

Politique de Lutte Contre le Blanchiment de capitaux et le Financement du Terrorisme (LCB-FT)

SERVICE CONFORMITÉ

Périmètre	Niveau de confidentialité
Groupe	Public

Statut	Date	Auteur
Création	Mai 2020	Service Conformité
Mise à jour	Janvier 2025	Service Conformité

Emplacement	
Stockage	SharePoint > Compliance > Corpus documentaire > LCB-FT > Politique LCB-FT
Accessibilité	Intranet et extranet

I - PRÉAMBULE	3
1. Les textes de référence	3
2. Le champ d'application	4
II - DÉFINITIONS	4
III - DISPOSITIFS LCB-FT	7
3. Mesurer le risque	8
4. Former et informer	8
5. Connaître le client	8
6. Traiter les soupçons persistants	12
IV - CONTRÔLE CONTINU	12
V - INFORMATIONS AU SEIN DU GROUPE	12
1. Échange d'informations au sein du Groupe	12
2. Conservation des documents	13
VI - SANCTIONS	13
VII - DISPOSITIONS FINALES	13

I - PRÉAMBULE

Les règles et orientations décrites dans la présente politique traduisent les exigences réglementaires applicables aux prestataires de services immobiliers et sont applicables à Emeria et à ses sociétés (ci-après dénommées « Le Groupe »). La politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) est sous la responsabilité du Service Conformité, lui-même sous la direction du Service Juridique.

Cette politique doit être appliquée par chaque collaboratrice et collaborateur, elle définit l'ensemble des procédures, des contrôles et le niveau de surveillance à mettre en place pour atténuer les risques conformément aux obligations réglementaires en vigueur. Elle est mise à jour régulièrement pour garantir sa pertinence, son adaptation aux évolutions législatives.

L'instance dirigeante, consciente des enjeux et de sa responsabilité en matière de conformité et de prévention des risques liées au blanchiment de capitaux et au financement du terrorisme est impliquée pleinement dans cette lutte. Elle est tenue informée des principaux points d'alertes et des principaux risques.

Le Groupe assure le pilotage du dispositif LCB-FT au sein de l'entité mère et de ses filiales. Les référents conformité désignés dans chaque société du Groupe sont chargés de diffuser les politiques, procédures et dispositifs du Groupe à l'échelon local.

Lorsque les obligations réglementaires locales sont plus contraignantes que celles du Groupe, les entités assujetties doivent s'y conformer. Il leur appartient d'adapter ces spécificités dans une procédure opérationnelle qui leur est propre.

1. Les textes de référence

- Directive (UE) 2018/1673 du Parlement Européen et du Conseil du 23 octobre 2018
- 5^e directive européenne (5AMLD) : Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018.
- Recommandations GAFI
- Articles L561-1 et suivants du Code monétaire et financier français
- Articles 324-1 et suivants du Code Pénal

En cas de doute ou de besoin d'assistance pour l'application de la présente politique, le Service Conformité peut être saisi à l'adresse suivante : compliance@emeria.eu

2. Le champ d'application

Quel est le personnel concerné ?

Cette politique s'adresse à l'ensemble des personnes détenant un mandat ou exerçant une fonction au sein du Groupe : mandataires sociaux, dirigeants, salariés, collaborateurs occasionnels (intérimaires, alternants, stagiaires, bénévoles).

Elle doit aussi être respectée et appliquée à tous les partenaires, sous-traitant, fournisseur, donneur d'ordre, client et prospect.

Quels sont les métiers concernés ?

- La transaction
- La gestion locative pour les loyers mensuels supérieurs ou égaux à 10.000 euros
- Les activités de courtage d'assurance, de réassurance et de mandataire d'intermédiation en assurance

II - DÉFINITIONS

La lutte contre le blanchiment de capitaux et le financement du terrorisme doit être une pratique quotidienne de la vie professionnelle. L'engagement de chacune et chacun est essentiel pour assurer un niveau de vigilance approprié et la maîtrise des risques. Afin de comprendre les enjeux (LCB-FT), il est important d'appréhender correctement ces notions et concepts exposés ci-dessous :

- **le blanchiment de capitaux** : est le fait de faciliter, par tout moyen, la justification mensongère de l'origine des fonds, des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect¹.

Constitue également un blanchiment de capitaux le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit.

Le blanchiment est puni pénalement de 5 ans et 375 000 € d'amende.

