30/09/2025
ESMA65-294529287-4737

Orientations

relatives à la sous-traitance à des prestataires de services en nuage

Table des matières

1 Champ d'application

Qui ?

1. Les présentes orientations s'appliquent aux autorités compétentes et i) aux dépositaires de fonds d'investissement alternatifs (FIA) visés à l'article 21, paragraphe 3, point c), et à l'article 21, paragraphe 3, troisième alinéa, de la directive AIFMD, lorsqu'ils ne sont pas des entités financières auxquelles le règlement DORA s'applique, et ii) aux dépositaires d'OPCVM visés à l'article 23, paragraphe 2, point c), de la directive OPCVM, lorsqu'ils ne sont pas des entités financières auxquelles le règlement DORA s'applique.[1]

Quoi ?

2. Les présentes orientations s'appliquent suivant les dispositions ci-après :

   a) pour les dépositaires de FIA : l'article 21 de la directive sur les gestionnaires de fonds d'investissement alternatifs ; article 98 du règlement délégué (UE) 2013/231 de la Commission ;

   b) pour les dépositaires d'OPCVM : les articles 22, 22 bis et 23, paragraphe 2, de la directive OPCVM ; article 32 de la directive 2010/43/UE de la Commission ; article 2, paragraphe 2, point j), article 3, paragraphe 1, article 13, paragraphe 2, articles 15, 16 et 22 du règlement délégué (UE) 2016/438 de la Commission.

Quand ?

3. Les présentes orientations s'appliquent à compter de la date de leur publication sur le site web de l'ESMA dans toutes les langues officielles de l'UE et à tous les accords d'externalisation en nuage conclus, renouvelés ou modifiés à compter de cette date.

4. Compte tenu de l'application du règlement DORA, les précédentes orientations de l'ESMAsur l'externalisation à des fournisseurs de services en nuage cessent de s'appliquer aux entités financières soumises au règlement DORA visées à l'article 2 dudit règlement. Pour les dépositaires de FIA et pour les dépositaires d'OPCVM visés au paragraphe 1 ci-dessus, les précédentes orientations de l'ESMA sur l'externalisation à des prestataires de services en nuage continueront de s'appliquer

[1] En ce qui concerne les accords d'externalisation vers le cloud, les entités financières telles que définies à l'article 2, paragraphes 1 et 2 du Règlement (UE) 2022/2554 du Parlement européen et du Conseil relatif à la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 (règlement DORA), sont soumises aux règles spécifiques énoncées dans le règlement DORA et les règlements délégués et d'exécution de la Commission.

jusqu'à la date de publication des présentes orientations sur le site web de l'ESMA dans toutes les langues officielles de l'UE.

2 Références législatives, abréviations et définitions

2.1 Références législatives

Règlement instituant l'ESMA	Règlement (UE) nº 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/77/CE de la Commission[2]
Directive AIFMD	Directive 2011/61/UE du Parlement européen et du Conseil du 8 juin 2011 sur les gestionnaires de fonds d'investissement alternatifs et modifiant les directives 2003/41/CE et 2009/65/CE ainsi que les règlements (CE) nº 1060/2009 et (UE) nº 1095/2010[3]
Règlement délégué (UE) 2013/231 de la Commission	Règlement délégué (UE) 2013/231 de la Commission du 19 décembre 2012 complétant la directive 2011/61/UE du Parlement européen et du Conseil en ce qui concerne les dérogations, les conditions générales d'exercice, les dépositaires, l'effet de levier, la transparence et la surveillance[4]
Directive OPCVM	Directive 2009/65/CE du Parlement européen et du Conseil du 13 juillet 2009 portant coordination des dispositions législatives, réglementaires et administratives concernant certains organismes de placement collectif en valeurs mobilières (OPCVM)[5]
Directive 2010/43/UE de la Commission	Directive 2010/43/UE de la Commission du 1er juillet 2010 portant mesures d'exécution de la directive 2009/65/CE du Parlement européen et du Conseil en ce qui concerne les exigences organisationnelles, les conflits d'intérêts, la

[2] JO L 331 du 15.12.2010, p. 84.
[3] JO L 174 du 1.7.2011, p. 1.
[4] JO L 83 du 22.3.2013, p. 1.
[5] JO L 302 du 17.11.2009, p. 32.

	conduite des affaires, la gestion des risques et le contenu de l'accord entre le dépositaire et la société de gestion[6]
Règlement DORA	Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011[7]
Règlement RGPD	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)[8]

2.2 Abréviations

CSP	Prestataire de services en nuage
ESMA	Autorité européenne des marchés financiers
UE	Union européenne

2.3 Définitions

fonction	tous processus, services ou activités;
fonction importante ou critique	toute fonction dont une anomalie ou une défaillance de l'exécution est susceptible de nuire sérieusement: a) au respect par une entreprise des obligations qui lui incombent en vertu de la législation applicable; b) à la performance financière d'une entreprise; ou

[6] JO L 176 du 10.7.2010, p. 42.
[7] *JO L 333 du 27.12.2022, p. 1.*
[8] JO L 119 du 4.5.2016, p. 1-88.

