Luxembourg, le 19 août 2022

Lettre circulaire 22/16
relative à la sous-traitance d'activités ou de fonctions opérationnelles importantes ou critiques

L'article 81 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances (ci-après la « LSA ») prévoit que les entreprises d'assurance et de réassurance luxembourgeoises informent préalablement et en temps utile le CAA de leur intention de sous-traiter des activités ou des fonctions opérationnelles importantes ou des fonctions compliance, audit interne ou actuarielle (jugées critiques) ainsi que de toute évolution importante ultérieure concernant ces fonctions ou ces activités.

Dans ce contexte, la présente lettre circulaire a pour objet de préciser les exigences du CAA en matière de sous-traitance d'activités ou de fonctions opérationnelles importantes ou critiques et leur notification au CAA. Par ailleurs, au vu du recours croissant à la sous-traitance et afin de faciliter le suivi, le CAA met à disposition des entreprises un formulaire informatique qui peut être téléchargé à partir du site internet du CAA. Ce formulaire est à remplir et à envoyer au CAA.

1. Définitions

Aux fins de la présente lettre circulaire, on entend par :

- accord de sous-traitance : un accord, quelle que soit sa forme, conclu entre une personne physique ou morale du secteur des assurances et un prestataire de services, soumis ou non à un contrôle, en vertu duquel ce prestataire de services exécute, soit directement, soit par un tiers, une procédure, un service ou une activité, qui serait autrement exécuté par la personne elle-même.

- prestataire de services : un tiers, personne morale ou physique différente de l'entité légale de l'entreprise d'assurance ou de réassurance, exécutant au titre d'un accord de sous-traitance tout ou partie d'une procédure, d'un service ou d'une activité.

2. Bases juridiques et prudentielles

La présente circulaire est basée principalement sur les textes suivants :

- les articles 32 (paragraphe 21), 43 (paragraphe 19), 65, 71, 81 et 300 de la LSA,
- l'article 274 du règlement délégué (UE) 2015/35 de la Commission du 10 octobre 2014 complétant la directive 2009/138/CE du Parlement européen et du Conseil sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II) (ci-après le « Règlement délégué »),
- la Lettre circulaire 15/13 du Commissariat aux Assurances relative à des orientations supplémentaires de l'EIOPA concernant le régime 'Solvabilité 2',
- les orientations 14, 60, 61, 62, 63 et 64 des lignes directrices de l'EIOPA sur le système de gouvernance (cf. EIOPA-BOS-14/253),

- le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

3. Analyse préalable à la sous-traitance

Avant de conclure un accord de sous-traitance d'une activité ou d'une fonction d'assurance ou de réassurance avec des prestataires de services, l'entreprise d'assurance ou de réassurance doit :

a) évaluer les risques liés à l'accord de sous-traitance ;

b) vérifier que les conditions énoncées à l'article 65 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances sont remplies ;

c) tenir compte de l'étendue du contrôle qu'elle exerce sur le prestataire ou de l'influence qu'elle peut avoir sur les actions de ce dernier lorsque celui-ci est membre du même groupe ;

d) évaluer si l'accord de sous-traitance concerne une activité ou fonction opérationnelle importante ou critique, conformément au point 4 de la présente lettre circulaire, et le cas échéant vérifier que les conditions énoncées à l'article 81, paragraphe 2, de la LSA sont respectées.

Dans tous les cas, il appartient à l'entreprise d'assurance ou de réassurance de vérifier que la sous-traitance est conforme à toutes les lois et règlementations en lien avec la sous-traitance.

4. Évaluation des activités ou fonctions opérationnelles importantes ou critiques

Avant de conclure un accord de sous-traitance, l'entreprise d'assurance ou de réassurance doit évaluer et documenter si et dans quelle mesure l'accord de sous-traitance concerne une activité ou fonction opérationnelle importante ou critique. En procédant à cette évaluation et documentation, l'entreprise d'assurance ou de réassurance doit examiner si l'activité ou la fonction visée est susceptible de devenir importante ou critique à l'avenir.