Exemple : Madame X se rapproche d'une agence immobilière du sud de la France pour acheter un bien d'exception à 3 millions d'euros. Son mari, qui vit comme elle dans un pays en dehors de l'Union européenne, versera les fonds depuis son compte situé dans un paradis fiscal. Monsieur X est connu dans son pays comme étant un trafiquant de drogue notoire. L'argent qui va servir à financer le bien immobilier pourrait être l'argent issu du trafic de drogue.

Concrètement, le blanchiment de capitaux désigne le processus par lequel des fonds acquis illégalement, par exemple à travers la criminalité ou la fraude, sont rendus légitimes en passant par une série de transactions financières. Le but est de rendre le système le plus opaque possible afin de dissimuler l'origine frauduleuse des fonds."

Le secteur de l'immobilier est particulièrement ciblé par les pratiques de blanchiment de capitaux : il permet de blanchir d'importantes sommes d'argent par l'investissement dans les biens immobiliers.

¹ Art 324-1 du Code Pénal

Il est donc impératif que chaque collaboratrice et collaborateur respecte les obligations normatives imposées et fasse preuve de vigilance au quotidien dans sa pratique professionnelle.

- **le financement du terrorisme** : est le fait de financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des biens quelconques ou en donnant des conseils à cette fin, dans l'intention de voir ces fonds, valeurs ou biens utilisés ou en sachant qu'ils sont destinés à être utilisés, en tout ou partie, en vue de commettre l'un quelconque des actes de terrorisme prévus, indépendamment de la survenance éventuelle d'un tel acte².
- **le client en relation d'affaires** : un client est considéré comme engagé dans une « relation d'affaires », lorsqu'il y a un contrat entre le professionnel et le client utilisant ses services en application duquel plusieurs opérations successives sont réalisées entre les cocontractants, ou qui crée pour ceux-ci des obligations continues. Ainsi, peut notamment être considérée comme une relation d'affaires :
 - Un client qui réalise plusieurs opérations la même année.
 - Un client qui donne mandat au professionnel.
 - Un client qui signe un bail pour une location.
 - Un client ayant souscrit un contrat d'assurance.
- **le client occasionnel** : le client occasionnel est celui qui réalise une opération ponctuelle, hors contrat, auprès d'un professionnel assujéti.
- **une personne politiquement exposée (PPE)** : est une personne exerçant (ou ayant exercé) une haute fonction publique (fonctions politiques, juridictionnelles ou administratives) pour le compte d'un État (France y compris). Cette personne peut également être un membre direct de sa famille ou une personne connue pour lui être étroitement associée³.

Concrètement, certaines personnes qui occupent de hautes fonctions (Assemblée nationale, gouvernement, magistrature...) sont considérées comme des personnes politiquement exposées. En dehors de la sphère politique, cette catégorie inclut également certaines personnes étroitement associées au PPE (famille, proches). Il faut considérer qu'en vertu des pouvoirs conférés par leurs fonctions, les PPE présentent un risque accru de participer à des pratiques de blanchiment de capitaux voire de financement du terrorisme. Par conséquent, une surveillance et un contrôle complémentaires sont nécessaires.

Exemple : Dans l'affaire des Panama Papers, plusieurs grands dirigeants et notamment des PPE ont été éclaboussés par cet énième scandale relatif à l'évasion fiscale comme David Cameron, Premier ministre britannique et son homologue islandais Sigmundur David Gunnlaugsson. Plusieurs hauts dirigeants plaçaient leurs actifs en dehors des radars des fiscaux nationaux.