	c) à la solidité ou à la continuité des principaux services et activités d'une entreprise
services en nuage	services fournis au moyen de l'informatique en nuage;
informatique en nuage ou «nuage»[9]	concept qui permet l'accès en réseau à un ensemble modulable et variable de ressources physiques ou virtuelles partageables (par exemple, les serveurs, systèmes d'exploitation, réseaux, logiciels, applications et équipements de stockage) avec autoapprovisionnement et administration à la demande;
prestataire de services en nuage	tiers fournissant des services en nuage dans le cadre d'un accord de sous-traitance de services en nuage;
accord de sous-traitance de services en nuage	accord, quelle que soit sa forme, y compris les accords de délégation, entre: (i) une entreprise et un prestataire de services en nuage par lequel ce prestataire de services en nuage exerce une fonction qui serait autrement assurée par l'entreprise elle-même; ou (ii) une entreprise et un tiers qui n'est pas un prestataire de services en nuage, mais qui s'appuie de manière significative sur un prestataire de services en nuage pour exercer une fonction qui serait autrement assurée par l'entreprise elle-même. Dans ce cas, la référence à un «prestataire de services en nuage» dans les présentes orientations devrait être interprétée comme faisant référence à ce tiers.
sous-sous-traitance	situation dans laquelle le prestataire de services en nuage transfère la fonction sous-traitée (ou une partie de cette fonction) à un autre prestataire de services dans le cadre d'un accord de sous-traitance;

[9] Le terme «informatique en nuage» est souvent abrégé en «nuage». Le terme «nuage» est utilisé dans le reste du document pour faciliter la consultation.

modèle de déploiement en nuage	manière d'organiser le nuage en fonction du contrôle et du partage des ressources physiques ou virtuelles. Les modèles de déploiement en nuage comprennent les nuages communautaires[10], hybrides[11], privés[12] et publics[13];
entreprises	a) les dépositaires visés à l'article 21, paragraphe 3, point c), et à l'article 21, paragraphe 3, troisième alinéa, de la directive AIFMD [dépositaires de fonds d'investissement alternatifs (FIA)]; b) les dépositaires visés à l'article 23, paragraphe 2, point c), de la directive OPCVM («dépositaires d'OPCVM»).

3 Objectif

5. Les présentes orientations se fondent sur l'article 16, paragraphe 1, du règlement instituant l'ESMA. Les présentes orientations visent, d'une part, à établir des pratiques de surveillance cohérentes, efficientes et efficaces au sein du système européen de surveillance financière (ESFS) et, d'autre part, à assurer une application commune, uniforme et cohérente des exigences visées à la section 1.1 de la rubrique «Quoi?» lorsque les entreprises sous-traitent à des prestataires de services en nuage. En particulier, les présentes orientations visent à aider les entreprises et les autorités compétentes à identifier, traiter et assurer le suivi des risques et des défis découlant des accords de sous-traitance de services en nuage, depuis la décision de sous-traiter jusqu'à la mise en place de stratégies de retrait, en passant par la sélection d'un prestataire de services en nuage et le suivi des activités sous-traitées.

4 Obligations de conformité et de déclaration

4.1 Statut des orientations

6. En application de l'article 16, paragraphe 3, du règlement instituant l'ESMA, les autorités compétentes et les entreprises mettent tout en œuvre pour respecter les présentes orientations.

[10] Un modèle de déploiement en nuage où les services en nuage sont mis à la disposition exclusive et partagés par un groupe donné de clients de services en nuage ayant des exigences communes et liés les uns aux autres, et où les ressources sont contrôlées par au moins un membre de ce groupe;
[11] Un modèle de déploiement en nuage faisant intervenir au moins deux modèles de déploiement différents.
[12] Un modèle de déploiement en nuage où les services en nuage sont mis à la disposition exclusive d'un seul client de services en nuage, qui contrôle les ressources
[13] Un modèle de déploiement en nuage où les services en nuage sont susceptibles d'être proposés à n'importe quel client de services en nuage et les ressources sont contrôlées par le fournisseur de services en nuage

7. Les autorités compétentes auxquelles les présentes orientations s'appliquent devraient s'y conformer en les intégrant à leur cadre juridique et/ou de surveillance national, le cas échéant, y compris lorsque certaines orientations données visent en premier lieu les entreprises. Dans ce cas, les autorités compétentes devraient, par leur surveillance, veiller à ce que les entreprises se conforment aux orientations.

4.2 Exigences en matière de rapports

8. Dans un délai de deux mois à compter de la date de la publication des orientations sur le site web de l'ESMA dans toutes les langues officielles de l'UE, les autorités compétentes auxquelles s'appliquent les présentes orientations doivent notifier à l'ESMA si elles i) respectent, ii) ne respectent pas, mais entendent respecter, ou iii) ne respectent pas et n'entendent pas respecter les orientations.

9. En cas de non-respect, les autorités compétentes doivent également notifier à l'ESMA, dans un délai de deux mois à compter de la date de la publication des orientations sur le site web de l'ESMA dans toutes les langues officielles de l'UE, les motifs pour lesquels elles ne respectent pas les orientations. Un formulaire de notification est disponible sur le site web de l'ESMA. Une fois le formulaire rempli, il est transmis à l'ESMA.

