesures prises.

Lors de l'identification de la personne faisant l'objet des sanctions, il est nécessaire d'identifier les mesures prises pour sanctionner cette personne. Ces mesures sont décrites dans l'acte juridique mettant en œuvre la

Sanctions : il est donc nécessaire d'identifier la sanction exacte qui est appliquée à la personne afin de garantir une application légale et correcte des mesures.

REFUS DE LA TRANSACTION OU DE LA RELATION D'AFFAIRES ET LEUR RÉSILIATION

Il est interdit à l'entreprise d'établir une relation d'affaires et la relation d'affaires ou la transaction établie sera résiliée (à moins qu'il ne soit objectivement impossible de le faire) dans les cas suivants :

- la société soupçonne un blanchiment d'argent ou un financement du terrorisme ;
- il est impossible pour la société d'appliquer les mesures CDD, parce que le client ne soumet pas les données pertinentes ou refuse de les soumettre, ou parce que les données soumises ne permettent pas de s'assurer que les données collectées sont adéquates ;
- le client dont le capital est constitué d'actions ou d'autres titres au porteur souhaite établir la relation d'affaires ;
- le client, qui est une personne physique derrière laquelle se trouve une autre personne réellement bénéficiaire, souhaite établir la relation d'affaires (soupçon d'utilisation d'une personne agissant en tant que façade) ;
- le profil de risque du client ne correspond plus à l'appétit pour le risque de la société (c'est-à-dire que le niveau de profil de risque du client est "interdit").

En cas de résiliation de la relation d'affaires conformément au présent chapitre, la société transfère les avoirs du client dans un délai raisonnable, mais de préférence au plus tard dans le mois qui suit la résiliation et dans leur ensemble, sur un compte ouvert dans un établissement de crédit enregistré ou ayant son siège dans un État contractant de l'Espace économique européen ou dans un pays où sont appliquées des exigences équivalentes à celles établies dans les directives pertinentes du Parlement européen et du Conseil. Dans des cas exceptionnels, les actifs peuvent être transférés sur un compte autre que celui du client ou émis en espèces. Quel que soit le destinataire des fonds, l'information minimale donnée en anglais dans les détails de paiement du transfert des actifs du client est que le transfert est lié à la cessation extraordinaire de la relation avec le client.

OBLIGATION DE DÉCLARATION

L'entreprise doit suspendre la transaction, quel qu'en soit le montant (sauf dans les cas où cela est objectivement impossible en raison de la nature de l'opération monétaire ou de la transaction, de son mode d'exécution ou d'autres circonstances) et, par l'intermédiaire de son MLRO, doit rendre compte au FCIS de l'activité ou des circonstances qu'elle identifie dans le cadre de ses activités économiques et par lesquelles elle le fait :

- la société a établi que le client effectue une transaction suspecte ;

- l'entreprise sait ou soupçonne que des actifs de quelque valeur que ce soit proviennent directement ou indirectement d'une activité criminelle ou d'une participation à une telle activité.

Les caractéristiques minimales des transactions suspectes sont indiquées dans les lignes directrices élaborées par le FCIS (l'une des annexes des présentes lignes directrices).

Les rapports spécifiés ci-dessus doivent être effectués avant la réalisation de la transaction si l'entreprise soupçonne ou sait que des actes de blanchiment de capitaux ou de financement du terrorisme ou des délits connexes sont commis et si ces circonstances sont identifiées avant la réalisation de la transaction.

Si la nécessité du rapport susmentionné se fait sentir, l'employé qui en a eu connaissance doit en informer immédiatement le MLRO.

Dans tous les cas (c'est-à-dire également dans la situation où une activité ou une circonstance est identifiée après la réalisation de la transaction), l'**obligation de déclaration pour les rapports susmentionnés doit être exécutée immédiatement, mais au plus tard dans les trois heures ouvrables** suivant l'identification de l'activité ou de la circonstance ou l'émergence du soupçon réel (c'est-à-dire la situation où le soupçon ne peut pas être dissipé).

Obligation de déclaration concernant certains types de transactions

L'entreprise, par l'intermédiaire de son MLRO, doit envoyer des informations au FCIS au plus tard dans les 7 jours ouvrables suivant l'identification des transactions de change de monnaie virtuelle ou des transactions en monnaie virtuelle, si la valeur journalière de ces transactions est égale ou supérieure à 15 000 euros ou au montant équivalent en monnaie étrangère ou en monnaie virtuelle, que la transaction soit ou non conclue dans le cadre d'une ou de plusieurs transactions monétaires connexes.

Dans les cas précisés ci-dessus, les informations communiquées au FCIS comprennent

- les données confirmant l'identité du client et, lorsque la transaction est effectuée par l'intermédiaire d'un représentant, les données confirmant l'identité de ce dernier ;
- le montant de la transaction ;
- la devise dans laquelle la transaction a été exécutée ;
- la date d'exécution de la transaction ;
- les modalités d'exécution de l'opération monétaire ;
- l'entité au profit de laquelle l'opération monétaire a été exécutée (si possible) ;
- les autres données spécifiées dans les instructions FCIS correspondantes.

Tous les rapports décrits dans le présent chapitre sont envoyés conformément aux lignes directrices de la société en matière de rapports, par le biais d'un canal sécurisé garantissant une confidentialité totale (l'une des annexes des présentes lignes directrices).

