

1. Général

1.1 Déclaration de Politique

Il est de la politique de Games & More BV que tous les membres du personnel participent activement à la prévention de l'exploitation des services de Games & More BV par les criminels et les terroristes à des fins de blanchiment d'argent ou à financer une activité terroriste par des gains obtenus par des paris sur le site web de la société. Cette participation a pour objectifs :

assurer la conformité de Games & More BV avec toutes les lois applicables, les instruments statutaires de régulation, et les exigences de l'organisme de contrôle pertinent

protéger la société et tout son personnel en tant qu'individus contre les risques associés aux violations de la loi, des réglementations et des exigences de contrôle

préserver la bonne réputation de Games & More BV contre le risque de dommages à la réputation présentés par l'implication dans les activités de blanchiment d'argent et de financement du terrorisme

contribuer positivement à la lutte contre le crime et le terrorisme Pour atteindre ces objectifs, il est de la politique de Games & More BV d'adopter et de maintenir des systèmes et des contrôles efficaces en matière de blanchiment d'argent et de financement du terrorisme, qui sont proportionnés aux risques identifiés dans l'évaluation des risques de la société. Ces systèmes et contrôles sont conçus pour être conformes à la législation en vigueur et aux exigences réglementaires, et ils sont revus régulièrement pour s'assurer qu'ils restent efficaces et proportionnés aux risques auxquels la société est exposée.

chaque membre du personnel doit respecter ses obligations personnelles selon son rôle et sa position au sein de l'entreprise

les considérations commerciales ne seront jamais autorisées à prendre le pas sur les engagements de Games & More BV en matière de lutte contre le blanchiment d'argent

la société nommera un responsable du signalement du blanchiment d'argent (MLRO) et un employé désigné pour assurer la continuité en son absence, et ils recevront toute l'aide et la coopération nécessaires de la part de tous les membres du personnel pour accomplir les tâches de leurs nominations. Toute référence au MLRO dans ce document inclura celle de l'employé désigné si le MLRO est temporairement absent.

1.2 Définition

Games & More BV estime qu'avant de mettre en œuvre sa Procédure de Gestion de la Fraude, il est essentiel d'identifier d'une part ce qu'est le blanchiment d'argent, et d'autre part ce qui constitue le financement du terrorisme.

Le blanchiment d'argent est le mouvement ou la dissimulation de produits criminels dans le but d'obscurcir le lien entre le crime et les fonds générés, afin de pouvoir bénéficier des profits du crime. L'objectif ultime est donc de dissimuler l'origine des fonds.

Le financement du terrorisme est le processus de mise à disposition de fonds ou d'autres actifs, directement ou indirectement, à des groupes terroristes ou à des terroristes individuels pour soutenir leurs opérations. Cela peut se faire par le biais de fonds provenant de sources légitimes ou d'une combinaison de sources légales et illégales. En effet, le financement provenant de sources légales est une différence clé entre les organisations terroristes et les organisations criminelles traditionnelles impliquées dans les opérations de blanchiment d'argent. Bien qu'il puisse sembler logique que le financement provenant de sources légitimes n'ait pas besoin d'être blanchi, il y a néanmoins souvent un besoin pour les terroristes d'obscurcir ou de déguiser les liens entre l'organisation ou le terroriste individuel et ses sources de financement légitimes. Par conséquent, le financement du terrorisme est principalement préoccupé par l'obscurcissement du bénéficiaire final des fonds.

Dans certains cas où une STR ou une SAR doit être soumise, la communication doit être réduite au minimum en raison de mandats légaux. De tels cas impliquant des tiers peuvent parfois prendre beaucoup plus de temps que d'habitude et nous n'avons pas de vision ou la capacité d'accélérer de tels procédures. Parfois, des examens de gestion ou juridiques sont également nécessaires, ce qui augmente les délais de résolution.

2. L'Approche Basée sur le Risque

2.1 Définition

Conformément aux lois applicables, Games & More BV adopte une approche basée sur le risque. Il identifie et analyse donc ses risques et utilise ensuite des mesures, des politiques, des contrôles et des procédures pour contrer tout risque indésirable, y compris ceux liés à la réalisation des risques de blanchiment d'argent et de financement du terrorisme. L'approche permet une certaine flexibilité et un pouvoir discrétionnaire significatif à exercer par Games & More BV. Il appartient à Games & More BV de montrer, par une documentation adéquate, y compris mais sans s'y limiter, un processus d'analyse des risques, qu'il a évalué tous les risques et mis en place de manière adéquate des mesures pour contrôler ces risques. À cet égard, cette politique décrit les étapes spécifiques que Games & More BV adoptera afin de garantir que sa conduite est conforme à l'Approche Basée sur le Risque en ce qui concerne la prise en compte et l'identification de ces risques qui touchent directement au blanchiment d'argent et au financement du terrorisme.

2.2 Évaluation des Risques

La gestion des risques comprend :

- i) reconnaissance de l'existence du risque
- ii) réalisation d'une évaluation des risques, et
- iii) mise en place de systèmes et de stratégies pour gérer et contrôler les risques identifiés.

Il ne fait aucun doute que le secteur des jeux à distance est considéré comme risqué. L'évaluation des risques identifiera cependant les principaux risques auxquels la société est confrontée ainsi que le niveau de ces risques, de sorte que, par conséquent, les mesures nécessaires soient adoptées pour gérer et contrôler les risques identifiés. Cette procédure précisera les contrôles et les processus à suivre afin de garantir que les risques que Games & More BV a identifiés et auxquels il sera confronté dans le cadre de ses opérations ne se concrétiseront pas. L'évaluation des risques organisationnels de Games & More BV, qui doit être approuvée par le conseil d'administration, prend en compte les facteurs suivants :

i. Risque Produit/Service/Transaction

Certains produits/services/transactions de jeu sont plus vulnérables à l'exploitation criminelle que d'autres. Cela inclut, par exemple, les produits ou services de jeu qui permettent au client d'influencer le résultat d'un jeu, que ce soit seul ou en collusion avec d'autres.

ii. Risque d'Interface

Cela fait référence au canal par lequel Games & More BV établit une relation d'affaires et/ou par lequel les transactions sont effectuées. Les interactions non en face à face, telles que celles concernant l'interface commerciale de Games & More BV, ne sont plus automatiquement considérées comme à haut risque, tant que des mesures et contrôles technologiques pour contrer le risque accru de fraude à l'identité ou d'usurpation d'identité sont adoptés. Games & More BV veillera à adopter un bon mélange de méthodes de vérification basées à la fois sur des sources documentaires et électroniques comme mentionné ci-dessous, afin de contrer les risques mentionnés. Par exemple, bien que Games & More BV utilise des bases de données électroniques, il est bien conscient que les bases de données ne confirment que les détails d'identification fournis correspondent à ceux d'une personne réelle, et non que le client est réellement cette personne. La fourniture de documents d'identification supplémentaires fournira une preuve supplémentaire que Games & More BV était justifié de considérer que le client est réellement la personne qu'il prétend être.