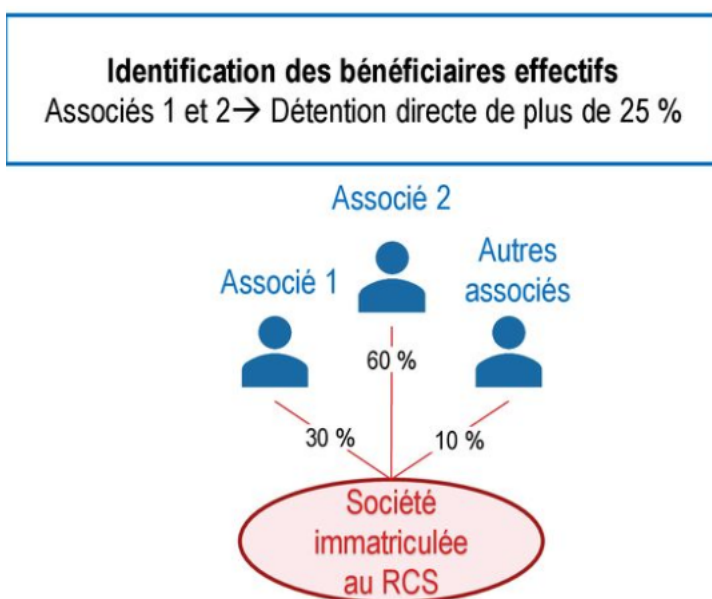
- **le gel des avoirs** : mesures prises par les autorités gouvernementales ou internationales afin d'empêcher l'accès à des fonds, des actifs ou d'autres ressources économiques appartenant à des individus, des entités ou des groupes spécifiques. La France dispose d'un dispositif national de gel des fonds et ressources économiques qui appartiennent à, sont possédés, détenus ou contrôlés par des personnes physiques ou morales, ou toute autre entité qui commettent, tentent

² Art 421-2-2 du Code Pénal

³ [Guide du GAFI en matière de PPE](#)

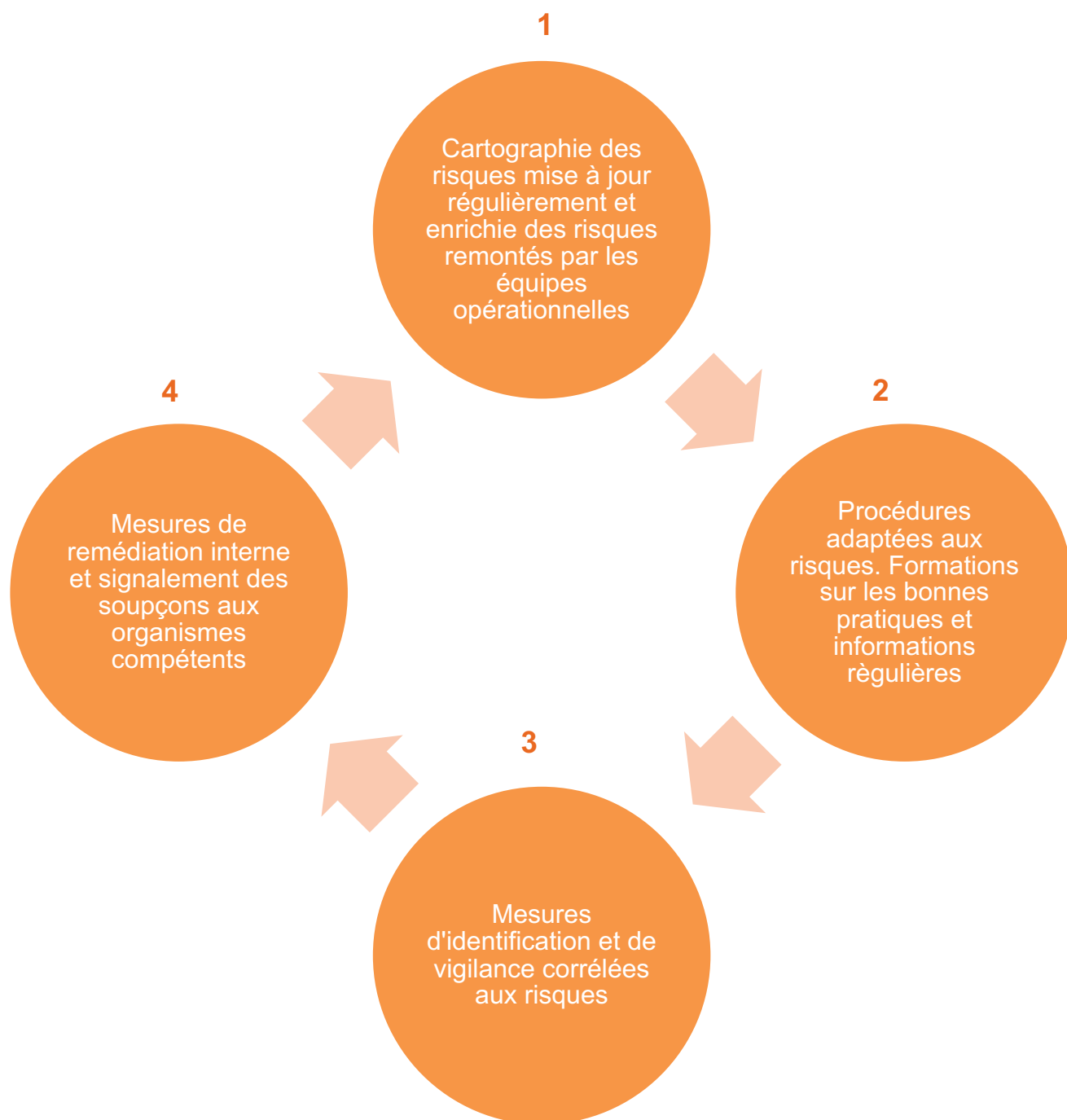
de commettre, facilitent ou financent des actes de terrorisme, y incitent ou y participent. Ces dispositifs permettent de répondre aux prescriptions de la [résolution 1373 \(2001\) du Conseil de sécurité des Nations Unies](#).

