SwissBanking

Juin 2020, 2ème édition

Guide «Cloud»

Recommandations pour sécuriser le cloud banking

Table des matières

Avant-propos

Des modèles d'affaires innovants, des processus plus performants: telles sont les nouvelles possibilités que les prestations de cloud computing offrent aux banques et aux négociants en valeurs mobilières. En faisant migrer son infrastructure des systèmes sur site (dans les locaux des banques, sur place ou en local) vers le cloud, le secteur bancaire améliore durablement sa compétitivité. Toutefois, le recours aux prestations de cloud computing est actuellement grevé d'incertitudes légales et réglementaires qui entravent cette migration ciblée.

Sous la direction de l'Association suisse des banquiers (ASB), un groupe de travail a élaboré un guide légal et réglementaire (ci-après le «Guide») pour les banques et négociants en valeurs mobilières qui recourent à des prestations de cloud computing. L'objet de ce Guide est de formuler des recommandations auxquelles les établissements et les prestataires pourront se référer pour l'acquisition et la mise en œuvre de prestations de cloud computing.

Le Guide comprend deux parties. La première est une introduction générale à la question du cloud. Elle présente l'utilité et les avantages de cette technologie pour les banques, puis met en lumière les aspects réglementaires que l'ASB juge prioritaires ainsi que les solutions qu'elle propose. La deuxième partie expose en détail les recommandations légales et réglementaires de l'ASB.

Le document ci-après ne prétend pas à l'exhaustivité. Il sera mis à jour et complété au vu des évolutions techniques et juridiques à venir. La dernière version du Guide fera l'objet d'une publication.

Synthèse

- Le **recours au cloud** est un **facteur critique de succès** pour la Suisse et pour sa place financière. Toutefois, la bonne utilisation du cloud par les banques supposait de lever au préalable un certain nombre d'incertitudes légales et juridiques.
- Pour ce faire, l'ASB a institué un **groupe de travail** qui s'est attaché à élaborer dans les meilleurs délais un **guide juridiquement non contraignant**. Il s'agit d'un outil d'interprétation destiné aux professionnels. Il se focalise sur quatre domaines où les incertitudes sont considérées comme fortes, voire de nature à entraver une migration vers le cloud, à savoir:
  - **gestion et suivi (gouvernance)**: choix du prestataire et de ses sous-traitants, accord en cas de changement de sous-traitants
  - **traitement des données**: traitement de données concernant les clients des banques et secret bancaire
  - **autorités et procédures**: transparence et coopération entre les établissements et les prestataires en ce qui concerne les mesures administratives et judiciaires
  - **audit**: contrôle des prestations de cloud computing et de l'infrastructure de type cloud utilisée pour fournir ces prestations
- La clarification des questions réglementaires dans **le Guide permet aux banques d'agir avec rapidité et souplesse**, tout en proposant des solutions pragmatiques et sûres. Cette approche est préférable à une réglementation spécifique au cloud, qui serait longue à élaborer, non neutre sur le plan technologique et rapidement dépassée par les évolutions technologiques.
- Indépendamment du Guide, **il appartient à chaque banque d'analyser les risques** inhérents à une migration vers le cloud et de décider dans quelle mesure elle entend recourir à des prestations de cloud computing.

Bases du cloud banking

Utilité et avantages du cloud banking

La compétitivité de la place financière suisse passe par l'innovation numérique et par l'agilité face aux évolutions qui se font jour. Elle passe donc par le recours à des prestations de cloud computing. Ces dernières permettent de proposer des produits innovants et de réaliser des économies de coûts. En outre, les prestataires spécialisés dans le cloud computing sont à même d'améliorer la sécurité de l'infrastructure bancaire. Dès lors, les prestations de cloud computing et le cloud banking constituent un facteur critique de succès pour la place financière suisse.

Sans le savoir, de nombreux clients des banques utilisent des prestations de cloud computing au quotidien. Ils envoient des courriels, écoutent de la musique en streaming ou stockent leurs photos de vacances sur le cloud. Ce qui fonctionne pour les particuliers devrait être possible aussi pour des banques hautement spécialisées exerçant des activités complexes. Or ce n'est pas le cas aujourd'hui, en raison de diverses incertitudes légales et réglementaires.

La migration de l'infrastructure et des processus vers le cloud permet aux banques d'accélérer considérablement la maturation commerciale de leurs produits et services innovants, d'où un net gain de compétitivité. Elle leur permet également de bénéficier des nouvelles technologies, comme par exemple l'intelligence artificielle, sans avoir à réaliser d'importants investissements en matériel et logiciels. Grâce au volumineux pool de données désormais accessible et à la puissance de traitement disponible, il devient possible d'analyser de grandes quantités de données en temps réel et ainsi, par exemple, de proposer des prestations de conseil innovantes et personnalisées ou d'automatiser des processus complexes en matière de compliance et de risque. Par ailleurs, les gains d'efficience sont nets en ce qui concerne le développement et l'expérimentation de nouveaux systèmes et de nouvelles applications: sur le cloud, il est plus facile de tester et d'approfondir des idées nouvelles, puis de les abandonner ou au contraire de les concrétiser en fonction des résultats obtenus. Enfin, l'utilisation du cloud assure une totale transparence des coûts et donc une gestion d'entreprise plus efficace. Dans la mesure où seules sont facturées les prestations auxquelles il est fait appel, les entreprises peuvent réagir avec souplesse aux fluctuations de leurs besoins, en activant ou désactivant des ressources informatiques. L'offre de fonctionnalités est disponible en «self service» à des coûts adaptables.