iii. Risque Géographique

Il s'agit du risque posé à Games & More BV par l'emplacement géographique des clients, mais aussi par les emplacements géographiques de ses fournisseurs et prestataires de services. L'élément à prendre en compte dans le cadre de cette procédure de gestion de la fraude est principalement celui attribuable aux clients et à l'origine des fonds desdits clients. La nationalité, la résidence et le lieu de naissance d'un client doivent être pris en compte, car ils peuvent indiquer un risque géographique accru. Les pays ayant un système faible de lutte contre le blanchiment d'argent et le financement du terrorisme, les pays connus pour souffrir d'un niveau significatif de corruption, et les pays soumis à des sanctions internationales en relation avec le terrorisme ou la prolifération des armes de destruction massive seront considérés comme à haut risque. Le contraire est également vrai et peut donc être considéré comme présentant un risque moyen ou faible.

Les évaluations des risques sont des 'travaux en cours'. Ces évaluations doivent être constamment réévaluées à mesure que de nouveaux risques émergent. Des risques

peuvent surgir en raison de changements technologiques, qui peuvent rendre le blanchiment d'argent ou les tentatives de financement du terrorisme plus faciles à réaliser. D'autres changements incluent l'élargissement de la clientèle ou l'ajout de jeux et de méthodes de paiement présentant un profil de risque différent de ceux déjà offerts, ce qui nécessitera une révision de l'évaluation des risques de l'entreprise. En l'absence de tels changements, Games & More BV réévaluera son évaluation des risques commerciaux au moins une fois par an, afin d'évaluer si des modifications y sont nécessaires. Pour déterminer le niveau de risque posé par un client, l'accumulation de tous les indicateurs pertinents sera prise en compte. Ceux-ci, ensemble, déterminent le profil de risque du joueur contribuant à la totalité du profil de risque d'un joueur.

iv. Risque Client

Cela concerne le type de client à qui le service est fourni. L'évaluation du risque posé par une personne physique est généralement basée sur l'activité économique de la personne et/ou la source de sa richesse. En identifiant le niveau de risque inhérent à une relation, Games & More BV évaluera quelle serait la probabilité qu'un client puisse blanchir les produits du crime via le service de Games & More BV. Un client à haut revenu qui parie un quart de son salaire mensuel n'est probablement pas un risque élevé, même si le montant misé est important. En revanche, une personne au salaire minimum qui dépense son seul salaire en paris sera plus probablement un risque élevé. De plus, l'individu sera examiné afin de déterminer s'il est une personne politiquement exposée (PEP), ou associée d'une manière ou d'une autre à une PEP. Des vérifications seront également effectuées pour s'assurer que l'individu n'est pas soumis à des sanctions ou à d'autres mesures légales.

3. Diligence Due envers le Client (CDD)

3.1 Procédure

La Procédure de Gestion de la Fraude se concentrera maintenant sur la connaissance des clients et l'identification des risques liés à leurs transactions et à l'origine de leurs fonds, tant en ce qui concerne l'endroit où les fonds ont été obtenus qu'à la source des fonds d'où le client a envoyé les fonds.

Comme décrit ci-dessus, une évaluation des risques ne peut jamais être un exercice universel. Games & More BV effectuera à cet égard une évaluation des risques lors de la conclusion d'une relation d'affaires avec un client ou de la réalisation d'une transaction occasionnelle pour un client. Pour plus de clarté, Games & More BV n'acceptera que des joueurs individuels, pas des joueurs corporatifs. L'évaluation des risques mentionnée permettra à Games & More BV de développer un profil de risque concernant le client et de catégoriser le risque comme faible, moyen ou élevé, lui permettant ainsi d'identifier les contrôles à adopter. Le profil de risque du joueur ne sera pas terminé lors de l'inscription. La partie inscription du processus ne signifiera que le début de la collecte d'informations, et le profil de risque sera donc augmenté et affiné avec le développement de la relation avec le joueur. Cela étant dit, s'il y a un changement dans la relation d'affaires entretenue avec le client, ce qui entraîne donc un changement dans le risque identifié, les mesures adoptées pour contrôler le risque seront adaptées en conséquence. De plus, la surveillance continue, telle qu'expliquée plus en détail ci-dessous, garantira que tout changement de risque soit

déecté dès que possible. Le niveau de surveillance sera proportionné au risque posé par le client particulier, mais des systèmes seront mis en place pour détecter les situations risquées en développement.

Pour commencer, Games & More BV adopte des mesures CDD afin de déterminer qui sont ses clients. Tous les détails collectés à l'étape de l'inscription sont utilisés pour créer le profil du client. Un profilage supplémentaire est effectué, en fonction de l'activité du client et également des aspects comportementaux particuliers. Cet aspect du profilage aidera à déterminer le risque associé au joueur particulier et facilitera également l'identification d'un comportement inhabituel futur. La CDD est divisée en trois parties ci-dessous :

A. Identification et Vérification du Client

L'identification consiste à recueillir les détails personnels du joueur. Ces informations sont recueillies pendant le processus d'inscription. Les informations personnelles à recueillir pour commencer la procédure Connaître Votre Client (KYC) comprennent la collecte des détails personnels suivants :

a. Nom et prénom

b. Adresse résidentielle permanente

c. Date de naissance, car le joueur doit avoir plus de dix-huit ans (ou tout autre âge applicable dans la juridiction particulière du joueur)

d. Adresse e-mail valide

e. Lieu de naissance

f. Nationalité, et

g. Numéro de référence d'identité, le cas échéant.

Une fois que les informations ci-dessus sont fournies, Games & More BV vérifiera d'abord si l'individu en question est une Personne Politiquement Exposée (PEP), un membre de la famille du PEP, ou un associé professionnel proche du PEP. Une base de données électronique fiable, telle que [opensanctions.org](https://www.opensanctions.org) et [complyadvantage.com](https://www.complyadvantage.com) sera intégrée et utilisée à cet égard. S'il est déterminé qu'un individu est un PEP ou en relation avec un PEP d'une manière ou d'une autre, alors l'individu sera considéré lui-même comme un PEP et ne sera pas autorisé à s'inscrire en tant que joueur avec Games & More BV, car ce dernier a une politique stricte de non-acceptation des PEP en tant que joueurs. Cela signifie donc que la détermination de savoir si un individu est un PEP (selon la définition ci-dessus) aura lieu lors de l'étape d'inscription.

