Luxembourg, le 5 août 2021

Lettre circulaire 21/15 portant modification et complément de la lettre circulaire 20/13 du Commissariat aux Assurances relative à la sous-traitance à des prestataires de services en nuage (« cloud computing »)

Par la lettre circulaire 20/13, le Commissariat aux Assurances (ci-après le « CAA ») a informé les entreprises d'assurance et de réassurance soumises à sa surveillance que le CAA appliquera pleinement les « Orientations relatives à la sous-traitance à des prestataires de services en nuage » (référence EIOPA-BoS-20-002) publiées le 24 avril 2020 par l'Autorité Européenne des Assurances et des Pensions professionnelles (ci-après l'« EIOPA »).

Dans ce contexte, la présente lettre circulaire a pour objet de reprendre l'ensemble des orientations susvisées et d'intégrer certaines exigences additionnelles du CAA.

Nous nous permettons de souligner qu'il convient de lire la présente lettre circulaire en conjonction avec la loi modifiée du 7 décembre 2015 sur le secteur des assurances et ses règlements d'exécution, le 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 (ci-après le « règlement délégué »), les orientations de l'EIOPA relatives au système de gouvernance (EIOPA-BoS-14/253) ainsi que le règlement général sur la protection des données (RGPD) et les exigences de l'autorité compétente en la matière, la Commission nationale pour la protection des données (CNPD).

1. Définitions

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

Prestataire de services	un tiers exécutant au titre d'un accord de sous-traitance tout ou partie d'une procédure, d'un service ou d'une activité.
Prestataire de services en nuage	un prestataire de services, tel que défini ci-dessus, chargé, au titre d'un accord de sous-traitance, de fournir des services en nuage.
Services en nuage	des services fournis au moyen de l'informatique en nuage, à savoir un modèle permettant d'accéder partout, aisément et à la demande, par le réseau, à des ressources informatiques configurables mutualisées (réseaux, serveurs, stockage, applications et services par exemple) qui peuvent être rapidement mobilisées et libérées avec un minimum d'effort ou d'intervention d'un prestataire de services.
Nuage public	une infrastructure en nuage accessible au grand public en vue d'une utilisation ouverte
Nuage privé	une infrastructure en nuage accessible à une seule entreprise en vue d'une utilisation exclusive.
Nuage communautaire	une infrastructure en nuage accessible à une communauté

	spécifique d'entreprises, par exemple plusieurs entreprises d'un même groupe, en vue d'une utilisation exclusive.
Nuage hybride	une infrastructure en nuage composée d'au moins deux infrastructures en nuage distinctes.
Fonction de sécurité de l'information	l'entreprise doit désigner parmi ses salariés une personne qui a pour responsabilité l'utilisation des services en nuage et est garant des compétences du personnel gérant les ressources des services en nuage. L'entreprise doit attribuer cette fonction à une personne qualifiée et maîtrisant les enjeux d'une sous-traitance à un prestataire de services en nuage. Cette fonction peut être exercée par des personnes cumulant déjà d'autres fonctions. Par dérogation, la fonction de sécurité de l'information peut être désignée à une personne d'une entité faisant partie du groupe auquel l'entreprise appartient, pour autant qu'elle soit rattachée hiérarchiquement au dirigeant agréé de l'entreprise.

2. Services en nuage et sous-traitance

L'entreprise doit établir si un accord avec un prestataire de services en nuage relève de la définition de la sous-traitance conformément à la loi modifiée du 7 décembre 2015 sur le secteur des assurances. Lors de l'évaluation, il convient de prendre en considération :

a) si l'activité ou fonction opérationnelle (ou une partie de celle-ci) sous-traitée est exercée de manière récurrente ou continue; et

b) si cette activité ou fonction opérationnelle (ou une partie de celle-ci) relèverait normalement du champ d'application des activités ou fonctions opérationnelles qui seraient ou pourraient être exercées par l'entreprise dans le cadre de ses activités commerciales habituelles, même si l'entreprise n'a pas exercé cette activité ou fonction opérationnelle dans le passé.

Lorsqu'un accord 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.

Dans les cas où l'entreprise sous-traite des activités ou fonctions opérationnelles à des prestataires de services qui ne sont pas des prestataires de services en nuage mais qui dépendent largement d'infrastructures en nuage pour fournir leurs services (par exemple, lorsque le prestataire de services en nuage fait partie d'une chaîne de sous-sous-traitance), l'accord relatif à cette sous-traitance relève du champ d'application de la présente lettre circulaire.

3. Principes généraux en matière de gouvernance de la sous-traitance de services en nuage

Sans préjudice de l'article 274, paragraphe 3 du règlement délégué, l'organe d'administration, de gestion ou de contrôle (ci-après l'« AMSB ») de l'entreprise doit veiller à ce que toute décision de sous-traiter des activités ou fonctions opérationnelles importantes ou critiques à des prestataires de services en nuage soit fondée sur une évaluation approfondie des risques, y compris tous les risques pertinents découlant de l'accord, tels que les risques liés aux technologies de l'information et de la communication (ci-après les « TIC »), le risque de non-continuité des activités, les risques juridiques, le risque de non-conformité, le risque de concentration, les autres risques opérationnels et les risques associés à la migration des données et/ou à la phase de mise en œuvre, le cas échéant.

En cas de sous-traitance d'activités ou de fonctions opérationnelles importantes ou critiques à des prestataires de services en nuage, l'entreprise doit, le cas échéant, tenir compte des variations de son profil de risque dues à ses accords de sous-traitance de services en nuage dans son évaluation interne des risques et de la solvabilité (ci-après l'« ORSA »).

L'utilisation des services en nuage doit être compatible avec les stratégies de l'entreprise (par exemple, la stratégie en matière de TIC, la stratégie de sécurité de l'information, la stratégie de gestion des risques opérationnels) ainsi qu'avec les politiques et les procédures internes, qui doivent être mises à jour, si nécessaire.