Lorsqu'un accord de sous-traitance avec un prestataire de services couvre des activités ou fonctions opérationnelles multiples, l'entreprise doit tenir compte de tous les aspects de l'accord dans son évaluation.

La détermination si la fonction ou activité sous-traitée est critique ou importante demeure sous la responsabilité de l'entreprise. Lors de l'évaluation, l'entreprise doit prendre en compte la question si elle ne serait pas en mesure de fournir ses services aux preneurs d'assurance sans ladite fonction ou activité. D'autres facteurs utiles pour l'évaluation à considérer sont :

Incidence sur le plan d'activités

a) la sous-traitance d'une fonction clé ou d'une activité principale ;

b) la taille, la nature, l'importance et la complexité des activités, fonctions ou services fournis par l'accord de sous-traitance ;

c) la contribution de l'activité ou de la fonction sous-traitée aux revenus et aux bénéfices ;

d) le coût de la sous-traitance par rapport aux frais généraux de l'entreprise d'assurance ou de réassurance ;

e) la poursuite de l'activité et la résilience opérationnelle de l'entreprise d'assurance ou de réassurance ;

Incidence sur le contrôle et la supervision

f) le droit d'émettre des lignes directrices générales et des instructions particulières à l'adresse du prestataire de services sur les éléments à prendre en considération dans l'exercice des fonctions ou activités sous-traitées ;

g) l'étendue du contrôle et de la supervision par l'entreprise d'assurance et de réassurance ;

h) l'exposition globale de l'entreprise d'assurance ou de réassurance (et/ou du groupe le cas échéant) à un même prestataire de services ;

Incidence sur l'image de marque

i) les risques de réputation de l'entreprise d'assurance ou de réassurance ;

j) la protection des données à caractère personnel et non personnel et l'impact éventuel sur l'entreprise d'assurance ou de réassurance, les preneurs ou d'autres personnes concernées par une violation des règles issues du secret professionnel ainsi que du non-respect de la confidentialité ou d'un manquement à la garantie de la disponibilité et de l'intégrité des données, sur la base notamment du règlement (UE) 2016/6797[1].

L'entreprise doit également réévaluer le caractère important ou critique de l'activité ou fonction opérationnelle précédemment sous-traitée, si la nature, l'ampleur ou la complexité des risques inhérents à l'accord subissent un changement significatif.

Les fonctions clés définies dans la directive Solvabilité 2 sont toujours considérées comme fonctions critiques et importantes.

Les évaluations mentionnées ci-dessus doivent faire l'objet d'une documentation appropriée.

5. Secret des assurances

Dans le cadre d'une entreprise soumise aux règles énoncées à l'article 300 de la LSA et dont la sous-traitance à des prestataires de services comprend des données à caractère personnel des parties prenantes aux contrats d'assurances (preneur(s), assuré(s), bénéficiaire(s)) ou permettant d'identifier les parties prenantes aux contrats d'assurances, il incombe à l'entreprise :

a) d'effectuer une analyse juridique pour déterminer s'il est nécessaire que le preneur d'assurance ait accepté la sous-traitance suivant les termes décrits à l'article 300, paragraphe 2bis de la LSA[2];

b) de documenter et mettre à jour de manière régulière l'analyse décrite sous a) en fonction de l'évolution/extension des activités ou des conditions générales et particulières ainsi que de la jurisprudence applicable ;

c) de s'assurer que le personnel travaillant pour le prestataire de services ou ses sous-traitants ne peuvent en aucun cas accéder aux données à caractère personnel des parties prenantes aux contrats d'assurances sans avoir obtenu au préalable l'accord explicite de l'entreprise et sans qu'un mécanisme de surveillance soit mis à la disposition de l'entreprise pour contrôler les accès réalisés, ces accès doivent rester exceptionnels ;

d) de vérifier que les accès du prestataire de services sont restreints et encadrés par des mesures préventives et de détection en ligne avec les bonnes pratiques de sécurité et contrôlées au moins annuellement ;

e) de s'assurer que des mesures de protection suffisantes soient prises afin d'éviter que des personnes non autorisées ne puissent accéder à leurs systèmes. En particulier, l'entreprise devra prévoir que les télécommunications soient cryptées ou encore protégées selon d'autres moyens techniques disponibles de nature à assurer la sécurité des communications.