Le compte sera officiellement ouvert une fois que l'e-mail du joueur aura été vérifié. Dans toute situation où le joueur est immédiatement identifié comme étant à haut risque, Games & More BV peut immédiatement demander des détails personnels supplémentaires et vérifier les mêmes détails fournis. Dans tous les cas, Games & More BV veillera à tout moment à

pouvoir déterminer que le client est bien celui qu'il prétend être et que les mesures adoptées sont suffisamment efficaces pour contrer le risque de fraude d'identité et d'usurpation d'identité.

La vérification consiste à confirmer les détails personnels recueillis aux fins d'identification à l'aide de données, d'informations et de documentation indépendantes obtenues auprès de sources fiables. Si des incohérences dans les informations personnelles fournies par le client sont identifiées, Games & More BV envisagera d'adopter des mesures d'identification et de vérification supplémentaires.

Cela se fera de l'une des deux manières suivantes : i. Sources Documentaires,

En règle générale, cette méthode de vérification sera effectuée en se référant à des documents délivrés par le gouvernement contenant une image photographique avec l'identité du joueur (par exemple, passeport, carte d'identité, permis de conduire, etc.). Si l'adresse résidentielle du joueur ne peut être vérifiée à l'aide de l'un des documents mentionnés ci-dessus, Games & More BV demandera des documents alternatifs fiables tels qu'une facture de services publics récente, des relevés de compte bancaire, la correspondance de l'État ou d'entités publiques, etc., afin de pouvoir vérifier l'adresse. Les documents demandés seront reçus par courrier électronique et, si nécessaire, des documents notariés pourront être demandés.

Games & More BV s'assurera que tous les documents reçus sont clairs, lisibles, de bonne qualité et authentiques ou reflètent des documents authentiques. Certains documents, tels que les passeports, peuvent être plus faciles à vérifier, car ils peuvent être vérifiés par rapport à d'autres sources. Dans d'autres cas, comme pour les factures de services publics, le processus de vérification peut être moins facile. Games & More BV effectuera des vérifications supplémentaires en utilisant des programmes logiciels/applications spécifiques; qui seront intégrés en tant que solution pour aider les utilisateurs dans leur travail.

En ce qui concerne la validité des informations fournies, Games & More BV tiendra également compte d'autres données collectées auprès du joueur telles que la géolocalisation, les données d'adresse IP, etc. qui, dans des circonstances normales, devraient corroborer les données contenues dans les documents fournis par le joueur. Il y aura des exceptions, où l'adresse IP ne correspondra pas au pays / emplacement. De telles instances devront être vérifiées au cas par cas et une vérification / clarification sera obtenue directement auprès du joueur.

ii. Moyens Électroniques

Ceux-ci comprennent des sources comme E-ID ou Bank-ID et des bases de données commerciales électroniques. Games & More BV est bien conscient que la fiabilité de ces bases de données peut ne pas être toujours la meilleure. À cet égard, il considérera quelle source d'information alimente la base de données et si ces données sont généralement connues pour être maintenues à jour. Lors de l'utilisation des bases de données électroniques mentionnées, Games & More BV utilisera également d'autres preuves documentaires pour une meilleure confirmation/fiabilité. C'est parce qu'un résultat positif sur la base de données électronique signifiera seulement qu'il existe un individu dont les détails

personnels correspondent à ceux fournis par le client, mais pas que le client est cet individu. D'autre part, lors de l'utilisation de sources électroniques comme E-ID et Bank-ID, qui ne peuvent être accessibles qu'avec les références détenues par un individu spécifique, aucun moyen de vérification supplémentaire ne sera demandé, car ces sources sont considérées comme fournissant un lien suffisamment solide.

B. Obtention d'informations sur l'objet et la nature prévue de la relation d'affaires

L'objectif derrière l'ouverture d'un compte de jeu est assez évident et donc aucune clarification sur la raison de la demande d'ouverture de compte ne sera recherchée. Cependant, il peut y avoir un motif caché sur la base duquel le compte a été ouvert, peut-être même pour le blanchiment d'argent ou le financement du terrorisme. Si Games & More BV a des soupçons qu'un tel motif caché subsiste, alors il mènera une enquête plus approfondie et demandera des données et des documents supplémentaires pour justifier ses soupçons ou confirmer qu'il n'y a effectivement aucune indication justifiable d'un motif illégal.

Il n'y a pas de délai ou de période spécifique pour mener ces vérifications supplémentaires, car elles seront simplement effectuées lorsque le soupçon survient. Par conséquent, l'enquête peut avoir besoin d'être menée dès l'inscription, alors que dans d'autres cas, elle ne sera pas nécessaire avant que les seuils obligatoires AML ne soient atteints.

C. Surveillance Continue

Une fois qu'un compte de joueur est ouvert, la relation avec le joueur ne s'arrête pas là. La surveillance continue sera mise en place pour assurer que les transactions qui sont effectuées sont conformes à ce que Games & More BV s'attend de ce client. Cela comprend la vérification que les transactions correspondent à la norme de jeu attendue de ce joueur, tant en termes de montant que de fréquence. Games & More BV utilisera des outils et des systèmes de surveillance automatisés pour faciliter la mise en œuvre de la surveillance continue, qui seront intégrés dans son système de jeu pour déterminer tout comportement suspect ou inhabituel dans la relation d'affaires avec le joueur.

En résumé, la CDD comprendra l'identification et la vérification du client, l'obtention d'informations sur l'objet et la nature prévue de la relation d'affaires, et la surveillance continue de la relation d'affaires.

Une surveillance continue adéquate implique également d'examiner attentivement les transactions et les habitudes de jeu du joueur afin de s'assurer qu'elles sont conformes à la connaissance de Games & More BV du joueur, de son activité de jeu et de son profil de risque. Si les deux ne coïncident pas, Games & More BV remettra également en question la situation. Chaque fois que Games & More BV demande des informations supplémentaires, il prendra toujours note de ses conclusions afin de prouver sa conformité. Si une incohérence identifiée persiste sans être résolue avec succès, Games & More BV analysera si un rapport doit être soumis aux autorités compétentes et prendra également une décision s'il juge nécessaire de suspendre le compte du joueur.

Enfin, en ce qui concerne les PEP, un scénario peut survenir où un joueur n'a pas été considéré comme un PEP lors de l'étape d'inscription, mais le devient au cours de la relation d'affaires. Si, lors de la surveillance continue, Games & More BV prend conscience d'un tel changement, Games & More BV mettra fin à sa relation d'affaires car il a une politique stricte de non-acceptation des PEP en tant que joueurs. Si c'est le cas que pour une raison ou une autre, l'individu n'avait pas été identifié comme PEP même s'il était un PEP lors de l'étape d'inscription, mais est par la suite identifié comme tel, Games & More BV annulera tous les gains obtenus par l'individu, et transférera ensuite les fonds déposés, à la source originale d'où proviennent les fonds. Il fermera ensuite le compte du joueur, selon la procédure décrite à la section 3.3 ci-dessous.