4. Mise à jour de la politique écrite de sous-traitance

En cas de sous-traitance à des prestataires de services en nuage, il convient que l'entreprise mette à jour la politique écrite de sous-traitance (par exemple en la révisant, en ajoutant une annexe distincte ou en élaborant de nouvelles politiques spécifiques) et les autres politiques internes pertinentes (par exemple, la sécurité de l'information), en tenant compte des spécificités de la sous-traitance de services en nuage au moins dans les domaines suivants:

a) les rôles et les responsabilités des fonctions de l'entreprise concernées, en particulier l'AMSB, et les fonctions responsables des TIC, de la sécurité de l'information, de la conformité, de la gestion des risques et de l'audit interne;

b) les processus et les procédures de déclaration nécessaires à l'approbation, à la mise en œuvre, au suivi, à la gestion et au renouvellement, le cas échéant, des accords de sous-traitance de services en nuage liée à des activités ou fonctions opérationnelles importantes ou critiques;

c) la supervision des services en nuage proportionnée à la nature, à l'ampleur et à la complexité des risques inhérents aux services fournis, y compris

- l'évaluation des risques des accords de sous-traitance de services en nuage et la procédure de vigilance à l'égard des prestataires de services en nuage, y compris la fréquence de l'évaluation des risques;
- les contrôles de surveillance et de gestion (par exemple, la vérification de l'accord de niveau de service);
- les normes et contrôles de sécurité;

d) en ce qui concerne la sous-traitance de services en nuage liée à des activités ou fonctions opérationnelles importantes ou critiques, il convient de faire référence aux exigences contractuelles décrites au point 12 de la présente lettre circulaire;

e) les exigences en matière de documentation et la notification écrite au CAA relative à la sous-traitance de services en nuage liée à des activités ou fonctions opérationnelles importantes ou critiques;

f) en ce qui concerne chaque accord de sous-traitance de services en nuage qui couvre des activités ou fonctions opérationnelles importantes ou critiques, l'exigence d'une « stratégie de retrait » documentée et, le cas échéant, suffisamment testée, qui soit proportionnée à la nature, à l'ampleur et à la complexité des risques inhérents aux services fournis. La stratégie de retrait peut faire intervenir une série de procédures de résiliation, y compris, mais pas nécessairement, l'interruption, la réintégration ou le transfert des services inclus dans l'accord de sous-traitance de services en nuage.

5. Notification écrite au CAA

Les exigences de notification écrite visées à l'article 81, paragraphe 3 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances 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 à des prestataires de services en nuage. Si une activité ou fonction opérationnelle sous-traitée, précédemment classée comme non importante ou non critique, devient importante ou critique, l'entreprise doit en informer le CAA.

La notification écrite de l'entreprise doit comprendre, compte tenu du principe de proportionnalité, au moins les informations suivantes:

a) une brève description de l'activité ou fonction opérationnelle sous-traitée;

b) une description des bénéfices opérationnels et financiers attendus pour l'entreprise ;

c) une description des bénéfices opérationnels et financiers attendus pour les parties prenantes aux contrats d'assurances (preneur(s), assuré(s), bénéficiaire(s));

d) la date de début et, le cas échéant, la prochaine date de renouvellement du contrat, la date de fin et/ou les délais de préavis pour le prestataire de services en nuage et pour l'entreprise;

e) la législation applicable à l'accord de sous-traitance;

f) le nom du prestataire de services en nuage, le numéro d'immatriculation de la société, l'identifiant de la personne morale (si disponible), le siège social et autres coordonnées pertinentes, ainsi que le nom de son entreprise mère (le cas échéant); en cas de groupe, l'appartenance ou non du prestataire de services en nuage au groupe;

g) les modèles de services et de déploiement en nuage (c.-à-d. en nuage public/privé/hybride/communautaire), la nature spécifique des données conservées et les lieux (c.-à-d. les pays ou régions) où ces données seront stockées;

h) un bref résumé des raisons pour lesquelles l'activité ou fonction opérationnelle sous-traitée est considérée comme importante ou critique;

i) la date de la dernière évaluation du caractère important ou critique de l'activité ou fonction opérationnelle sous-traitée.

6. Exigences en matière de documentation

Dans le cadre de son système de gouvernance et de gestion des risques, l'entreprise doit tenir un registre de ses accords de sous-traitance de services en nuage, par exemple sous la forme d'un registre spécifique actualisé au fil du temps. L'entreprise doit également tenir un registre des accords de sous-traitance de services en nuage résiliés pendant une période de conservation appropriée soumise à la réglementation nationale.

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

a) les informations à notifier au CAA;

b) en cas de groupe, les entreprises d'assurance ou de réassurance et les autres entreprises entrant dans le périmètre de la consolidation prudentielle qui utilisent les services en nuage;

c) la date de l'évaluation des risques la plus récente et un bref résumé des principaux résultats;

d) la personne ou l'organe de décision (par exemple l'AMSB) de l'entreprise qui a approuvé l'accord de sous-traitance de services en nuage;

e) les dates des derniers audits et des prochains audits prévus, le cas échéant;

f) le nom des sous-traitants auxquels des parties significatives d'une activité ou fonction opérationnelle importante ou critique sont sous-sous-traitées, y compris les pays où les sous-traitants sont enregistrés, où le service sera exécuté et, le cas échéant, les lieux (c.-à-d. les pays ou les régions) où les données seront stockées;

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

h) si l'activité ou fonction opérationnelle importante ou critique sous-traitée soutient ou non des activités économiques soumises à des exigences horaires pour leur fonctionnement;

i) les coûts budgétaires annuels estimés;

j) si l'entreprise dispose d'une stratégie de retrait en cas de résiliation par l'une des parties ou en cas d'interruption des services par le prestataire de services en nuage.