10. Les entreprises ne sont pas tenues de notifier si elles se conforment ou non aux présentes orientations.

5 Orientations relatives à la sous-traitance à des prestataires de services en nuage

Orientation 1. Gouvernance, supervision et documentation

11. Une entreprise devrait avoir une stratégie de sous-traitance de services en nuage définie et actualisée, qui soit compatible avec les stratégies pertinentes de l'entreprise ainsi qu'avec les politiques et les procédures internes, notamment en ce qui concerne les technologies de l'information et de la communication, la sécurité de l'information et la gestion des risques opérationnels.

12. Une entreprise devrait:

    a) attribuer clairement les responsabilités en matière de documentation, de gestion et de contrôle des accords de sous-traitance de services en nuage au sein de son organisation;
    b) allouer des ressources suffisantes pour garantir le respect des présentes orientations et de toutes les exigences juridiques applicables à ses accords de sous-traitance de services en nuage;

c) établir une fonction de supervision de la sous-traitance de services en nuage ou désigner les membres de son personnel d'encadrement supérieur qui rendent compte directement à l'organe de direction et qui sont chargés de la gestion et de la supervision des risques des accords de sous-traitance de services en nuage. Lorsqu'elles appliquent cette orientation, les entreprises devraient prendre en compte la nature, l'ampleur et la complexité de leurs activités, y compris en termes de risque pour le système financier, et des risques inhérents aux fonctions sous-traitées et s'assurer que leur organe de direction possède les compétences techniques nécessaires pour comprendre les risques liés aux accords de sous-traitance de services en nuage. Les entreprises de petite taille et moins complexes devraient au moins assurer une répartition claire des tâches et des responsabilités pour la gestion et la supervision des accords de sous-traitance de services en nuage.

13. Une entreprise devrait suivre l'accomplissement des activités, les mesures de sécurité et le respect des niveaux de service convenus par ses prestataires de services en nuage. Ce suivi devrait être fondé sur le risque, en se concentrant principalement sur les fonctions importantes ou critiques qui ont été sous-traitées.

14. Une entreprise devrait réévaluer si ses accords de sous-traitance de services en nuage concernent une fonction importante ou critique, périodiquement et chaque fois que le risque, la nature ou l'ampleur d'une fonction sous-traitée a sensiblement changé.

15. Une entreprise devrait maintenir à jour un registre d'informations sur tous ses accords de sous-traitance de services en nuage, en faisant la distinction entre la sous-traitance de fonctions importantes ou critiques et les autres accords de sous-traitance. Pour faire la distinction entre la sous-traitance de fonctions importantes ou critiques et les autres accords de sous-traitance, l'entreprise devrait fournir un bref résumé des raisons pour lesquelles la fonction sous-traitée est ou n'est pas considérée comme importante ou critique. Dans le respect de la législation nationale, une entreprise devrait également tenir un registre des accords de sous-traitance de services en nuage résiliés pendant une période appropriée.

16. Pour les accords de sous-traitance de services en nuage qui concernent des fonctions importantes ou critiques, le registre devrait inclure au moins les informations suivantes, pour chaque accord de sous-traitance de services en nuage:

    a) un numéro de référence;
    b) 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;
    c) une brève description de la fonction sous-traitée, y compris les données qui sont sous-traitées et si ces données comprennent des données à caractère personnel

(par exemple en fournissant une indication par «Oui» ou «Non» dans un champ de données distinct);

d) une catégorie attribuée par l'entreprise pour refléter la nature de la fonction sous-traitée (par exemple, une technologie de l'information, une fonction de contrôle), qui devrait faciliter l'identification des différents types d'accords de sous-traitance de services en nuage;
e) si la fonction importante ou critique sous-traitée soutient ou non des opérations métier soumises à des exigences horaires pour leur fonctionnement;
f) le nom ou la marque (le cas échéant) du prestataire de services en nuage, son pays d'immatriculation, le numéro d'immatriculation de la société, l'identifiant de la personne morale (si disponible), son siège social, ses coordonnées pertinentes, ainsi que le nom de son entreprise mère (le cas échéant);
g) la législation applicable à l'accord de sous-traitance de services en nuage et, le cas échéant, le choix de la juridiction;
h) le type de modèles de services et de déploiement en nuage, ainsi que la nature spécifique des données détenues et les lieux (à savoir les régions ou les pays) où ces données peuvent être stockées;
i) la date de la dernière évaluation du caractère important ou critique de la fonction sous-traitée; et la date de la prochaine évaluation prévue;
j) la date de la dernière évaluation des risques/du dernier audit du prestataire de services en nuage, accompagnée d'un bref résumé des principaux résultats, et la date de la prochaine évaluation des risques prévue/du prochain audit prévu;
k) la personne ou l'organe de décision de l'entreprise qui a approuvé l'accord de sous-traitance de services en nuage;
l) le nom des éventuels sous-sous-traitants auxquels une fonction importante ou critique (ou des parties significatives de celle-ci) est sous-sous-traitée, y compris les pays où les sous-sous-traitants sont enregistrés, où le service sous-sous-traité sera exécuté et les lieux (à savoir les régions ou les pays) où les données seront stockées;
m) le coût budgétaire annuel estimé de l'accord de sous-traitance de services en nuage.