3.2 Calendrier et application des mesures de CDD

Comme décrit plus haut, le compte du joueur sera ouvert avec succès une fois que le joueur se sera inscrit en fournissant les informations personnelles de base demandées. Le système est configuré pour empêcher les mineurs de s'inscrire en rejetant toute date de naissance insérée qui signifierait que le joueur a moins de dix-huit ans (ou tout autre âge selon la législation spécifique - comme la Lettonie - 21 ans).

La vérification des détails du joueur (à l'exception des confirmations de PEP) peut avoir lieu à tout moment à la discrétion de Games & More BV. Cependant, au moins, elle doit être effectuée lorsque le montant déposé par les joueurs atteint la valeur cumulée de 1 000 €. Peu importe que ces dépôts aient été effectués via une seule opération ou plusieurs opérations qui semblent être liées ou non. Games & More BV mettra donc en place un système qui calcule quotidiennement si le joueur a atteint la limite de dépôt de 1 000 € sur son compte. Un autre facteur important que le système inclura est l'identification de comptes multiples possibles, ces comptes ayant été spécifiquement créés pour escroquer l'entreprise par des abus de bonus ou spécifiquement pour ne jamais atteindre la limite de dépôt requise de 1 000 €, et donc assurer que le compte reste non vérifié.

Jusqu'à ce que ce seuil soit atteint, Games & More BV effectuera une surveillance continue conformément au point C de la section 3.1 ci-dessus, afin de s'assurer que les informations du joueur sont toujours correctes. De plus, si Games & More BV remarque à tout moment des incohérences entre les informations fournies par le joueur et toute autre information qu'il acquiert, Games & More BV remettra en question les divergences et prendra toute mesure corrective qu'il jugera nécessaire. En outre, s'il soupçonne un blanchiment d'argent ou un financement du terrorisme, il suivra la procédure décrite à la section 4 ci-dessous.

Une fois le seuil mentionné atteint, le profil de risque du joueur sera confirmé, sur la base de l'évaluation des risques effectuée conformément à la section 2.2 ci-dessus. Ce dernier aura lieu avant l'expiration de trente jours à compter du moment où le seuil de 1 000 € est atteint. L'évaluation des risques déterminera si le risque posé par l'individu est faible, moyen ou élevé. Les mesures adoptées pour contrôler le risque en question varient, selon le tableau ci-dessous:

Risque identifié Mesures adoptées

Faible

Vérification des détails personnels

La surveillance continue est effectuée pour s'assurer que la relation reste à faible risque et que le seuil n'est pas dépassé à nouveau

Tout cas suspecté de blanchiment d'argent ou de financement du terrorisme doit être signalé

Des détails personnels supplémentaires jugés nécessaires par Games & More BV sont recueillis

La vérification des détails personnels a lieu en utilisant des documents contenant des photographies de l'individu

Moyen

Les informations sur la source de richesse sont recueillies

La surveillance continue est effectuée afin de pouvoir détecter des activités inhabituelles et de maintenir les informations et le profil à jour

Tout cas suspecté de blanchiment d'argent ou de financement du terrorisme doit être signalé

Des détails personnels supplémentaires jugés nécessaires par Games & More BV sont recueillis

La vérification des détails personnels a lieu en utilisant des documents contenant des photographies de l'individu

Élevé

Les informations sur la source de richesse sont recueillies

La surveillance continue est effectuée afin de pouvoir détecter des activités inhabituelles et de maintenir les informations et le profil à jour

Les sources de fonds peuvent devoir être déterminées pour des transactions spécifiques

Games & More BV permettra aux joueurs de continuer à utiliser leur compte de jeu tant qu'il obtient encore les informations et/ou documents nécessaires auprès du joueur concerné. Cependant, jusqu'à ce que Games & More BV obtienne effectivement les informations et/ou documents mentionnés et vérifie l'identification du joueur, il ne permettra pas au joueur d'effectuer des retraits de son compte, indépendamment du montant impliqué. De plus, si trente jours se sont écoulés depuis que le seuil de 1 000 € a été atteint, et que le joueur n'a pas fourni les informations et/ou documents demandés, Games & More BV peut mettre fin à la relation d'affaires avec le joueur, selon la procédure décrite dans la section suivante.

3.3 Résiliation de la relation commerciale

Games & More BV mettra fin à sa relation commerciale avec un joueur s'il ne fournit pas les informations et/ou documents demandés, que Games & More BV lui a demandés à plusieurs reprises. Games & More BV annulera tous les gains et transférera ensuite les fonds déposés à la source d'origine d'où proviennent les fonds. Toute approbation d'une telle action doit être prise par la direction senior et seulement après avoir vérifié qu'il n'y a aucune restriction sur le transfert des fonds. Si Games & More BV trouve impossible de remettre les fonds au joueur par les mêmes canaux, il les remettra, en dernier recours, à un compte unique détenu par une institution de crédit ou financière dans une juridiction réputée au nom du joueur. Si un tel compte n'est pas disponible, les fonds continueront à être détenus au nom des joueurs. Les fonds continueront à être détenus sur le compte jusqu'à ce que le joueur fournisse les détails adéquats pour le transfert. Si cela ne se produit jamais, après l'écoulement de 30 mois, les fonds restant sur le compte seront remis à l'AUTORITÉ DE JEU DE CURAÇAO. Lors du transfert de ces fonds, Games & More BV indiquera dans les instructions accompagnant les fonds qu'ils sont transférés en raison de l'impossibilité de compléter le CDD. Games & More BV examinera également s'il y a des motifs de déposer un rapport de transaction suspecte (STR), conformément à la procédure énoncée ci-dessous.