- **le bénéficiaire effectif (BE)** : désigne, la ou les personnes physiques qui seules ou de concert détiennent, directement ou indirectement, plus de 25% du capital ou des droits de vote de la société, ou exercent, par tout autre moyen, un pouvoir de contrôle sur les organes de gestion, d'administration ou de direction de la société ou sur l'Assemblée Générale des Associés.



En l'absence de soupçon de blanchiment, le représentant légal ou dirigeant peut être considéré à titre subsidiaire comme le bénéficiaire effectif, lorsqu'une personne physique n'a pas pu être déterminée en application des critères de détention de plus de 25% des parts, actions ou droits de vote ou de contrôle par tout autre moyen. Pour les personnes morales de droit public françaises situées dans l'espace économique européen ou dans un pays tiers équivalent, au regard des règles de transparence qui les régissent, il convient d'identifier le représentant légal.

- **la cellule de renseignement financier** : organisme national chargé de recueillir, analyser et enrichir les déclarations de soupçons que les professionnels assujettis sont tenus, par la loi, de lui transmettre concernant des faits suspects susceptibles de relever du blanchiment, des infractions sous-jacentes associées ou du financement du terrorisme. En France, la cellule de renseignement financier compétente est TRACFIN.
- **le GAFI (Groupe d'Action Financière Internationale)** : organisme intergouvernemental, créé en 1989 par le G7 qui a élaboré une série de 40 recommandations reconnues comme étant la norme internationale en matière LCB-FT et qui surveille les progrès réalisés par ses membres dans leur mise en œuvre.
- **Le risque pays** : risque associé à des transferts et transactions financières impliquant des pays spécifiques qui présentent des déficiences stratégiques dans leur régime LCB-FT.



Emeria et ses filiales se doivent de mettre en place une organisation interne et des procédures adaptées à ses secteurs d'activité. Le Groupe s'assure de la conformité de sa politique aux lois et règlements nationaux et internationaux, il réalise une mise à jour régulière de celle-ci afin de protéger son intégrité.

Le respect de cette politique permet d'éviter que le Groupe et ses filiales ne s'exposent à une atteinte de sa réputation et/ou une perte financière pour manquement aux normes applicables en matière LCB-FT. Parallèlement, elle permet de protéger chaque collaboratrice et collaborateur du risque de participation au blanchiment de capitaux et de financement du terrorisme.

3. Mesurer le risque

Conformément à ses obligations réglementaires et aux recommandations des autorités compétentes, le Groupe adopte une approche par les risques. L'établissement d'une cartographie des risques permet d'analyser, identifier et hiérarchiser les risques susceptibles d'être rencontrés dans le cadre de ses activités. La cartographie permet une vision claire et structurée des activités, zones et services à risque dans l'entité. A partir de celle-ci, des procédures sont élaborées, des mesures de prévention, d'atténuation, de contrôle et d'élimination des risques sont identifiées.

La cartographie des risques est actualisée et mise à jour régulièrement ce qui permet d'adapter les stratégies de gestion des risques.