En cas de sous-traitance d'activités ou de fonctions opérationnelles non importantes ou non critiques, l'entreprise 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 en nuage.

L'entreprise doit mettre à la disposition du CAA, sur sa demande, toutes les informations nécessaires

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

7. Analyse préalable à la sous-traitance

Avant de conclure un quelconque accord avec des prestataires de services en nuage, l'entreprise doit:

a) évaluer si l'accord de sous-traitance de services en nuage concerne une activité ou fonction opérationnelle importante ou critique, conformément au point 9 de la présente lettre circulaire;

b) identifier et évaluer tous les risques pertinents de l'accord de sous-traitance de services en nuage conformément au point 10 de la présente lettre circulaire;

c) mettre en œuvre une procédure de vigilance à l'égard du prestataire de services en nuage potentiel, conformément au point 11 de la présente lettre circulaire;

d) identifier et évaluer les conflits d'intérêts que la sous-traitance est susceptible d'engendrer conformément aux exigences énoncées à l'article 274, paragraphe 3, point b) du règlement délégué.

8. Secret des assurances

Dans le cadre d'une entreprise soumise aux règles énoncées à l'article 300 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances et dont la sous-traitance à des prestataires de services en nuage 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 loi modifiée du 7 décembre 2015 sur le secteur des assurances[1].

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 des jurisprudences applicables

c) de s'assurer que le personnel travaillant pour le prestataire de services en nuage ou ses sous-traitants ne peuvent en aucun cas accéder aux données à caractère personnel des parties prenantes aux contrats d'assurances et aux systèmes qu'une entreprise détient sur l'infrastructure en nuage 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.

   Lorsque l'accès découle d'une obligation légale ou est lié à des situations d'extrême urgence suite à un incident technique critique touchant une partie ou l'ensemble des clients du fournisseur de services en nuage, il est possible de prévoir que l'information concernant l'accès, qui devra être faite par le fournisseur de services en nuage à l'entreprise, pourra être effectuée à posteriori et ce dans les meilleurs délais. Dans ces cas, les accès réalisés doivent être documentés par l'entreprise.

d) de vérifier que les accès du prestataire de services en nuage sont restreints et encadrés par des mesures préventives et détectives en ligne avec les bonnes pratiques de sécurité et auditées au moins annuellement.

[1] 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.

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.

9. Évaluation des activités ou fonctions opérationnelles importantes ou critiques

Avant de conclure un accord de sous-traitance avec des prestataires de services en nuage, l'entreprise doit évaluer si l'accord de sous-traitance de services en nuage concerne une activité ou fonction opérationnelle qui est importante ou critique. En procédant à cette évaluation, le cas échéant, l'entreprise doit examiner si l'accord est susceptible de devenir important ou critique à l'avenir. L'entreprise doit également réévaluer la caractère important ou critique de l'activité ou fonction opérationnelle précédemment sous-traitée à des prestataires de services en nuage, si la nature, l'ampleur ou la complexité des risques inhérents à l'accord subit un changement significatif.

Lors de l'évaluation, l'entreprise doit tenir compte, conjointement avec les résultats de l'évaluation des risques, au moins des facteurs suivants:

a) l'incidence potentielle de toute perturbation significative de l'activité ou fonction opérationnelle sous-traitée ou de l'incapacité du prestataire de services en nuage à assurer les services aux niveaux de service convenus sur:
   - le respect permanent des obligations réglementaires de l'entreprise;
   - la résilience et la viabilité des finances et de la solvabilité de l'entreprise à court et à long termes;
   - la poursuite de l'activité et la résilience opérationnelle de l'entreprise;
   - les risques opérationnels de l'entreprise, y compris les risques liés à la conduite, aux TIC et les risques juridiques;
   - les risques pour la réputation de l'entreprise;

b) l'incidence éventuelle de l'accord de sous-traitance de services en nuage sur la capacité de l'entreprise:
   - à identifier, suivre et gérer tous les risques pertinents;
   - à se conformer à toutes les exigences légales et réglementaires;
   - à effectuer des audits appropriés concernant l'activité ou fonction opérationnelle sous-traitée;

c) l'exposition globale de l'entreprise (et/ou du groupe le cas échéant) à un même prestataire de services en nuage et l'incidence cumulative éventuelle des accords de sous-traitance dans un même domaine d'activité;

d) la taille et la complexité des domaines d'activité de l'entreprise concernés par l'accord de sous-traitance de services en nuage;

e) la possibilité, si nécessaire ou souhaitable, de transférer l'accord de sous-traitance de services en nuage proposé vers un autre prestataire de services en nuage ou de réintégrer les services (la « substituabilité »);

f) la protection des données à caractère personnel et non personnel et l'impact éventuel sur l'entreprise, les preneurs ou d'autres sujets concernés d'une violation 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[2]. L'entreprise doit notamment prendre en considération les données relevant du secret des affaires et/ou sensibles (par exemple, les données sur la santé des preneurs).

[2] 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.)

10. Évaluation des risques de la sous-traitance de services en nuage

En général, l'entreprise doit adopter une approche proportionnée à la nature, à l'ampleur et à la complexité des risques inhérents aux services sous-traités à des prestataires de services en nuage. Il s'agit notamment d'évaluer l'incidence éventuelle de toute sous-traitance de services en nuage, en particulier sur les risques opérationnels de l'entreprise et sur les risques pour sa réputation.

