Procédure interne concernant le respect de la législation anti‑blanchiment *(Art. 8 de la Loi du 18 septembre 2017* *relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l’utilisation des espèce)*

|  |  |
| --- | --- |
| **Renseignements sur le bureau du courtier en assurances** | |
| Nom du bureau |  |
| Adresse |  |
| Numéro d’entreprise |  |
| Gérants |  |
| RD |  |
| PCP |  |
| Siège(s) d'exploitation |  |
| AMLCO |  |
| Date d’entrée en vigueur |  |

# [SOMMAIRE](#_Toc67385642)

[1. CADRE 3](#_Toc67906537)

[2. ORGANISATION ET CONTRÔLE INTERNE 5](#_Toc67906538)

[**2.1** **LES RESPONSABLES DU BUREAU** 5](#_Toc67906539)

[**2.2**  **Sensibilisation et formation DU PERSONNEL** 6](#_Toc67906540)

[**2.3** **LE CONTRÔLE INTERNE** 7](#_Toc67906541)

[**2.4** **LE CODE AML : LA RÉPARTITION DES TÂCHES AVEC LES ENTREPRISES D'ASSURANCE** 7](#_Toc67906542)

[3. L’ÉVALUATION GLOBALE DES RISQUES 8](#_Toc67906543)

[4. VIGILANCE À L’ÉGARD DE LA CLIENTÈLE ET DES OPÉRATIONS 9](#_Toc67906544)

[**4.1** **ÉTAPE 1 : OBLIGATION D'IDENTIFICATION ET DE VÉRIFICATION DE L'IDENTITÉ** 10](#_Toc67906545)

[**4.2** **ÉTAPE 2 : L’ÉVALUATION INDIVIDUELLE DES RISQUES** 15](#_Toc67906546)

[**4.2** **ÉTAPE 3 : L'ACCEPTATION DES CLIENTS** 15](#_Toc67906547)

[**4.4** **ÉTAPE 4 : VIGILANCE CONTINUE ET DÉTECTION D’OPÉRATIONS ATYPIQUES** 16](#_Toc67906548)

[**4.5** **CAS PARTICULIERS DE VIGILANCE ACCRUE** 18](#_Toc67906549)

[5. ANALYSE DES OPÉRATIONS ATYPIQUES ET DÉCLARATION DE SOUPCONS 23](#_Toc67906550)

[**5.1** **ANALYSE D’OPÉRATIONS ATYPIQUES ET DÉCLARATION INTERNE** 23](#_Toc67906551)

[**5.2** **DÉCLARATION EXTERNE DE SOUPCONS À LA CTIF** 27](#_Toc67906552)

[**5.3** **DÉCLARATION EXTERNE À LA TRÉSORERIE (SPF FINANCES)** 28](#_Toc67906553)

[6. OBLIGATION DE CONSERVATION 29](#_Toc67906554)

Ce document a été mis à jour sur la base de la récente modification législative (loi du 20 juillet 2020 et AR du 23 septembre 2020), de la communication de la FSMA du 6 octobre 2020 sur le rapport d'activité annuel et du code AML du 24 novembre 2020 du secteur des assurances.

# CADRE

La loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces (ci-après *« la Loi »*) est le cadre de la lutte contre les pratiques de blanchiment. Il s’agit d’une loi préventive visant à prévenir ces pratiques en matière de blanchiment de capitaux et de financement du terrorisme (ci-après *« BC/FT »)*. C'est grâce à un effort conjoint des pouvoirs publics et des entités concernées telles que les entreprises d'assurances, les établissements de crédit et les intermédiaires financiers que les portes du système financier restent fermées aux capitaux de la criminalité.

La Loi décrit le **« blanchiment de capitaux** »[[1]](#footnote-1) (BC) comme suit :

*1° la conversion ou le transfert de capitaux ou d’autres biens, dont celui qui s’y livre sait qu’ils proviennent d’une activité criminelle ou d'une participation à une telle activité, dans le but de dissimuler ou de déguiser l’origine illicite de ces capitaux ou biens ou d’aider toute personne impliquée dans une telle activité à échapper aux conséquences juridiques des actes qu’elle a commis ;*

*2° le fait de dissimuler ou de déguiser la nature, l’origine, l’emplacement, la disposition, le mouvement ou la propriété réels des capitaux ou des biens ou des droits qui y sont liés, dont celui qui s’y livre sait qu’ils proviennent d’une activité criminelle ou d'une participation à une telle activité ;*

*3° l’acquisition, la détention ou l’utilisation de capitaux ou de biens, dont celui qui s’y livre sait, au moment où il les réceptionne, qu’ils proviennent d'une activité criminelle ou d’une participation à une telle activité ;*

*4° la participation à l’un des actes visés aux 1°, 2° et 3°, le fait de s’associer pour le commettre, de tenter de le commettre, d’aider ou d’inciter quelqu’un à le commettre ou de le conseiller à cet effet, ou de faciliter l’exécution d’un tel acte.*

Sont considérées comme activités criminelles, le terrorisme ou le financement du terrorisme, la criminalité organisée, le trafic illicite de drogue, le trafic illicite d’armes, le trafic d’êtres humains, la traite des êtres humains, l’exploitation de la prostitution ; l’utilisation illégale de substances à effet hormonal sur les animaux, ou le commerce illégal de telles substances, le trafic illicite d’organes ou de tissus humains, la fraude au préjudice des intérêts financiers de l’Union européenne, la fraude fiscale grave, organisée ou non, la fraude sociale, le détournement par des personnes exerçant une fonction publique et la corruption, la criminalité environnementale grave, la contrefaçon de monnaie ou de billets de banque, la contrefaçon de biens, la piraterie, un délit boursier, l’appel public irrégulier à l’épargne, la fourniture de services bancaires, financiers, d’assurance ou de transferts de fonds, ou le commerce de devises, ou toute autre quelconque activité réglementée, sans disposer de l’agrément requis ou des conditions d’accès pour l’exercice de ces activités, l’escroquerie, l’abus de confiance, l’abus de biens sociaux, la prise d’otages, le vol, l’extorsion, l’état de faillite et la fraude informatique.

La Loi décrit par ailleurs le « **financement du terrorisme** »[[2]](#footnote-2) (FT) comme

*le fait de réunir ou de fournir des fonds ou d’autres moyens matériels, par quelque moyen que ce soit, directement ou indirectement, avec l’intention qu’ils soient utilisés ou en sachant qu’ils seront utilisés, en tout ou en partie, par une organisation terroriste ou par un terroriste agissant seul, même en l’absence de lien avec un acte terroriste précis.*

La Loi s'applique en particulier :

* Aux intermédiaires d’assurances non exclusifs actifs dans les branches « vie » et à leurs sous-agents[[3]](#footnote-3) ;
* Aux courtiers en services bancaires et services d’investissement[[4]](#footnote-4).

Ils veillent au respect par leurs collaborateurs, à savoir les membres du personnel et les sous‑agents.

La Loi prévoit quatre obligations :

1. **Évaluation globale des risques :**Une évaluation des risques au niveau du bureau.
2. **Une organisation et un contrôle interne de qualité :**

Le développement d’une structure de prévention et de contrôle interne appropriée, avec une attention particulière pour la formation.

1. **Vigilance à l’égard des clients, des opérations effectuées par eux, leurs mandataires, leurs bénéficiaires contractuels et, en cas de personne morale, leurs bénéficiaires effectifs :**
2. les obligations d’identification, de vérification de l’identité et de conservation des données d’identification et des documents ;
3. l’évaluation des caractéristiques du client et de l'objet et la nature de la relation d'affaires envisagée et, le cas échéant, la collecte d’informations complémentaires à cet effet ;
4. la vigilance continue à l’égard des relations d’affaires et des opérations.
5. **Analyse des opérations atypiques et déclaration de soupçons :**
6. Vérifier s’il peut être question de blanchiment de capitaux ou de financement du terrorisme ;
7. L’obligation de communiquer toute donnée, tout soupçon ou indice à cet égard à la Cellule de Traitement des Informations Financières (CTIF) ;
8. L'obligation de signaler le gel des avoirs à la Trésorerie (SPF Finances) ;
9. La prise de mesures supplémentaires.

Ce manuel contient les procédures et mesures de contrôle interne[[5]](#footnote-5) sur la base des obligations énumérées ci-dessus. Il tient compte de la nature et de la taille[[6]](#footnote-6) du bureau.

Le rapport annuel d'activité expose les mesures concrètes que le bureau prend en exécution de la Loi, des règlements et du présent manuel.

# ORGANISATION ET CONTRÔLE INTERNE

## **2.1 LES RESPONSABLES DU BUREAU**

Le bureau désigne deux responsables qui veillent au respect de la Loi :

Au sein d’une petite entreprise, les deux fonctions de « haut dirigeant responsable » et de « responsable anti-blanchiment opérationnel » (AMLCO) peuvent être exercées par une seule et même personne. Un intermédiaire personne physique exerce toujours lui-même ces fonctions.

1. **Un haut dirigeant responsable**   
   Ce haut dirigeant responsable fait partie de la direction effective. Son rôle est de s’assurer que les mesures opérationnelles adéquates sont prises et qu’elles sont proportionnées aux résultats de l'évaluation globale des risques. Il est également appelé « responsable anti-blanchiment stratégique ».
2. **Le responsable anti-blanchiment opérationnel (AMLCO)**Le responsable anti-blanchiment « opérationnel » ou AMLCO est un membre de la direction effective ou un travailleur chargé, au niveau opérationnel, du respect des procédures[[7]](#footnote-7).

Pour notre bureau :

Le haut dirigeant responsable est : (nom)

E-mail/tél.

L’AMLCO : (nom)

E-mail/tél.