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1.)

2 En l'absence d'une jurisprudence sur la forme du consentement, il n'est pas exclu que certaines parties prenantes au contrat puissent contester devant les tribunaux la validité de leurs consentements.

6. Périmètre des sous-traitances à notifier

Les entreprises d'assurance et de réassurance de droit luxembourgeois doivent notifier au CAA :

- La sous-traitance d'activités considérées par l'entreprise comme critiques ou importantes ;
- La sous-traitance d'une fonction clé définie par la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (ci-après la « directive Solvabilité 2) ;
- Toute évolution importante ultérieure concernant ces fonctions ou ces activités ;
- Toute activité sous-traitée qui entraîne une modification majeure du plan d'activités.

De manière générale, les activités principales d'une entreprise d'assurance ou de réassurance qui sont entièrement sous-traitées sont à considérer comme importantes ou critiques. De simples droits de contrôle, contrôles effectifs, communications de directives générales ou d'instructions individuelles à l'attention du sous-traitant ne permettent pas de justifier l'absence d'une sous-traitance entière conformément à ce qui précède.

La sous-traitance des tâches opérationnelles des fonctions clés, confiée à un tiers différent de l'entité légale concernée, doit faire l'objet d'une notification, sauf si l'évaluation établit que le fait de ne pas fournir la fonction externalisée ou de la fournir de manière inappropriée n'aurait pas d'impact négatif sur l'efficacité de la fonction clé.

Lorsqu'une sous-traitance informatique ou une chaîne de sous-traitance, consistant exclusivement en une externalisation informatique, est basée sur une infrastructure de cloud computing telle que définie dans la lettre circulaire 21/15, les termes de la présente lettre circulaire ne sont pas applicables. En pareil cas, l'entreprise d'assurance ou de réassurance doit se conformer aux exigences de la lettre circulaire 21/15.

Est exclue de la notification prévue par la présente lettre circulaire la sous-traitance à un professionnel du secteur de l'assurance (ci-après « PSA ») tel que prévu par les dispositions du titre III chapitre 1er de la LSA :

- de la gestion journalière ou ;
- d'une fonction clé définie dans la directive Solvabilité 2 ;

par une entreprise de réassurance ou d'assurance qui a pour objet la fourniture d'une couverture de (ré)assurance portant sur les risques de l'entreprise ou des entreprises auxquelles elle appartient ou bien les risques d'une ou plusieurs autres entreprises du groupe dont elle fait partie.

Est également exclu de la présente lettre circulaire, le recours à des intermédiaires pour la distribution des produits d'assurance ou de réassurance qui doit se faire dans le respect des dispositions légales et réglementaires applicables.

La souscription de contrats ou le règlement de sinistres par un intermédiaire d'assurance qui n'est pas un salarié de l'entreprise d'assurance est toutefois à considérer comme activité de sous-traitance, si cette activité est considérée comme critique ou importante.

7. Principe de notification écrite au CAA

Les exigences de notification écrite visées à l'article 81, paragraphe 3 de la LSA et précisées par les orientations de l'EIOPA relatives au système de gouvernance sont applicables à toute sous-traitance d'activités ou de fonctions opérationnelles importantes ou critiques. La notification concerne également toute évolution importante ultérieure concernant ces fonctions ou activités. Une évolution importante ultérieure est notamment :

- un changement de prestataire ;
- un ajout d'une activité majeure à un contrat existant ;
- une réduction importante de l'effectif de l'entreprise ;
- des frais modifiés de plus de 20 % (en haut ou en bas) sur une base annuelle ;

- la contrepartie intra-groupe qui devient extra-groupe.

Par ailleurs, si une activité ou fonction opérationnelle sous-traitée, précédemment classée comme non importante ou non critique, devient importante ou critique, l'entreprise doit le notifier au CAA.