En cas de sous-traitance d'activités ou fonctions opérationnelles importantes ou critiques à des prestataires de services en nuage, l'entreprise doit:

a) tenir compte des coûts et avantages attendus de l'accord de sous-traitance de services en nuage proposé, y compris en soupesant les risques importants qui peuvent être réduits ou mieux gérés par rapport aux risques importants qui sont susceptibles de résulter de l'accord de sous-traitance de services en nuage proposé;

b) évaluer, le cas échéant et s'il y a lieu, les risques, y compris les risques juridiques, les risques liés aux TIC, les risques de non-conformité et pour la réputation, ainsi que les limites de la supervision posées par:

- le service en nuage sélectionné et les modèles de déploiement proposés (c'est-à-dire public/privé/hybride/communautaire);
- la migration et/ou la mise en œuvre;
- les activités et les données et systèmes connexes qu'il est envisagé de sous-traiter (ou qui ont été sous-traités), ainsi que leur sensibilité et les mesures de sécurité requises ;
- la stabilité politique et la situation en matière de sécurité des pays (au sein ou en dehors de l'UE) où les services sous-traités sont ou peuvent être fournis et où les données sont ou sont susceptibles d'être stockées. L'évaluation devrait prendre en compte:
    1. les lois en vigueur, et notamment les lois sur la protection des données;
    2. les dispositions en vigueur en matière d'application des lois;
    3. les dispositions du droit de l'insolvabilité qui s'appliqueraient en cas de défaillance d'un prestataire de services et les contraintes qui pourraient apparaître en ce qui concerne la récupération urgente des données de l'entreprise;
- la sous-sous-traitance, y compris les risques supplémentaires qui peuvent survenir si le sous-traitant est situé dans un pays tiers ou dans un pays différent de celui du prestataire de services en nuage et le risque que de longues et complexes chaînes de sous-sous-traitance réduisent la capacité de l'entreprise à superviser ses activités ou fonctions opérationnelles importantes ou critiques et la capacité des autorités de contrôle à les superviser efficacement;
- le risque de concentration global de l'entreprise vis-à-vis du même prestataire de services en nuage, notamment la sous-traitance à un prestataire de services en nuage qui n'est pas facilement substituable ou des accords de sous-traitance multiples avec le même prestataire de services en nuage. Lors de l'évaluation du risque de concentration, l'entreprise (et/ou le groupe, le cas échéant) doit tenir compte de tous ses accords de sous-traitance de services en nuage avec ce prestataire de services en nuage.

L'évaluation des risques doit être réalisée avant la mise en place d'une sous-traitance de services en nuage. Si l'entreprise se rend compte que des déficiences majeures et/ou des changements significatifs affectent les services fournis ou la situation du prestataire de services en nuage, elle devrait rapidement réexaminer ou réaliser de nouveau l'évaluation des risques. En cas de renouvellement d'un accord de sous-traitance de services en nuage, concernant son contenu et son champ d'application (par exemple, élargissement du champ d'application ou inclusion dans le champ d'application de fonctions opérationnelles importantes ou critiques qui n'étaient pas incluses auparavant), l'évaluation des risques doit être réalisée à nouveau.

11. Procédure de vigilance à l'égard du prestataire de services en nuage

L'entreprise doit s'assurer, dans sa procédure de sélection et d'évaluation, que le prestataire de services en nuage est approprié selon les critères définis par sa politique écrite de sous-traitance.

Des mesures de vigilance appropriées doivent être mises en œuvre à l'égard du prestataire de services en nuage avant de sous-traiter toute activité ou fonction opérationnelle. Si l'entreprise conclut un deuxième accord avec un prestataire de services en nuage qui a déjà fait l'objet d'une évaluation, elle doit déterminer, selon une approche fondée sur le risque, si la mise en œuvre d'une seconde procédure de vigilance appropriée est nécessaire. Si l'entreprise se rend compte que des déficiences majeures et/ou des changements significatifs affectent les services fournis ou la situation du prestataire de services en nuage, elle doit rapidement réexaminer ou mettre de nouveau en œuvre la procédure de vigilance.

En cas de sous-traitance de services en nuage liés à des fonctions opérationnelles importantes ou critiques, la procédure de vigilance doit inclure une évaluation de l'adéquation du prestataire de services en nuage (par exemple, les compétences, l'infrastructure, la situation économique, le statut juridique et le statut réglementaire). Le cas échéant, aux fins d'étayer la procédure de vigilance mise en œuvre, l'entreprise peut utiliser des éléments de preuve, des certifications fondées sur des normes internationales, des rapports d'audit de tiers reconnus ou des rapports d'audit interne.

L'entreprise conserve l'expertise nécessaire pour contrôler efficacement les prestations ou les tâches sous-traitées au prestataire de services en nuage et la gestion des risques associés à cette sous-traitance.

En outre, l'entreprise doit s'assurer que le personnel en charge de la gestion des ressources de services en nuage, l'audit interne et la fonction de sécurité de l'information disposent des compétences suffisantes pour assurer leurs fonctions sur base de formations appropriées sur la gestion et la sécurité des ressources de services en nuage spécifiques au fournisseur de services en nuage. La fonction de sécurité de l'information est responsable de la mise en application de cette exigence.

12.Exigences contractuelles

Les droits et obligations respectifs de l'entreprise et du prestataire de services en nuage doivent être clairement définis et consignés dans un accord écrit.

