

FINMA Circulaire 2018/3

Infomaniak Network Cartographie

Notre cartographie de l'externalisation de la FINMA vise à aider les banques, les négociants en valeurs mobilières et les compagnies d'assurance surveillés par l'Autorité fédérale de surveillance des marchés financiers (FINMA) à se conformer à la [circulaire FINMA 2018/3 sur l'externalisation](#).

Ce document établit des correspondances spécifiques pour chaque exigence et explique comment Infomaniak Network vous aide à respecter vos obligations, y compris des informations sur les droits d'audit, le droit de donner des instructions, la sécurité des données, la résiliation et l'externalisation en chaîne.

A Inventaire des fonctions externalisées			
14	Un inventaire des fonctions externalisées doit être établi et tenu à jour. Il comprendra une description de la fonction externalisée, le fournisseur (y compris les sous-traitants), le bénéficiaire et l'organe responsable au sein de l'entreprise (cf. Cm 20).	<p><u>Inventaire</u> : Il s'agit d'une considération pour le Client.</p> <p><u>Sous-traitants</u> : La liste des sous-traitants actuellement engagés par Infomaniak et autorisés par le Client est référencer dans le document : DPA annexe sous-traitants tiers</p>	DPA annexe sous-traitants tiers
15	Les entreprises d'assurance dressent cet inventaire dans le cadre du formulaire de saisie J du plan d'exploitation.	Il s'agit d'une considération pour le Client.	N/A
15.1	Les établissements financiers au sens des Cm 6.1 et 6.2 ainsi que les maisons de titres dressent cet inventaire dans le cadre de leurs principes organisationnels (art. 17 al. 3 OEFin).	Il s'agit d'une considération pour le Client.	N/A
B Choix, instruction et contrôle du prestataire			
16	Les exigences régissant l'exercice de la fonction sont définies et documentées préalablement à la conclusion du contrat, selon les buts poursuivis avec l'externalisation. Ceci englobe une analyse du risque qui intègre les réflexions économiques et opérationnelles essentielles ainsi que les risques et les opportunités qui leur sont liés	<p><u>Contrat</u> : Infomaniak établit un Contrat Général d'Utilisation (CGU) avec chacun de ses Clients, complété par des Conditions Particulières propres à chaque produit utilisé.</p> <p><u>Analyse de risque</u> : En fonction du service sélectionné par le Client et du niveau de gestion assuré par Infomaniak, il incombe au Client de mener sa propre analyse des risques associés à l'utilisation de nos services, en se basant notamment sur les informations fournies par Infomaniak.</p>	Politique de confidentialité
17	Le prestataire sera choisi après un examen de ses capacités professionnelles ainsi que de ses ressources humaines et financières. Si plusieurs fonctions sont externalisées auprès du même prestataire, il convient de prendre en compte le risque de concentration.	<p>Il est essentiel pour le Client de prendre toutes les précautions nécessaires et d'analyser soigneusement les risques potentiels liés à l'utilisation de nos services.</p> <p>Pour vous accompagner dans cette démarche, nous mettons à votre disposition des recommandations spécifiques dans notre réponse aux points 14 et 16.</p>	Infomaniak - A propos