Inversement, si une activité ou fonction opérationnelle sous-traitée, précédemment classée comme importante ou critique, devient non importante ou non critique, l'entreprise doit également en informer le CAA par simple courrier officiel.

La notification écrite de la sous-traitance d'une activité ou d'une fonction critique ou importante de l'entreprise doit être faite préalablement à la conclusion du contrat de sous-traitance à l'aide du formulaire informatique qui peut être téléchargé à partir du site internet du CAA pour être rempli.

La notification doit être fournie au moins un mois avant que la sous-traitance prévue ne soit effective.

Le CAA envoie, diligemment et en tout état de cause dans un délai de dix jours ouvrables suivant la réception de la notification un accusé de réception écrit à l'entreprise. Cet accusé de réception ne préjuge pas de la prise de mesures ultérieures dans le cadre d'un contrôle sur place s'il apparaît que la sous-traitance n'est pas conforme à toutes les lois et règlementations applicables.

Si le contrat de sous-traitance notifié n'est pas conclu ou signé, l'entreprise doit en informer le CAA dans les meilleurs délais.

Pour chaque sous-traitance d'une activité ou d'une fonction critique ou importante notifiée, le responsable de la vérification de la conformité doit évaluer et confirmer par écrit au CAA, dans les deux mois suivant la signature du contrat de sous-traitance, que :

- la sous-traitance n'entraîne la violation d'aucun texte de loi, en particulier des règles relatives à la protection des données ;
- le contrat de sous-traitance inclut les clauses telles que définies à l'article 274, paragraphe 4 du règlement délégué (UE) 2015/35 ;
- une diligence raisonnable du prestataire de services a été menée conformément à la section D01.X.0040 du formulaire de notification ;
- un contrôle régulier des performances et des résultats du prestataire de services est mis en place.

8. Formulaire de notification

Chaque formulaire comporte six sections qui sont relatives à :

1. D01.X.0010 - l'entreprise d'assurance ou de réassurance ;
2. D01.X.0020 - l'activité ou la fonction sous-traitée ;
3. D01.X.0030 - le prestataire de services (informations générales) ;
4. D01.X.0040 - le prestataire de services (diligence raisonnable) ;
5. D01.X.0050 - le prestataire de services (contrat de sous-traitance)et ;
6. D01.X.0060 - le contrôle et la gestion de la sous-traitance.

En cas de contrat de sous-traitance couvrant plusieurs activités ou fonctions critiques ou importantes (par exemple un contrat cadre), il est demandé de les notifier à l'aide d'un formulaire de notification par activité ou fonction critique ou importante.

Lors du remplissage des formulaires les précisions suivantes sont à considérer.

- D01.X.0020 (R0010) : Type d'activité ou de fonction

  - L'activité « distribution des produits »

    Il est notamment demandé de renseigner sous ce point toutes activités de sous-traitance relatives au règlement européen PRIIPs. Le recours à des intermédiaires pour la distribution

des produits d'assurance ou de réassurance qui doit se faire dans le respect des dispositions légales et réglementaires applicables est à exclure.

- Les « tâches opérationnelles des fonctions clés Solvabilité II »

  Les tâches opérationnelles effectuées dans le cadre des fonctions clés Solvabilité II qui sont confiées à un tiers différent de l'entité légale concernée, entreprise d'assurance ou de réassurance. La personne responsable de la fonction clé, au titre de l'article 42, paragraphe 2, de la directive Solvabilité 2 n'est pas visée. Il s'agit de savoir s'il y a des prestataires de services qui exécutent les missions et les travaux pour le compte de la personne responsable de la fonction clé.

- D01.X.0020 (R0030) : Sous-traitance intra- ou extra-groupe

  La sous-traitance d'une procédure, d'un service ou d'une activité à une société du même groupe que l'entreprise d'assurance ou de réassurance est à renseigner comme de la sous-traitance intragroupe.

- D01.X.0030 (R0250) : Informations sur la subdélégation de la sous-traitance

  Si le prestataire de services indique à la ligne R0250 (D01.X.0030) du formulaire de notification de sous-traiter lui-même 100% des activités ou fonctions convenues contractuellement dans le contrat de sous-traitance avec l'entreprise d'assurance ou de réassurance, le(s) prestataire(s) de services intervenant dans cette subdélégation sont à renseigner.