17. Pour les accords de sous-traitance de services en nuage qui concernent des fonctions non importantes ou non critiques, une entreprise devrait définir les informations à inclure dans le registre en fonction de la nature, de l'ampleur et de la complexité des risques inhérents à la fonction sous-traitée.

Orientation 2. Analyse préalable à la sous-traitance et procédure de vigilance

18. Avant de conclure un quelconque accord de sous-traitance de services en nuage, une entreprise devrait:

a) évaluer si l'accord de sous-traitance de services en nuage concerne une fonction importante ou critique;
b) identifier et évaluer tous les risques pertinents de l'accord de sous-traitance de services en nuage;
c) mettre en œuvre une procédure de vigilance à l'égard du prestataire de services en nuage potentiel;
d) identifier et évaluer les conflits d'intérêts que la sous-traitance pourrait entraîner.

19. L'analyse préalable à la sous-traitance et la procédure de vigilance à l'égard du prestataire de services en nuage potentiel devraient être proportionnées à la nature, à l'ampleur et à la complexité de la fonction que l'entreprise entend sous-traiter et aux risques inhérents à cette fonction. Elles devraient au moins comprendre une évaluation de l'incidence potentielle de l'accord de sous-traitance de services en nuage sur les risques opérationnels, juridiques, de non-conformité et pour la réputation de l'entreprise.

20. Si l'accord de sous-traitance de services en nuage concerne des fonctions importantes ou critiques, une entreprise devrait également:

a) évaluer tous les risques pertinents qui peuvent résulter de l'accord de sous-traitance de services en nuage, y compris les risques liés aux technologies de l'information et de la communication, à la sécurité de l'information, à la continuité des activités, à la législation et à la conformité, les risques pour la réputation, les risques opérationnels et les éventuelles limites de la supervision de l'entreprise posées par:
   i. le service en nuage choisi et les modèles de déploiement proposés;
   ii. les procédures de migration et/ou de mise en œuvre;
   iii. la sensibilité de la fonction et des données connexes qu'il est envisagé de sous-traiter et les mesures de sécurité qui devraient être prises;
   iv. l'interopérabilité des systèmes et des applications de l'entreprise et du prestataire de services en nuage, à savoir leur capacité à échanger des informations et à utiliser mutuellement les informations échangées;
   v. la portabilité des données de l'entreprise, à savoir la capacité de transférer facilement les données de l'entreprise d'un prestataire de services en nuage à un autre ou de les renvoyer à l'entreprise;
   vi. la stabilité politique, la situation en matière de sécurité et le système juridique (y compris les dispositions répressives en place, les dispositions de la législation en matière d'insolvabilité qui s'appliqueraient en cas de faillite du prestataire de services en nuage, les lois sur la protection des données en vigueur et la question de savoir si les conditions de transfert de données à caractère personnel vers un pays tiers dans le cadre du règlement RGPD sont remplies) des pays (au sein ou en dehors de l'UE) où les fonctions sous-traitées seraient assurées et où les données sous-traitées seraient stockées; en cas de sous-sous-traitance, les risques

supplémentaires qui peuvent survenir si le sous-sous-traitant est situé dans un pays tiers ou un pays différent de celui du prestataire de services en nuage et, dans le cas d'une chaîne de sous-sous-traitance, tout risque supplémentaire qui peut survenir, y compris en relation avec l'absence de contrat direct entre l'entreprise et le sous-sous-traitant qui exécute la fonction sous-traitée;

vii. une éventuelle concentration au sein de l'entreprise (notamment, le cas échéant, au niveau de son groupe) causée par des accords de sous-traitance de services en nuage multiples avec le même prestataire de services en nuage ainsi qu'une éventuelle concentration au sein du secteur financier européen, causée par de multiples entreprises faisant appel au même prestataire de services en nuage ou à un petit groupe de prestataires de services en nuage. Lors de l'évaluation du risque de concentration, l'entreprise devrait tenir compte de tous ses accords de sous-traitance de services en nuage (et, le cas échéant, des accords de sous-traitance de services en nuage au niveau de son groupe) avec ce prestataire de services en nuage;

b) tenir compte des coûts et avantages attendus de l'accord de sous-traitance de services en nuage, 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.

21. En cas de sous-traitance de fonctions importantes ou critiques, la procédure de vigilance devrait inclure une évaluation de l'adéquation du prestataire de services en nuage. Lorsqu'elle évalue l'adéquation du prestataire de services en nuage, une entreprise devrait veiller à ce que le prestataire de services en nuage possède la réputation commerciale, les compétences, les ressources (notamment humaines, informatiques et financières), la structure organisationnelle et, le cas échéant, l'(les) agrément(s) ou l'(les) enregistrement(s) pertinent(s) pour exercer la fonction importante ou critique de manière fiable et professionnelle et pour satisfaire à ses obligations pendant toute la durée de l'accord de sous-traitance de services en nuage. D'autres facteurs à prendre en considération quant à la procédure de vigilance à l'égard du prestataire de services en nuage comprennent notamment, mais sans limitation aucune:

a) la gestion de la sécurité de l'information et en particulier la protection des données personnelles, confidentielles ou autrement sensibles;
b) le service après-vente, y compris les plans et les contacts d'assistance, et les procédures de gestion des incidents;
c) les plans de continuité des activités et de rétablissement après sinistre.