Il est interdit à la société, à une unité structurelle de la société, à un membre du conseil d'administration, à un MLRO et à l'employé d'informer une personne, son bénéficiaire effectif, son représentant ou un tiers d'un rapport soumis à leur sujet au FCIS, d'un projet de soumission d'un tel rapport ou de la survenue

de signalement ainsi que d'un précepte émis par le FCIS ou de l'ouverture d'une procédure pénale.

OBLIGATION DE FORMATION

L'entreprise veille à ce que ses employés, ses sous-traitants et les autres personnes qui participent à ses activités sur une base similaire et qui effectuent des tâches importantes pour empêcher l'utilisation des activités de l'entreprise à des fins de blanchiment de capitaux ou de financement du terrorisme (les "personnes concernées") possèdent les qualifications requises pour ces tâches. Lorsqu'une personne concernée est recrutée ou engagée, ses qualifications sont vérifiées dans le cadre du processus de recrutement ou de nomination en procédant à un contrôle des antécédents, documenté à l'aide d'un formulaire standard spécial évaluant l'aptitude du salarié.

Conformément aux exigences applicables à la Société en matière d'aptitude des personnes concernées, la Société veille à ce que ces personnes reçoivent en permanence une formation et des informations appropriées afin de pouvoir remplir les obligations de la Société conformément à la législation applicable. La formation permet de s'assurer que ces personnes ont des connaissances dans le domaine de la lutte contre le blanchiment de capitaux et le financement du terrorisme dans une mesure appropriée compte tenu de leurs tâches et de leurs fonctions. La formation doit fournir, avant tout, des informations sur toutes les méthodes les plus récentes de blanchiment de capitaux et de financement du terrorisme et sur les risques qui en découlent.

Cette formation se réfère aux parties pertinentes du contenu des règles et réglementations applicables, à l'évaluation des risques de l'entreprise, aux lignes directrices et procédures de l'entreprise et aux informations qui devraient aider les personnes concernées à détecter les soupçons de blanchiment de capitaux et de financement du terrorisme. La formation est structurée sur la base des risques identifiés par la politique d'évaluation des risques.

Le contenu et la fréquence de la formation sont adaptés aux tâches et à la fonction de la personne sur les questions relatives aux mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme. Si les lignes directrices sont mises à jour ou modifiées d'une manière ou d'une autre, le contenu et la fréquence de la formation sont adaptés en conséquence.

Pour les nouveaux employés, la formation comprend un examen du contenu des règles et réglementations applicables, de la politique d'évaluation des risques de la société, des présentes lignes directrices et d'autres procédures pertinentes.

Les employés et les membres du conseil d'administration reçoivent une formation continue sous les auspices du MLRO, conformément au plan de formation suivant :

- Périodicité : au moins une fois par an pour les membres du conseil d'administration. Au moins une fois par an pour les employés de la société et les personnes concernées engagées.
- champ d'application : examen des règles et réglementations applicables, des lignes directrices de l'entreprise et d'autres procédures pertinentes. Informations spécifiques relatives aux éléments nouveaux/actualisés des règles et réglementations applicables. Rapport et échange d'expériences concernant les transactions examinées depuis la formation précédente.

En outre, les personnes concernées sont tenues informées en permanence des nouvelles tendances, des nouveaux modèles et des nouvelles méthodes, et reçoivent d'autres informations pertinentes pour la prévention du blanchiment de capitaux et du financement du terrorisme. La formation organisée doit être documentée électroniquement et confirmée par la signature de la personne concernée. Cette documentation doit inclure le contenu de la formation, les noms des participants et la date de la formation.

LA COLLECTE ET LE STOCKAGE DES DONNÉES, LES CARNETS DE BORD

La société, par l'intermédiaire de la personne (y compris les employés, les membres du conseil d'administration et le MLRO) qui reçoit en premier lieu les informations ou les documents pertinents, enregistre et conserve les données suivantes :

- toutes les données collectées dans le cadre de la mise en œuvre des mesures du CDD ;
- des informations sur les circonstances du refus de l'établissement de la relation d'affaires par l'entreprise ;
- les circonstances du refus d'établir une relation d'affaires à l'initiative du client si le refus est lié à l'application de mesures CDD par la société ;
- des informations sur toutes les opérations effectuées pour identifier la personne participant à la transaction ou le bénéficiaire effectif du client ;
- s'il est impossible d'effectuer les mesuresCDD ;
- des informations sur les circonstances de la cessation de la relation d'affaires en rapport avec l'impossibilité d'appliquer les mesures CDD
- la date ou la période de chaque transaction et une description du contenu de la transaction, y compris le montant de la transaction, la devise et le numéro de compte ou un autre identifiant (y compris le hachage des transactions en monnaie virtuelle et des portefeuilles de monnaie virtuelle liés à la transaction) ;
- les informations servant de base aux obligations de déclaration spécifiées dans les lignes directrices ;
- les données relatives à des transactions ou circonstances suspectes ou inhabituelles dont le FCIS n'a pas été informé (par exemple, des transactions complexes ou d'un montant inhabituel, des transactions effectuées selon un schéma inhabituel et des transactions qui n'ont pas d'objectif économique ou licite apparent, des relations d'affaires ou des opérations monétaires avec des clients de pays tiers où les mesures de prévention du blanchiment de capitaux et/ou du financement du terrorisme sont insuffisantes ou ne répondent pas aux normes internationales selon les informations officiellement publiées par les organisations intergouvernementales internationales).