4. Former et informer

Le Groupe garantit la formation de chaque collaboratrice et collaborateur. Dès leur arrivée dans le Groupe les nouvelles collaboratrices et les nouveaux collaborateurs qu'il soient permanents ou ponctuels (mandataire sociaux, dirigeants, salariés, collaborateurs occasionnels, intérimaires, stagiaires, alternants, apprentis, bénévoles...) se voient remettre un KIT de formation comprenant des documents explicatifs sur la lutte contre le blanchiment de capitaux et le financement du terrorisme. Le KIT comprend également des fiches simples de mise en situation afin d'illustrer différents cas et expliquer le comportement à adopter.

Si nécessaire, des communications internes seront réalisées dans les plus brefs délais (mailings ; intranet) afin d'informer les collaboratrices et collaborateurs de toute évolution de la loi.

En outre, un **réfèrent conformité** est désigné au sein de chaque société du groupe et permet de répondre aux questions éventuelles de chacune et de chacun. Dans le cas où celui-ci ne pourrait, en l'état de ses connaissances, apporter une réponse satisfaisante, il lui appartient de saisir le Service Conformité par mail à l'adresse compliance@emeria.eu.

Le Service Conformité se tient à disposition pour toutes difficultés ou questions relatives à la lutte contre le blanchiment de capitaux le financement du terrorisme.

5. Connaître le client

Adaptées à chaque situation, les mesures de vigilance et de contrôle sont corrélées au niveau de risque établi lors de l'entrée en relation. Le Groupe applique des mesures de contrôle et de vigilance à des degrés qui varient en fonction du client et de la relation d'affaires envisagée ou en cours. Ces degrés de contrôle et de vigilance permettent de prendre des mesures proportionnées au niveau de risque identifié pour chaque client ou transaction.

a. l'identification et vigilance normales 1^{er} niveau (KYC) :

Les mesures d'identification et de vigilance les plus allégées sont qualifiées de « normales ». Le Groupe garantit la mise en place de mesures de vigilances normales auprès de tous ses clients pour lesquels l'identification initiale ne présente pas de risques particuliers et ne nécessite pas une surveillance renforcée. Ces cas ne requièrent pas d'analyse approfondie car le risque de blanchiment de capitaux et de financement du terrorisme, au regard des éléments relevés, paraît faible.

❖ l'identification normale :

Elle doit permettre de connaître, les noms et prénoms, ainsi que la date et le lieu de naissance du client. En cas de client personne morale, il faut identifier sa forme juridique, sa dénomination sociale, son numéro d'immatriculation, ainsi que l'adresse du siège social. L'identification normale permet également d'identifier la nature de l'opération souhaitée, et de recueillir les justificatifs correspondants.

Dans le cadre de cette identification il faut alors :

- identifier le client sur la base d'une documentation officielle, en cours de validité et provenant d'une source indépendante et fiable.
- identifier et vérifier, le cas échéant, dans les mêmes conditions, l'identité des bénéficiaires effectifs.

Il est nécessaire de déterminer la ou les personnes physiques qui entrent dans la définition de bénéficiaire effectif et d'appliquer à ces personnes les obligations de vigilance adaptées à leur profil.

Exemple : La société O se porte acquéreur d'un bien immobilier pour la somme de 750 000 €. Après étude de la documentation, il s'avère que la société O appartient exclusivement à Mr X qui occupe une haute fonction exécutive. Mr X, bénéficiaire effectif, est donc considéré comme PPE. Dans ce cas, il convient d'appliquer des mesures de vigilances « complémentaires ».

- s'assurer d'avoir une bonne connaissance de l'objet et de la nature envisagée de la relation d'affaires.
- déterminer que la relation d'affaires n'implique pas de critères exigeants une classification plus stricte (la relation d'affaires n'implique pas de PPE ; les personnes ne sont pas soumises à une mesure restrictive ; la nature de l'opération envisagée est simple).

Ces mesures d'identification sont réalisées dès l'entrée en relation avec le client et à défaut, impérativement avant toute signature engageante.

Lorsque l'identification ne présente aucune particularité nécessitant un renforcement des contrôles, l'identification normale est suffisante. Les mesures de vigilances qui seront mises en place alors seront également qualifiées de normales.

❖ la vigilance normale :

Pendant toute la durée de la relation d'affaires, la fiche d'identification du client est mise à jour avec les éléments d'information nécessaires pour conserver une connaissance client appropriée au maintien et/ou à l'évolution de la relation d'affaire. Il est impératif de s'assurer de la cohérence des opérations effectuées avec les informations connues du client. (activités professionnelles ; profil de risque ; destination des fonds). Cette vigilance est continue tout au long de la relation client.