Sans préjudice des exigences définies à l'article 274 du règlement délégué, en cas de sous-traitance d'activités ou de fonctions opérationnelles importantes ou critiques à un prestataire de services en nuage, l'accord écrit entre l'entreprise et le prestataire de services en nuage doit comporter:

a) une description claire de la fonction sous-traitée à fournir (services en nuage, y compris le type de services de support);

b) la date de début et de fin de l'accord, le cas échéant, et les délais de préavis pour le prestataire de services en nuage et pour l'entreprise;

c) la compétence juridictionnelle et le droit applicable à l'accord (le contrat doit être soumis au droit et à une juridiction d'un des Etats membres de l'Union Européenne, de préférence du Grand-Duché de Luxembourg. Lorsque l'accord de sous-traitance signé est un contrat de groupe visant à permettre à l'entreprise ainsi qu'à d'autres entités du groupe de bénéficier des services en nuage, l'accord peut également être soumis à la loi du pays de l'entité du groupe signataire, y compris lorsque ce pays est situé en dehors de l'Union Européenne, pour autant que les règles de sous-traitance à des prestataires de service en nuage sont équivalentes à celles de l'Union Européenne[3]);

d) les obligations financières des parties;

e) si la sous-sous-traitance d'une activité ou fonction opérationnelle importante ou critique (ou

[3] Il appartient à l'entreprise de déterminer si les règles sont équivalentes. La table de correspondance prévue à l'article 6 de la présente lettre circulaire devra être complétée par les règles et orientations relatives à la sous-traitance à des prestataires de services en nuage applicables dans le pays de l'entité du groupe signataire.

de parties significatives de celle-ci) est permise et, dans l'affirmative, les conditions auxquelles la sous-sous-traitance significative est soumise (voir point 14 de la présente lettre circulaire);

f) le(s) lieu(x) (c.-à-d. les régions ou les pays) où les données pertinentes seront stockées et traitées [lieu(x) des centres de données], et les conditions à remplir, y compris l'obligation d'informer l'entreprise si le prestataire de services envisage de modifier le(s) lieu(x);

g) une résilience dans l'Union Européenne des services en nuage sous-traités. En cas de distribution des traitements, données et systèmes dans différents centres de données à travers le monde, l'un des centres au moins doit être localisé dans l'Union Européenne et doit si nécessaire pouvoir reprendre les traitements, données et systèmes distribués pour opérer de manière autonome les services en nuage fournis au prestataire de services. Lorsque tous les centres de données supportant les services en nuage sont localisés au sein de l'Union Européenne, l'exigence de résilience des services en nuage dans l'Union Européenne est supposée respectée de fait. Lorsque l'accord de sous-traitance signé est un contrat de groupe visant à permettre à l'entreprise ainsi qu'à d'autres entités du groupe en dehors de l'Union Européenne de bénéficier des services en nuage, la résilience dans l'Union Européenne est recommandée et doit être prise en compte dans l'analyse des risques de l'entreprise;

h) des dispositions concernant l'accessibilité, la disponibilité, l'intégrité, la confidentialité, la nature privée et la sécurité des données pertinentes, en tenant compte des spécifications du point 14 de la présente lettre circulaire;

i) le droit pour l'entreprise de contrôler régulièrement les prestations du prestataire de services en nuage;

j) les niveaux de service convenus, qui doivent inclure des objectifs de performance quantitatifs et qualitatifs précis afin de permettre un suivi en temps utile, de sorte que des mesures correctives appropriées puissent être prises dans les meilleurs délais si les niveaux de service convenus ne sont pas respectés;

k) les obligations d'information du prestataire de services en nuage envers l'entreprise, y compris, le cas échéant, les obligations de présenter des rapports pertinents pour la fonction de sécurité et les fonctions clés de l'entreprise, tels que les rapports de la fonction d'audit interne du prestataire de services en nuage;

l) si le prestataire de services en nuage doit souscrire une assurance obligatoire contre certains risques et, le cas échéant, le niveau de couverture d'assurance demandé;

m) l'obligation de mettre en œuvre et de tester les plans d'urgence de continuité de l'activité;

n) l'obligation pour le prestataire de services en nuage d'accorder à l'entreprise, à ses autorités de contrôle et à toute autre personne désignée par l'entreprise ou les autorités de contrôle:

- un accès complet à tous les locaux professionnels pertinents (sièges sociaux et centres opérationnels), y compris à l'ensemble des appareils, systèmes, réseaux, informations et données pertinents utilisés pour assurer la fonction sous-traitée, notamment les informations financières connexes, le personnel et les auditeurs externes du prestataire de services en nuage (« droits d'accès »);
- des droits inconditionnels en matière d'inspection et d'audit de l'accord de sous-traitance de services en nuage (« droits d'audit »), afin de leur permettre de contrôler l'accord de sous-traitance et de s'assurer du respect de toutes les exigences réglementaires et contractuelles applicables;

o) des dispositions visant à garantir que l'entreprise peut rapidement récupérer les données lui appartenant en cas d'insolvabilité, de résolution ou d'interruption des activités commerciales du prestataire de services en nuage.

p) des dispositions relatives aux cas de rupture du contrat, dans lesquelles le prestataire de services en nuage s'engage contractuellement à supprimer définitivement les données et systèmes données en sous-traitance dans un délai raisonnable sans préjudice des prescriptions légales.

En ce qui concerne les exigences contractuelles mentionnées par les lettres c) et g) ci-dessus, l'entreprise notifie au CAA lorsque ces exigences ne peuvent pas être respectées. Cette notification

doit comporter une argumentation détaillée justifiant le recours à ce prestataire de services en nuage et indiquant précisément les mesures de résilience envisagées en cas de défaillance de ce prestataire de services ou de défaillance des communications permettant d'y accéder.

13. Droits d'accès et d'audit

L'accord de sous-traitance de services en nuage ne doit pas limiter l'exercice effectif des droits d'accès et d'audit de l'entreprise, ainsi que les possibilités de contrôle des services en nuage afin de remplir ses obligations réglementaires.

L'entreprise doit exercer ses droits d'accès et d'audit, déterminer la fréquence des audits et les domaines et services à contrôler selon une approche fondée sur le risque, conformément à la section 8 des orientations de l'EIOPA relatives au système de gouvernance.

