Politique en matiere de la lutte contre le blanchiment de capitaux et le financement du terrorisme

Xerius Risk Solutions — BE1019111989 — RPM Anvers

Sommaire

Obligations générales en matière de BC/FT

Organisation et contrôle interne

Xerius Risk Solutions (XRS) dispose :

- d'une politique générale en matière de BC/FT ;
- d'une procédure générale, ainsi que de quelques procédures spécifiques pour les collaborateurs au niveau opérationnel.

Ces documents font l'objet d'une évaluation annuelle par l'AMLCO. Si ces évaluations révèlent des manquements ou des lacunes dans la politique et/ou les procédures, des mesures appropriées seront prises pour y remédier. Le principe « appliquer ou expliquer » s'applique à cet égard.

Les collaborateurs de XRS sont régulièrement sensibilisés (au moins une fois par an) et suivent, si nécessaire, des formations externes en matière de BC/FT. Chaque collaborateur de XRS est en possession d'une attestation BC/FT (PCP module 1 ou équivalent par diplôme) ; chaque collaborateur débutant, qui ne dispose pas encore de cette attestation, est censé l'obtenir au plus tard dans l'année qui suit son engagement.

Les attestations obtenues sont remises à l'AMLCO et conservées par celui-ci.

Évaluation globale des risques

L'AMLCO procède à une évaluation globale des risques pour identifier et évaluer les différents risques en matière de BC/FT auxquels l'entreprise est exposée. Cette évaluation globale des risques est mise à jour régulièrement (au moins une fois par an).

Dans le cadre de l'évaluation globale des risques, l'AMLCO tient toujours compte des variables suivantes[1] :

- la finalité d'un compte ou d'une relation ;
- le niveau d'actifs déposés par un client ou le volume des opérations effectuées ;
- la régularité ou la durée de la relation d'affaires.

Dans le cadre de l'évaluation globale des risques, l'AMLCO peut choisir de tenir compte des facteurs suivants indicatifs d'un risque potentiellement moins élevé2 :

- facteurs de risques inhérents aux clients :
  - sociétés cotées sur un marché réglementé et soumises à des obligations d'information, comportant l'obligation d'assurer une transparence suffisante des bénéficiaires effectifs ;
  - administrations ou entreprises publiques ;
  - clients qui résident dans des zones géographiques à risque moins élevé ;
- facteurs de risques liés aux produits, aux services, aux transactions ou aux canaux de distribution :
  - contrats d'assurance-vie dont la prime est faible ;
  - contrats d'assurance retraite qui ne comportent pas de clause de rachat anticipé et qui ne peuvent pas être utilisés comme garantie ;
  - régimes conventionnels de retraite, fonds de retraite ou dispositifs similaires versant des prestations de retraite aux salariés, pour lesquels les cotisations se font par déduction du salaire et dont les règles ne permettent pas aux bénéficiaires de transférer leurs droits ;
  - produits ou services financiers qui fournissent des services définis et limités de façon pertinente à certains types de clients, en vue d'un accès accru à des fins d'inclusion financière ;
  - produits pour lesquels les risques de BC/FT sont contrôlés par d'autres facteurs tels que l'imposition de limites de chargement ou la transparence en matière.

1 Art. 16, §2 + annexe 1 de la Loi anti-blanchiment.
2 Art. 16, §2 + annexe 2 de la Loi anti-blanchiment.

- facteurs de risque géographiques :
  - États membres ;
  - pays tiers dotés de systèmes efficaces de lutte contre le BC/FT ;
  - pays tiers identifiés par des sources crédibles comme présentant un faible niveau de corruption ou d'autre activité criminelle ;
  - pays tiers qui, d'après des sources crédibles telles que des évaluations mutuelles, des rapports d'évaluation détaillée ou des rapports de suivi publiés, ont des exigences de lutte contre le BC/FT correspondant aux recommandations révisées du GAFI et qui assurent la mise en oeuvre effective de ces exigences.

Dans le cadre de l'évaluation globale des risques, l'AMLCO tient compte des facteurs suivants indicatifs d'un risque potentiellement plus élevé3 :

- facteurs de risques inhérents aux clients :
  - relation d'affaires se déroulant dans des circonstances inhabituelles ;
  - clients résidant dans des zones géographiques à haut risque ;
  - personnes morales ou constructions juridiques qui sont des structures de détention d'actifs personnels ;
  - sociétés dont le capital est détenu par des actionnaires apparents (« nominee shareholders ») ou représenté par des actions au porteur ;
  - activités nécessitant beaucoup d'espèces ;
  - sociétés dont la structure de propriété paraît inhabituelle ou exagérément complexe au regard de la nature de leurs activités.
- facteurs de risques liés aux produits, aux services, aux transactions ou aux canaux de distribution :
  - services de banque privée ;
  - produits ou transactions susceptibles de favoriser l'anonymat ;
  - relations d'affaires ou opérations qui n'impliquent pas la présence physique des parties et qui ne sont pas assorties de certaines garanties telles qu'une signature électronique ;
  - paiements reçus de tiers inconnus ou non associés ;
  - nouveaux produits et nouvelles pratiques commerciales, notamment les nouveaux mécanismes de distribution, et utilisation de technologies nouvelles ou en cours de développement pour des produits nouveaux ou préexistants.
- facteurs de risque géographiques :
  - pays identifiés par des sources crédibles, telles que des évaluations mutuelles, des rapports d'évaluation détaillée ou des rapports de suivi publiés, comme n'étant pas dotés de systèmes efficaces de lutte contre le BC/FT ;
  - pays identifiés par des sources crédibles comme présentant des niveaux significatifs de corruption ou d'autre activité criminelle ;
  - pays faisant l'objet de sanctions, d'embargos ou d'autres mesures similaires imposés, par exemple, par l'Union européenne ou par les Nations unies ;
  - pays qui financent ou soutiennent des activités terroristes ou sur le territoire desquels opèrent des organisations terroristes désignées.