Le nom des responsables désignés est mentionné dans le dossier d’inscription électronique auprès de l’autorité de contrôle FSMA. Tout changement de responsable est immédiatement introduit. Pour les personnes morales, une copie de la décision de l'organe légal d'administration désignant les responsables est conservée dans le dossier au bureau.

L’AMLCO est responsable de :

* L’exécution de l’évaluation globale des risques[[8]](#footnote-8)
* La mise en œuvre des politiques, procédures et mesures de contrôle interne
* L’analyse des opérations atypiques et la rédaction de rapports écrits sur cette analyse.
* La déclaration de soupçons à la CTIF
* La sensibilisation et la formation du personnel ainsi que des agents, aussi bien théorique que pratique
* L’établissement du rapport d’activité, au moins une fois par an.[[9]](#footnote-9)

**Que faire en cas d’absence de l’AMLCO ?**

* **Absence planifiée de l’AMLCO**

Dans les cas d’absence prolongée planifiée de l’AMLCO, p. ex. longues vacances, l’accomplissement des tâches sera, autant que possible, délégué temporairement à un remplaçant fixe afin d'assurer la continuité. Dans les cas d’absence non planifiée de ce remplaçant fixe, la personne qui est chargée à ce moment de la direction effective du bureau assumera temporairement cette fonction.

* **Absence non planifiée de l’AMLCO**

En cas d'absence non planifiée de l'AMLCO et si ni le remplaçant fixe ni une personne de la direction effective ne sont présents, les collaborateurs individuels du bureau assumeront eux-mêmes la fonction d'AMLCO et procéderont, le cas échéant, à la déclaration à la CTIF.

## **2.2 Sensibilisation et formation DU PERSONNEL**

Les collaborateurs doivent connaître et comprendre les procédures et les mesures de contrôle interne en vigueur au sein du bureau. C’est pourquoi ils doivent disposer des connaissances requises en ce qui concerne les méthodes et critères applicables pour identifier les opérations qui peuvent être liées au BC/FT. L’AMLCO sensibilise les collaborateurs et veille à leur formation en matière de limitation des risques de BC/FT. Le bureau prévoit une formation permanente à cet effet. Celle-ci est proportionnelle en termes d’intensité et de fréquence à la nature et à la taille du bureau ainsi qu’aux risques de BC/FT auxquels elle est exposée.

La formation concerne, d’une part, le cadre juridique général applicable en matière de BC/FT et, d’autre part, les procédures et mesures de contrôle interne développées telles que reprises dans ce manuel. Outre la formation purement théorique, les collaborateurs concernés doivent être effectivement en mesure d’appliquer les mesures, d’identifier les opérations suspectes et de garantir le respect des dispositions contraignantes relatives aux embargos financiers.

Concrètement, les initiatives suivantes sont prises en matière de recyclage régulier :

1. **Pour les nouveaux collaborateurs ou les désignations dans une fonction à plus grande responsabilité**

Dans les \_\_\_\_\_ jours qui suivent l’engagement ou la désignation, la formation de base en matière de lutte contre le BC/FT est donnée. Cette formation est organisée sous la responsabilité de l’AMLCO. Elle peut consister en une formation par un institut de formation externe (EDFIN VZW), une formation interne ou un module d’e-learning mis à disposition par le bureau. En outre, l’AMLCO explique au collaborateur les procédures telles que reprises dans le présent manuel.

1. **Pour les collaborateurs existants**

Au moins tous les \_\_\_ ans, *[à déterminer par chaque bureau, mais au moins une fois tous les trois ans]* les collaborateurs suivent obligatoirement une formation en matière de lutte contre le BC/FT. Cette formation peut se faire en interne ou en externe. Les collaborateurs seront informés de la date en temps utile. L’AMLCO peut décider d’organiser des formations complémentaires.

1. **Concertation avec les collaborateurs**

L’AMLCO organise régulièrement une concertation interne avec les collaborateurs chargés d’opérations en matière d’assurances-vie. Lors de cette concertation, l'AMLCO signale les modifications de la réglementation et discute de l'application du présent manuel au fonctionnement quotidien du bureau. Lors de l'actualisation de l'évaluation globale des risques, l'AMLCO partage les résultats avec les collaborateurs. L’AMLCO peut rédiger des notes internes à ce sujet.

Les initiatives de formation prises sont mentionnées dans le rapport annuel d’activité relatif au BC/FT.

## **2.3 LE CONTRÔLE INTERNE**

Les mesures de contrôle interne visent à identifier les faiblesses des procédures. Le bureau peut ainsi prendre les mesures appropriées pour les éliminer.

Chaque année, l’AMLCO procède avec le collaborateur concerné à un échantillonnage des dossiers clients afin d’établir que les procédures sont respectées. Ces constatations peuvent donner lieu à une adaptation du présent manuel. Le rapport annuel d’activité mentionne le contrôle interne, le nombre de dossiers clients contrôlés et les constatations générales.

## **LE CODE AML : LA RÉPARTITION DES TÂCHES AVEC LES ENTREPRISES D'ASSURANCE**

Les compagnies d'assurance et les intermédiaires d'assurance sont soumis aux mêmes dispositions légales en matière de BC/FT. Afin de garantir le bon déroulement de la relation commerciale avec le client assuré, des accords ont été conclus au sein du secteur des assurances sur la répartition des tâches. Celles-ci sont définies dans le code anti-blanchiment du 24 novembre 2020. Le code anti-blanchiment peut être consulté sur le site web de la BZB-Fedafin :

<https://www.bzb-fedafin.be/fr-be/bib-sectoriel/codes-de-conduite/sectorcode-inzake-de-distributie-van-financiele-producten-tot-voorkoming-van-het-witwassen-van-geld-en-de-financiering-van-terrorisme-aml-code>

La répartition des tâches entre l'entreprise d'assurance et l'intermédiaire d'assurance est juridiquement fondée sur la relation en tant que tiers introducteur, mandataire ou sous-entrepreneur. Chacun reste responsable de la bonne exécution de ses propres obligations (cf. chapitre 2 du Code AML).

L'intermédiaire d'assurance effectue les tâches suivantes pour l'entreprise d'assurance :

* l’identification et la vérification de l’identité des clients et, le cas échéant, de leurs mandataires et bénéficiaires effectifs
* l’obligation d’identification des caractéristiques du client, de l’objet et de la nature de la relation d’affaires
* l’obligation de mise à jour des informations
* Détection des opérations atypiques : surveillance de première ligne

L'entreprise d'assurance effectue les tâches suivantes pour l'intermédiaire d'assurance

* Détection des opérations atypiques : surveillance de deuxième ligne
* Contrôle des embargos et déclaration à la Trésorerie

Cette répartition des tâches est précisée dans le présent manuel. Tous les éléments essentiels du code AML sont inclus dans ce manuel. Les annexes du Code AML contiennent entre autres des questionnaires qui peuvent être utilisés par l'intermédiaire d'assurance pour la détection des transactions atypiques, l'origine des fonds et l'identification des Personnes Politiquement Exposées.

# L’ÉVALUATION GLOBALE DES RISQUES

Comme première étape de l'approche basée sur les risques[[10]](#footnote-10) pour aborder le BC/FT, l'AMLCO procède à l'évaluation globale des risques pour le bureau. Il peut se faire assister par d’autres personnes lors de l’exécution de cette évaluation, mais l’AMLCO assume la responsabilité finale et donne des explications lors d’un contrôle par la FSMA.

L'évaluation globale des risques comprend l'identification et l'évaluation des risques de BC/FT auxquels le bureau est exposée. Grâce à cette évaluation globale des risques, le bureau peut se concentrer sur des situations qui impliquent des risques de BC/FT plus élevés et sur lesquelles les collaborateurs doivent exercer une vigilance accrue.

À cet effet, la FSMA met à disposition un tableau Excel « mon évaluation globale des risques » (ainsi qu’un guide pratique (voir <https://www.bzb-fedafin.be/fr-be/bib-sectoriel/infos-professionnelles/anti-blanchiment-info-fsma>). L'AMLCO utilise cet instrument pour l'évaluation globale des risques. Il sélectionne ainsi les risques pertinents pour l’activité. Cela nécessite un exercice de réflexion sous la responsabilité de l’AMLCO. Les risques qui ne sont pas abordés dans le tableau Excel sont ajoutés au tableau Excel.

Dès que les risques BC/FT ont été identifiés pour le bureau, l’AMLCO décrit un certain nombre de catégories de risques. Cela signifie que les situations nécessitant des mesures de vigilance identiques sont regroupées dans une même catégorie[[11]](#footnote-11).

La classification en catégories de risques doit comprendre au moins deux niveaux de risque : « standard » et « élevé ». On peut également opter pour trois niveaux : « bas », « standard » et « élevé ».

Notre bureau applique les niveaux de risque suivants :

Standard et élevé

*ou*

Bas, standard et élevé

*(biffez la ligne qui n’est pas d’application)*

Le bureau attribue un niveau de risque à tous les clients.

Options :

Notre bureau a ajouté un niveau de risque à chaque client dans le fichier clients électronique.

*Ou*

Notre bureau applique le niveau de risque standard et élevé. Les fiches clients des clients présentant un niveau de risque élevé mentionnent le risque élevé. Les autres fiches clients ont le niveau de risque standard.

L’évaluation globale des risques est documentée et tenue à la disposition de l’autorité de contrôle FSMA. Celle-ci sera mise à jour au moins une fois par an[[12]](#footnote-12) et aussi chaque fois que se produit un événement susceptible d’avoir des répercussions significatives sur un ou plusieurs risques. Un tel événement est par exemple la reprise totale d'un portefeuille d'assurance-vie par le bureau d'un autre intermédiaire ou une modification dans la clientèle comme l'acceptation de PPE ou de personnes morales, si celles-ci ne faisaient pas auparavant partie du portefeuille d'assurance-vie. D’autres événements pertinents sont par exemple la distribution de produits en dehors de la Belgique ou le recours à des tiers introducteurs. Les collaborateurs informent l’AMLCO d’un tel événement augmentant potentiellement le risque.