Certaines des données spécifiées ci-dessus sont introduites dans le journal (tel que décrit ci-dessous) par ordre chronologique sur la base des documents confirmant une opération monétaire ou une transaction ou d'autres documents juridiquement valables relatifs à l'exécution d'opérations monétaires ou de transactions, immédiatement et au plus tard dans les trois jours ouvrables suivant l'exécution d'une opération monétaire ou d'une transaction.

Les données spécifiées ci-dessus sont conservées pendant 8 ans après l'expiration de la relation d'affaires ou de la transaction achevée. Les données relatives à l'exécution de l'obligation de déclaration doivent être conservées pendant 5 ans après l'exécution de l'obligation de déclaration.

Les la correspondance relative à une relation commerciale avec le client doit être conservée pendant cinq ans à compter de la date de cessation des transactions ou de la relation commerciale.

Les documents et les données doivent être conservés de manière à permettre une réponse exhaustive et immédiate aux demandes formulées par le FCIS ou, conformément à la législation, par d'autres autorités de contrôle, des autorités d'enquête ou le tribunal.

L'entreprise met en œuvre toutes les règles de protection des données à caractère personnel en appliquant les exigences découlant de la législation en vigueur. L'entreprise est autorisée à traiter les données personnelles recueillies lors de la mise en œuvre du CDD uniquement dans le but de prévenir le blanchiment de capitaux et le financement du terrorisme, et les données ne doivent pas être traitées d'une manière qui ne correspond pas à l'objectif, par exemple, à des fins de marketing.

L'entreprise supprime les données conservées à l'expiration du délai, à moins que la législation régissant le domaine concerné n'établisse une procédure différente. Sur la base d'un précepte de l'autorité de contrôle compétente, les données importantes pour la prévention et la détection du blanchiment de capitaux ou du financement du terrorisme, ou pour les enquêtes en la matière, peuvent être conservées plus longtemps, mais pas plus de deux ans après l'expiration du premier délai.

Tenue des carnets d'immatriculation

Pour s'acquitter de ses obligations en matière de lutte contre le blanchiment d'argent, l'entreprise tient (complète) les registres d'enregistrement suivants, qui reflètent les opérations et transactions monétaires (ci-après dénommés "registres") :

- le journal des clients qui effectuent des transactions en monnaie virtuelle, que ces transactions soient effectuées occasionnellement ou dans le cadre d'une relation d'affaires ;
- le journal des opérations monétaires ou des transactions effectuées entre le client et l'entreprise avant que l'entreprise ne soit obligée d'appliquer des mesures de vigilance à l'égard de la clientèle ;
- registre des déclarations[23] et des transactions et opérations monétaires suspectes ;
- le registre des clients avec lesquels des transactions ou des relations d'affaires ont été refusées ou interrompues dans des circonstances liées à des violations de la procédure de prévention du blanchiment de capitaux et/ou du financement du terrorisme.

Le registre d'enregistrement des clients qui effectuent des transactions en monnaie virtuelle comprend les éléments suivants :

- les données confirmant l'identité du client et de son représentant (si la transaction monétaire est effectuée ou si la transaction est conclue par l'intermédiaire d'un représentant) : nom et prénom d'une personne physique, code d'identification personnel (date de naissance d'un client étranger), nationalité ; code personnel, si un tel code est fourni ;
- dans le cas de transactions en monnaie virtuelle ou de transactions pour lesquelles il n'est pas objectivement possible d'identifier le bénéficiaire, d'autres informations permettant d'identifier l'adresse en monnaie virtuelle sont disponibles.

[23] comme décrit dans le chapitre correspondant des présentes lignes directrices

liés à l'identité du propriétaire de la monnaie virtuelle : adresse IP (Internet Protocol), adresse électronique, etc ;

- Adresse(s) de la monnaie virtuelle liée(s) à la transaction et au(x) hachage(s) de la transaction ;
- méthode de transaction : dépôt ou retrait de monnaie virtuelle, la monnaie virtuelle est échangée contre de l'argent ou vice versa, la monnaie virtuelle est échangée contre d'autres monnaies virtuelles, la transaction d'échange de monnaie virtuelle a été médiatisée (échange p2p) ;

Le registre d'enregistrement des opérations monétaires ou des transactions effectuées entre le client et l'entreprise avant que l'entreprise ne soit tenue d'appliquer des mesures de vigilance à l'égard de la clientèle comprend les éléments suivants :

- les données confirmant l'identité du client et de son représentant (si la transaction monétaire est effectuée ou si la transaction est conclue par l'intermédiaire d'un représentant) : nom et prénom d'une personne physique, code d'identification personnel (date de naissance d'un client étranger), nationalité ; code personnel, si un tel code est fourni ;
- les données relatives à la transaction monétaire ou à l'opération : la date de la transaction, la description des actifs faisant l'objet de la transaction (espèces, biens immobiliers, monnaie virtuelle, etc.) et leur valeur (montant d'argent, devise dans laquelle la transaction monétaire ou l'opération est effectuée, valeur marchande des actifs, etc ;)
- la méthode de transaction : La monnaie virtuelle est échangée contre de l'argent ou vice versa, le client a effectué un prépaiement pour acheter de la monnaie virtuelle, etc.

