Sous-traitance à des prestataires de services en nuage

Quelles orientations pour les sociétés de gestion?

Décembre 2022

Obligations & objectifs des orientations de l'ESMA

Suite à la **publication** des **orientations de l'ESMA** concernant la **sous-traitance à des prestataires de services en nuage (cloud)** et à la déclaration de l'Autorité des Marchés Financiers (**AMF**) de s'y **conformer**, les sociétés de gestion sont tenues de **réexaminer leurs accords** de sous-traitance cloud afin de se conformer à leur tour aux orientations de l'ESMA.

Ces orientations ont pour **objectifs** de permettre aux sociétés de gestion ainsi qu'aux autorités compétentes de **mettre en avant**, de **traiter**, et **d'assurer le suivi des risques** et **menaces** qui résultent des accords de sous-traitance de services cloud, et ce sur **l'ensemble de la chaîne** allant de 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 par le suivi des activités sous-traitées.

Dates clés

31/05/2021 : Publication des orientations de l'ESMA concernant les accords de sous-traitance de services cloud

06/07/2021 : Accord de l'AMF pour se conformer aux orientations

31/07/2021 : Entrée en vigueur des orientations de l'ESMA

Mise en conformité aux orientations publiées par l'ESMA

31/12/2022 : Date limite pour se conformer aux orientations de l'ESMA

Orientations de l'ESMA

Les orientations émises par l'ESMA et avec lesquelles les sociétés de gestion doivent se mettre en conformité sont au nombre de 9 :

I. Gouvernance, supervision et documentation

Les sociétés de gestion faisant appel à des sous-traitants de services cloud sont tenues de **définir** et **actualiser** des **stratégies de sous-traitance de services en nuage**. Des **procédures** et une **organisation en interne** doivent être mises en place afin d'**assurer** le **contrôle des accords** de sous-traitance de services en nuage, **suivre la réalisation des activités**, **les mesures de sécurité** et **le respect des niveaux de services en nuage**.

Un **registre d'information** faisant la **distinction** entre la sous-traitance de **fonctions importantes ou critiques** et les **autres accords** de sous-traitance, doit être tenu et mis à jour. Les sociétés de gestion doivent **justifier** la distinction faite entre les fonctions importantes ou critiques et les autres accords.

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

Le choix d'une sous-traitance de services cloud nécessite en amont de :

- **Évaluer** l'accord de sous-traitance de services en nuage pour **identifier** s'il s'agit d'une fonction **importante ou critique**
- **Mettre en avant** et **évaluer** les **risques** pertinents
- **Mettre en place** une **procédure de vigilance** à l'égard du prestataire de services cloud
- **Identifier** et **évaluer** les éventuels **conflits d'intérêts** que la sous-traitance est susceptible d'entraîner

L'incidence potentielle de l'accord de sous-traitance de services cloud sur les risques opérationnels, juridiques, de non-conformité et de réputation doit être **évaluée** par les sociétés de gestion, lorsqu'il est question d'une **fonction importante ou critique**. Les **coûts** et **avantages** attendus de l'accord doivent être pris en compte.

III. Éléments contractuels clés

Un **accord écrit** doit être mis en place, comprenant les **droits et obligations** respectifs de la société de gestion et le prestataire choisi. **Une clause** donnant la possibilité à la société de gestion **de résilier** l'accord doit être expressément intégrée au contrat.

Si la sous-traitance concerne des **fonctions importantes ou critiques**, le contrat écrit doit comprendre certains éléments, notamment **une description claire** de la fonction sous-traitée, **la date de début** et de **fin de l'accord**, le délai **de préavis** ou les **obligations financières** de l'entreprise et du prestataire de services cloud. D'autres éléments importants sont énumérés dans l'article 28 de l'orientation 3 de la publication de l'ESMA relative à la sous-traitance à des prestataires de services en nuage.

IV. Sécurité de l'information

Les politiques et **procédures internes** ainsi que **l'accord écrit** entre les sociétés de gestion et le sous-traitant des services cloud doivent comprendre **les exigences** en matière de **sécurité de l'information** fixées en interne.

Les sociétés de gestion doivent **veiller** à ce que ces **exigences** soient **respectées**, notamment pour **protéger les données confidentielles, personnelles** et **sensibles**.

Des exigences, visant les **fonctions importantes ou critiques** ayant fait l'objet d'une sous-traitance cloud, sont fournies par l'ESMA, notamment en termes **d'organisation de la sécurité de l'information**, **de gestion des identités et des accès**, de **la sécurité des opérations et des réseaux**, de **localisation des données**, ou encore en termes de **continuité des activités et rétablissement après sinistre**. D'autres exigences sont mentionnées dans l'article 30 de l'orientation 4 de la publication de l'ESMA relative à la sous-traitance à des prestataires de services en nuage.

V. Stratégie de retrait

La société de gestion qui fait appel à des sous-traitants de services cloud pour des **fonctions importantes ou critiques** doit pouvoir **se retirer de l'accord** de sous-traitance sans pour autant impacter son **activité économique** et les **services fournis** à ses clients. Ce retrait ne doit pas se faire au détriment du respect des **obligations** en vertu de la législation applicable, ni de la **confidentialité**, de **l'intégrité** ou de la **disponibilité** des données traitées.