L’AMLCO note dans le rapport annuel d’activité les éventuelles adaptations à l’évaluation globale des risques.

# VIGILANCE À L’ÉGARD DE LA CLIENTÈLE ET DES OPÉRATIONS

Dans le cadre de l'approche basée sur les risques, le bureau a effectué l'évaluation globale des risques le *(date).*

Les catégories de risques **à risque élevé** suivantes ont été constatées :

1.

2.

3.

(…)

Il en résulte la politique suivante :

Le bureau applique toujours des mesures de vigilance dans les cas où elle identifie un risque standard.

Le bureau suit des mesures de vigilance **accrue** dans les cas où elle identifie un risque élevé. En cas de vigilance accrue, une attention supplémentaire est accordée à la vérification de l'identité, à l'origine des moyens et, lors de la conclusion de la relation d'affaires, l'approbation du dirigeant est demandée.

Vous trouverez ci-après la procédure pour réaliser une évaluation individuelle des risques et l'acceptation des clients.

## **4.1 ÉTAPE 1 : OBLIGATION D'IDENTIFICATION ET DE VÉRIFICATION DE L'IDENTITÉ**

L’identification consiste à rassembler et prendre connaissance des données d’identification afin de distinguer la personne de toute autre personne.

La vérification de l’identité consiste à confronter les données d’identification à une source d’information fiable qui peut confirmer ou réfuter ces données et est effectuée au moyen d’un justificatif dont une copie est prise sur papier ou sur support électronique.

Le code AML stipule que pour chaque nouvelle affaire, l’intermédiaire d’assurances fournit à l’entreprise d’assurances sur support papier ou électronique :

* + la proposition d’assurance ou un autre formulaire de souscription similaire ;
  + une copie (recto verso) des documents (d’identité) repris ci-dessous, établis dans une des langues nationales officielles ou dans les langues mentionnées dans les documents précontractuels de l’entreprise d’assurances ;

L’intermédiaire d’assurances doit également conserver ces documents dans son dossier.

1. **Qui sont les personnes à identifier ?**

* **Le preneur d’assurance :**

Il s'agit de la personne avec laquelle le bureau nouera une relation d'affaires, à savoir la conclusion du contrat d'assurance-vie.

* **Le mandataire du preneur d’assurance :**

Il s’agit de toute personne qui intervient au nom et pour le compte du preneur d’assurance.

* **L’assuré :**

L'assuré ne doit pas être identifié, sauf s'il est également preneur d'assurance, bénéficiaire contractuel ou bénéficiaire effectif.

* **Le bénéficiaire contractuel :**

L’identification et la vérification de l’identité de cette catégorie de bénéficiaires doivent avoir lieu au plus tard au moment de la demande du versement de la prestation assurée, mais avant le versement effectif.

* **Le bénéficiaire effectif :**

Il s’agit de la personne physique qui, en dernier ressort, possède ou contrôle une personne morale, par la détention directe ou indirecte d'un pourcentage suffisant des actions ou des droits de vote ou d'une participation suffisante dans cette entité (25 % selon la directive de l’UE).

1. **Qu’est-ce qui est étudié ?**

**L’objet de l’identification** est de recueillir les informations pertinentes relatives à ces personnes qui permettent de les distinguer de toute autre personne de façon suffisamment certaine, en tenant compte du niveau de risque identifié.

Cela signifie pour le bureau :

* Qu’en cas de **risque standard,** le collaborateur limite les informations qu’il recueille. Les informations recueillies doivent néanmoins demeurer suffisantes pour permettre de distinguer la personne concernée de toute autre personne de façon suffisamment certaine.
* Qu’en cas de **risque élevé,** le collaborateur doit s'assurer avec une attention accrue que les informations recueillies lui permettent de distinguer de façon incontestable la personne concernée de toute autre. Au besoin, il recueille à cette fin des informations complémentaires.

**POUR LES PERSONNES PHYSIQUES**

* Pour les **personnes physiques,** l'identification concerne le nom, le prénom, la date et le lieu de naissance. Dans la mesure du possible, des informations pertinentes concernant l'adresse doivent également être recueillies pour les personnes physiques.

Il s'agit des documents suivants : (cf. Code AML p.16 et suivantes : https://www.bzb-fedafin.be/fr-be/bib-sectoriel/codes-de-conduite/sectorcode-inzake-de-distributie-van-financiele-producten-tot-voorkoming-van-het-witwassen-van-geld-en-de-financiering-van-terrorisme-aml-code).

|  |  |
| --- | --- |
| Preneur d’assurance belge résidant en Belgique | La carte d’identité ou un moyen d'identification électronique proposé ou agréé par le service d'authentification conformément à la loi du 18 juillet 2017 relative à l'identification électronique ou via un service de confiance pertinent prévu par le Règlement 910/2014 (p. ex. Itsme, signature électronique de la carte d’identité...) |
| Preneur d'assurance belge résidant à l'étranger | Passeport |
| Preneur d’assurance de nationalité étrangère qui réside en permanence en Belgique | Carte d’identité ou, à défaut, la carte belge d’étranger |
| Preneur d'assurance de nationalité étrangère qui réside temporairement ou sous statut précaire en Belgique | Certificat d'inscription au registre des étrangers ou autre document émis par les autorités belges qui atteste de l'identité de la personne |
| Preneur d’assurance de nationalité étrangère qui réside en permanence à l’étranger | Carte d'identité ou passeport étrangers |
| Si la personne physique intervient comme mandataire | Délégation de pouvoir et carte d’identité |

**POUR LES PERSONNES MORALES**

Pour les **personnes morales,** l'identification porte sur la dénomination sociale, le siège social, le numéro BCE ou le numéro LEI[[13]](#footnote-13), les administrateurs et la prise de connaissance des dispositions relatives au pouvoir d'engager la personne morale.

Il s'agit des documents suivants : (cf. Code AML p. 14 e.s. : https://www.bzb-fedafin.be/fr-be/bib-sectoriel/codes-de-conduite/sectorcode-inzake-de-distributie-van-financiele-producten-tot-voorkoming-van-het-witwassen-van-geld-en-de-financiering-van-terrorisme-aml-code)

|  |  |
| --- | --- |
| L’identification et la vérification de l’identité d’une personne morale portent sur **la dénomination, le siège social, le numéro BCE[[14]](#footnote-14) ou le « Legal entity identifier » ou** **numéro LEI[[15]](#footnote-15), la liste des administrateurs et les dispositions légales ou statutaires relatives aux pouvoirs de représentation.** | **Documents probants**  Les documents peuvent être obtenus soit auprès du preneur d’assurance lui-même, soit via des sources officielles telles que les annexes au Moniteur belge ([http://www.moniteur.be/](http://www.staatsblad.be/)) et la Banque Carrefour des Entreprises (http://kbopub.economie.fgov.be).  Pour les publications officielles (par exemple les annexes au Moniteur belge), il suffit d'en conserver la référence.  Si les documents ne sont pas rédigés dans une langue usuelle de travail de l'entreprise d'assurances et de l'intermédiaire d'assurances, les documents doivent être traduits. |
| Identification et vérification de l’identité de la personne morale | * les derniers statuts coordonnés ou les statuts actualisés, tels qu'ils ont été déposés au greffe du tribunal de l'entreprise ou publiés dans les annexes au Moniteur belge ; * la liste actualisée des administrateurs ; * la publication de la nomination des administrateurs aux annexes du Moniteur belge ou tout autre document qui prouve leur qualité (comptes annuels, acte authentique passé devant notaire…) ; * la dernière publication aux annexes du Moniteur belge des pouvoirs de représentation de la personne morale ; * un extrait du registre central des bénéficiaires   effectifs (Registre UBO). |
| Identification et vérification de l'identité du ou des bénéficiaires effectifs de la personne morale | Voir tableau ci-dessus : personne physique +  Questionnaire (Annexe 9 – Code AML : <https://www.bzb-fedafin.be/fr-be/bib-sectoriel/codes-de-conduite/sectorcode-inzake-de-distributie-van-financiele-producten-tot-voorkoming-van-het-witwassen-van-geld-en-de-financiering-van-terrorisme-aml-code>) ou questionnaire par biais de la compagnie d’assurances |
| Si la personne morale intervient comme mandataire | Délégation de pouvoir et carte d’identité |

**La vérification de l'identité de la personne morale se fait sur la base des données d'identité recueillies.**Pour satisfaire à cette obligation, le bureau doit également confronter tout ou partie des données d'identification recueillies à un ou plusieurs documents probants ou sources fiables et indépendantes d'information permettant de confirmer ces données, en vue d'acquérir un degré suffisant de certitude qu'elle connaît les personnes concernées, ceci en tenant compte du niveau de risque identifié :

* Accès au Registre national
* Accès au registre UBO
* Vérification auprès de la Banque-carrefour des entreprises
* Vérification dans le Moniteur belge
* Vérification dans les publications de la Banque nationale

Le bureau procède à une **vérification simplifiée de l’identité** pour les clients qui sont un établissement de crédit agréé, un établissement financier, une société cotée en bourse, une instance publique belge ou un organisme public européen.

Pour l'identification et la vérification de l'identité des bénéficiaires effectifs (UBO), le bureau utilise soit la "déclaration du bénéficiaire effectif" (annexe 9 du code AML), soit un document fourni par la compagnie d'assurance. Dans le cas d'une personne morale dont la structure de propriété semble inhabituelle ou excessivement complexe compte tenu de la nature de l'activité, cela doit être signalé à l'AMLCO.

1. **Quand l'identification a-t-elle lieu ?**

L'identification et la vérification de l'identité du **preneur d'assurance** ont lieu **avant** que le bureau n’entame une relation d'affaires avec les clients.