Le registre d'enregistrement des déclarations, des opérations monétaires suspectes et des transactions comprend, par ordre chronologique, les éléments suivants :

- les données confirmant l'identité du client et de son représentant (si la transaction monétaire est effectuée ou si la transaction est conclue par l'intermédiaire d'un représentant) : nom et prénom d'une personne physique, code d'identification personnel (date de naissance d'un client étranger), nationalité ; code personnel, si un tel code est fourni ;
- le critère approuvé par le ministère de l'intérieur de la République de Lituanie, selon lequel il est reconnu que la transaction ou l'opération monétaire du client est considérée comme suspecte, la transaction ou l'opération est conforme ;
- Méthode d'exécution de l'opération ou de la transaction monétaire suspecte ;
- Date et heure de l'opération monétaire ou de la transaction suspecte, caractéristiques des actifs faisant l'objet de la transaction (espèces, etc.) et leur valeur (montant d'argent, devise utilisée pour la conduite de l'opération monétaire ou de la transaction, valeur marchande de l'actif) ;
- les données relatives au(x) bénéficiaire(s) de la transaction : nom complet et numéro d'identification personnel d'une personne physique (dans le cas d'un étranger : date de naissance, le cas échéant, numéro d'identification personnel ou toute autre séquence unique de symboles attribuée à la personne concernée à des fins d'identification

- Coordonnées du client : numéro(s) de téléphone, adresse(s) électronique(s), personne(s) de contact, numéro(s) de téléphone, adresse(s) électronique(s), etc ;
- Description des actifs que le client ne peut contrôler ou utiliser à partir du moment de la suspension de l'opération monétaire suspecte ou de la transaction (lieu et autres informations caractérisant les actifs) ;
- En cas de transaction monétaire suspecte ou de transaction qui n'a pas été suspendue, les raisons pertinentes ;
- Méthodes de gestion des comptes ;
- Autres détails pertinents, selon la décision de l'employé.

L'entreprise inclut dans le registre d'enregistrement des clients, lorsque des transactions ou des relations commerciales ont été interrompues, les éléments suivants, par ordre chronologique :

- les données confirmant l'identité du client et de son représentant (si la transaction monétaire est effectuée ou si la transaction est conclue par l'intermédiaire d'un représentant) : nom et prénom d'une personne physique, code d'identification personnel (date de naissance d'un client étranger), nationalité ; code personnel, si un tel code est fourni ;
- les données relatives à la transaction monétaire ou à l'opération : la date de la transaction, la description des actifs faisant l'objet de la transaction (espèces, biens immobiliers, monnaie virtuelle, etc.) et leur valeur (montant d'argent, devise dans laquelle la transaction monétaire ou l'opération est effectuée, valeur marchande des actifs, etc ;)
- dans le cas de transactions en monnaie virtuelle ou de transactions pour lesquelles il n'est pas objectivement possible d'identifier le bénéficiaire, d'autres informations permettant de relier l'adresse de la monnaie virtuelle à l'identité du propriétaire de la monnaie virtuelle : adresse de protocole Internet (IP), adresse de courrier électronique, etc ;
- dans le cas de transactions en monnaie virtuelle, la ou les adresses en monnaie virtuelle liées à la transaction et le ou les hashs de la transaction ;
- les données relatives au(x) bénéficiaire(s) du client : nom complet et numéro d'identification personnel d'une personne physique (dans le cas d'un étranger : date de naissance, le cas échéant, numéro d'identification personnel ou toute autre séquence unique de symboles attribuée à la personne concernée à des fins d'identification personnelle), et dans le cas d'une personne morale, titre, forme juridique, adresse du siège social et numéro d'enregistrement, si un tel numéro a été attribué ;
- Motifs de résiliation des transactions ou des relations d'affaires en cas d'infraction à la procédure de prévention du blanchiment de capitaux et/ou du financement du terrorisme.

Procédure de tenue et de gestion des carnets d'enregistrement

Le stockage des données du journal est effectué et conservé sur un support électronique par le membre du conseil d'administration, s'il est en voyage d'affaires ou s'il n'est pas disponible pour d'autres raisons valables, par un autre employé, comme indiqué dans l'ordre spécial du directeur, qui définit l'étendue des tâches et des responsabilités confiées à une personne agissant en tant que remplaçant.

Le conseil d'administration désigne un employé chargé d'assurer la protection des données figurant dans les registres d'immatriculation et traitées sur un support électronique, contre toute suppression, modification ou utilisation non autorisée par des tiers non autorisés.

Les détails sont stockés à l'aide d'un logiciel permettant d'exporter les détails stockés vers Microsoft Office Excel, Word ou un logiciel équivalent à code ouvert, sans porter atteinte à l'intégrité des détails.

La tenue des registres d'enregistrement est vérifiée par un membre du conseil d'administration, s'il est en voyage d'affaires ou s'il n'est pas disponible pour d'autres raisons valables, ou par un autre employé responsable désigné par la société, comme indiqué dans l'ordre spécial du directeur, qui définit l'étendue des fonctions et des responsabilités attribuées à une personne agissant en tant que suppléant.

Il est interdit aux employés de l'Entreprise d'informer ou de faire savoir de toute autre manière à un Client ou à d'autres personnes que des informations sur les opérations monétaires en cours ou les transactions effectuées par un Client, ou sur l'enquête qui en résulte, sont communiquées au FCIS.