18	Lors de la décision statuant sur l'outsourcing et du choix du prestataire, les possibilités et les conséquences d'un changement doivent être prises en considération. Le prestataire doit offrir la garantie d'un exercice durable de la fonction.	Changements : Tout au long de la durée de son contrat, le Client dispose d'un accès permanent à ses données, lui permettant ainsi d'effectuer des importations et exportations grâce aux outils disponibles ou en sollicitant l'assistance du service clientèle d'Infomaniak.	N/A
18.1	La réintégration ordonnée de la fonction externalisée ou le transfert à un autre prestataire doivent être garantis.	Voir la ligne du dessus	N/A
19	Les compétences respectives de l'entreprise et du prestataire doivent être déterminées et délimitées contractuellement, notamment pour ce qui est des interfaces et des responsabilités.	Consulter le Contrat Général d'Utilisation (CGU) disponible sur notre site internet : https://www.infomaniak.com/fr/cgv/conditions-generales	Conditions Generales
20	Le système de contrôle interne de l'entreprise doit s'étendre à la fonction externalisée. Il convient d'identifier, de surveiller, de quantifier et de piloter systématiquement les risques essentiels liés à l'externalisation. L'entreprise désigne en son sein un organe responsable, chargé de la surveillance et du contrôle du prestataire. Les activités de ce dernier seront surveillées et évaluées de façon suivie, de sorte que les éventuelles mesures nécessaires puissent être prises rapidement.	Le Client peut consulter l'état actuel des services proposés par Infomaniak sur la page web accessible à l'adresse https://www.infomaniakstatus.com . De plus, le Manager Infomaniak offre un système d'Actualités destiné à tenir les Clients informés. Selon le service concerné, ces derniers ont également la possibilité de visualiser les activités et journaux d'actions et d'utilisateurs.	Infomaniak status Infomaniak Actualités
21	L'entreprise s'assure que le prestataire lui reconnaisse le droit de lui donner des instructions et de procéder aux contrôles nécessaires à cet effet.	Voir la ligne du dessus	N/A
C Externalisations au sein d'un groupe			
22	Concernant les exigences exposées aux Cm 16 à 21 et 32 à 35, l'ancrage au sein d'un groupe peut être pris en compte dans la mesure où il est démontré que les risques habituellement liés à une externalisation n'existent pas ou que certaines exigences ne sont pas pertinentes ou sont réglementées autrement.	Il s'agit d'une considération pour le Client.	N/A
D Responsabilité			
23	L'entreprise continue à assumer vis-à-vis de la FINMA la même responsabilité que celle qui serait la sienne si elle exerçait elle-même la fonction externalisée. Elle doit garantir à tout moment la conduite en bonne et due forme des affaires.	Il s'agit d'une considération pour le Client.	N/A
E Sécurité			
24	En cas d'externalisations déterminantes pour la sécurité (notamment dans le domaine informatique), l'entreprise et le prestataire fixent par contrat les exigences en matière de sécurité. L'entreprise doit veiller à leur respect.	Les exigences en matière de sécurité sont incluses dans les Conditions Générales d'Utilisation (CGU). Les mesures techniques et organisationnelles mises en place sont détaillées dans l'annexe de l'Accord de Traitement des Données (DPA) d'Infomaniak. Cette dernière a élaboré une Politique de Sécurité de l'Information accessible publiquement sur son site web et s'est engagée à atteindre des objectifs ainsi qu'à entreprendre des actions spécifiques relatives à la Sécurité de l'Information (SI). Pour maintenir un niveau élevé de conformité à la sécurité de l'information, Infomaniak est certifiée ISO 27001 et effectue régulièrement des audits internes et externes indépendants, au minimum une fois par an.	Conditions Generales DPA annexe mesures techniques et organisationnelles Politique qualité, SI, énergétique et environnementale Certificat ISO 27001