22. Le cas échéant et afin d'étayer la procédure de vigilance mise en œuvre, une entreprise peut également utiliser des certifications fondées sur des normes internationales et des rapports d'audit interne ou externe.

23. Si une 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, si nécessaire, mettre de nouveau en œuvre l'analyse préalable à la sous-traitance et la procédure de vigilance à l'égard du prestataire de services en nuage.

24. Si une entreprise conclut un nouvel accord ou renouvelle un accord existant avec un prestataire de services en nuage qui a déjà fait l'objet d'une évaluation, elle devrait déterminer, selon une approche fondée sur le risque, si la mise en œuvre d'une nouvelle procédure de vigilance est nécessaire.

Orientation 3. Éléments contractuels clés

25. Les droits et obligations respectifs d'une entreprise et de son prestataire de services en nuage devraient être clairement consignés dans un accord écrit.

26. L'accord écrit devrait prévoir expressément la possibilité pour l'entreprise de le résilier, le cas échéant.

27. En cas de sous-traitance de fonctions importantes ou critiques, l'accord écrit devrait comprendre au moins:

    a) une description claire de la fonction sous-traitée;

    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 législation applicable à l'accord et, le cas échéant, le choix de la juridiction;

    d) les obligations financières de l'entreprise et du prestataire de services en nuage;

    e) si la sous-sous-traitance est autorisée et, dans l'affirmative, dans quelles conditions, compte tenu de l'orientation 7;

    f) le(s) lieu(x) (à savoir les régions ou les pays) où la fonction sous-traitée sera assurée et où les données seront traitées et stockées, et les conditions à remplir, y compris l'obligation d'informer l'entreprise si le prestataire de services en nuage envisage de modifier le(s) lieu(x);

    g) les dispositions relatives à la sécurité de l'information et à la protection des données à caractère personnel, compte tenu de l'orientation 4;

    h) le droit pour l'entreprise d'assurer un suivi régulier des performances du prestataire de services en nuage dans le cadre de l'accord de sous-traitance de services en nuage, compte tenu de l'orientation 6;

    i) les niveaux de service convenus, qui devraient inclure des objectifs de performance quantitatifs et qualitatifs 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;

j) les obligations d'information du prestataire de services en nuage envers l'entreprise et, 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 préparés par la fonction d'audit interne du prestataire de services en nuage;

k) des dispositions concernant la gestion des incidents par le prestataire de services en nuage, y compris l'obligation pour le prestataire de services en nuage de signaler à l'entreprise, sans retard injustifié, les incidents qui ont affecté le fonctionnement du service contractuel de l'entreprise;

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) les exigences pour que le prestataire de services en nuage mette en œuvre et teste les plans de continuité des activités et de rétablissement après sinistre;

n) l'obligation pour le prestataire de services en nuage d'accorder à l'entreprise, à ses autorités compétentes et à toute autre personne désignée par l'entreprise ou les autorités compétentes le droit d'accéder («droits d'accès») et d'inspecter («droits d'audit») les informations, les locaux, les systèmes et les dispositifs pertinents du prestataire de services en nuage dans la mesure où cela est nécessaire pour suivre les performances du prestataire de services en nuage dans le cadre de l'accord de sous-traitance de services en nuage et sa conformité aux exigences réglementaires et contractuelles en vigueur, compte tenu de l'orientation 6;

o) des dispositions visant à garantir que les données que le prestataire de services en nuage traite ou stocke pour le compte de l'entreprise puissent être consultées, récupérées et restituées à l'entreprise en cas de besoin, compte tenu de l'orientation 5.

Orientation 4. Sécurité de l'information

28. Une entreprise devrait fixer des exigences en matière de sécurité de l'information dans ses politiques et procédures internes et dans l'accord écrit de sous-traitance de services en nuage et vérifier de manière continue le respect de ces exigences, notamment pour protéger les données confidentielles, personnelles ou autrement sensibles. Ces exigences devraient être proportionnées à la nature, à l'ampleur et à la complexité de la fonction que l'entreprise sous-traite vers le prestataire de services en nuage et aux risques inhérents à cette fonction.

29. À cette fin, en cas de sous-traitance de fonctions importantes ou critiques, et sans préjudice des exigences applicables prévues par le règlement RGPD, une entreprise, appliquant une approche fondée sur le risque, devrait au moins:

a) *organisation de la sécurité de l'information:* veiller à une répartition claire des rôles et responsabilités en matière de sécurité de l'information entre l'entreprise et le prestataire de services en nuage, notamment en ce qui concerne la détection des menaces, la gestion des incidents et la gestion des correctifs, et s'assurer que le prestataire de services en nuage est effectivement en mesure d'assumer ses rôles et responsabilités;
b) *gestion des identités et des accès:* veiller à ce que des mécanismes d'authentification forte (par exemple, authentification multifacteurs) et des contrôles d'accès soient mis en place afin d'empêcher tout accès non autorisé aux données de l'entreprise et aux ressources back-end en nuage;
c) *chiffrement et gestion des clés:* veiller à ce que des technologies de chiffrement appropriées soient utilisées, le cas échéant, pour les données en transit, les données en mémoire, les données au repos et les sauvegardes de données, en association avec des solutions de gestion des clés appropriées pour limiter le risque d'accès non autorisé aux clés de chiffrement; en particulier, l'entreprise devrait envisager des technologies et des processus de pointe lors du choix de sa solution de gestion des clés;
d) *sécurité des opérations et des réseaux:* envisager des niveaux appropriés de disponibilité des réseaux, de segmentation des réseaux (par exemple, isolement des locataires dans l'environnement partagé du nuage, séparation opérationnelle en ce qui concerne le web, la logique applicative, le système d'exploitation, le réseau, le système de gestion de bases de données (SGBD) et les couches de stockage) et des environnements de traitement (par exemple, tests, tests d'acceptation par l'utilisateur, développement, production);
e) *interfaces de programmation d'applications (API):* examiner les mécanismes d'intégration des services en nuage avec les systèmes de l'entreprise afin de garantir la sécurité des API (par exemple, établir et maintenir des politiques et procédures de sécurité de l'information pour les API par le biais de plusieurs interfaces systèmes, juridictions et fonctions d'entreprise afin d'empêcher la divulgation, la modification ou la destruction non autorisée de données);
f) *continuité des activités et rétablissement après sinistre:* veiller à la mise en place de contrôles efficaces en matière de continuité des activités et de rétablissement après sinistre (par exemple en fixant des exigences minimales de capacité, en sélectionnant des options d'hébergement géographiquement dispersées, avec la possibilité de passer de l'une à l'autre, ou en demandant et en examinant la documentation relative au mode de transport des données de l'entreprise entre les différents systèmes du prestataire de services en nuage, ainsi qu'en envisageant la possibilité de reproduire les images des machines dans un lieu de stockage indépendant, suffisamment isolé du réseau ou mis hors ligne);

g) *localisation des données*: adopter une approche fondée sur le risque en ce qui concerne le stockage des données et le(s) lieu(x) de traitement des données (à savoir les régions ou les pays);
h) *conformité et suivi*: vérifier que le prestataire de services en nuage respecte les normes de sécurité de l'information internationalement reconnues et a mis en place des contrôles de sécurité de l'information appropriés (par exemple en demandant au prestataire de services en nuage de fournir la preuve qu'il effectue des examens pertinents de la sécurité de l'information et en effectuant des évaluations et des tests réguliers des mesures de sécurité de l'information du prestataire de services en nuage).

Orientation 5. Stratégies de retrait

30. En cas de sous-traitance de fonctions importantes ou critiques, une entreprise devrait s'assurer qu'elle est en mesure de se retirer de l'accord de sous-traitance de services en nuage sans perturber indûment ses activités économiques et les services qu'elle fournit à ses clients, et sans que ce soit au détriment du respect des obligations qui lui incombent en vertu de la législation applicable, ni de la confidentialité, de l'intégrité et de la disponibilité de ses données. À cet effet, une entreprise devrait:

a) élaborer des plans de retrait complets, documentés et suffisamment testés. Ces plans devraient être mis à jour si nécessaire, y compris en cas de modifications de la fonction sous-traitée;
b) identifier des solutions alternatives et élaborer des plans de transition pour retirer et transférer la fonction et les données sous-traitées, du prestataire de services en nuage et, le cas échéant, de tout sous-sous-traitant, vers un autre prestataire de services en nuage indiqué par l'entreprise ou les renvoyer directement à l'entreprise. Ces solutions devraient être définies en tenant compte des difficultés qui peuvent survenir 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 l'accord écrit de sous-traitance de services en nuage comporte l'obligation pour le prestataire de services en nuage de soutenir le transfert ordonné de la fonction sous-traitée et le traitement des données y afférent, du prestataire de services en nuage et de tout sous-sous-traitant vers un autre prestataire de services en nuage indiqué par l'entreprise ou directement à l'entreprise au cas où celle-ci activerait la stratégie de retrait. L'obligation de soutenir le transfert ordonné de la fonction sous-traitée, et le traitement des données y afférent, devrait inclure, le cas échéant, la suppression sécurisée des données des systèmes du prestataire de services en nuage et de tout sous-sous-traitant.

31. Lors de l'élaboration des plans et des solutions de retrait visés aux points a) et b) ci-dessus («stratégie de retrait»), l'entreprise devrait envisager les mesures suivantes:

a) définir les objectifs de la stratégie de retrait;
b) définir les événements déclencheurs qui pourraient activer la stratégie de retrait. Ces mesures devraient comprendre au moins la résiliation de l'accord de sous-traitance de services en nuage à l'initiative de l'entreprise ou du prestataire de services en nuage et l'échec ou toute autre interruption portant à conséquences de l'activité du prestataire de services en nuage;
c) réaliser une analyse de l'impact sur l'activité qui soit proportionnée à la fonction sous-traitée afin de déterminer les ressources humaines et matérielles nécessaires à la mise en œuvre de la stratégie de retrait;
d) attribuer les rôles et les responsabilités pour gérer la stratégie de retrait;
e) tester la pertinence de la stratégie de retrait, en utilisant une approche fondée sur le risque (par exemple, en effectuant une analyse des coûts potentiels, des impacts, des ressources et des conséquences en matière de délais de transfert d'un service sous-traité vers un autre prestataire);
f) élaborer des critères de réussite de la transition.