3.4 Relations B2B

Games & More BV effectuera également des exercices de diligence raisonnable avant d'entrer dans toute relation commerciale avec des tiers. Ces exercices seront menés par la direction senior conjointement avec le département juridique et le MLRO. Tout comme le CDD, la diligence raisonnable commerciale (BDD) cherchera à identifier quels risques émergeraient si Games & More BV s'engageait dans des affaires avec le tiers. Lors de cette évaluation, il sera déterminé si la source, la nature et le volume des affaires à introduire via le tiers peuvent être établis. Games & More BV accordera également beaucoup d'importance au fait qu'un fournisseur est déjà un fournisseur approuvé selon les exigences de l'AUTORITÉ DE JEU DE CURAÇAO. Il est également considéré comme positif qu'un fournisseur qui n'est pas actuellement approuvé cherche à obtenir l'approbation au moment de contracter avec Games & More BV. L'évaluation cherchera également à établir si le tiers a des relations commerciales avec d'autres tiers qui sont connus pour ne pas être réputés, ou si le tiers mène ses affaires dans ou depuis une juridiction non réputée. À cet égard, Games & More BV demandera au tiers de lui fournir les originaux/certifiés conformes de toute la documentation nécessaire, y compris le certificat de constitution de la société, le mémorandum et les statuts, le certificat de bonne réputation, les états financiers annuels, l'identification des dirigeants de la société ainsi qu'une liste d'actionnaires, et une lettre de référence bancaire, confirmant que les affaires de la société sont traitées de manière satisfaisante. Une fois qu'il a été déterminé que le tiers mène ses affaires de manière à ne pas compromettre la position de Games & More BV, les parties conviendront des conditions de la relation commerciale et signeront les accords et documents pertinents. Dans le cadre de la BDD, Games & More BV effectuera une surveillance continue pour s'assurer que le tiers mène toujours ses affaires de manière diligente, en fonction de leur propre expérience

de la manière dont les services sont fournis. De plus, Games & More BV se réserve également le droit d'inclure une clause de droit d'audit dans l'accord qu'il signe avec le tiers, si cela est jugé nécessaire.

Toute révision de la lutte contre le blanchiment d'argent sera séparément notée dans le dossier du tiers. Dans tous les cas, Games & More BV se réserve toujours le droit de résilier sa relation commerciale avec un tiers si elle estime qu'en faisant affaire avec le tiers, elle met en danger sa conformité avec ses obligations de lutte contre le blanchiment d'argent et le financement du terrorisme. La notification à l'AUTORITÉ DE JEU DE CURAÇAO sera donnée selon l'accord et selon les exigences de la même autorité.

3.5 Confiance et agents

Games & More BV peut décider de se fier aux informations et documents recueillis lors de l'étape d'intégration du client par un tiers, et/ou engager un agent. Dans l'un ou l'autre des cas, Games & More BV s'assurera que le tiers est établi dans un État membre de l'UE ou une juridiction réputée qui adopte les mêmes mesures de lutte contre le blanchiment d'argent ou de lutte contre le financement du terrorisme que celles énoncées dans les lois applicables de Curaçao, ou des mesures équivalentes. Pour déterminer ce dernier, Games & More BV s'appuiera sur des sources réputées telles que les rapports d'évaluation du Groupe d'action financière sur le blanchiment d'argent, les rapports de pays du FMI, etc.

Si Games & More BV décide de se fier aux informations fournies par un tiers, elle peut toujours demander au joueur de lui fournir des documents de vérification. Dans de telles circonstances, Games & More BV effectuera toujours elle-même l'évaluation des risques basée sur le client, déterminera la notation de risque du client et effectuera une surveillance continue. La relation entre Games & More BV et le tiers sera exposée dans un accord, et l'une des conditions sera celle du tiers fournissant à Games & More BV des documents concernant les joueurs, immédiatement sur demande. Games & More BV inclura également une clause de droit d'audit dans l'accord et testera effectivement cet arrangement périodiquement, pour s'assurer que les détails et la documentation personnels nécessaires des joueurs sont collectés selon les spécifications convenues.

Une copie de cette procédure sera également fournie au tiers afin de garantir que les exigences de CDD et les seuils applicables sont correctement communiqués, et ainsi le tiers n'aura jamais l'excuse qu'il n'était pas au courant des exigences de l'entreprise applicables. Games & More BV peut, lorsque la loi le permet, choisir d'utiliser les services d'agents pour intégrer ou servir les clients. Games & More BV peut demander à l'agent d'effectuer les contrôles et mesures nécessaires de lutte contre le blanchiment d'argent/le financement du terrorisme lors de l'intégration ou de la prestation de services à l'un des clients de Games & More BV. Dans tous les cas, cependant, Games & More BV s'assurera que toute application des mesures de CDD est effectuée avec diligence et conformément aux lois applicables. Games & More BV est bien consciente qu'en exerçant la confiance ou en utilisant des agents, elle reste en fin de compte responsable de s'assurer qu'elle respecte ses obligations de lutte contre le blanchiment d'argent/le financement du terrorisme.

4. Déclaration d'activité et de transactions suspectes

4.1 Nomination de l'Officier de déclaration du blanchiment d'argent (MLRO)

Bien que la description détaillée des responsabilités du MLRO soit exposée dans la Politique des rôles et responsabilités des ressources humaines, la principale responsabilité du MLRO sera de prendre en compte tous les rapports internes de transactions inhabituelles ou suspectes qui sont soulevés au sein de l'entreprise, et de donner suite à ces rapports et également de déposer un STR auprès de l'Unité d'analyse du renseignement financier (FIAU), lorsque cela est jugé nécessaire. Le MLRO agira également comme le principal canal par lequel toutes les communications avec la FIAU seront menées. Il veillera à ce que Games & More BV mette en œuvre efficacement les politiques et procédures qu'elle a adoptées pour répondre à ses obligations de lutte contre le blanchiment d'argent/le financement du terrorisme. Le MLRO sera responsable de surveiller toutes les mises à jour sur les sanctions

telles que celles du Groupe d'action financière (FATF) et du Bureau de contrôle des avoirs étrangers (OFAC). Il mettra ensuite le reste du personnel au courant de toutes les modifications apportées aux listes de sanctions et de tout changement fondamental à la loi applicable. Games & More BV veillera à ce que la personne nommée MLRO jouisse d'une ancienneté et d'un commandement suffisants pour pouvoir agir indépendamment de sa direction.

Le MLRO aura accès à toutes les informations/documentation et employés de l'entreprise nécessaires pour exercer efficacement ses obligations. Games & More BV a également nommé un employé désigné qui serait en mesure d'agir en tant que MLRO pendant l'absence du MLRO. Les nominations du MLRO ainsi que de l'employé désigné seront portées à la connaissance de l'AUTORITÉ DE JEU DE CURAÇAO, afin que l'AUTORITÉ DE JEU DE CURAÇAO, ainsi que la FIAU, puissent adresser des questions et des demandes directement à eux, chaque fois que le besoin se fait sentir. Ainsi, ces individus agiront comme point de contact entre Games & More BV et les autorités compétentes en matière de lutte contre le blanchiment d'argent/le financement du terrorisme.

4.2 Signalement des activités et transactions suspectes

Games & More BV peut développer un soupçon ou avoir des motifs raisonnables de suspecter qu'une activité sur un compte est liée au blanchiment d'argent ou au financement du terrorisme. À ce moment-là, Games & More BV veillera à ce que toutes les exigences de CDD soient remplies, indépendamment du fait qu'un seuil applicable ait été atteint. Il soumettra donc un STR dès que possible.