Le bureau satisfait à ses obligations d'identification et de vérification de l'identité **du bénéficiaire contractuel** du contrat d’assurance-vie dès que celui-ci est désigné ou identifiable. Le bureau satisfait à son obligation au plus tard au moment du rachat ou de l’avance, mais avant son versement effectif.

L'identification et la vérification de l'identité du **mandataire** éventuel du preneur d'assurance doivent avoir lieu avant que ce mandataire ne fasse usage de son pouvoir qui engage le preneur d'assurance qu'il représente.

En cas de cession partielle ou totale **à un tiers** du contrat d'assurance-vie, le bureau, si elle a connaissance de cette cession, identifie le bénéficiaire du contrat concerné au moment de la cession à la personne physique ou morale ou à la construction juridique qui reçoit pour son propre profit la valeur du contrat cédé.

Dans le cadre de l’identification, le questionnaire est soumis **à chaque client** afin de déterminer s’il répond ou non aux critères d’une Personne Politiquement Exposée. Ce questionnaire est ou l’annexe 6 du code AML ou le questionnaire fourni par la compagnie d’assurance.

1. **Que faire en cas d'identification à distance ?**

**En cas d'identification "à distance", la vigilance est toujours accrue.**

Dans le cas où le bureau ne peut pas s'assurer visuellement que la personne à identifier est bien le titulaire de la carte d'identité ou d'un autre document d'identification probant, des mesures spécifiques supplémentaires sont nécessaires. Toutefois, cela ne s'applique pas à l'identification au moyen d'un certificat qualifié qui présuppose une identification préalable en face à face du titulaire et atteste de la fiabilité du prestataire de services de certification, comme l'application "Itsme" ou d'autres applications proposées par des fournisseurs informatiques commerciaux[[16]](#footnote-16).

Selon les circonstances de l'affaire, il peut s'agir de l'un des éléments suivants

les mesures suivantes :

* + une vérification de la légitimité ou de la validité de la copie de la carte d'identité électronique via le site Internet suivant : https://www.checkdoc.be ;[[17]](#footnote-17)
  + La demande d'un autre élément de preuve ; cette mesure est en tout cas requise si l'identité est contrôlée sur la base d'une copie d'un élément de preuve ;[[18]](#footnote-18)
  + l'obligation de compléter les données concernant la personne à identifier au moyen du questionnaire pour l'examen complémentaire ;
  + l'introduction d'une procédure d'identification en face à face par la suite ;
  + l'envoi de la correspondance nominative à l'adresse de la personne à identifier.

Si le bureau soupçonne que la personne à identifier choisit l'identification à distance afin de dissimuler plus facilement sa véritable identité, la procédure prévue au point "f." est appliquée. Que faire en cas de non-respect de l'obligation d'identification et de vérification de l'identité. En outre, un rapport écrit doit être fait à l'AMLCO.

1. **Que faire en cas de doute après une identification ?**

Une nouvelle identification et vérification de l'identité sont nécessaires dans les cas suivants :

* lorsque lors de l’identification initiale, il existe des raisons de douter de l'exactitude ou de la véracité des données d'identification fournies par le preneur d'assurance et si celui-ci n’apparaît pas de bonne foi ;
* lorsque postérieurement à l'identification d'un preneur d'assurance en vue de nouer avec lui une relation d'affaires, apparaissent des raisons de croire que les données d'identification qu’il a fournies à cette occasion étaient inexactes ou mensongères ;
* lorsqu'il y a des raisons de douter que la personne qui souhaite réaliser une opération dans le cadre d'une relation d'affaires antérieurement nouée est effectivement le preneur d'assurance identifié en vue de cette relation d'affaires ou son mandataire autorisé et identifié.

Lorsque des soupçons de fausses informations ou de changement de personnalité semblent fondés après cette nouvelle identification et cette vérification d'identité, ou lorsqu'un assuré refuse de se soumettre à la nouvelle identification ou a un comportement suspect, un rapport écrit doit être établi à l'intention de l'AMLCO et, le cas échéant, signalé à la CTIF. Le contrat d'assurance-vie ne peut être conclu. Si le contrat a déjà été conclu, il doit être gelé et tout paiement de prime supplémentaire doit être refusé.

1. **Qu’en est-il en cas de non-respect de l’obligation d’identification et de vérification de l’identité**

Si le bureau ne peut satisfaire à ses obligations d'identification et de vérification de l'identité d'un client, de ses mandataires ou de ses bénéficiaires effectifs, elle s’abstiendra de nouer une relation d'affaires avec ce client ou d’effectuer des opérations pour ce client. Un rapport écrit interne est adressé à l'AMLCO.

Il faut mettre fin à une relation d'affaires déjà nouée.

L’AMLCO examinera également si les causes de l'impossibilité de satisfaire à ces obligations sont de nature à susciter un soupçon de BC/FT et s'il y a lieu d'en informer la CTIF. Un rapport écrit en est établi par l’AMLCO.

## **4.2 ÉTAPE 2 : L’ÉVALUATION INDIVIDUELLE DES RISQUES**

Après avoir constaté l'identité du client, le collaborateur procède à l'évaluation individuelle des risques BC/FT, compte tenu des caractéristiques particulières du client et des résultats de l'évaluation globale des risques (cf. chapitre 3 du manuel).

Pour l'évaluation **des caractéristiques particulières** **du client**, le collaborateur se base sur toutes les informations recueillies par le bureau dans le cadre de l'identification et de la vérification du client, de ses mandataires et bénéficiaires effectifs, les informations relatives aux caractéristiques du client et concernant l'objet et la nature de la relation d'affaires. Ainsi que toute autre information recueillie dans le cadre de la vigilance continue. (par ex. le client a une profession nécessitant beaucoup d'argent liquide ou pas, questionnaire PPE...

Après la réalisation de cette évaluation individuelle, chaque client se voit attribuer un profil de risque.

Le point de départ est que le client est un risque standard.

Lorsque Le collaborateur, dans le cadre de cette évaluation individuelle des risques, identifie que le client entre dans la catégorie des risques élevés sur la base de l'évaluation générale des risques (cf. chapitre 3 du présent manuel) ou identifie un cas de risque élevé sur la base des caractéristiques particulières, le client se voit attribuer le niveau "risque élevé" et le bureau prend des mesures de vigilance accrues.

Des mesures de vigilance simplifiée sont appliquées en cas de risque (faible ou) standard.

Pour tout événement dans le cadre de la relation d'affaires (comme le rachat de l'assurance-vie), on examinera si le profil de risque doit être actualisé.

## **ÉTAPE 3 : L'ACCEPTATION DES CLIENTS**

Une fois que l'évaluation individuelle des risques a été effectuée, la relation d'affaires est nouée ou non.

1. Pour les clients avec **un risque standard**, l'acceptation du client est effectuée par le collaborateur.
2. Pour les clients à **risque élevé** ou dans les cas particuliers de vigilance accrue (voir 5.5 du manuel), l'acceptation du client est effectuée par un dirigeant du bureau, à savoir \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. L'acceptation doit se faire après une vérification approfondie de l'identité et un examen de l'origine des fonds.

A cette fin, les questionnaires (Annexe 3 personnes physiques ou annexe 4 personnes morales) inclus dans le Code AML ou des questionnaires similaires des compagnies d'assurance peuvent être utilisés. A la demande des compagnies d'assurance (voir Code AML p. 23), ces questionnaires sont également remplis à partir d'un montant de prime de 250.000 € pour un risque standard et de 100.000 € pour un risque élevé.

1. Le bureau ne noue **jamais** de relation d’affaires avec des personnes soumises aux dispositions contraignantes en matière d’embargos et de sanctions.

Ces dernières concernent :

* les personnes soupçonnées de participer à des activités terroristes. Il s’agit des personnes figurant sur la liste nationale du terrorisme. La liste actuelle peut être consultée via : [https://finances.belgium.be/fr/tresorerie/sanctions-financieres/sanctions-financi%c3%a8res-nationales-%c2%ab-la-liste-nationale-%c2%bb](https://financien.belgium.be/nl/thesaurie/financiele-sancties/nationale-financi%C3%ABle-sancties-%E2%80%98de-nationale-lijst%E2%80%99)
* les personnes concernées par les mesures d'embargo financier de l'ONU et/ou de l'UE. Un aperçu actuel peut être consulté via : [https://finances.belgium.be/fr/sur\_le\_spf/structure\_et\_services/administrations\_generales/tr%c3%a9sorerie/contr%c3%b4le-des-instruments-1-2](https://financien.belgium.be/nl/over_de_fod/structuur_en_diensten/algemene_administraties/thesaurie/controle-financi%C3%ABle-2/financi%C3%ABle).

Pour ces dispositions contraignantes en matière de sanctions et d’embargos, le bureau effectue un premier contrôle avec les moyens dont elle dispose. Dans le cadre des accords avec le secteur dans le Code AML (p. 7), l’entreprise d’assurances procède à un contrôle approfondi également pour le compte de l'intermédiaire d'assurance.

Conformément à la disposition 5.1 du présent manuel, l’AMLCO signale à la Trésorerie (SPF Finances) quand une prise de contact a eu lieu par les personnes susmentionnées au cours de laquelle il a été constaté qu’elles sont soumises aux dispositions contraignantes en matière d’embargos et de sanctions.

En complément à ce qui précède, nous appliquons pour l'acceptation des clients par notre bureau :

1. …

P. ex. vente à distance,

## **4.4 ÉTAPE 4 : VIGILANCE CONTINUE ET DÉTECTION D’OPÉRATIONS ATYPIQUES**

Une fois que le bureau a accepté le client et noué la relation d’affaires, elle exerce une vigilance continue et proportionnée au niveau de risque identifié, ce qui implique notamment :

1. **La détection d’opérations atypiques**

Pendant la relation d'affaires, une analyse approfondie des opérations est effectuée et, si nécessaire, de l'origine des fonds. Dans le cas d'opérations, il est vérifié qu'il ne s'agit pas d'opérations atypiques, c'est-à-dire d'opérations qui ne sont pas cohérentes par rapport aux caractéristiques du client, à l'objet et à la nature de la relation d'affaires ou de l'opération envisagée, ou au profil de risque du client et qui, de ce fait, sont susceptibles d’être liées au blanchiment de capitaux ou au financement du terrorisme. La constatation de ces opérations atypiques est signalée en interne (voir chapitre 5 de ce manuel).