32. Une entreprise devrait inclure des indicateurs des événements déclencheurs de la stratégie de retrait dans son suivi et sa supervision continus des services fournis par le prestataire de services en nuage dans le cadre de l'accord de sous-traitance de services en nuage.

Orientation 6. Droits d'accès et d'audit

33. Une entreprise devrait s'assurer que l'accord écrit de sous-traitance de services en nuage n'empêche pas l'entreprise et l'autorité compétente d'exercer effectivement ses droits d'accès et d'audit et les options de supervision du prestataire de services en nuage.

34. Une entreprise devrait s'assurer que l'exercice des droits d'accès et d'audit (par exemple, la fréquence des audits et les domaines et services devant faire l'objet d'un audit) prend en considération le fait que la sous-traitance est liée à une fonction importante ou critique, ainsi que la nature et l'ampleur des risques et les incidences potentielles de l'accord de sous-traitance de services en nuage sur l'entreprise.

35. Si l'exercice des 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 en ayant un impact sur les niveaux de service, la confidentialité, l'intégrité et la disponibilité des données), le prestataire de services en nuage devrait fournir à l'entreprise une justification claire des raisons pour lesquelles cela créerait un risque et le prestataire de services en nuage devrait convenir avec l'entreprise d'autres moyens d'obtenir un résultat 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).

36. 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 accords de sous-traitance de services en nuage, avoir recours:

    a) à des certifications et à des rapports d'audit interne ou externe de tiers mis à disposition par le prestataire de services en nuage;
    b) à des audits groupés effectués conjointement avec d'autres clients du même prestataire de services en nuage ou à des audits groupés effectués par un auditeur tiers désigné par plusieurs clients du même prestataire de services en nuage.

37. En cas de sous-traitance de fonctions importantes ou critiques, une entreprise devrait évaluer si les certifications et les rapports d'audit interne ou externe de tiers visés au paragraphe 37, point a), sont adéquats et suffisants pour respecter les obligations qui lui incombent en vertu de la législation applicable et devrait s'efforcer de ne pas s'appuyer uniquement sur ces certifications et rapports au fil du temps.

38. En cas de sous-traitance de fonctions importantes ou critiques, une entreprise ne devrait recourir aux certifications et aux rapports d'audit interne ou externe de tiers visés au paragraphe 37, point a), que si elle:

    a) estime que le périmètre des certifications ou des rapports d'audit couvre les systèmes essentiels du prestataire de services en nuage (par exemple, les processus, les applications, les infrastructures, les centres de données), les contrôles essentiels identifiés par l'entreprise ainsi que le respect de la législation pertinente applicable;
    b) évalue de manière approfondie et régulière le contenu des certifications ou des rapports d'audit, et s'assure que les certifications ou les rapports ne sont pas obsolètes;
    c) s'assure que les systèmes et contrôles essentiels du prestataire de services en nuage sont couverts dans les futures versions des certifications ou des rapports d'audit;
    d) est satisfaite 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, ses qualifications, son expertise ainsi que la réexécution/vérification des éléments probants inclus dans le dossier d'audit sous-jacent);
    e) s'assure 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 des contrôles essentiels en place;
    f) a le droit contractuel de demander l'extension du périmètre des certifications ou des rapports d'audit à d'autres systèmes et contrôles pertinents du prestataire de services en nuage; le nombre et la fréquence de ces demandes de modification du périmètre devraient être raisonnables et légitimes du point de vue de la gestion des risques;

g) conserve le droit contractuel d'effectuer, à sa discrétion, des audits sur site en ce qui concerne la fonction sous-traitée.

39. Une entreprise devrait veiller à ce que, avant une visite sur place, y compris par un tiers désigné par l'entreprise (par exemple un auditeur), un avis préalable soit fourni dans un délai raisonnable au prestataire de services en nuage, à moins qu'une notification préalable ne soit pas possible en raison d'une situation d'urgence ou de crise ou qu'elle conduise à une situation où l'audit ne serait plus efficace. Cet avis devrait indiquer le lieu, le but de la visite et le personnel qui y participera.

40. Compte tenu du niveau élevé de complexité technique des solutions en nuage et des problèmes juridictionnels spécifiques qu'elles posent, le personnel chargé de l'audit - qu'il s'agisse des auditeurs internes de l'entreprise ou d'auditeurs agissant en son nom - devrait avoir les compétences et les connaissances nécessaires pour évaluer correctement les services en nuage concernés et procéder à un audit efficace et pertinent. Cela devrait également s'appliquer au personnel des entreprises qui examine les certifications ou les rapports d'audit fournis par le prestataire de services en nuage.