Dans le cas où, au cours de la relation, un ou plusieurs éléments viendraient à influencer sur la catégorisation du profil client, des mesures de vigilances renforcées et/ou complémentaires peuvent être nécessaires.

b. l'identification et vigilance complémentaires :

❖ **l'identification complémentaire :**

Dans certains cas déterminés par la loi, il est obligatoire d'appliquer des contrôles et une vigilance complémentaires. En raison de ces critères spécifiques, les personnes identifiées présentent des risques plus élevés d'être impliquées dans le blanchiment de capitaux et le financement du terrorisme. En plus des éléments « d'identification normale », il est nécessaire de procéder à un contrôle dit « complémentaire » et de maintenir un niveau de vigilance accru durant la relation d'affaires.

Lorsque l'identification de la personne révèle que :

- Le client ou le bénéficiaire effectif sont des Personnes Politiquement Exposées. (La qualité de PPE couvre également les proches directs de la personne PPE et les personnes physiques assurant sa représentation permanente).
- Les opérations sont réalisées avec un client établi sur un territoire inscrit sur une liste de pays à risques.

❖ **la vigilance complémentaire :**

Dans ces deux cas de figure, des mesures complémentaires de vigilance devront être mises en œuvre :

- l'identification dès le début de la relation du PPE. Si en cours de relation le client devient PPE il faudra une nouvelle catégorisation du client et appliquer les procédures et contrôles complémentaires.
- s'assurer de l'origine du patrimoine, des fonds, impliqués dans la relation ou la transaction.
- des diligences accrues, par des recherches et contrôles plus poussés qui permettront d'éclaircir la situation.
- surveillance renforcée et continue de l'activité.

Tous ces éléments doivent permettre de prendre la décision de nouer ou de maintenir une relation d'affaires avec cette personne.

Dans le cas où il est impossible de réaliser l'une des mesures complémentaires et /ou le client refuse de donner les éléments nécessaires au contrôle de son identité et/ou de l'opération, la décision sera prise conformément aux obligations réglementaires, de ne pas rentrer ou de rompre la relation d'affaires avec le client.

En cas de sérieux doute sur la licéité de l'opération souhaitée, ces soupçons seront remontés sans délai aux organismes de contrôle nationaux compétents.

c. l'identification et vigilance renforcées :

Lorsqu'en présence de certaines caractéristiques propres au produit ou à l'opération il semble que le risque de blanchiment de capitaux ou de financement du terrorisme doive être considéré comme élevé, un examen dit « renforcé » doit être réalisé dans le cadre des obligations de contrôle et vigilance renforcés.

❖ l'identification renforcée

Les critères suivants, sans être exhaustifs, peuvent être considérés comme caractéristiques d'un risque élevé de blanchiment de capitaux et/ou de financement du terrorisme :

Si :

- l'opération est complexe en raison de sa nature ou du nombre de ses intervenants.
- le montant de l'opération apparaît sans raison valable élevé.
- l'opération semble être sans justification économique.
- l'opération est sans objet licite.
- la transaction est réalisée pour un bien immobilier de prestige.
- il y a un écart entre le montant du bien à vendre ou à louer et sa valeur réelle.

❖ Vigilance renforcée

Quand dans le cadre de l'opération ou la transaction l'un ou plusieurs des points susmentionnés apparaissent, il est nécessaire de prendre des mesures adaptées :

- une évaluation méticuleuse des risques de l'opération et/ou transaction doit être réalisée.
- le niveau de risque de l'opération ou la transaction doit être actualisée.
- si nécessaire, le Groupe réalise un signalement de toute activité qui paraît suspecte aux autorités compétentes et ce en temps utile.
- si nécessaire, il faut suspendre la relation d'affaire le temps d'effectuer de plus amples vérifications.
- si les vérifications font apparaître un soupçon de blanchiment de capitaux et/ou de financement du terrorisme, il convient d'en informer l'autorité de contrôle (TRACFIN) et de suivre les consignes données concernant l'issue de la transaction.

Il est tout à fait possible, au regard des éléments d'identification et des caractéristiques de l'opération de devoir réaliser des mesures de vigilance complémentaires et des mesures de vigilances renforcées.

À chaque étape de la vérification, il est impératif de conserver la preuve de toutes les diligences réalisées.