CONTRÔLE INTERNE DE L'EXÉCUTION DES LIGNES DIRECTRICES

La mise en œuvre des lignes directrices fait l'objet d'un contrôle interne par le membre du conseil d'administration ou par l'employé désigné par le conseil d'administration pour exercer les fonctions correspondantes (ci-après dénommé "responsable du contrôle interne" dans le présent chapitre). Le responsable du contrôle interne doit disposer des compétences, des outils et de l'accès aux informations nécessaires dans toutes les unités structurelles de l'entreprise.

Le responsable du contrôle interne exerce des fonctions de contrôle interne au moins dans les domaines suivants :

- le respect par l'entreprise de la politique d'évaluation des risques et de l'appétit pour le risque ;
- Mise en œuvre des mesures du CDD ;
- la mise en œuvre des sanctions ;
- l'obligation de l'entreprise de refuser la transaction ou la relation d'affaires et leur résiliation ;
- l'obligation de déclaration de la société au FCIS ;
- l'obligation de formation de l'entreprise concernant les exigences en matière de lutte contre le blanchiment d'argent et le financement du terrorisme ;
- l'obligation de l'entreprise de collecter et de conserver les données.

Les mesures exactes de mise en œuvre du contrôle interne sont déterminées par le responsable du contrôle interne et doivent correspondre à la taille de la société ainsi qu'à la nature, à l'étendue et au niveau de complexité des activités et des services fournis. Les bureaux de contrôle interne doivent prendre en compte au moins les domaines d'examen spécifiés ci-dessus. Les mesures de contrôle interne sont exécutées au moment déterminé par le responsable du contrôle interne et à la fréquence qu'il fixe, au moins une fois par mois, si la nature de la mesure n'en dispose pas autrement de manière expresse. Les résultats de la mise en œuvre des mesures de contrôle interne (ci-après, dans le présent chapitre, les données de contrôle interne) sont enregistrés séparément des autres données et conservés pendant cinq ans. Seuls les membres du conseil d'administration et le responsable du contrôle interne peuvent avoir accès aux données du contrôle interne.

Données de contrôle. Le responsable du contrôle interne ne peut donner accès aux données de contrôle interne à d'autres employés ou à des tiers (conseillers, auditeurs, etc.) qu'avec l'accord préalable du conseil d'administration. Les personnes ayant accès aux données de contrôle interne ne doivent les divulguer à personne sans l'accord préalable du conseil d'administration.

Les données de contrôle interne sont sauvegardées par ordre chronologique dans un format permettant de les analyser et de les relier de manière compréhensible à d'autres données pertinentes.

Le responsable du contrôle interne présente le rapport de contrôle interne au conseil d'administration au moins une fois par trimestre et à l'assemblée générale des actionnaires de la société au moins une fois par an. Le rapport de contrôle interne fourni comprend au moins les éléments suivants :

- période d'exercice du contrôle interne ;
- le nom et la fonction de la personne chargée du contrôle interne ;
- la description des mesures de contrôle interne qui ont été prises ;
- les résultats du contrôle interne ;
- les conclusions générales du contrôle interne exercé ;
- Les déficiences constatées ont été éliminées au cours de la période d'exercice du contrôle interne ;
- Les déficiences constatées, qui n'ont pas été éliminées à la fin de la période d'exercice du contrôle interne ;
- les mesures à mettre en œuvre pour éliminer les déficiences constatées.

Le conseil d'administration examine le rapport de contrôle interne fourni et prend une résolution à son sujet. Le responsable du contrôle interne est informé de l'essence de cette résolution dans un format qui peut être reproduit par écrit. Pour cette raison, le conseil d'administration est tenu de :

- analyser les résultats du contrôle interne effectué ;
- mettre en œuvre des actions visant à éliminer les déficiences constatées.

La société doit revoir et, si nécessaire, mettre à jour la procédure de contrôle interne au moins une fois par an et dans les cas suivants :

- à la suite de la publication par la Commission européenne des résultats d'une évaluation du risque de blanchiment de capitaux et de financement du terrorisme à l'échelle de l'UE (disponible sur le site web de la Commission européenne http://ec.europa.eu) ;
- après la publication des résultats de l'évaluation nationale du risque de blanchiment de capitaux et de financement du terrorisme (publiée dans la section "Évaluation nationale du risque de blanchiment de capitaux et de financement du terrorisme" de la section "Prévention du blanchiment de capitaux" du site web www.fntt.lt) ;
- dès réception d'une instruction du FCIS visant à renforcer les procédures de contrôle interne applicables ;

- en cas d'événements ou de changements importants dans la gestion et les activités de l'opérateur de monnaie virtuelle dépositaire et de l'opérateur de change de monnaie virtuelle.

Évaluation des risques et appétit pour le risque

L'objectif de la mise en œuvre des mesures de contrôle interne pour la conformité de la société avec la politique d'évaluation des risques établie (y compris l'appétit pour le risque établi) est l'examen des circonstances suivantes :

- L'entreprise établit et utilise une approche fondée sur le risque lorsqu'elle fournit des services aux clients (par exemple, les mesures CDD sont mises en œuvre en fonction du niveau de risque) ;
- L'entreprise a déterminé les facteurs qui influent sur l'apparition des risques de blanchiment d'argent et de financement du terrorisme et ces facteurs sont pertinents ;
- L'entreprise a déterminé et évalué la ML/TF de tous les services qu'elle fournit ;
- L'entreprise a établi le profil de risque du client avant d'effectuer des transactions ou de nouer des relations d'affaires ;
- La société met régulièrement à jour le profil de risque du client ;
- L'entreprise respecte l'appétit pour le risque établi ;
- L'entreprise tient un registre de tous les incidents conformément à la politique d'évaluation des risques établie ;
- La politique d'évaluation des risques a été revue au cours de l'année écoulée et rien n'indique que le MLRO ait exigé une révision antérieure.