25	L'entreprise et le prestataire élaborent un dispositif de sécurité qui permet en cas d'urgence la continuité de la fonction externalisée. Lors de l'élaboration et de l'application du dispositif de sécurité, l'entreprise doit faire preuve du même degré de diligence que celui qu'elle adopterait si elle exerçait elle-même la fonction externalisée.	Nous mettons en œuvre des Plans de Continuité d'Activités (PCA) et des Plans de Reprise d'Activités (PRA), basés sur les actifs identifiés dans notre Système de Management de la Sécurité de l'Information (SMSI). Ces plans font l'objet d'une revue annuelle et d'un plan de tests afin de garantir leur efficacité. De plus, nous proposons des conseils et des recommandations aux clients qui souhaitent intégrer nos services dans leurs propres plans de continuité d'activités. Un article de blog dédié à ce sujet est disponible à l'adresse suivante : https://news.infomaniak.com/plan-de-reprise-activite	Plan de reprise d'activité (PRA) informatique : les solutions de protection contre les cyberattaques
F Audit et surveillance			
26	L'entreprise, sa société d'audit et la FINMA doivent être en mesure de vérifier le respect des dispositions prudentielles auprès du prestataire. Un droit de regard et d'examen intégral, permanent et sans entraves sur la fonction externalisée doit leur être reconnu par contrat.	Infomaniak prend conscience que les organismes réglementés par la FINMA ont besoin de procéder à des audits approfondis de ses services. Ainsi, nous accordons certains droits d'audit, d'accès et d'informations aux entités concernées et à leurs autorités de surveillance, conformément aux dispositions légales applicables. Les entités réglementées bénéficient d'un accès permanent à leurs données hébergées chez Infomaniak et peuvent également permettre à leur autorité de surveillance d'y avoir accès si nécessaire.	N/A
27	Les activités d'audit peuvent être déléguées à l'organe de révision du prestataire s'il dispose des compétences matérielles requises. En présence d'une telle délégation, la société d'audit de l'entreprise peut se reposer sur les résultats de l'audit effectué par l'organe de révision du prestataire.	Nos produits subissent fréquemment des examens indépendants visant à évaluer leurs contrôles de sécurité, de confidentialité et de conformité. À l'issue de ces évaluations, ils reçoivent diverses certifications, attestations de conformité ou rapports d'audit, témoignant de leur adhésion aux normes internationales en matière de sécurité, de protection des données et de gouvernance. Ces distinctions constituent autant de preuves tangibles de notre engagement constant en faveur de la qualité et de la fiabilité de nos solutions.	N/A
28	L'externalisation d'une fonction ne doit pas compliquer la surveillance par la FINMA, notamment en cas de transfert à l'étranger.	Aucune disposition de notre contrat ne vise à limiter ou à entraver la capacité d'une entité réglementée ou de l'autorité de surveillance à contrôler efficacement nos services.	N/A
29	Si le prestataire n'est pas assujéti à la surveillance de la FINMA, il doit s'engager par contrat envers l'entreprise à mettre à la disposition de la FINMA tous les renseignements et documents relatifs au domaine d'activités transféré dont la FINMA a besoin pour remplir ses tâches de surveillance. Lorsque les activités d'audit sont déléguées à l'organe de révision du prestataire, son rapport doit, sur demande, être mis à la disposition de la FINMA, de l'organe de révision interne et de la société d'audit de l'entreprise externalisatrice.	Sur demande et en fonction des besoins spécifiques de chaque Client, Infomaniak peut communiquer son rapport d'audit réalisé par un tiers, sous réserve de préserver la confidentialité des informations contenues dans ledit document.	N/A
G Transfert à l'étranger			
30	Un transfert à l'étranger est autorisé à condition que l'entreprise puisse expressément garantir qu'elle-même, sa société d'audit ainsi que la FINMA peuvent exercer et faire appliquer leurs droits de regard et d'examen.	Pour plus d'informations sur les droits d'audit, d'accès et d'information, reportez-vous au point 26 qu'Infomaniak accorde aux entités réglementées, aux autorités de contrôle et à leurs auditeurs.	N/A

31	La capacité d'assainissement et de liquidation de l'entreprise en Suisse doit être garantie. Il faut que l'accès aux informations nécessaires à cet effet soit possible à tout moment en Suisse.	Infomaniak coopérera de manière raisonnable avec ses clients en cas de changement de direction, de cession ou de toute autre restructuration organisationnelle.	N/A
G Contrat			
32	L'externalisation doit reposer sur un contrat écrit ou sur un contrat dont la forme permet d'apporter une preuve au moyen d'un texte. Outre la désignation des parties et une description de la fonction, ce dernier doit au minimum présenter le contenu évoqué ci-après (Cm 33 à 34) :	Les droits et responsabilités des parties sont définis dans le Contrat Général d'Utilisation (CGU) d'Infomaniak : https://www.infomaniak.com/fr/cgv/conditions-generales	Conditions Generales
33	L'entreprise s'assure d'être informée suffisamment tôt du recours, ou du changement de recours, à des sous-traitants exerçant des fonctions essentielles et de pouvoir mettre un terme à l'outsourcing de manière ordonnée au sens du Cm 18.1. En cas de recours à des sous-traitants, les obligations et les garanties du prestataire nécessaires au respect de la présente circulaire doivent leur être transférées.	L'article 5 de l'Accord de Traitement des Données (DPA) d'Infomaniak assure au Client que toute modification relative aux sous-traitants sera traitée conformément aux dispositions contractuelles en vigueur. Cet article expose également les obligations et garanties associées à ces changements, offrant ainsi une vision complète des responsabilités partagées entre Infomaniak et ses clients lorsque des prestataires tiers sont sollicités dans le cadre de la gestion des services.	Accord de Traitement des Données (DPA)
34	Il faut prendre des mesures contractuelles concrétisant la mise en œuvre des exigences visées par la présente circulaire, notamment aux Cm 21, 24, 26, 29, 30 et 31.	Voir les points 20, 24, 26, 29, 30 et 31	N/A
35	L'entreprise doit définir une procédure interne d'autorisation pour les projets d'outsourcing, ainsi que les compétences pour la conclusion de contrats en la matière.	Il s'agit d'une considération pour le Client.	N/A