Afin de déterminer la fréquence et l'étendue de l'exercice de ses droits d'accès ou d'audit, l'entreprise doit examiner si la sous-traitance de services en nuage est liée à une activité ou fonction opérationnelle importante ou critique, la nature et l'ampleur des risques ainsi que l'impact que les accords de sous-traitance de services en nuage auront sur elle.

Si l'exercice de ses droits d'accès ou d'audit, ou l'utilisation de certaines techniques d'audit, crée un risque pour l'environnement du prestataire de services en nuage et/ou d'un autre client du prestataire de services en nuage (par exemple, l'impact sur les niveaux de service, la disponibilité des données, les aspects de confidentialité), l'entreprise et le prestataire de services en nuage doivent convenir d'autres moyens de fournir à l'entreprise un niveau d'assurance et de service similaire (par exemple, l'inclusion de contrôles spécifiques à tester dans un rapport ou une certification spécifique produite par le prestataire de services en nuage).

Afin d'exploiter plus efficacement les ressources d'audit et de réduire la charge organisationnelle pesant sur le prestataire de services en nuage et ses clients, les entreprises peuvent, sans préjudice de leur responsabilité finale concernant les activités exercées par leurs prestataires de services en nuage, avoir recours:

a) à des certifications et à des rapports d'audit internes ou externes mis à disposition par le prestataire de services en nuage;

b) à des audits groupés (c'est-à-dire réalisés conjointement avec d'autres clients du même prestataire de services en nuage), ou des audits groupés réalisés par un tiers désigné par elles.

En cas de sous-traitance de services en nuage liée à des activités ou fonctions opérationnelles importantes ou critiques, les entreprises ne doivent recourir à la méthode visée au point a) ci-dessus, que si elles:

a) veillent à ce que le périmètre de la certification ou du rapport d'audit couvre les systèmes (par exemple, les procédures, les applications, les infrastructures, les centres de données, etc.) et les contrôles identifiés par l'entreprise et évalue le respect des exigences réglementaires pertinentes;

b) évaluent de manière approfondie et régulière le contenu des nouvelles certifications ou des nouveaux rapports d'audit, et s'assurent que les certifications ou les rapports ne sont pas obsolètes;

c) s'assurent que les systèmes et contrôles essentiels sont couverts dans les futures versions de la certification ou du rapport d'audit;

d) sont satisfaites de l'aptitude de la partie chargée de la certification ou de l'audit (par exemple, en ce qui concerne la rotation de l'entreprise chargée de la certification ou de l'audit, les qualifications, l'expertise, la réexécution/vérification des éléments probants inclus dans le dossier d'audit sous-jacent);

e) s'assurent que les certifications sont délivrées et que les audits sont réalisés conformément aux normes appropriées et qu'ils incluent un test relatif à l'efficacité opérationnelle des contrôles essentiels en place;

f) ont le droit contractuel de demander l'extension du périmètre des certifications ou des rapports d'audit à d'autres systèmes et contrôles pertinents; le nombre et la fréquence de ces

demandes de modification du périmètre doivent être raisonnables et légitimes du point de vue de la gestion des risques;

g) conservent le droit contractuel d'effectuer des audits individuels sur place, à leur discrétion, en ce qui concerne la sous-traitance de services en nuage liée à des activités ou fonctions opérationnelles importantes ou critiques; ce droit doit être exercé en cas de besoins spécifiques qui ne peuvent être satisfaits par d'autres types d'interactions avec le prestataire de services en nuage.

En ce qui concerne la sous-traitance de fonctions opérationnelles importantes ou critiques à des prestataires de services en nuage, l'entreprise doit évaluer si les certifications et les rapports de tiers visés au paragraphe 5, lettre a) du point 13 de la présente lettre circulaire, sont adéquats et suffisants pour se conformer à ses obligations réglementaires et, selon une approche fondée sur le risque, ne devrait pas se fier uniquement à ces certifications et rapports sur le long terme.

Avant une visite prévue sur place, la partie qui doit exercer son droit d'accès (entreprise, auditeur ou tiers agissant au nom de l'entreprise ou des entreprises) doit fournir un avis préalable dans un délai raisonnable, à moins qu'une notification préalable n'ait pas été possible en raison d'une situation d'urgence ou de crise. Cet avis doit indiquer le lieu et le but de la visite et le personnel qui y participera.

Compte tenu du niveau élevé de complexité technique des solutions en nuage, l'entreprise doit vérifier que le personnel chargé de l'audit – qu'il s'agisse de ses auditeurs internes ou de l'équipe d'auditeurs agissant en son nom, ou des auditeurs désignés par le prestataire de services en nuage – ou, le cas échéant, le personnel qui examine la certification par un tiers ou les rapports d'audit du prestataire de services, aient acquis les connaissances et les compétences adéquates pour procéder aux évaluations et/ou aux audits pertinents.

14. Sécurité des données et des systèmes

L'entreprise doit veiller à ce que les prestataires de services en nuage respectent les réglementations européennes et nationales ainsi que les normes appropriées en matière de sécurité des TIC.

En cas de sous-traitance d'activités ou de fonctions opérationnelles importantes ou critiques à des prestataires de services en nuage, l'entreprise doit en outre définir des exigences spécifiques en matière de sécurité de l'information dans le contrat de sous-traitance et contrôler régulièrement le respect de ces exigences.