- D01.X.0050 (R0030-R0170) : Conformité du contrat de sous-traitance avec les exigences de l'article 274 du Règlement délégué

  L'entreprise d'assurance ou de réassurance doit dresser une table de correspondance portant sur la conformité des dispositions du contrat de sous-traitance avec les exigences de l'article 274, paragraphe 4, du règlement délégué. Cette table de correspondance doit être disponible auprès de l'entreprise.

- D01.X.0050 (R0220) : Le droit applicable au contrat de sous-traitance

  Il est demandé de renseigner sous ce point la compétence juridictionnelle et le droit applicable au contrat de sous-traitance (de préférence le droit et les juridictions du Grand-Duché de Luxembourg).

- D01.X.0050 (R0240) : Le type de coût (honoraires ou commission)

  Il est demandé de préciser si le coût de la sous-traitance est facturé via des honoraires ou via des commissions.

- D01.X.0060: Personne de l'entreprise d'assurance ou de réassurance responsable de l'activité ou de la fonction sous-traitée

  Il s'agit du responsable de la fonction clé lorsque la sous-traitance concerne les tâches opérationnelles effectuées dans le cadre l'une des fonctions clés définies par la directive Solvabilité 2. Dans les autres cas, c'est la personne qui est responsable de la supervision et de la qualité des services fournis par le prestataire de services.

9. Exigences en matière de documentation

Dans le cadre de son système de gouvernance et de gestion des risques, l'entreprise d'assurance ou de réassurance doit tenir un registre de ses accords de sous-traitance, par exemple sous la forme d'un registre spécifique actualisé au fil du temps.

En cas de sous-traitance d'activités ou de fonctions opérationnelles importantes ou critiques, l'entreprise d'assurance ou de réassurance doit consigner toutes les informations suivantes :

a) le nom des sous-traitants y compris les pays où les sous-traitants sont enregistrés ;

b) les résultats et la date de l'évaluation du caractère critique ou importante de la fonction ou de l'activité ;

c) les résultats des évaluations de la substituabilité (par exemple, facile, difficile ou impossible) du prestataire de services ;

d) les contrats de sous-traitance signés ;

e) la date de la décision de l'organe d'administration, de gestion ou de contrôle de l'entreprise d'assurance ou de réassurance qui a approuvé l'accord de sous-traitance ;

f) les résultats des évaluations de performance du prestataire de services ;

g) la vérification de compétence et d'honorabilité du prestataire de services pour exercer une activité ou une fonction clé sous-traitée ;

h) la vérification que le prestataire de services a mis en place des plans d'urgence adéquats pour faire aux situations d'urgence ou d'interruption de son activité ;

i) une liste des personnes responsables chez les prestataires de services des fonctions critiques ou importantes qui leur ont été sous-traitées.

En cas de sous-traitance d'activités ou de fonctions opérationnelles non importantes ou non critiques, l'entreprise d'assurance ou de réassurance doit définir les informations à consigner en fonction de la nature, de l'ampleur et de la complexité des risques inhérents aux services fournis par le prestataire de services.

L'entreprise d'assurance ou de réassurance doit mettre à la disposition du CAA, sur sa demande, toutes les informations nécessaires pour lui permettre de procéder au contrôle de la sous-traitance, y compris une copie de l'accord de sous-traitance ainsi que la politique de sous-traitance conformément à l'orientation 63 des orientations d'EIOPA relatives au système de gouvernance.

L'entreprise doit faire une auto-évaluation, y compris une table de correspondance, portant sur la conformité de l'accord de sous-traitance avec la présente lettre circulaire, l'article 274 du Règlement délégué et les orientations d'EIOPA relatives au système de gouvernance.

Dispositions finales

La présente lettre circulaire s'applique à partir du 1er novembre 2022 à tous les accords de sous-traitance de services conclus ou modifiés à partir de cette date.

Le Comité de Direction