L'évaluation globale des risques est documentée, tenue à jour et mise à la disposition des autorités de contrôle, à savoir la FSMA et la BNB.

3 Art. 16, §2 + annexe 3 de la Loi anti-blanchiment.

Obligations spécifiques en matière de BC/FT

Identification et vérification de l'identité (acceptation du client)

La personne à identifier

4XRS identifie et vérifie l'identité de tous ses clients. Il peut s'agir de personnes physiques ou d'entités légales.

Objet de l'identification et vérification de l'identité

L'identification des clients s'effectue par la collecte des informations pertinentes nécessaires.

Pour les personnes physiques, cela implique :

- le prénom ;
- le nom ;
- la date de naissance ;
- le lieu de naissance ; et
- l'adresse.

Les informations collectées sont vérifiées au moyen d'une copie recto verso de la carte d'identité du client identifié. La copie de cette carte d'identité est conservée dans le dossier du client pendant toute la durée de la relation d'affaires avec le client, et pendant encore 10 ans après la fin de celle-ci5.

Au cours de la relation d'affaires, il peut arriver que l'identité du client doive être vérifiée à nouveau. Dans ce cadre, si la copie précédente de la carte d'identité a expiré, une nouvelle copie peut être demandée au client6.

Moment de l'identification et de la vérification de l'identité

La règle générale est que l'identité de chaque client est contrôlée et vérifiée.

L'identification et la vérification de l'identité du client se déroulent en principe avant l'entrée en relation d'affaires.

Une exception est faite en ce qui concerne la PLCI et les contrats INAMI, car il s'agit de produits à faible risque en matière de BC/FT.

Pour ces produits, l'identification et la vérification de l'identité du client peuvent être reportées jusqu'après l'entrée en relation d'affaires. L'identité du client doit toutefois être établie et vérifiée dans les meilleurs délais après que la relation d'affaires avec le client a commencé.

Non-respect de l'obligation d'identification et de vérification de l'identité

Lorsqu'un client ne peut pas être identifié ou que son identité ne peut pas être vérifiée, XRS s'abstient d'engager une relation d'affaires, ou la relation d'affaires déjà établie est immédiatement réduite.

Caractéristiques du client et finalité et nature de la relation d'affaires

Les caractéristiques du client, ainsi que l'objectif et la nature de la relation d'affaires, doivent être évalués.

En ce qui concerne les caractéristiques du client, il faut vérifier s'il s'agirait éventuellement d'une personne politiquement exposée ou d'un membre de la famille d'une personne politiquement exposée.

Les informations relatives aux caractéristiques du client ainsi qu'à l'objet et à la nature de la relation d'affaires doivent être obtenues au plus tard au moment de l'entrée en relation d'affaires.

4 Art. 21 de la Loi anti-blanchiment.
5 Le délai de 10 ans est un délai imposé par la Loi anti-blanchiment. Ce délai peut être prolongé sur la base d'une législation contraire.
6 Voir également à ce sujet l'explication relative au devoir de vigilance (point 3.3 du présent document)

Devoir de vigilance

Vigilance continue

La vigilance continue implique :

- un examen attentif des opérations effectuées pendant la durée de la relation d'affaires (si nécessaire, de l'origine des fonds est vérifiée) ;
- la mise à jour (active) des données.

Au cours de la relation d'affaires, il est important de vérifier si le client est une personne politiquement exposée ou un membre de la famille d'une personne politiquement exposée.

Si, au cours de la relation d'affaires, un client devient une personne politiquement exposée ou un membre de la famille d'une personne politiquement exposée, une vigilance accrue s'appliquera jusqu'à ce que le client ne soit plus une personne politiquement exposée ou un membre de la famille d'une personne politiquement exposée.

L'obligation de vigilance continue est remplie comme suit au sein de XRS.

- Les données à caractère personnel sont contrôlées et actualisées chaque année. Si des données manquent ou ne sont plus correctes, il est demandé de le signaler.

Vigilance accrue

Une vigilance accrue s'applique dans les situations suivantes.