Aux fins du paragraphe ci-dessus, en cas de sous-traitance d'activités ou de fonctions opérationnelles importantes ou critiques à des prestataires de services en nuage, l'entreprise, en appliquant une approche fondée sur le risque et en tenant compte de ses responsabilités et de celles du prestataire de services en nuage, doit:

a) convenir clairement des rôles et des responsabilités entre le prestataire de services en nuage et l'entreprise en ce qui concerne les activités ou fonctions opérationnelles concernées par la sous-traitance de services en nuage, qui doivent être clairement répartis;

b) définir et décider d'un niveau approprié de protection des données confidentielles, de continuité des activités sous-traitées, d'intégrité et de traçabilité des données et des systèmes dans le cadre de la sous-traitance de services en nuage envisagée;

c) envisager des mesures spécifiques, le cas échéant, applicables aux données en transit, aux données en mémoire et aux données au repos, par exemple l'utilisation de technologies de cryptage associées à une gestion des clés appropriée

d) examiner les mécanismes d'intégration des services en nuage avec les systèmes des entreprises, par exemple, les interfaces de programmation d'applications et une procédure rigoureuse de gestion de l'accès des utilisateurs;

e) garantir contractuellement que la disponibilité du trafic du réseau et la capacité prévue répondent, le cas échéant et dans la mesure du possible, à de fortes exigences de continuité;

f) définir et décider d'exigences de continuité appropriées garantissant des niveaux adéquats à chaque stade de la chaîne technologique, le cas échéant;

g) disposer d'une procédure de gestion des incidents rigoureuse et bien documentée, incluant les responsabilités respectives, par exemple par la définition d'un modèle de coopération en

cas d'incidents réels ou suspectés;

h) adopter une approche fondée sur le risque en ce qui concerne le(s) lieu(x) de stockage et de traitement des données (c'est-à-dire le pays ou la région) et les considérations relatives à la sécurité de l'information;

i) contrôler le respect des exigences relatives à l'efficacité et à l'efficience des mécanismes de contrôle mis en œuvre par le prestataire de services en nuage qui permettent d'atténuer les risques liés aux services fournis.

15. Sous-sous-traitance d'activités ou de fonctions opérationnelles importantes ou critiques

Si la sous-sous-traitance de fonctions opérationnelles importantes ou critiques (ou d'une partie de celles-ci) est permise, l'accord de sous-traitance de services en nuage entre l'entreprise et le prestataire de services en nuage doit:

a) préciser tous les types d'activités qui sont exclus d'une sous-sous-traitance potentielle;

b) indiquer les conditions à respecter en cas de sous-sous-traitance (par exemple, le sous-sous-traitant devra aussi respecter pleinement les obligations pertinentes du prestataire de services en nuage). Ces obligations comprennent les droits d'audit et d'accès ainsi que la sécurité des données et des systèmes;

c) indiquer que le prestataire de services en nuage conserve l'entière responsabilité et assure intégralement la supervision des services sous-sous-traités;

d) prévoir l'obligation pour le prestataire de services en nuage d'informer l'entreprise de tout changement significatif prévu concernant les sous-traitants ou les services sous-sous-traités qui pourrait affecter la capacité du prestataire de services à s'acquitter des obligations qui lui incombent en vertu de l'accord de sous-traitance de services en nuage. La période de notification de ces changements doit permettre à l'entreprise de procéder à tout le moins à une évaluation des risques liés aux effets des changements proposés avant que le changement effectif concernant les sous-sous-traitants ou les services sous- sous-traités ne prenne effet;

e) garantir, dans les cas où un prestataire de services en nuage prévoit des changements concernant un sous-sous-traitant ou les services sous-sous-traités qui auraient un effet négatif sur l'évaluation des risques des services convenus, que l'entreprise a le droit de s'opposer à ces changements et/ou le droit de résilier et de sortir du contrat.

16. Suivi et supervision des accords de sous-traitance de services en nuage et protection du consommateur

L'entreprise doit suivre régulièrement l'accomplissement des activités, les mesures de sécurité et le respect du niveau de service convenu par ses prestataires de services en nuage selon une approche fondée sur le risque. L'accent doit être mis sur la sous-traitance de services en nuage liée à des fonctions opérationnelles importantes ou critiques.

Pour ce faire, l'entreprise doit mettre en place des mécanismes de suivi et de supervision qui doivent tenir compte, lorsque cela est possible et approprié, de la présence d'une sous-sous-traitance de fonctions opérationnelles importantes ou critiques ou d'une partie de celles-ci.

Lorsqu'il y a interruption des services donnés en sous-traitance suite à la défaillance du prestataire de services en nuage de plus d'un jour, l'entreprise doit documenter dans un registre :

a) la durée et la nature de la défaillance;

b) les impacts de la défaillance pour les clients de l'entreprise et le nombre de clients affectés;

c) les mesures de compensation mises en place par l'entreprise;

d) les actions prises par l'entreprise pour informer ses clients de la défaillance ainsi que des mesures de compensation;

e) les impacts financiers pour l'entreprise;

f) les impacts réputationnels et stratégiques pour l'entreprise;

g) les impacts réglementaires;

h) les mesures de remédiation prises par l'entreprise;

Ce registre doit être mis à la disposition du CAA sur sa simple demande. La sous-traitance à un prestataire de services en nuage ne devra en aucun cas se faire au détriment de la qualité des services offerts aux clients.

L'AMSB doit être périodiquement informé des risques identifiés et des défaillances observées dans le cadre de la sous-traitance de services en nuage liée à des activités ou fonctions opérationnelles importantes ou critiques.

Afin d'assurer le suivi et la supervision adéquats de leurs accords de sous-traitance de services en nuage, les entreprises doivent employer suffisamment de ressources ayant les connaissances et les compétences adéquates pour contrôler les services sous-traités en nuage. Le personnel de l'entreprise chargé de ces activités doit posséder les connaissances en matière de TIC et de gestion d'entreprise jugées nécessaires.