4.2.1 Procédures de déclaration internes

Comme indiqué plus en détail dans la section 6 ci-dessous, tout le personnel communiquant avec les joueurs, ou ayant accès aux informations sur les affaires des clients, recevra une formation en matière de lutte contre le blanchiment d'argent. De cette manière, ils seraient en mesure d'identifier quelle action du joueur devrait raisonnablement les amener à soupçonner qu'une tentative de blanchiment d'argent ou de financement du terrorisme est

en cours ou a été commise. Par exemple, ils devraient s'attendre à ce que si un joueur tente de s'inscrire avec plus d'un compte auprès de Games & More BV, ou s'il dépose des montants considérables au cours d'une seule session au moyen de plusieurs cartes prépayées, alors de telles actions devraient constituer des indicateurs ou des signaux d'alarme qui devraient les amener à questionner le comportement du joueur. À ce stade, l'employé peut subtilement chercher des explications auprès du joueur, sans divulguer son soupçon au joueur. Cette divulgation est interdite, que ce soit directement ou indirectement, et donc tous les membres du personnel doivent être astucieux à cet égard. Si l'officier ne parvient pas à obtenir d'informations convaincantes, et après avoir pleinement réfléchi, l'officier est toujours soupçonneux d'une infraction, alors à ce moment-là, il informera son supérieur immédiat. De toute évidence, avant de signaler à son supérieur, l'employé devra être convaincu qu'il y a une indication claire d'intention de contourner les mesures de sécurité, et que l'utilisation du système financier à des fins criminelles est présente.

Il peut y avoir des cas où le manager n'est pas d'accord avec l'officier, mais l'officier estime toujours qu'il a des motifs raisonnables de soupçonner un acte répréhensible. Dans de telles circonstances, l'employé doit de toute façon informer le MLRO de ses soupçons. L'employé peut discuter de la question directement avec le MLRO et n'est en aucun cas obligé d'informer ou d'impliquer son manager. À réception du rapport interne de l'employé, le MLRO en accusera réception par écrit, en se référant au rapport par sa date et son numéro de fichier unique, sans inclure le nom de la ou des personnes suspectées. De cette manière, l'obligation légale de l'officier de signaler sera considérée comme ayant été remplie. L'employé ne sera autorisé à discuter de la question qu'en interne avec la direction, ou avec d'autres employés, si cela est jugé nécessaire, après avoir obtenu l'approbation du MLRO. Toute discussion externe est interdite et sera considérée comme une divulgation. Si des circonstances surviennent rendant difficile pour l'employé de communiquer avec le joueur sans risquer de déclencher une alerte, l'employé doit demander conseil et suivre les instructions du MLRO. Cette procédure constitue la procédure interne de Games & More BV pour signaler une activité et des transactions suspectes.

4.2.2 Procédures de déclaration externes

Comme déjà décrit dans la section précédente, le MLRO recevra et évaluera les rapports internes de suspicion. Il ouvrira et tiendra un journal détaillant les progrès liés à chaque rapport, notant toute information qui doit être documentée afin de garantir qu'un suivi adéquat des raisons ayant conduit à sa décision soit conservé. Une telle documentation peut également être utilisée pour aider les autorités dans toute analyse ou enquête sur le blanchiment d'argent suspecté ou le financement du terrorisme, lorsque ces détails sont directement demandés par le MLRO. Ce journal sera détenu par le MLRO et ne sera accessible qu'à lui, et ne fera pas partie du dossier du joueur. Le MLRO rassemblera toutes les informations nécessaires et posera toutes les questions à n'importe lequel des employés de Games & More BV dans le cadre de son enquête. Les employés (qu'ils aient soumis le rapport interne ou non) fourniront au MLRO les informations pertinentes. Ce faisant, ils ne violeront pas leur obligation de confidentialité envers le client. Une fois que le MLRO décide qu'il existe des motifs raisonnables justifiant la soumission d'un STR via le système de soumission en ligne de l'Autorité, il fera cette divulgation formelle à la FIAU au nom de Games & More BV. Aucune copie des rapports internes ou externes ne sera faite. Le MLRO conservera ces dossiers en sécurité. Le MLRO informera, le cas échéant, l'auteur du rapport

interne si une divulgation formelle a été faite ou non. Suite à une divulgation formelle, le MLRO prendra les mesures requises par les autorités en lien avec la divulgation et suivra en conséquence leurs instructions.

4.2.3 Qu'est-ce qui devrait donner lieu à une activité suspecte?

Pour plus de clarté, le rapport STR couvrira :

Toute activité qui amène Games & More BV à penser qu'une personne est liée au blanchiment d'argent/financement du terrorisme ou à tout produit du crime, ou que l'un des deux est commis, ou peut être commis, indépendamment du fait que des transactions aient eu lieu ou non.

Tout cas où des faits objectifs amèneront Games & More BV à avoir des motifs raisonnables de suspecter que le blanchiment d'argent/financement du terrorisme ou des produits du crime peut avoir lieu.

Games & More BV sera tenue de soumettre un STR à la FIAU concernant l'activité menée sur la base de sa licence de jeu de Curaçao, et d'en informer en conséquence l'AUTORITÉ DE JEU DE CURAÇAO, si nécessaire et selon les instructions données par la FIAU.

4.2.4 Arrêt/continuation du travail suite à un soupçon

En raison de la nature des produits et services de jeu offerts par Games & More BV, et de la nature des transactions en question, Games & More BV ne sera pas toujours en mesure de s'abstenir d'effectuer une transaction en attente avant le dépôt d'un STR. En effet, si Games & More BV s'abstient d'accepter une transaction alors qu'elle le fait habituellement instantanément, le retard dans l'acceptation peut amener le joueur à savoir qu'il est soupçonné d'activité frauduleuse. Tout retard peut porter préjudice à une analyse ou une enquête sur la transaction suspectée. Par conséquent, chaque fois que Games & More BV soupçonne le blanchiment d'argent/le financement du terrorisme, Games & More BV continuera à exécuter la transaction suspectée. Cependant, Games & More BV soumettra un STR à la FIAU immédiatement après l'exécution de la transaction.