Mise en œuvre des mesures de diligence raisonnable à l'égard des clients

L'objectif de la mise en œuvre des mesures de contrôle interne pour la conformité de la société avec la mise en œuvre des mesures de CDD est un examen des circonstances suivantes :

- la société applique les mesures CDD prescrites par les lignes directrices à tous les clients concernés ;
- l'entreprise recueille les documents et informations appropriés lors de l'application des mesures CDD ;
- l'entreprise vérifie correctement les données et les documents recueillis lors de l'application des mesures CDD ;
- l'entreprise applique le niveau approprié de mesures CDD (par exemple, des mesures EDD, etc.) ;
- l'entreprise applique des mesures de détection et de prévention appropriées à des clients spécifiques (par exemple, PPE, pays à haut risque, etc.) ;
- la société procède à l'identification des clients conformément à la procédure établie ;
- la société identifie correctement le(s) représentant(s) des clients ;
- la société identifie correctement les bénéficiaires effectifs des clients ;

- la société identifie correctement le statut PEP des clients ;
- l'entreprise identifie correctement l'objet et la nature de la relation d'affaires ou de la transaction ;
- la société surveille correctement les relations commerciales avec les clients.

Lors de l'application des mesures de CED à l'égard des personnes physiques ou morales résidant ou établies dans des pays tiers à haut risque déterminés par la Commission européenne, l'entreprise doit :

- obtenir des informations complémentaires sur le client et le BO ;
- obtenir des informations supplémentaires sur la nature envisagée de la relation d'affaires ;
- obtenir des informations sur l'origine des fonds et le patrimoine du client et de BO ;
- obtenir des informations sur les raisons des transactions envisagées ou réalisées ;
- obtenir l'approbation du directeur général pour établir des relations d'affaires avec ces clients ou consentir à poursuivre les relations d'affaires avec ces clients
- réaliser l'EDD en augmentant le nombre et le calendrier des contrôles et en sélectionnant les types de transactions qui devront faire l'objet d'un examen plus approfondi ;
- veiller à ce que le premier paiement d'un client soit effectué à partir d'un compte détenu auprès d'un établissement de crédit lorsque celui-ci est établi dans un État membre de l'UE ou dans un pays tiers appliquant des exigences équivalentes à celles de la loi et placé sous la surveillance des autorités compétentes.

Actuellement, les pays tiers à haut risque déterminés par la Commission européenne sont listés dans le règlement délégué de la Commission n° 2016/1675 du 14 juillet 2016 complétant la directive (UE) 2015/849 du Parlement européen et du Conseil en identifiant les pays tiers à haut risque présentant des insuffisances stratégiques et modifié par les règlements suivants :

Règlement délégué n° 2018/105 de la Commission du 27 octobre 2017 modifiant le règlement délégué (UE) 2016/1675, en ce qui concerne l'ajout de l'Éthiopie à la liste des pays tiers à haut risque figurant dans le tableau du point I de l'annexe ;

Règlement délégué n° 2018/212 de la Commission du 13 décembre 2017 modifiant le règlement délégué (UE) 2016/1675 complétant la directive (UE) 2015/849 du Parlement européen et du Conseil, en ce qui concerne l'ajout du Sri Lanka, de Trinité-et-Tobago et de la Tunisie au tableau figurant au point I de l'annexe ;

Règlement délégué n° 2018/1467 de la Commission du 27 juillet 2018 modifiant le règlement délégué (UE) 2016/1675 complétant la directive (UE) 2015/849 du Parlement européen et du Conseil, en ce qui concerne l'ajout du Pakistan au tableau figurant au point I de l'annexe.

Sur la base des résultats de l'évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme, si un niveau élevé de risques de blanchiment de capitaux et de financement du terrorisme en République de Lituanie est identifié en relation avec les pays tiers à haut risque déterminés par la Commission européenne, l'entreprise, lorsqu'elle noue ou entretient des relations de correspondant international avec des institutions financières établies dans ces pays, doit prendre une ou plusieurs mesures supplémentaires pour réduire efficacement le risque de blanchiment de capitaux et de financement du terrorisme :

- appliquer des mesures supplémentaires de suivi renforcé des relations d'affaires afin de réduire le risque de blanchiment d'argent et de financement du terrorisme ;
- rendre plus stricte la déclaration des opérations et transactions monétaires suspectes ;
- limiter les relations d'affaires ou les transactions avec des personnes physiques ou morales établies dans des pays tiers à haut risque identifiés par la Commission européenne.

Si ces mesures supplémentaires ne suffisent pas à réduire ce risque, l'entreprise doit refuser de s'engager dans une relation de correspondant international avec ces institutions financières, cesser de le faire ou mettre fin à cette relation.

Actuellement, les pays tiers à haut risque figurant sur les listes du GAFI des États présentant de graves lacunes dans le domaine de la prévention du blanchiment de capitaux et du financement du terrorisme et de la lutte contre ces délits peuvent être consultés à l'adresse suivante : http://www.fatf-gafi.org/countries/#high-risk. Toutefois, étant donné que la liste change régulièrement, l'entreprise doit s'assurer que la liste n'a pas été modifiée et prendre les mesures qui s'imposent si nécessaire.