6. Traiter les soupçons persistants

Comme précédemment annoncé, dans le cas où, il apparaît qu'en raison de la nature, de l'identité de la personne, de la transaction ou de l'opération il existe des soupçons ou des motifs raisonnables de soupçonner que les fonds ont une origine illégale ou pourraient servir au financement de terrorisme, le service Conformité réalise un signalement de l'activité suspecte aux autorités compétentes dans les plus brefs délais.

La cartographie est enrichie continuellement des risques rencontrés et des informations relevées par les équipes opérationnelles.

Si nécessaire des mesures correctives sont mise en œuvre et permettent l'actualisation des mesures préventives existantes afin de résoudre les situations non conforme aux obligations réglementaires en vigueur.

IV - CONTRÔLE CONTINU

Emeria et ses filiales s'assure d'une **vigilance constante** de ses clients et leur opérations qu'ils réalisent à travers notamment :

- Une revue périodique de la base client ;
- Une surveillance générale des transactions réalisée à différents niveaux ;
- Une analyse de cohérence des opérations réalisées avec une connaissance actualisée du client.
- Des outils de détection et de contrôle.

Si Emeria ou l'une de ses filiales se trouve face à une **opération atypique** ou **suspecte** :

- Une déclaration de soupçons auprès de la cellule de renseignement financier nationale compétente devra être effectuée.
- En présence d'un client ou bénéficiaire effectif inscrit sur un registre national de gel des avoirs, Emeria et ses filiales réalisent les diligences nécessaires propres à chaque législation et mettent fin à la relation d'affaires, le cas échéant.

La procédure de lanceur d'alerte stipule les conditions dans lesquelles le Groupe fournit une garantie de confidentialité au lanceur d'alerte.

V - INFORMATIONS AU SEIN DU GROUPE

1. Échange d'informations au sein du Groupe

Le dispositif LCB-FT mis en œuvre par Emeria est centralisé au niveau du Groupe.

La présente politique est commune à l'ensemble du Groupe Emeria. Les collaborateurs et les dirigeants du Groupe peuvent partager entre eux les informations relatives aux obligations de contrôles et vigilances relatives à la lutte anti-blanchiment.

Les entités assujetties se doivent d'informer rapidement le service Conformité du Groupe lorsqu'elles savent, soupçonnent ou ont des motifs raisonnables de soupçonner que des fonds, quel que soit le montant concerné, proviennent d'une activité criminelle ou sont liés au financement **du terrorisme**.

Des déclarants officiels y sont et seuls ces derniers procéderont, dans la plus grande confidentialité et le cas échéant, aux déclarations de soupçons auprès de la cellule de renseignement financier (TRACFIN). Les informations recueillies ne doivent en aucun cas être partagées, fût-ce avec des collaborateurs et dirigeants d'entités du groupe ou même avec les dirigeants d'Emeria.

2. Conservation des documents

Toute la documentation relative aux diligences effectuées envers le client doit être conservée pendant une durée n'excédant pas cinq ans à compter de la fin de la relation d'affaires ou à compter de la réalisation de l'opération ponctuelle selon la législation en vigueur. Cette période est prévue sous réserve d'exigences légales plus restrictives en matière de conservation des données.

Le système d'archivage doit permettre aux personnes en charge de répondre rapidement à toute demande relevant d'une autorité compétente.

Chaque filiale est tenue de se renseigner et de connaître la loi nationale qui lui est applicable en matière d'archivage et de conservation des données.

VI - SANCTIONS

En cas de non-respect de la présente politique, les mesures disciplinaires prévues par le règlement intérieur du Groupe peuvent être prises.

Par ailleurs, des sanctions pénales, telles qu'une peine d'emprisonnement et une amende, peuvent également être encourues. Les entités ou individus affectés par la violation des obligations de lutte contre le blanchiment de capitaux et le financement du terrorisme peuvent demander réparation et obtenir des dommages-intérêts.

VII - DISPOSITIONS FINALES

La présente politique est applicable dès sa publication sur le réseau [intranet](#) du Groupe. Elle est mise en œuvre sous la responsabilité du Service Conformité Groupe et mise à jour par celui-ci.

LES BONS RÉFLEXES :

Pour toutes questions en matière LCB-FT vous pouvez vous rapprocher du référent conformité de votre entité juridique en premier lieu. En cas de besoin le Service Conformité Groupe se tient à votre disposition : compliance@emeria.eu