Orientation 7. Sous-sous-traitance

41. Si la sous-sous-traitance de fonctions importantes ou critiques (ou des parties significatives de celles-ci) est permise, l'accord de sous-traitance de services en nuage entre l'entreprise et le prestataire de services en nuage devrait:

a) préciser toute partie ou tout aspect de la fonction sous-traitée qui est exclu d'une sous-sous-traitance potentielle;
b) indiquer les conditions à respecter en cas de sous-sous-traitance;
c) préciser que le prestataire de services en nuage reste responsable et est tenu de superviser les services qu'il a sous-sous-traités afin de s'assurer que toutes les obligations contractuelles entre le prestataire de services en nuage et l'entreprise sont constamment respectées;
d) comprendre l'obligation pour le prestataire de services en nuage de signaler à l'entreprise toute sous-sous-traitance prévue ou les changements substantiels apportés à celle-ci, en particulier lorsque cela pourrait affecter la capacité du prestataire de services de communication à respecter ses obligations au titre de l'accord de sous-traitance de services en nuage conclu avec l'entreprise. La période de notification fixée dans l'accord écrit devrait laisser à l'entreprise suffisamment de temps pour procéder au moins à une évaluation des risques de la sous-sous-traitance proposée ou des changements substantiels apportés à celle-ci et pour s'y opposer ou les approuver explicitement, comme indiqué au point e) ci-dessous;
e) s'assurer que l'entreprise a le droit de s'opposer à la sous-sous-traitance prévue ou aux changements substantiels apportés à celle-ci, ou qu'une approbation

explicite est nécessaire avant que la sous-sous-traitance proposée ou les changements substantiels apportés n'entrent en vigueur;

f) s'assurer que l'entreprise a le droit contractuel de résilier l'accord de sous-traitance de services en nuage avec le prestataire de services en nuage dans le cas où elle s'oppose à la sous-sous-traitance proposée ou aux changements substantiels apportés à celle-ci et en cas de sous-sous-traitance abusive (par exemple lorsque le prestataire de services en nuage procède à la sous-sous-traitance sans en informer l'entreprise ou lorsqu'il enfreint gravement les conditions de la sous-sous-traitance spécifiées dans le contrat de sous-traitance).

42. L'entreprise devrait s'assurer que le prestataire de services en nuage supervise de manière appropriée le sous-sous-traitant.

Orientation 8. Notification écrite aux autorités compétentes

43. L'entreprise devrait notifier par écrit à son autorité compétente, en temps utile, les accords de sous-traitance de services en nuage prévus qui concernent une fonction importante ou critique. L'entreprise devrait également notifier en temps utile et par écrit à son autorité compétente les accords de sous-traitance de services en nuage qui concernent une fonction précédemment classée comme non importante ou non critique et qui est ensuite devenue importante ou critique.

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

a) la date de début de l'accord de sous-traitance de services en nuage 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;
b) une brève description de la fonction sous-traitée;
c) un bref résumé des raisons pour lesquelles la fonction sous-traitée est considérée comme importante ou critique;
d) le nom ou la marque (le cas échéant) du prestataire de services en nuage, son pays d'immatriculation, le numéro d'immatriculation de la société, l'identifiant de la personne morale (si disponible), son siège social, ses coordonnées pertinentes, ainsi que le nom de son entreprise mère (le cas échéant);
e) la législation applicable à l'accord de sous-traitance de services en nuage et, le cas échéant, le choix de la juridiction;
f) les modèles de déploiement en nuage et la nature spécifique des données détenues par le prestataire de services en nuage et les lieux (à savoir les régions ou les pays) où ces données seront stockées;
g) la date de la dernière évaluation du caractère important ou critique de la fonction sous-traitée;

h) la date de la dernière évaluation des risques ou du dernier audit du prestataire de services en nuage, accompagnée d'un bref résumé des principaux résultats, et la date de la prochaine évaluation des risques ou du prochain audit prévu;
i) la personne ou l'organe de décision de l'entreprise qui a approuvé l'accord de sous-traitance de services en nuage;
j) le nom des éventuels sous-sous-traitants auxquels des parties significatives d'une fonction importante ou critique sont sous-sous-traitées, y compris le pays ou la région où les sous-sous-traitants sont enregistrés, où le service sous-sous-traité sera exécuté, et où les données seront stockées.

Orientation 9. Surveillance des accords de sous-traitance de services en nuage

45. Les autorités compétentes devraient évaluer les risques découlant des accords de sous-traitance de services en nuage conclus par les entreprises dans le cadre de leur processus de surveillance. Cette évaluation devrait notamment porter sur les accords relatifs à la sous-traitance de fonctions importantes ou critiques.

46. Les autorités compétentes devraient s'assurer qu'elles sont en mesure de mener une surveillance efficace, en particulier lorsque les entreprises sous-traitent des fonctions importantes ou critiques exercées en dehors de l'UE.

47. Les autorités compétentes devraient évaluer, selon une approche fondée sur le risque, si les entreprises:

a) mettent en place la gouvernance, les ressources et les processus opérationnels nécessaires pour conclure, mettre en œuvre et superviser de manière appropriée et efficace des accords de sous-traitance de services en nuage;
b) identifient et gèrent tous les risques pertinents liés à la sous-traitance de services en nuage.

48. Lorsque des risques de concentration sont identifiés, les autorités compétentes devraient suivre l'évolution de ces risques et évaluer à la fois leur impact potentiel sur les autres entreprises qu'elles surveillent et la stabilité du marché financier.