Dans le cadre des accords dans le Code AML avec le secteur des assurances, les entreprises d’assurances avec lesquelles le bureau collabore ont un système automatisé de surveillance pour la détection d’opérations atypiques qui n’ont peut-être pas été détectées par le bureau (Surveillance de deuxième ligne).

1. **Tenue à jour des données**

Le bureau se charge de la tenue à jour des données détenues, notamment lorsque des éléments pertinents au regard de l'évaluation individuelle des risques sont modifiés.

Citons par exemple un changement de preneur d'assurance ou de bénéficiaire contractuel, une modification de l'activité professionnelle, une modification du siège social ou de la forme juridique de la personne morale, une modification de l'actionnariat.

1. **Quand faut-il mettre à jour les données d'identification ?**

Les données d’identification du preneur d’assurance, de son/ses mandataire(s) éventuel(s) et du/des bénéficiaire(s) effectif(s), ainsi que des autres informations relatives au profil du preneur d’assurance lors :

* **de chaque événement du contrat**, à savoir : l’échéance finale (liquidation ou décès), toute résiliation par le preneur d’assurance dans les 30 jours suivant la souscription du contrat d’assurance, tout rachat, toute avance, toute remise en vigueur d’un contrat réduit ou racheté ou toute modification significative du contrat. Un versement ordinaire n’est pas un événement. Un versement qui excède la finalité du contrat ou qui ne correspond pas au profil du preneur d'assurance est un événement. Un réinvestissement auprès de la même entreprise d’assurances ou dans le même groupe n’est pas un événement ;
* **de chaque nouveau contrat** ;
* **ou si cela s’avère nécessaire** (indication que les données ne sont plus à jour, sont inexactes ou mensongères ou lorsqu’on doute que la personne initialement identifiée est effectivement la personne qui souhaite réaliser l’opération).

Ne doit, entre autres, jamais être considéré(e) a priori comme anodin(e) :

* un changement d’adresse ;
* un changement de preneur d'assurance ou de bénéficiaire du contrat ;
* une modification du statut de la personne morale qui souscrit le contrat ou est le bénéficiaire

du contrat ;

* un changement significatif de l'actionnariat, sauf s'il s'agit d'une société cotée en bourse,

ou de la délégation de pouvoirs en vigueur au sein de cette personne morale.

1. **Qui fait la mise à jour des données d'identification?**

Si le preneur d’assurance s’adresse à l'intermédiaire d’assurances, ce dernier tient à jour les données d’identification du preneur d’assurance, du (des) mandataire(s) éventuel(s), du (des) bénéficiaire(s) effectif(s) et du bénéficiaire contractuel, ainsi que toute autre information relative au profil du preneur d'assurance, en ce compris le statut de PPE.

L’intermédiaire d'assurances en informe l’entreprise d'assurances, lui fournit les documents requis et les informations collectées sur le profil du preneur d'assurance25 et garde une copie pour son propre compte.

Si les données sont mises à jour par l’entreprise d’assurances (notamment dans le cas où le preneur d'assurance, le mandataire ou le bénéficiaire prendrait directement contact avec l’entreprise d'assurances), il appartient à cette dernière d’informer l'intermédiaire d'assurances et de transmettre les informations reçues.

1. **Comment mettre à jour les données d'identification ?**

La mise à jour des données et la vérification de ces données est effectuée conformément au au chapitre 4.1 du présent manuel. Les nouvelles données d’identification doivent être contrôlées au moyen d'une pièce justificative appropriée comme dans le cas d'une identification initiale.

Dans le cadre de la mise à jour des informations détenues à propos des clients, il convient également d'identifier les clients qui sont devenus des PPE, des membres de la famille de ces personnes ou des personnes connues pour être étroitement associées à ces personnes. Le cas échéant, un membre d'un niveau élevé de la hiérarchie décide de maintenir ou non la relation d'affaires et les mesures de vigilance accrue prévues.

La mise à jour des informations implique, lorsque cela est pertinent, que soit également mise

à jour l'évaluation individuelle des risques du client concerné et, le cas échéant, que l'étendue des mesures de vigilance continue mises en œuvre soit adaptée.

A cet égard, il convient d’être attentif à des clignotants éventuels. S’il constate un clignotant, l’intermédiaire d’assurances :

* informera la personne qu'il ne peut pas, sur la base de sa politique d’acceptation, procéder à l'exécution de sa demande et que celle-ci a été transmise à l'entreprise d'assurances, sans lui préciser toutefois qu'une enquête pour BC/FT est en cours ;
* transmettra simultanément le questionnaire complété, repris à l’Annexe 3 ou 4, aussi bien à son AMLCO qu’à l’entreprise d’assurances. Ces derniers examineront individuellement la nécessité d'une déclaration à la CTIF et, le cas échéant, à la Trésorerie[[19]](#footnote-19).

Si une déclaration à la CTIF a été effectuée, il convient d’attendre les instructions de cette dernière. En cas de déclaration à la CTIF par l'intermédiaire d’assurances ou l’entreprise d’assurances, chaque partie décidera au cas par cas s’il est utile, à la lumière des objectifs poursuivis, d’informer l’autre partie concernée sans toutefois en avertir ni le client ni tout autre tiers.

Si aucune déclaration n’a été faite à la CTIF, l’intermédiaire d’assurances et l’entreprise d’assurances se concertent au sujet de l’exécution de la transaction ou du paiement de la prestation.

1. **Quelles sont les conséquences si la mise à jour s’avère impossible ?**

Si les causes de l'impossibilité de satisfaire à l'obligation de mise à jour sont de nature à susciter un soupçon de BC/FT, il y a lieu d'en informer la CTIF et de ne plus accepter de primes dans le(s) contrat(s) concerné(s) après cette notification.

## **4.5 CAS PARTICULIERS DE VIGILANCE ACCRUE**

Le bureau fait toujours preuve de vigilance accrue dans les cas suivants :

1. **Un pays tiers à haut risque**Dans le cadre des relations avec des personnes physiques ou morales ou avec des constructions juridiques qui sont établies dans un pays tiers à haut risque[[20]](#footnote-20). Plusieurs organismes peuvent désigner des pays comme étant à haut risque. Il s’agit du GAFI (organisation internationale basée à Paris), de la Commission européenne et du Conseil National de Sécurité belge. Ce dernier n'a pas encore établi sa propre liste.  
   Pour rationaliser tout cela, ces données sont rassemblées sur le site du SPF Finances / Trésorerie [https://finances.belgium.be/fr/pays-hauts-risques](https://financien.belgium.be/nl/landen-met-een-hoog-risico)  
     
   Dans le cadre d'une relation d'affaires avec un client ou de transactions relatives à un pays tiers à haut risque, les mesures[[21]](#footnote-21) de vigilance renforcée suivantes sont appliquées :

* 1° obtenir des informations supplémentaires sur le client et sur le ou les bénéficiaires effectifs ; 2° obtenir des informations supplémentaires sur la nature envisagée de la relation d'affaires ;
* 3° obtenir des informations sur l’origine des fonds et l’origine du patrimoine du client et du ou des bénéficiaires effectifs ;
* 4° obtenir des informations sur les raisons des opérations envisagées ou réalisées ;
* 5° obtenir d'un membre d'un niveau élevé de la hiérarchie l'autorisation de nouer ou de maintenir la relation d'affaires ;
* 6° mettre en œuvre une surveillance renforcée de la relation d'affaires en augmentant le nombre et la fréquence des contrôles effectués et en déterminant les schémas de transaction qui nécessitent un examen plus approfondi ;
* 7° veiller à ce que, le cas échéant, le premier paiement soit réalisé par l'intermédiaire d'un compte ouvert au nom du client auprès d'un établissement de crédit soumis à des normes de vigilance à l'égard de la clientèle au moins aussi élevées que celles prévues dans la Loi BC/FT.

1. **Les paradis fiscaux**

Dans le cadre de relations d’affaires et d’opérations liées à un État à fiscalité inexistante ou peu élevée[[22]](#footnote-22), les paradis fiscaux

Ceci est établi dans l’Arrêté Royal du 1er mars 2016. (<https://www.etaamb.be/fr/arrete-royal-du-01-mars-2016_n2016003097.html>)

La vigilance accrue signifie qu'il y a des enquêtes supplémentaires sur l'identité des personnes impliquées et l'origine des fonds.

1. **Les Personnes Politiquement Exposées**

Les relations d'affaires et les transactions avec des personnes politiquement exposées (PPE)[[23]](#footnote-23), les membres de leur famille et leurs associés constituent un risque élevé.

Une PPE est une personne physique qui occupe ou a occupé une fonction publique importante.