Lorsqu'elle applique les mesures de détection et de réduction des risques à l'égard des personnes physiques ou morales résidant ou établies dans des pays tiers à haut risque figurant sur les listes du GAFI des États présentant de graves lacunes en matière de prévention du blanchiment de capitaux et du financement du terrorisme et de lutte contre ces délits, l'entreprise doit :

- recevoir l'approbation du Senior Manager pour conclure une relation d'affaires avec ces clients ou pour poursuivre une relation d'affaires avec ces clients ;
- prendre les mesures appropriées pour établir l'origine des richesses et des fonds liés à la relation d'affaires ou à la transaction ;
- effectuer un contrôle continu renforcé de la relation d'affaires avec ces clients.

Pour déterminer quels clients présentent des risques élevés de blanchiment de capitaux et de financement du terrorisme, l'entreprise doit procéder à une évaluation des risques liés aux relations d'affaires. En tenant compte des résultats de l'évaluation des risques de l'entreprise, de l'évaluation des risques nationaux et de l'évaluation des risques supranationaux, l'entreprise doit être particulièrement attentive lorsqu'elle évalue les risques de blanchiment de capitaux et de financement du terrorisme potentiellement posés par les personnes et entités suivantes :

- les négociants en marchandises qui, dans le cadre de leur activité, effectuent ou reçoivent normalement des paiements en espèces d'un montant significatif ;
- les entités opérant dans les sous-secteurs financiers ou les produits qui traitent des espèces (par exemple, les bureaux de change, les transferts de fonds, certains produits de monnaie électronique) ;
- certaines entreprises FinTech (c'est-à-dire des services financiers basés sur la technologie et soutenus par la technologie), en particulier avec un nombre élevé de Relations d'affaires non face à face ;
- les opérateurs de plateformes d'échange de monnaies virtuelles et/ou les fournisseurs de portefeuilles de dépôt ;
- Autres entités obligées, en particulier les fournisseurs de services de câblage et/ou de loteries et d'appareils de jeux de hasard ;
- les organisations à but non lucratif ;
- d'autres.

En outre, lors de l'évaluation des risques de blanchiment d'argent et de financement du terrorisme potentiellement posés par les clients, l'entreprise doit accorder une attention particulière aux éléments suivants :

- les Clients pour lesquels une DOD a été précédemment soumise ;
- les clients qui ont été inclus dans le passé dans les listes de sanctions financières internationales ou nationales et autres ;
- les clients qui font l'objet d'une demande ou d'une information reçue de la CRF, d'autres autorités chargées des enquêtes préliminaires, du bureau du procureur ou d'un tribunal concernant des informations sur un client ou ses opérations ou transactions monétaires susceptibles d'être liées à des activités de blanchiment d'argent et de financement du terrorisme ou à d'autres activités criminelles.

Pour déterminer l'existence d'un risque accru de blanchiment de capitaux et de financement du terrorisme, l'entreprise doit au moins évaluer les facteurs suivants :

- caractéristiques du client :
- la relation d'affaires du client est menée dans des circonstances inhabituelles qui n'ont pas de but économique apparent ou de but licite visible ;
- le domicile du client se trouve dans un pays tiers ;
- les personnes morales et les organismes sans personnalité juridique exercent des activités d'entreprise individuelle de gestion immobilière ;
- la société a des actionnaires formels agissant pour le compte d'une autre personne ou détient des actions au porteur ;
- l'argent liquide est dominant dans l'entreprise ;
- la structure des capitaux propres de l'entité juridique est apparemment inhabituelle ou excessivement complexe compte tenu de la nature des activités de l'entité juridique,
- les caractéristiques du produit, du service, de la transaction ou du canal de service :
- la banque privée ;
- peut créer des conditions favorables à l'anonymat ;

- Les relations d'affaires ou les transactions occasionnelles sont conclues ou exécutées sans présence physique ;

- des paiements sont reçus de tiers inconnus ou non liés ;

- le produit ou la pratique commerciale, y compris le mécanisme de prestation de services, sont nouveaux, de même que l'utilisation de technologies nouvelles ou en cours de développement impliquées dans le travail avec des produits nouveaux et anciens,

- les caractéristiques du territoire ;

- selon les données des rapports ou documents similaires du GAFI ou d'une autre organisation régionale similaire, des non-conformités significatives sont constatées dans le système de lutte contre le blanchiment de capitaux et le financement du terrorisme par rapport aux exigences internationales ;

- selon les données des organisations gouvernementales et non gouvernementales mondialement reconnues qui surveillent et évaluent le niveau de corruption, un niveau élevé de

la corruption ou d'autres activités criminelles sont établies dans l'État ;

- l'État fait l'objet de sanctions, d'un embargo ou de mesures similaires imposées, par exemple, par l'UE ou les Nations unies ;
- l'État finance ou soutient des activités terroristes, ou des organisations terroristes figurant sur les listes établies par les organisations internationales opèrent sur le territoire de l'État.