4.2.5 Interdiction de divulgation

- ✓ Divulgations à l'autorité de supervision, dans ce cas l'AUTORITÉ DE JEU DE CURAÇAO;
- ✓ Divulgations entre personnes assujetties au sein du même groupe;
- ✓ Divulgations entre une personne assujettie exerçant une « activité pertinente » et une autre personne exerçant des activités similaires et où des exigences similaires sont imposées par la juridiction. Les personnes étant au sein de la même personne morale ou au sein d'une structure plus grande à laquelle elles appartiennent, ayant une propriété, une gestion communes;

✓ Partage d'informations basé sur la même transaction, où les personnes assujetties et l'activité connexe sont soumises aux mêmes obligations légales et les personnes sont de la même catégorie professionnelle et ont donc des obligations similaires en matière de secret professionnel et de protection des données;

✓ Divulgations par une personne assujettie au cours de procédures engagées à l'égard de retards dans l'exécution de transactions, où la personne assujettie suivait en fait les instructions selon la FIAU;

✓ Divulgarion par une personne assujettie à une autorité de surveillance selon la demande faite par l'autorité de surveillance, à cet égard, l'AUTORITÉ DE JEU DE CURAÇAO.

Games & More BV prendra également en considération avec soin toutes les mesures qu'elle décide d'adopter vis-à-vis du joueur soupçonné, suite à la soumission d'un STR. Afin de ne pas compromettre une enquête, avant d'entreprendre une telle action, Games & More BV cherchera des conseils auprès des analystes de la FIAU. Games & More BV considérera autant que possible tous les risques associés avant de prendre une décision sur la manière de continuer à interagir avec le joueur.

5. Procédure de Gestion des Paiements

Lorsqu'un joueur fait une demande de retrait, quel que soit le mode de paiement utilisé, Games & More BV s'assurera, avant d'accéder à une telle demande, que l'institution à laquelle les fonds doivent être virés est située dans une juridiction réputée et a des exigences équivalentes en matière de lutte contre le blanchiment d'argent/contre-terrorisme applicables à Games & More BV. Il va sans dire que cela s'applique également aux institutions d'où proviennent les dépôts des joueurs. En règle générale, les retraits ne seront traités qu'à la même source d'où proviennent les fonds. Cette mesure limitera le risque de blanchiment d'argent ou de financement du terrorisme réussis.

De plus, aucun dépôt ou retrait en espèces ne sera effectué. Les demandes de retrait seront traitées selon la procédure suivante :

✓ Les demandes de retrait seront traitées immédiatement sur demande.

✓ Aucun retrait en espèces ne peut être traité en aucune circonstance. Les transactions en espèces sont spécifiquement interdites et en fait il n'y a pas de méthodes que les joueurs peuvent appliquer pour traiter tout transfert de fonds en espèces.

✓ Le gameplay sera vérifié ainsi que toutes les transactions financières.

✓ Games & More BV examinera également si les individus jouent équitablement, ou si le système de jeu a été manipulé de quelque manière que ce soit, ou si le système est en panne, et si le joueur profitait d'un bug sans en informer Games & More BV, conformément aux exigences des Termes & Conditions.

✓ Il sera également fait référence à savoir si la vérification CDD a été effectuée. Si elle n'a pas encore été effectuée car l'exigence de dépôt n'a pas été atteinte, une décision de gestion est prise quant à savoir s'il est jugé nécessaire d'effectuer la vérification CDD à ce stade avant de compléter le processus de retrait.

✓ L'évaluation des risques est également effectuée / vérifiée pour s'assurer que le risque du joueur vis-à-vis de son activité avec Games & More BV est déterminé.

✓ Les exigences CDD applicables seront conformes à la section 3.2 ci-dessus.

✓ Si le joueur ne fournit pas les documents nécessaires pour que la vérification ait lieu, lorsqu'il est sollicité, ou s'il devient clair que la vérification ne peut avoir lieu parce que l'individu a agi frauduleusement, les retraits ne seront pas traités. Une fois qu'il devient clair pour Games & More BV que l'individu tentait d'agir frauduleusement, il bloquera le compte du joueur, annulera tous les gains et retournera simplement le dépôt au compte d'où proviennent les fonds.

✓ Dans l'éventualité où les retraits ne peuvent être traités vers le compte d'où proviennent les fonds, comme lorsque le joueur utilise Mastercard ou Paysafecard, alors Games & More BV demandera formellement les documents de vérification du joueur et demandera également les détails d'un autre système de paiement qui peut être confirmé au nom du joueur et donc minimiser le risque de virer des fonds à une personne différente de celle qui avait initialement viré les dépôts. Ce processus est en place pour décourager le vol de cartes de crédit et l'usurpation d'identité.

In the case where a manual payout is required due to account closures, the payouts will be paid within 10 business days, so long the amount does not exceed the weekly withdrawal limit.

In the event that source of funds/source of wealth documents are required, the decision will be made within 30 days upon receiving all required documents. If the provided documents require further documents to be sent, this deadline shifts to 30 days since receiving the last document. In case the documents are not provided within 30 days, the account will be restricted and the decision on how to proceed with the funds is at the management and legal department discretion.

6. Formation

Il est de la politique de Games & More BV que tout le personnel ayant un contact avec les clients, ou ayant accès à des informations sur les affaires des clients, reçoive une formation en matière de lutte contre le blanchiment d'argent afin de s'assurer que ses connaissances et sa compréhension sont à un niveau approprié. La formation sera également dispensée au moins une fois par an afin de maintenir la sensibilisation et de s'assurer que les obligations légales de l'entreprise sont remplies. Toute formation donnée prendra en compte la praticité d'attribuer différentes tâches au personnel en fonction de leur rôle, et toutes les informations accessibles seront basées sur le besoin de savoir. Cependant, une formation sur l'ensemble

du processus sera fournie aux employés, afin de garantir que chaque agent a une compréhension globale des procédures de diligence raisonnable, KYC, AML et de paiement, car elles sont étroitement liées.

Compte tenu de la gravité des obligations imposées par la loi et les règlements, et de la gravité des sanctions possibles, le MLRO veillera à ce que l'information sur ces obligations soit disponible pour tous les membres du personnel à tout moment. Le MLRO veillera également à ce que la formation continue soit fournie, c'est-à-dire au fur et à mesure des besoins, même sur la base de demandes directes faites par les employés.

Les programmes de formation comprendront des tests pour s'assurer que chaque individu a atteint le niveau de connaissance et de compréhension approprié. Les tests peuvent être effectués de diverses manières, que ce soit par des tests formels, une évaluation par la discussion d'études de cas, ou d'autres moyens. Une attention particulière sera accordée aux besoins de formation de la direction et de l'équipe de conformité, dont les connaissances et la compréhension doivent être les plus complètes.