La loi comprend une liste de fonctions :

1° les chefs d'État, les chefs de gouvernement, les ministres et les secrétaires d'État :

a) le Roi ;

b) le Premier Ministre, Ministre-Président, Vice-Premier Ministres, Vice-Ministres-Présidents, Ministres et secrétaires d'Etat;

2° les parlementaires ou les membres d’organes législatifs similaires :

a) le président de la Chambre, le président du Sénat, le Président du Parlement, les membres du parlement, les sénateurs, les sénateurs cooptés, les présidents de commissions et membres de commissions;

3° les membres des organes dirigeants des partis politiques :

a) les membres de la direction du parti, le conseil politique, le comité de direction, la gestion journalière et le secrétariat du parti;  
4° les membres des cours suprêmes, des cours constitutionnelles ou d'autres hautes juridictions, y compris administratives, dont les décisions ne sont pas susceptibles de recours, sauf circonstances exceptionnelles :

a) conseiller à la Cour de cassation (en ce compris le premier président, le président et les présidents de section);

b) conseiller à la Cour d'appel (en ce compris le premier président et les présidents de chambre);

c) conseiller à la Cour du travail (en ce compris le premier président et les présidents de chambre);

d) conseillers suppléants de ces trois cours ;

e) le premier Président, les présidents, les présidents de chambre, les conseillers d'Etat, les assesseurs et auditeurs au Conseil d'Etat;

5° les membres des cours des comptes et des conseils ou directoires des banques centrales :

a) le Gouverneur et les membres du Comité de direction et du Conseil de régence de la Banque nationale de la Belgique ;

b) le premier président, les présidents et conseillers à la Cour des comptes ;

6° les ambassadeurs, les consuls, les chargés d'affaires et les officiers supérieurs des forces armées :

a) les ambassadeurs, les consuls et les chargés d'affaires ;

b) les officiers revêtus du grade de général ou d'amiral qui sont désignés par le Roi pour exercer une fonction spécifique ;

c) les officiers revêtus du grade de lieutenant-général ou vice-amiral qui sont désignés à leur emploi, selon le cas, par le Roi ou le ministre de la Défense;

d) les officiers revêtus du grade de général-major ou amiral de division qui sont désignés à leur emploi, selon le cas, par le Roi ou le ministre de la Défense;  
e) les officiers revêtus du grade de général de brigade ou amiral de flotille qui sont désignés par le Roi pour exercer une fonction spécifique;

7° Les membres des organes d'administration, de direction ou de surveillance des entreprises publiques :

a) le Chief Executive Officer, l'Administrateur Délégué, le président, les administrateurs et membres du conseil d'administration, le président et les membres du comité de direction et du comité exécutif, les commissaires au gouvernement;  
b) les directeurs, les directeurs adjoints et les membres du conseil d'une organisation internationale établie sur le territoire belge, ou les personnes qui occupent une position équivalente en son sein.

La même vigilance s'applique à :

* + Les membres de la famille des PPE, à savoir le conjoint ou une personne considérée comme équivalente au conjoint, les enfants et leurs conjoints ou personnes considérées comme équivalentes au conjoint et les parents[[24]](#footnote-24).
  + Personnes connues pour être des proches collaborateurs[[25]](#footnote-25) de personnes politiquement exposées

Cette obligation s’applique jusque 12 mois après que la personne politiquement exposée a cessé d’exercer une fonction politique exposée.

Dans le cas de relations d'affaires avec des personnes politiquement exposées, les mesures de vigilance accrue suivantes s'appliquent :

* Obtenir l'autorisation de la direction générale pour établir ou poursuivre des relations d'affaires avec ces personnes
* Déterminer l'origine des actifs et des fonds utilisés dans les relations d'affaires ou les transactions avec ces personnes
* Exercer une surveillance renforcée sur la relation d'affaires.

Pour déterminer la qualité de PPE, un questionnaire est toujours présenté dans le cadre de l'identification, dans lequel il est examiné si le client, un mandataire du client ou le bénéficiaire effectif a la qualité de PPE. Au moment du paiement, les compagnies d'assurance vérifient si le bénéficiaire est un PPE.

Pour réaliser cette identification, les propositions d'assurance des compagnies d'assurance contiennent :

* soit la définition de personne politiquement exposée au sens de la loi BC/FT (cf. Annexe 6) ;
* soit une série de questions (exemples - cf. Annexe 6) inspirées de cette définition, afin de déterminer si le preneur d’assurance ou son mandataire est une personne politiquement exposée. Si le preneur d’assurance reconnaît par sa signature relever de la définition ou répond positivement à l’une de ces questions, l’intermédiaire d’assurances remplira également le questionnaire « personne physique » (Annexe 3 du code AML) ou « personne morale » (Annexe 4 du code AML) et le transmettra à son AMLCO, ainsi qu’à l’entreprise d’assurances, lorsqu’une relation a déjà été établie avec cette dernière.

L’intermédiaire d’assurances doit interroger le client ou le mandataire afin de vérifier si celui-ci est une PPE. L’entreprise d’assurances vérifie lors du versement si le bénéficiaire est une PPE.

1. **Trusts, fiducies, associations de fait, fondations privées et fondations d’utilité publique, asbl et aisbl, sociétés momentanées et sociétés simple**

Dans le code AML, il est recommandé de ne pas souscrire de contrats avec :

* des trusts, fiducies et entités similaires ;
* des associations de fait sans véritable organisation.   
  Il est question d’une véritable organisation si l’association dispose par exemple d’un ou plusieurs mandataires généraux et/ou de statuts.

Dans les autres cas, une vigilance particulière est de mise en place.

* 1. **Quand une preuve de l’origine des fonds doit-elle être demandée ?**

Une preuve de l’origine des fonds doit être demandée en cas de risque plus élevé.

Le code anti-blanchiment prévoit[[26]](#footnote-26) qu'un certificat d'origine des fonds est demandé lorsqu'au moins deux des trois conditions suivantes sont remplies :

* en cas de présence d'un clignotant ;
* lorsque la prime > 250.000 €. Attention, il s’agit du montant total de la prime que le client

souhaite investir. Si cet investissement a lieu par le biais de plusieurs contrats auprès de différentes entreprises d’assurances, seul l’intermédiaire d’assurances en est informé et c’est à lui également de compléter le questionnaire[[27]](#footnote-27). Les entreprises d’assurances concernées ne sont elles-mêmes pas à même de détecter que le montant de la prime est dépassé et qu'une vigilance accrue est nécessaire ;

* malgré un questionnaire soigneusement complété, des doutes subsistent sur l'origine des fonds.

Cette preuve peut être un acte de vente, un acte d’héritage...

* 1. **LA COOPÉRATION AVEC DES TIERS INTRODUCTEURS**

Les obligations de vigilance peuvent être remplies par des tiers introducteurs[[28]](#footnote-28) avec lesquels le bureau collabore. La responsabilité finale reste toutefois à charge du bureau.

L’AMLCO vérifie préalablement à la coopération avec le tiers introducteur que cette entité relève du champ d’application de la Loi et que le tiers introducteur a une obligation de conservation de ses documents.

Si le bureau fait appel à un tiers introducteur, celui-ci doit s'engager par écrit à ce que :

* Le tiers introducteur transmette immédiatement les informations concernant l'identité du client et de ses mandataires et bénéficiaires effectifs, et concernant les caractéristiques du client et l'objet et la nature envisagée de la relation d'affaires, qui sont nécessaires à l'exécution des obligations de vigilance confiées au tiers introducteur
* Le tiers introducteur transmette sans délai au bureau, à première demande, une copie des documents probants ou sources fiables d'information au moyen desquels il a vérifié l'identité du client et, le cas échéant, de ses mandataires et bénéficiaires effectifs.

# ANALYSE DES OPÉRATIONS ATYPIQUES ET DÉCLARATION DE SOUPCONS

## **5.1 ANALYSE D’OPÉRATIONS ATYPIQUES ET DÉCLARATION INTERNE**

Les collaborateurs analysent les opérations dans le cadre de la vigilance continue.

Dans ce cadre, ils examinent s'il s'agit ou non d'une opération atypique. En cas de risque accru ou si un feu clignotant est détecté, un examen supplémentaire sera effectué, auquel cas le questionnaire Annexe 3 (personne physique) et Annexe 4 (personne morale) du Code AML peut être utilisé.

Une opération atypique est une opération qui n’est pas cohérente par rapport aux caractéristiques du client, à l'objet et à la nature de la relation d'affaires ou de l'opération concernée, ou au profil de risque du client et qui, de ce fait, est susceptible d’être liée au blanchiment de capitaux ou au financement du terrorisme[[29]](#footnote-29) ;

Le Code AML du secteur des assurances reprend des clignotants qui peuvent indiquer une opération atypique :

La détection se fait par la supervision de première ligne (en contact direct avec le client) et la supervision de deuxième ligne (via un logiciel adapté). Dans le code anti-blanchiment, il a été convenu que la compagnie d'assurance effectuera le contrôle de deuxième ligne via un système de contrôle informatisé.

Ces opérations atypiques/clignotants qui sont spécifiques aux intermédiaires en assurances sont énumérés ci-dessous :

**Enquête complémentaire lors de l'acceptation de clients (nouveaux clients)**

* le montant de la prime est ≥ 250 000 € en cas de risque standard ;
* le montant de la prime est ≥ 100 000 € en cas de risque élevé ;
* pour chaque situation où la totalité des primes versées par un client au cours des 12 derniers mois pour un risque standard ou élevé est supérieure à 250 000 euros ;
* personnes pour lesquelles le même assureur ou le même groupe a déjà averti la CTIF d'une connaissance ou d'un soupçon de BC/FT ;
* personnes dont le document d’identification probant contient des « éléments suspects » (le document semble manipulé, documents probants périmés…) ;
* nouveaux clients qui concluent une relation d'affaires « à distance », où l’on suppose que le client opte pour celle-ci afin de dissimuler sa véritable identité ;
* personnes enregistrées, établies ou qui ont leur domicile dans un pays hors de l’EEE ;
* personnes pour lesquelles il apparaît que le contact avec l'intermédiaire ou l’entreprise d'assurances s'est déroulé « dans des circonstances suspectes » (par exemple : le client est toujours accompagné d'une autre personne et/ou semble être sous pression) ;
* personnes considérées comme PPE (personnes politiquement exposées) ;
* personnes qui n'indiquent pas de domicile fixe ;
* certaines structures sans personnalité juridique ;
* constructions juridiques avec ou sans personnalité juridique qui ne sont pas suffisamment claires ;
* personnes enregistrées, établies ou qui ont leur domicile dans un pays ou territoire qualifié par la BNB ou le GAFI de pays ou territoire non coopératif en matière de lutte contre le BC/FT ou qui requiert une vigilance accrue. [[30]](#footnote-30)
* Le client a des liens avec un paradis fiscal.[[31]](#footnote-31)