Mise en œuvre des sanctions

L'objectif de la mise en œuvre des mesures de contrôle interne pour la conformité de la société avec la mise en œuvre des sanctions est un examen des circonstances suivantes :

- la société applique la procédure d'identification d'une personne faisant l'objet de sanctions ou d'une transaction violant des sanctions ;
- la société prend des mesures si elle identifie une personne faisant l'objet de sanctions ou une transaction violant des sanctions.

Obligation de refuser une transaction ou une relation d'affaires et de la rompre

L'objectif de la mise en œuvre des mesures de contrôle interne pour le respect par la société de l'obligation de refuser une transaction ou une relation d'affaires et de mettre fin à celle-ci est l'examen des circonstances suivantes :

- l'entreprise refuse une transaction ou une relation d'affaires si elle est obligatoire en vertu des lignes directrices ;
- l'entreprise refuse ou met fin à une transaction ou à une relation d'affaires si cela est obligatoire conformément aux lignes directrices.

Obligation de déclaration

L'objectif de la mise en œuvre des mesures de contrôle interne visant à assurer la conformité de la société avec l'obligation de déclaration est l'examen des circonstances suivantes :

- l'entreprise envoie des rapports et des informations au FCIS, si les lignes directrices l'exigent (y compris les lignes directrices pertinentes du FCIS) ;
- les rapports envoyés au FCIS sont remplis conformément aux lignes directrices du FCIS.

Obligation de formation

L'objectif de la mise en œuvre des mesures de contrôle interne pour la conformité de la société avec l'obligation de formation dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme est un examen des circonstances suivantes :

- tous les employés (y compris le MLRO et les membres du conseil d'administration) ont reçu une formation appropriée ;
- chaque employé (y compris le MLRO et les membres du conseil d'administration) a suivi une formation au cours des 360 derniers jours.

Obligation de collecte et de conservation des données

L'objectif de la mise en œuvre des mesures de contrôle interne pour le respect par la société de l'obligation de collecte et de conservation des données est l'examen des circonstances suivantes :

- toutes les données qui doivent être sauvegardées conformément aux lignes directrices (ci-après dans ce chapitre - les données sauvegardées) ont été correctement sauvegardées dans l'ordre chronologique avec un format qui permet de les analyser et de les relier de manière compréhensible à d'autres données pertinentes ;
- seuls les employés (y compris le MLRO et les membres du conseil d'administration) ou des tiers autorisés ont accès aux données sauvegardées ;
- tous les journaux de bord pertinents sont conservés conformément aux lignes directrices ;
- les données sauvegardées sous forme électronique ont été sauvegardées ;
- les données sauvegardées dans d'autres formats (par exemple sur papier) sont sauvegardées sous forme électronique ;
- les données sauvegardées sont irrévocablement effacées conformément aux lignes directrices.

ANNEXES

Titre de l'annexe	Description du document
Politique d'évaluation des risques	Établit les principes de la gestion des risques de l'entreprise (y compris l'évaluation des risques et les facteurs de risque) en ce qui concerne le blanchiment d'argent et le financement du terrorisme. Risques liés au financement du terrorisme.
Profils des clients	Tableau pour l'évaluation des risques des clients et la documentation de cette évaluation. Inclut les facteurs de risque de chaque catégorie de risque.
Procédure d'accueil du client	Définit les instructions pour l'intégration du client utilisées dans le cadre de la mise en œuvre des mesures de vigilance à l'égard de la clientèle
Questionnaires	La quantité d'informations demandées lors de l'exécution des mesures CDD (y compris l'application des mesures EDD, la demande de SoW/SoF, etc.)
Liste des sources	Contient une liste non exhaustive de ressources pouvant être utilisées pour la mise en œuvre de mesures CDD.
Liste des critères de blanchiment de capitaux et d'identification des opérations ou transactions financières suspectes	Instructions et exemples de transactions et d'autres circonstances qui doivent être considérées comme suspectes du point de vue de la lutte contre le blanchiment d'argent et le financement du terrorisme.
La liste des employés et leurs responsabilités	La liste des employés avec leurs responsabilités dans le cadre des lignes directrices spécifiées
Carnets de bord	Le tableau est utilisé pour la tenue des journaux de bord.
Formulaire de rapport du MLRO	Le formulaire de rapport, que le MLRO doit fournir trimestriellement au conseil d'administration.
Lignes directrices pour remplir les formulaires de transmission d'informations au FCIS	Les lignes directrices du FCIS pour remplir les formulaires pertinents et les formulaires eux-mêmes.

Suspension des opérations ou transactions monétaires suspectes et transmission au FCIS d'informations sur les opérations ou transactions monétaires suspectes	Les lignes directrices FCIS pertinentes.
Exigences techniques pour l'identification du client par transmission vidéo en direct	Lignes directrices de la FCIS sur les exigences techniques pertinentes
Protocole de formation	Projet de document à remplir pour chaque formation dispensée par l'entreprise aux personnes concernées (y compris la familiarisation avec les lignes directrices).
Résolution d'approbation des lignes directrices	Le projet de résolution des cadres supérieurs de l'entreprise pour l'approbation des présentes lignes directrices.

TABLEAU DE CONTRÔLE DES VERSIONS

Version	Date d'approbation	Changements Description
1.0	jj.mm.aaaa	Première édition
1.1	28.03.2023	Version actualisée
1.2	11.07.2023	Version actualisée
2.0	07.08.2023	Deuxième numéro
2.1	06.12.2023	Version actualisée
2.2	18.03.2024	Version actualisée

Mariana Achim
18.03.2024