- L'identité d'un client ne peut pas ou pas suffisamment être vérifiée.
- Cela peut entraîner la fin de la collaboration.
- Le client est établi dans un pays tiers qui fait l'objet d'une vigilance accrue.
- L'AMLCO mettra à jour annuellement la liste des pays qui font l'objet d'une vigilance accrue et la communiquera aux collaborateurs.
- Le client est connu comme une personne politiquement exposée ou comme un membre de la famille d'une personne politiquement exposée.

Si nécessaire, des mesures peuvent être prises pour établir l'origine du patrimoine et des fonds utilisés dans la relation d'affaires ou les opérations du client.

Pour vérifier si le client est une personne politiquement exposée ou un membre de la famille d'une personne politiquement exposée, il convient de lui poser une question ou de lui fournir les documents pertinents. En cas de réponse positive, un questionnaire détaillé sera remis au client. Le client doit le compléter, le signer et le renvoyer, après quoi le questionnaire sera analysé.

Toute situation de vigilance accrue doit faire l'objet d'une déclaration à l'AMLCO. Dans ce cas, l'AMLCO établit un rapport écrit avec le déclarant. Ce rapport est documenté et conservé.

Déclaration de soupçons

Interne

Les collaborateurs peuvent déclarer leurs soupçons de BC/FT à l'AMLCO.

Une déclaration doit être faite par écrit ou par voie électronique, après quoi l'AMLCO examinera le soupçon de plus près avec le déclarant. Tant la déclaration que l'enquête se déroulent dans la plus grande discrétion de la part des deux parties.

Une fois l'enquête terminée et le soupçon confirmé, une déclaration sera introduite auprès de la CTIF.

Déclaration à la CTIF

Une déclaration est faite à la CTIF s'il existe un soupçon ou un motif raisonnable de soupçonner que :

- des fonds, quel qu'en soit le montant, sont liés au BC/FT ;
- des opérations ou tentatives d'opérations sont liées au BC/FT ;
- un fait connu est lié au BC/FT.

L'AMLCO est responsable de la déclaration à la CTIF. Si, pour quelque raison que ce soit, l'AMLCO n'est pas en mesure de faire la déclaration ou n'est pas apte à la faire, le déclarant peut également s'adresser directement à la CTIF. Cette procédure constitue toutefois une exception à la règle.

Toute déclaration à la CTIF se fait soit par écrit, soit par voie électronique, et ce, avant l'exécution de l'opération.

Lorsque la déclaration à la CTIF ne peut pas avoir lieu avant l'exécution de l'opération, la déclaration doit avoir lieu immédiatement après l'exécution de l'opération. La raison pour laquelle la déclaration ne peut pas avoir lieu avant l'exécution de l'opération doit être mentionnée.

La CTIF peut demander des renseignements complémentaires. Si XRS reçoit une telle demande, elle y apporte son entière collaboration et répond à la demande dans le délai imparti par la CTIF.

Interdiction de divulgation

En aucun cas, un client ou un tiers concerné ne sera informé que :

- des informations ou des renseignements sont, seront ou ont été fournis à la CTIF ;
- une analyse en matière de BC/FT est en cours ou pourrait être entamée.

Protection des déclarants

Les déclarants sont protégés de toute menace et/ou tout acte hostile.

Conservation et protection des données et des documents

À des fins de prévention, de détection ou d'enquête par la CTIF ou d'autres autorités compétentes, XRS doit collecter et conserver certains documents et informations.

- Données d'identification des personnes physiques et copies des pièces probantes de la vérification d'identité. Ces données sont conservées pendant une période de 10 ans à compter de la fin de la relation d'affaires avec le client[7].
- Pièces probantes et données d'enregistrement des opérations nécessaires à l'identification et à la reconstitution précise de l'opération effectuée. Ces données sont conservées pendant une période de 10 ans à dater de l'exécution de l'opération[8].
- Le rapport qui doit être établi à la suite de l'analyse de l'opération atypique et de la déclaration de soupçon. [9]Ce rapport doit être conservé pendant 7 ans s'il a été établi en 2017, pendant 8 ans s'il a été établi en 2018 et pendant 9 ans s'il a été établi à partir de 2019.

Sans préjudice d'autres lois applicables, les documents et informations susmentionnés seront supprimés à l'expiration des délais de conservation susmentionnés.

Les données à caractère personnel relèvent du champ d'application du RGPD. Toutefois, les données à caractère personnel traitées dans le cadre du BC/FT sont collectées sur la base d'une obligation légale.

7 Art. 60, 1° de la Loi anti-blanchiment.
8 Art. 60, 2° de la Loi anti-blanchiment.
9 Art. 60, 3° de la Loi anti-blanchiment.

Par conséquent, le client auquel s'applique la législation en matière de BC/FT ne peut pas se prévaloir[10] :

- du droit d'accès à ses données et de rectification de ses données ;
- du droit à l'oubli ;
- du droit à la portabilité des données ;
- du droit de formuler des objections ;
- du droit de ne pas faire l'objet d'un profilage ;
- du droit de notification des failles de sécurité.

Les pièces probantes des données à caractère personnel sont conservées de deux manières différentes. D'une part, une version papier des informations est conservée et stockée via Merak et, d'autre part, une version électronique est conservée sur un support électronique.

10 Art. 65 de la Loi anti-blanchiment.