Le département des ressources humaines (RH) :

- ✓ informera chaque membre du personnel des programmes de formation qu'ils sont tenus de suivre, et du calendrier pour l'achèvement ;

- ✓ vérifiera que chaque membre du personnel a terminé les programmes de formation qui lui sont assignés, en envoyant des rappels à ceux qui n'ont pas terminé les programmes selon le calendrier applicable ;

- ✓ tiendra des registres de la formation terminée, y compris les résultats des tests ou autres évaluations démontrant que chaque individu a atteint un niveau de compétence approprié ;

- ✓ mettra à jour les dossiers personnels des employés avec les détails de la formation suivie et les résultats obtenus le cas échéant ;

- ✓ se référera à la direction pour les cas où les membres du personnel ne répondent pas ou dont les résultats sont insatisfaisants, pour émettre des réprimandes ou fournir une formation supplémentaire selon le cas individuel.

Le MLRO aura accès à tous les dossiers détenus par le département des ressources humaines.

À la fin d'un cycle de formation, le département des ressources humaines veillera à la continuité de la formation continue et obtiendra également des mises à jour du MLRO concernant les changements qui se produisent dans le domaine, afin que le RH puisse s'assurer que la formation à jour est organisée et fournie à tous les membres du personnel.

Les responsables de ligne fourniront également un retour d'information au département des ressources humaines concernant :

- ✓ l'efficacité des programmes terminés ; et

- ✓ faire des suggestions quant à différentes méthodes de livraison.

Les responsables de ligne compléteront la formation fournie au personnel de soutien en donnant des conseils au jour le jour sur :

- ✓ le type d'instructions et de transactions des clients qui comptent comme 'significatives' et qui doivent donc être portées à leur attention

- ✓ identifier les instructions et transactions des clients qui, bien que n'étant pas de nature normalement comptées comme 'significatives', sont en quelque sorte inhabituelles ou anormales et doivent être considérées en ce qui concerne une suspicion possible de blanchiment d'argent ou de financement du terrorisme. Le MLRO déterminera les besoins de formation pour son propre rôle, et veillera à ce qu'il/elle suive l'éducation professionnelle continue (EPC) requise pour remplir ses obligations légales.

L'objectif de toute la formation fournie est de s'assurer que le personnel est capable d'identifier toute tentative ou activité réelle de blanchiment d'argent ou de financement du terrorisme exercée par les joueurs lors de l'utilisation des services de Games & More BV.

Chipstars utilise un fournisseur tiers externe pour la procédure de vérification de la diligence raisonnable simplifiée et n'est pas responsable des erreurs si une erreur se produit du côté des fournisseurs externes.

7. Conservation des dossiers d'informations sur la diligence raisonnable des clients
Lorsque des informations sont collectées à des fins de CDD, le personnel du service responsable doit :

- ✓ conserver des dossiers dans le dossier client.

- ✓ enregistrer les cas où les informations demandées n'ont pas été fournies, ou les explications fournies n'ont pas été satisfaisantes.

- ✓ s'assurer que tous les dossiers sont conservés de manière cohérente afin qu'ils soient accessibles et compréhensibles par les autres membres du personnel autorisés, y compris le MLRO.

Les dossiers de transactions et de clients à partir de la date de la transaction et de la fin de la relation commerciale respectivement, sont conservés aussi longtemps que Games & More BV a une raison légale valable de conserver ces dossiers. Ces raisons se limitent uniquement aux obligations légales auxquelles Games & More BV doit se conformer, telles que les obligations de lutte contre le blanchiment d'argent, les réglementations fiscales, etc.

Les dossiers sont par conséquent archivés. Les joueurs ont la possibilité d'accéder aux transactions depuis leur profil pendant une période de 2 mois. Passé ce délai, les détails sur les transactions peuvent être demandés via le support client à gmbvcuracao@gmail.com.

Si Games & More BV détermine qu'il est nécessaire de conserver le dossier d'un joueur pendant une période prolongée en raison du fait qu'un rapport a été déposé concernant ce joueur, tous les dossiers pertinents seront conservés dans le système en direct et non archivés. Ceci est fait afin de garantir que Games & More BV se conforme à ses obligations en matière de lutte contre le blanchiment d'argent. Une fois l'enquête / l'investigation terminée et le MLRO informé en conséquence, les dossiers seront traités de manière similaire à toutes les autres informations et la même politique d'archivage s'appliquera alors.

8. Surveillance et gestion de la conformité

La conformité à cette politique doit être constamment testée et assurée. Le Conseil d'Administration se réserve le droit de faire appel à des auditeurs externes pour examiner si l'entreprise respecte les mesures énoncées dans cette procédure. Les résultats de ces audits et toutes les recommandations appropriées d'action seront rapportés au Conseil d'Administration. Ce dernier demandera ensuite un retour d'information de la part de la direction concernant les suggestions faites par les auditeurs. Sur la base des recommandations et des commentaires de la direction, les administrateurs prendront une décision sur les processus / procédures à modifier ou à introduire. Un calendrier de mise en œuvre sera également discuté et décidé. Les commentaires sur la mise en œuvre de tout changement doivent être rapportés aux administrateurs, car ils sont en fin de compte responsables des opérations de l'entreprise.

Le MLRO sera évidemment impliqué et son apport sera considéré comme primordial dans ce processus. Il sera chargé de surveiller les aspects des politiques et procédures de CDD et de lutte contre le blanchiment d'argent de l'entreprise. Toute déficience dans ces procédures ou la conformité à celles-ci, qui nécessite une rectification urgente, sera traitée immédiatement par le MLRO, qui signalera ces incidents au Conseil d'Administration si nécessaire. Il demandera également au Conseil de lui fournir tout soutien nécessaire.

Le MLRO auditera la procédure directement, au moins une fois par an. Le MLRO rapportera également ses conclusions au Conseil d'Administration. Ce rapport comprendra :

- ✓ un résumé des changements dans l'environnement réglementaire(s) dans lequel Games & More BV opère.
- ✓ un résumé des activités AML au sein de l'entreprise, y compris le nombre de rapports de suspicion internes reçus par le MLRO et le nombre de divulgations faites aux Autorités.
- ✓ les détails de toute carence en matière de conformité sur laquelle une action a déjà été prise, avec des rapports sur les résultats.

✓ les détails de toute carence en matière de conformité sur laquelle une action doit être prise, avec des actions recommandées, y compris un calendrier suggéré et le soutien de la direction requis.

✓ un aperçu des plans pour le développement continu du personnel impliqué, y compris des activités de formation et de sensibilisation périodiques pour tout le personnel concerné.

Lorsqu'une action de gestion est indiquée, le Conseil d'Administration demandera à la direction de fournir ses commentaires et le calendrier des mesures nécessaires.

Cette procédure sera révisée et mise à jour au moins tous les six mois. Cependant, cela peut se produire plus fréquemment, si des changements dans la législation ou les directives sont introduits à tout moment, ou si cela est jugé nécessaire.