Les modalités de retrait doivent comprendre :

- Des plans de retrait complets, documentés et testés, incluant les événements déclencheurs du retrait ainsi que les rôles et responsabilités des intervenants et une analyse d'impacts
- Des solutions alternatives et les modalités de transition/transfert de la fonction sous-traitée vers cette solution alternative
- Les obligations contractuelles du sous-traitant en cas d'activation du plan de retrait et son rôle pour soutenir le transfert de la fonction sous-traitée vers la solution alternative

VI. Droits d'accès et d'audit

L'accord écrit de sous-traitance de services entre le prestataire et la société de gestion doit permettre à cette dernière, ainsi qu'à l'**autorité compétente**, d'exercer les **droits d'accès et d'audit** et les options de **supervision** qui en découlent, du moment que cela ne crée pas un risque pour l'environnement du prestataire ou pour ses clients.

La société de gestion peut avoir recours à des **certifications**, à des **rapports d'audit interne** ou **externe** ou bien, mettre en place des audits groupés effectués conjointement avec d'autres clients du même prestataire.

En cas de sous-traitance de **fonctions importantes** ou **critiques**, les éléments suivants doivent être pris en considération pour la validation des certifications et rapports d'audit de tiers :

- **Périmètre de certification** ou des **rapports d'audit**, leur **contenu** et leur **évolution**
- **Niveau d'expertise** de la partie en charge de la certification ou de l'audit
- **Déroulement des audits** et **certifications** ainsi que **les tests de contrôle** en place
- Possibilité d'**étendre les certifications** ou rapports d'audit à d'autres contrôles pertinents

VII. Sous-sous-traitance

En cas de sous-sous-traitance de **fonctions importantes** ou **critiques** (ou des parties significatives de celles-ci), la société de gestion doit s'assurer que le prestataire de services **supervise** de manière appropriée le **sous-sous-traitant**. L'accord de sous-traitance doit inclure :

- Le **périmètre** de la sous-sous-traitance et les **conditions** à respecter
- Les **responsabilités** et **obligations** qui incombent au prestataire sous-traitant
- La possibilité d'avoir un **droit de regard** sur le recours à la sous-sous-traitance
- La possibilité de s'**opposer** à la sous-sous-traitance prévue ou aux changements substantiels et de **résilier** le contrat en conséquence

VIII. Notification écrite aux autorités compétentes

En cas d'accord de sous-traitance de **fonctions importantes** ou **critiques**, la société de gestion doit en notifier par écrit son **autorité compétente**. Elle doit également le faire quand les accords concernent une fonction précédemment classée comme non importante ou non critique et qui est ensuite devenue importante ou critique.

La notification doit comprendre au moins les informations suivantes :

- Les **date** et **délais** de l'accord, la **législation applicable** et les **modèles de déploiement** en cloud
- La **description de la fonction** sous-traitée et des raisons de son classement comme **importante** ou **critique**
- La **personne** ou **l'organe de décision** de la société de gestion ayant **approuvé** l'accord de sous-traitance de services cloud
- **L'identité** du prestataire de services cloud et les **modalités d'évaluation de risques** à son égard
- Les modalités de **sous-sous-traitance** si applicable

IX. Surveillance des accords de sous-traitance de services en nuage

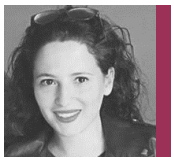
Les **autorités compétentes** doivent pouvoir **évaluer les risques** découlant des accords de sous-traitance de services cloud conclus par une société de gestion, notamment la sous-traitance de **fonctions importantes** ou **critiques**, et particulièrement lorsque ces fonctions importantes ou critiques sont exercées **hors de l'UE**.

L'évaluation des risques opérée par les autorités compétentes doit se faire selon une **approche fondée sur le risque** et porter sur:

- La **mise en place**, par la société de gestion, d'une **gouvernance**, de **ressources** et de **processus opérationnels** pour **conclure**, **mettre en œuvre** et **superviser** des accords de sous-traitance
- **L'identification et la gestion**, par la société de gestion, de tous les risques pertinents liés à la sous-traitance de services cloud

En cas de **concentration des risques**, les autorités compétentes doivent **contrôler l'évolution** de ces risques et **mesurer** leur **impact potentiel** sur les **autres entreprises** et sur la **stabilité** du marché financier.

Document réalisé par



Meryem El Halfi, Consultante Senior
Mob : +33 752 20 20 63
Mail : meryem.elhalfi@sagalink-consulting.com

Slim Hachouch, Consultant Senior
Mob : +33 749 35 27 28
Mail : slim.hachouch@sagalink-consulting.com

Qui sommes-nous ?

L'alliance d'expertises fortes et complémentaires, le partage de valeurs humaines : Beam Advisory et Sagalink Consulting forment désormais une équipe de 70 consultants spécialisés dans les métiers de la Gestion d'actifs, de la Banque privée, des Services aux Investisseurs et des Marchés de Capitaux, ainsi que dans les fonctions Finance, Risques et Conformité. Notre savoir-faire alliant expertise métier et conseil nous permet de cerner au mieux les enjeux de nos clients sur l'ensemble de leur chaîne de valeur et d'identifier pour eux les leviers de croissance les plus performants, faisant ainsi le lien entre leurs métiers et leurs projets.

Par la force de leurs convictions, Beam Advisory et Sagalink Consulting ont su gagner la confiance de leurs clients ; parmi eux, des grands groupes bancaires et des acteurs indépendants de tailles variées.

Contact

Beam Advisory Sagalink Consulting
WeWork – 33 rue La Fayette – 75009 Paris
+33 1 49 96 54 43
www.beamadvisory.com
www.sagalink-consulting.com