17. Droit de résiliation et stratégies de retrait

En cas de sous-traitance de services en nuage liée à des activités ou fonctions opérationnelles importantes ou critiques, l'entreprise doit prévoir, dans le cadre de l'accord de sous-traitance de services en nuage, une clause de stratégie de retrait clairement définie qui lui permette de résilier l'accord, le cas échéant. La résiliation doit être rendue possible sans nuire à la continuité et à la qualité des services qu'elle fournit aux preneurs. Pour ce faire, l'entreprise doit:

a) élaborer des plans de sortie complets, basés sur les services, documentés et suffisamment testés (par exemple, en effectuant une analyse des coûts potentiels, des impacts, des ressources et des conséquences en matière de délais des différentes options de sortie possibles);

b) identifier des solutions alternatives et élaborer des plans de transition appropriés et réalisables pour lui permettre de retirer et de transférer les activités et les données existantes, du prestataire de services en nuage vers d'autres prestataires de services, ou de les renvoyer à l'entreprise. Ces solutions doivent être définies en tenant compte des difficultés qui peuvent survenir en raison de la localisation des données, en prenant les mesures nécessaires pour assurer la continuité des activités pendant la phase de transition;

c) veiller à ce que le prestataire de services en nuage lui apporte un soutien adéquat lors du transfert des données, systèmes ou applications sous-traités à un autre prestataire de services ou directement à l'entreprise;

d) convenir avec le prestataire de services en nuage qu'une fois retransférées à l'entreprise, ses données seront supprimées complètement et de manière sécurisée par le prestataire de services en nuage dans toutes les régions.

Lors de l'élaboration des stratégies de retrait, l'entreprise doit:

a) définir les objectifs de la stratégie de retrait;

b) définir les événements déclencheurs (par exemple, des indicateurs de risque clés signalant un niveau de service inacceptable) qui pourraient activer la stratégie de retrait;

c) réaliser une analyse de l'impact sur l'activité proportionnellement aux activités sous-traitées afin de déterminer les ressources humaines et matérielles nécessaires à la mise en œuvre du plan de sortie ainsi que le temps requis à cet effet;

d) attribuer les fonctions et les responsabilités pour la gestion des plans de sortie et des activités de transition;

e) élaborer des critères de réussite de la transition.

18. Contrôle des accords de sous-traitance de services en nuage par les autorités de contrôle

Le CAA procède à l'analyse des incidences potentielles des accords de sous-traitance de services en nuage conclus par les entreprises dans le cadre de leur processus de contrôle prudentiel. L'analyse des incidences se concentre, en particulier, sur les accords de sous-traitance liés à des activités ou fonctions opérationnelles importantes ou critiques.

Dans le cadre du contrôle des accords de sous-traitance de services en nuage conclus par les entreprises, le CAA prend en considération les risques suivants:

a) les risques liés aux TIC;

b) les autres risques opérationnels (y compris les risques juridiques et de non- conformité, le risque lié à la sous-traitance et à la gestion par un tiers);

c) le risque pour la réputation;

d) le risque de concentration, y compris au niveau des pays et des secteurs.

Dans son évaluation, le CAA inclut les aspects suivants selon une approche fondée sur le risque:

a) la pertinence et l'efficacité des procédures de gouvernance et des procédures opérationnelles de l'entreprise liées à l'approbation, à la mise en œuvre, au suivi, à la gestion et au renouvellement des accords de sous-traitance de services en nuage;

b) si l'entreprise dispose de ressources suffisantes ayant les connaissances et les compétences adéquates pour contrôler les services sous-traités en nuage;

c) si l'entreprise identifie et gère tous les risques mis en évidence par la présente lettre circulaire.

Dans le cas d'un groupe, le contrôleur du groupe doit veiller à ce que les incidences de la sous-traitance de services en nuage liée à des activités ou fonctions opérationnelles importantes ou critiques soient prises en compte dans l'évaluation des risques liés au contrôle du groupe, en tenant compte des exigences énoncées aux paragraphes 2 et 3 du point 18 de la présente lettre circulaire et des caractéristiques individuelles de gouvernance et opérationnelles du groupe.

Si la sous-traitance de services en nuage liée à des activités ou fonctions opérationnelles importantes ou critiques implique plusieurs entreprises établies dans différents États membres et est gérée de manière centralisée par la société mère ou par une filiale du groupe (par exemple, une entreprise ou une société de services du groupe telle que le fournisseur de TIC du groupe), le contrôleur du groupe et/ou les autorités de contrôle compétentes des entreprises concernées par la sous-traitance de services en nuage doivent discuter, le cas échéant, des incidences de la sous-traitance de services en nuage sur le profil de risque du groupe au sein du collège des contrôleurs.

Lorsque des préoccupations sont identifiées qui conduisent à conclure qu'une entreprise ne dispose plus d'accords de gouvernance solides ou ne se conforme pas aux exigences réglementaires, le CAA prend des mesures appropriées, telles que, par exemple, exiger de l'entreprise qu'elle améliore l'accord de gouvernance, limiter ou restreindre le champ d'application des fonctions sous-traitées ou exiger sa sortie d'un ou de plusieurs accords de sous-traitance. En particulier, compte tenu de la nécessité pour l'entreprise de veiller à la continuité des opérations, l'annulation de contrats pourrait être nécessaire si la surveillance et le respect des exigences réglementaires ne peuvent être garantis par d'autres mesures.

Dispositions finales

La présente lettre circulaire s'applique à partir du 1er novembre 2021 à tous les accords de sous-traitance de services en nuage conclus ou modifiés à partir de cette date.

Les entreprises doivent réviser et modifier en conséquence les accords existants de sous-traitance de services en nuage liés à des activités ou fonctions opérationnelles importantes ou critiques en vue d'assurer le respect des présentes orientations le 31 décembre 2022 au plus tard.

Dans les cas où la révision des accords de sous-traitance de services en nuage liée à des activités ou fonctions opérationnelles importantes ou critiques ne serait pas achevée d'ici le 31 décembre 2022, l'entreprise doit en informer le CAA en indiquant les mesures prévues pour conclure la révision ou l'éventuelle stratégie de retrait.

Le Comité de Direction