**Refus auprès de clients existants dans le cadre de la vigilance continue**

* opérations effectuées par des personnes agissant au nom et pour le compte du preneur d'assurance ou du bénéficiaire, à l'exception des opérations effectuées par des représentants légaux, des mandataires judiciaires, des personnes soumises aux dispositions de la Loi et personnes présentant un lien familial ou socio-économique avec ce preneur d'assurance ou ce bénéficiaire ;
* opérations effectuées par des preneurs d'assurance ou des bénéficiaires contractuels « accompagnés et contrôlés » ;
* refus de collaboration de la part du preneur d'assurance ;
* le preneur d'assurance ou le bénéficiaire contractuel refuse de répondre à des questions supplémentaires, comme celles en rapport avec son profil de client ;
* (tentative de) paiement en espèces (sauf en cas d'épargne-pension) ;
* paiement par une banque établie dans un pays ou un territoire considéré par le GAFI comme présentant un risque élevé de BC/FT, ou figurant sur une liste d’Embargo Financier ou Liste du Terrorisme publiée par la Trésorerie ;
* opérations dont l’origine des fonds n’est pas expliquée par le preneur d’assurance (tant en matière d’assurances-vie que de crédits hypothécaires[[32]](#footnote-32)) ;
* opérations qui ne sont pas cohérentes avec le profil du preneur d’assurance connu de l’assureur ou de l’intermédiaire (par exemple, opérations qui ne sont pas cohérentes avec son activité professionnelle).

**Enquête complémentaire auprès de clients existants dans le cadre de la vigilance continue**

* le montant de la prime est ≥ 250 000 € en cas de risque standard ;
* le montant de la prime est ≥ 100 000 € en cas de risque élevé ;
* pour chaque situation où la totalité des primes versées par un client au cours des 12 derniers mois pour un risque standard ou élevé est supérieure à 250 000 euros ;
* modifications inhabituelles du contrat (par exemple, la durée initiale du contrat est raccourcie sans raison fondée, un changement de bénéficiaire atypique…) ;
* opérations pour lesquelles le preneur d'assurance ou le bénéficiaire contractuel demande à plusieurs reprises un règlement accéléré (sauf s'il existe une justification objective à cet égard) ;
* contrat dénué d'intérêt réel pour le preneur d'assurance ;
* le preneur d'assurance montre un intérêt (anormal) pour un rachat non planifié ;
* le preneur d’assurance choisit une tarification inhabituelle ou défavorable ;
* paiement par le biais d’un compte dont le titulaire n’est pas le preneur d’assurance (sauf situations prévues dans la politique de l’assureur) ;
* paiement en débitant un compte ouvert auprès d'un agence de change ;
* paiement par le biais d’un compte de transit sans indication du titulaire ;
* paiement par le biais d'une banque qui n’est pas membre du GAFI, qui n'est pas considéré comme un pays ou territoire non coopératif ou par le biais d'une banque d'un pays figurant sur une liste d’Embargo Financier de la BNB ;
* plusieurs souscriptions en peu de temps ;
* absence de lien familial ou socio-économique entre le preneur d'assurance et le bénéficiaire (effectif) ;
* les paiements de primes entraînent un dépassement de la règle des 80 % ;
* le versement est demandé sur un compte qui n'est pas ouvert au nom du preneur d'assurance ou du bénéficiaire (effectif) ;
* le versement est demandé sur un compte ouvert dans un État non membre de l’Union européenne ou du GAFI, en particulier sur un compte dans un pays soumis à un embargo financier ;
* le montant de l’opération ne correspond pas au profil économique de la personne concernée ;
* le prélèvement implique une pénalité de rachat considérable (sauf si réemploi auprès du même assureur ou groupe) ;
* le prélèvement intervient peu de temps après la souscription du contrat ;
* le remboursement d'un crédit hypothécaire dans les trois ans suivant la conclusion du crédit ;
* aucun lien stable et logique entre la durée planifiée du séjour en Belgique et la durée du contrat ;
* paiement par le biais d’un compte d'un intermédiaire ;
* paiement au profit d’un bénéficiaire contractuel qui est l’actionnaire de contrôle ou administrateur du preneur d’assurance-personne morale, sauf dans le cadre d’une assurance du deuxième pilier qui respecte la règle des 80 % ;
* la souscription d'un contrat du deuxième pilier ou le versement d'une importante prime de back-service par un preneur d'assurance qui se trouve dans une situation structurelle financièrement précaire ;
* les contrats d’assurance-vie individuels avec prime de risque dans le cadre desquels la couverture décès réduit fortement le rendement et la couverture décès est résiliée dans les 1 an suivant la souscription du contrat ;
* constructions juridiques avec ou sans personnalité juridique qui ne sont pas suffisamment claires ;
* personnes enregistrées, établies ou ayant leur domicile dans un pays ou territoire qualifié par le Groupe d’action financière contre le blanchiment de capitaux comme pays ou territoire qui nécessite une vigilance accrue ou exécution ou demande d’un paiement par l’intermédiaire d’une banque établie dans l’un de ces pays ou territoires.
* le preneur d'assurance demande à l'entreprise d'assurances une attestation de placement des fonds, à l'exception des attestations fiscales ;
* le prélèvement implique une pénalité de rachat considérable (sauf si réemploi auprès du même assureur ou groupe) ;
* le client a des liens avec un paradis fiscal.[[33]](#footnote-33)

La CTIF a elle aussi énuméré à l’égard des assurances-vie une série de pratiques courantes pouvant servir de point de départ.[[34]](#footnote-34)

* À la conclusion du contrat d’assurance, le client se préoccupe avant tout de son droit de résilier le contrat avant terme et du montant dont il pourra disposer à la résiliation.
* Un contrat d'assurance-vie avec des primes très élevées est conclu.
* La souscription d'un contrat d'assurance est suivie par un rachat en demandant que le paiement se fasse par chèque au profit d'un tiers pour un montant disproportionné par rapport aux revenus du signataire.
* Plusieurs contrats d'assurance sont souscrits sur une courte période
* Il est souscrit un contrat d'assurance avec paiement des primes à partir de l’étranger, notamment d’un centre financier offshore.
* Le client est accompagné d’un tiers lors de la conclusion du contrat.
* Le preneur d’assurance n’est pas le titulaire du compte par le biais duquel s’effectue le paiement des primes.
* Le bénéficiaire initial d’une police est remplacé en cours de contrat par une personne sans lien évident avec le signataire.
* Il est demandé de payer les primes en espèces.

OPTION :

Vu la nature et la taille de notre bureau, la liste suivante de critères pour les opérations atypiques s’applique en particulier :

…

Le bureau veille à ce que les informations fournies par des lanceurs d'alerte soient effectivement examinées et que les mesures nécessaires soient prises pour remédier aux situations anormales.

Ces notifications sont mentionnées dans le rapport annuel d’activité.

La personne qui signale une infraction de bonne foi sera protégée des mesures négatives découlant de ce signalement ou en rapport avec celui-ci.

Les collaborateurs sont encouragés à signaler en interne (« whistleblowing ») une opération qu’ils considèrent comme atypique ou le fait de ne pas pouvoir satisfaire aux obligations de vigilance. Les collaborateurs sont protégés contre toute menace ou tout acte d’agression, et en particulier contre toute action préjudiciable ou discriminatoire de l’employeur. La déclaration peut se faire de manière anonyme.

La déclaration de l'opération atypique se fait directement par le collaborateur à l'AMLCO sans suivre la voie hiérarchique.

L’analyse de l’opération atypique a lieu sous la responsabilité de l’AMLCO afin de déterminer si ces opérations peuvent être suspectées d'être liées au blanchiment de capitaux ou au financement du terrorisme. Il établit à ce sujet un rapport écrit.

L’AMLCO tient un registre dans lequel sont consignées les infractions et sont mentionnées les suites qui y sont données ou la raison pour laquelle il n’a pas été jugé nécessaire de le faire (p. ex. la raison pour laquelle on a estimé que le signalement n’était pas fondé).

## **5.2 DÉCLARATION EXTERNE DE SOUPCONS À LA CTIF**

Sur la base de l'analyse de la notification interne de l'opération atypique (5.1), l'AMLCO signale à la CTIF, lorsque le bureau sait, soupçonne ou a des motifs raisonnables de soupçonner :

* que des fonds, quel qu'en soit le montant, sont liés au blanchiment de capitaux ou au financement du terrorisme ;
* que des opérations ou tentatives d'opérations sont liées au blanchiment de capitaux ou au financement du terrorisme ;
* qu'un fait dont elle a connaissance est lié au blanchiment de capitaux ou au financement du terrorisme.

L'obligation de déclaration à la CTIF ne requiert pas l'identification, par le bureau, de l'activité criminelle sous-jacente au blanchiment de capitaux.

La déclaration à la CTIF est en principe effectuée par l'AMLCO, mais si celui-ci ne peut le faire, l'obligation incombe à tout le monde.

La déclaration à la CTIF se fait par écrit. L’AMLCO met à la disposition des collaborateurs un modèle de document qui permet de communiquer à la CTIF le soupçon de BC/FT.

Le bureau effectue la déclaration avant l'exécution de l'opération et fait également savoir à la CTIF quand l'opération doit être exécutée, à moins qu'il ne soit pas possible, en raison de sa nature, de différer l'exécution de l'opération ou à moins que le report puisse être de nature à empêcher la poursuite de ses bénéficiaires.

La CTIF peut s'opposer à l'exécution de toute opération et détermine quelles opérations sont concernées par l'opposition, et informe immédiatement le bureau de sa décision par écrit.

Cette opposition dure au maximum 5 jours ouvrables, sauf si elle est prolongée par le procureur du Roi.

Le bureau ne révèle ni au client concerné ni à des tiers que des informations ou renseignements sont, seront ou ont été transmis à la CTIF ou qu'une analyse pour blanchiment de capitaux ou pour financement du terrorisme est en cours ou susceptible de l'être.

Le fait de dissuader un client de participer à une activité illégale ne constitue pas une divulgation au sens de la loi.

La communication d'informations effectuée de bonne foi à la CTIF n’entraîne en aucun cas une responsabilité civile, pénale ou disciplinaire. La CTIF s'efforce de garantir l'anonymat des déclarants.

Contact pour déclaration à la CTIF :   
Cellule de traitement des informations financières  
Avenue de la Toison d’Or, 55 / boîte 1 – 1060 Bruxelles

Tél. : + 32 (0) 2 533 72 11  
Fax : +32 (0) 2 533 72 00  
E-mail : [info@ctif-cfi.be](mailto:info@ctif-cfi.be)

## **5.3 DÉCLARATION EXTERNE À LA TRÉSORERIE (SPF FINANCES)**

En principe, l'AMLCO notifie l'Administration générale du Trésor lorsqu'il y a un contact avec des personnes soumises aux dispositions contraignantes des sanctions financières et des embargos contre des pays et des personnes. Sur la base du code anti-blanchiment, la compagnie d'assurance assume cette tâche de contrôle et de notification.

Il s'agit de pays et de personnes coupables notamment de violations des droits de l'homme, de déstabilisation d'États souverains, etc. Ces listes sont également disponibles auprès du SPF Finances. ([https://finances.belgium.be/fr/sur\_le\_spf/structure\_et\_services/administrations\_generales/tr%c3%a9sorerie/contr%c3%b4le-des-instruments-1-2](https://financien.belgium.be/nl/over_de_fod/structuur_en_diensten/algemene_administraties/thesaurie/controle-financi%C3%ABle-2/financi%C3%ABle)). Ces listes émanent des Nations Unies et de l'Union européenne. Ces sanctions et embargos comprennent le gel de capitaux ou une interdiction de nouer des relations avec des clients.

Outre les listes internationales de pays, il existe aussi **une liste de personnes** qui se sont vu imposer des mesures dans la lutte contre le terrorisme. Les avoirs financiers de ces personnes sont gelés. Il s'agit d'une liste nationale de noms et de données d'identité. Aucune relation d’affaires n’est nouée avec ces personnes. ([https://finances.belgium.be/fr/tresorerie/sanctions-financieres/sanctions-financi%C3%A8res-nationales-%C2%AB-la-liste-nationale-%C2%BB](https://financien.belgium.be/sites/default/files/20191108-%20Nationale%20lijst.xlsx))

La source officielle de ces informations est le site web du SPF Finances (finances.belgium.be).

Contact pour déclaration à la Trésorerie (SPF Finances)  
E-mail : [quesfinvragen.tf@minfin.fed.be](mailto:quesfinvragen.tf@minfin.fed.be)

# OBLIGATION DE CONSERVATION

Le bureau conserve :

* les informations d'identification et une copie des documents probants ou du résultat de la consultation du registre national / registre UBO ;
* les pièces justificatives et les enregistrements des opérations qui sont nécessaires pour identifier et reconstituer précisément les opérations effectuées ;
* le rapport sur les opérations atypiques établi par le bureau ;

Et cela pendant 10 ans à dater de la fin de la relation d'affaires.

Les données sont conservées \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (indiquez sur quel(s) support(s)).

Le bureau effacera les données à caractère personnel à l’issue de la période de conservation.

1. **RAPPORT D’ACTIVITÉ**

Une fois par an, l’AMLCO soumet un rapport d’activité au haut dirigeant responsable. Il y note les éventuelles adaptations à l'évaluation globale des risques, les déclarations d'opérations atypiques et les initiatives de formation prises.

Ce rapport doit permettre au haut dirigeant responsable de prendre connaissance de l'évolution des risques de BC/FT que court le bureau et de s'assurer que les politiques, procédures et mesures de contrôle interne appliquées sont appropriées.

Cette procédure interne a été approuvée par la direction effective le ………………………………..

Signature :

…

1. Art. 2 de la Loi [↑](#footnote-ref-1)
2. Art. 3 de la Loi [↑](#footnote-ref-2)
3. Art. 5, 19° de la Loi [↑](#footnote-ref-3)
4. Art. 5, 17° de la Loi [↑](#footnote-ref-4)
5. Art. 8 de la Loi [↑](#footnote-ref-5)
6. Si la nature et la taille du bureau le justifient, il convient de prévoir (1) une fonction d’audit indépendante chargée de tester les politiques, procédures et mesures de contrôle interne visées et (2) des procédures de vérification, lors du recrutement et de l’affectation des membres de son personnel ou de la désignation de ses agents ou distributeurs, que ces personnes disposent d'une honorabilité adéquate en fonction des risques liés aux tâches et fonctions à exercer ; [↑](#footnote-ref-6)
7. L’AMLCO dispose : (1) De l’honorabilité professionnelle nécessaire pour exercer cette fonction avec intégrité, (2) De l’expertise adéquate, de la connaissance du cadre légal et réglementaire belge en matière de prévention du blanchiment de capitaux et du financement du terrorisme, (3) de la disponibilité nécessaire pour exercer la fonction (4) du niveau hiérarchique et des pouvoirs au sein du bureau, qui sont nécessaires à l’exercice effectif, indépendant et autonome de ces fonctions et (5) du pouvoir de proposer, de sa propre initiative, à l’organe légal d’administration ou à la direction effective de l’entité assujettie, toutes mesures nécessaires ou utiles, en ce compris la mise en œuvre des moyens requis, pour garantir la conformité et l’efficacité des mesures internes de lutte contre le BC/FT. [↑](#footnote-ref-7)
8. Art. 3, 1° du Règlement du 3 juillet 2018, *M.B.,* 7 août 2018 [↑](#footnote-ref-8)
9. Art. 3 et 8 du Règlement du 3 juillet 2018, *M.B.,* 7 août 2018 [↑](#footnote-ref-9)
10. Circulaire FSMA du 27 juin 2019, n° 2019/12, p. 4, disponible sur [https://www.fsma.be/fr/lutte-contre-le-blanchiment-de-capitaux-et-le-financement-du-terrorisme](https://www.fsma.be/nl/strijd-tegen-witwassen-van-geld-en-financiering-van-terrorisme) (rubrique « Circulaires et communications » > « Circulaires ») ; Newsletter intermédiaires de juillet 2019 « 2e étape : définissez votre cadre organisationnel » disponible via [https://www.fsma.be/fr/intermediaire-dassurances](https://www.fsma.be/nl/verzekeringstussenpersoon) (rubrique « Newsletter »). [↑](#footnote-ref-10)
11. Article 4 du règlement du 3 juillet 2018. [↑](#footnote-ref-11)
12. Article 17 de la loi du 18 septembre 2017. [↑](#footnote-ref-12)
13. <https://www.gleif.org/en/about/this-is-gleif>. [↑](#footnote-ref-13)
14. [https://economie.fgov.be/fr/themes/entreprises/banque-carrefour-des](https://economie.fgov.be/nl/themas/ondernemingen/kruispuntbank-van). [↑](#footnote-ref-14)
15. <https://www.gleif.org/en/about/this-is-gleif>. [↑](#footnote-ref-15)
16. https://www.itsme.be/fr/security [↑](#footnote-ref-16)
17. Avec checkdoc.be, vous pouvez vérifier si un document d'identité belge est connu des autorités comme étant volé, perdu, expiré, invalide ou non délivré. [↑](#footnote-ref-17)
18. Tels que le passeport (pour les personnes résidant à l'étranger), un certificat qualifié, .. [↑](#footnote-ref-18)
19. *La déclaration à la Trésorerie sera effectuée par l’entreprise d’assurances, au nom de l’entreprise d'assurances et de l'intermédiaire concerné.* [↑](#footnote-ref-19)
20. *Art. 38, al. 1er de la Loi* [↑](#footnote-ref-20)
21. Ces mesures supplémentaires ont été introduites par la loi du 20 juillet 2020 [↑](#footnote-ref-21)
22. Art. 39, 1° et 2° de la Loi [↑](#footnote-ref-22)
23. Art. 41 de la Loi [↑](#footnote-ref-23)
24. Art. 4.29° de la Loi [↑](#footnote-ref-24)
25. Art. 4.30° de la Loi [↑](#footnote-ref-25)
26. P. 22 du code AML [↑](#footnote-ref-26)
27. Le Code AML fait référence aux questionnaires de l'annexe 3 (personne physique) et de l'annexe 4 (personne morale). [↑](#footnote-ref-27)
28. Art. 42 de la Loi [↑](#footnote-ref-28)
29. Règlement art. 1, 7° [↑](#footnote-ref-29)
30. finances.belgium.be/fr/pays-hauts-risques. [↑](#footnote-ref-30)
31. [https://www.etaamb.be/fr/arrete-royal-du-01-mars-2016\_n2016003097.html](https://www.etaamb.be/nl/koninklijk-besluit-van-01-maart-2016_n2016003097.html) [↑](#footnote-ref-31)
32. Cela vaut uniquement pour l’assureur qui octroie des crédits hypothécaires, pas pour un intermédiaire en assurances [↑](#footnote-ref-32)
33. [https://www.etaamb.be/fr/arrete-royal-du-01-mars-2016\_n2016003097.html](https://www.etaamb.be/nl/koninklijk-besluit-van-01-maart-2016_n2016003097.html) [↑](#footnote-ref-33)
34. CTIF juillet 2016 : blanchiment d'argent et assurance-vie : une description des méthodes de blanchiment d'argent utilisées. [↑](#footnote-ref-34)