La migration vers le cloud évite aux banques d'avoir à développer ou acquérir des compétences et des ressources pour leur propre infrastructure informatique: elle est donc particulièrement attrayante pour les petits établissements. Ces derniers ont ainsi accès à des technologies autrefois réservées aux grandes entreprises (démocratisation de l'accès à la technologie) et génératrices d'économies d'échelle significatives.[1]

Les petites banques, en particulier, ont de plus en plus de mal à satisfaire aux exigences croissantes concernant les systèmes informatiques (sécurité informatique, installation de patchs[2], gestion du cycle de vie de l'infrastructure informatique).

On observe que les banques suisses, de plus en plus, prennent conscience des avantages du cloud computing et souhaitent migrer vers le cloud. Par ailleurs, la concurrence règne désormais entre les prestataires nationaux et internationaux, ce dont on ne peut que se réjouir. En raison de la spécificité de leurs besoins, les banques ne peuvent pas encore exploiter pleinement cette offre pléthorique, en particulier pour ce qui concerne les données des clients. Mais le recours croissant aux prestations de cloud computing contribuera à renforcer la place financière et l'écosystème financier en Suisse.

1 En raison des coûts marginaux, de nombreuses banques sont dans l'incapacité de mettre en place des prestations de cloud computing au même prix que les prestataires spécialisés. Avec la concentration croissante des tâches, les ressources informatiques peuvent être activées ou désactivées à volonté, ce qui permet de les adapter précisément aux variations d'activité.

2 Un patch est un petit programme que l'on ajoute à un logiciel pour y apporter des corrections.

Définitions

Le **cloud computing** est un modèle de traitement des données qui, par le biais d'un réseau, permet d'accéder aisément, à tout moment et en tout lieu, à un pool partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, systèmes de stockage, applications et services). Ces ressources peuvent être mises à disposition rapidement, moyennant un minimum de tâches d'administration et de faibles interactions avec les fournisseurs de services. Le cloud peut être utilisé selon trois variantes («Infrastructure as a Service» (IaaS), «Platform as a Service» (PaaS), «Software as a Service» (Saas)). Le type de cloud (cloud privé, cloud communautaire, cloud public, cloud hybride) dépend du mode de fourniture des prestations[3].

Quant au **cloud banking**, il se définit comme la mise à disposition et la fourniture de prestations de services bancaires et financiers sur la base de la technologie du cloud computing.

Questions réglementaires concernant le cloud banking

Au vu du potentiel important que recèle le cloud banking, l'ASB s'engage activement en faveur d'une amélioration des conditions-cadres. Les autorités, les prestataires et la branche nourrissent à cet effet un dialogue très régulier.

A l'heure actuelle toutefois, les incertitudes légales et réglementaires sont la source de risques difficiles à appréhender et constituent dès lors un obstacle non négligeable à la diffusion des prestations de cloud computing à plus grande échelle. Ces incertitudes concernent notamment les domaines suivants:

- **gestion et suivi (gouvernance)**: choix du prestataire et de ses sous-traitants, accord en cas de changement de sous-traitants
- **traitement des données**: traitement de données concernant les clients des banques et secret bancaire
- **autorités et procédures**: transparence et coopération entre les établissements et les prestataires en ce qui concerne les mesures administratives et judiciaires
- **audit**: contrôle des prestations de cloud computing et de l'infrastructure de type cloud utilisée pour fournir ces prestations

En particulier, on manquait jusqu'ici de références quant à l'interprétation du dispositif légal en vigueur et l'on ignore quelles sont les mesures techniques, organisationnelles et contractuelles à prendre pour atténuer les risques dans les cas précités.

En proposant le Guide ci-après, le groupe de travail de l'ASB tente d'élaborer des lignes directrices à l'intention des banques et les négociants en valeurs mobilières, dans le but de faciliter le recours aux prestations de cloud computing. L'ASB joue ainsi un rôle important en contribuant à clarifier le cadre juridique dans lequel s'inscrit le cloud banking. La méthode retenue est efficace et évite que toutes les banques aient à procéder individuellement aux mêmes clarifications. En outre, le groupe de travail réunit de précieuses compétences. La sécurité juridique est de nature à favoriser une large diffusion de la technologie du cloud computing, ce qui encouragera le développement de produits innovants et génèrera des économies de coûts: c'est dans l'intérêt de chaque établissement et de ses clients.

Le Guide de l'ASB est un recueil de recommandations auquel les banques et les prestataires pourront se référer pour l'acquisition et la mise en œuvre de prestations de cloud computing. Ce Guide intègre également des interprétations visant à remédier aux incertitudes juridiques ou à l'absence de jurisprudence quant aux difficultés parfois inédites liées au recours à des prestations de cloud computing. Il permet d'agir de manière rapide et flexible en appliquant des solutions pragmatiques. Cette approche est préférable à une réglementation spécifique au cloud, qui serait longue à élaborer, non neutre sur le plan technologique et rapidement dépassée. Les établissements désireux d'utiliser le présent Guide doivent toutefois prendre en compte leur taille ainsi que la complexité de leur modèle d'affaires, selon une approche basée sur les risques et proportionnée.

3 Définition d'après le NIST (2011) https://csrc.nist.gov/publications/detail/sp/800-145/final.

Principales solutions proposées par l'ASB dans le Guide

A) Choix du prestataire et des sous-traitants, changements les concernant

But des recommandations formulées dans le Guide:
l'établissement dispose à tout moment des informations requises pour pouvoir choisir un prestataire approprié, selon une approche basée sur les risques et en tenant compte des sous-traitants essentiels dudit prestataire.

A des fins d'efficacité et de compétitivité, les prestataires se réservent fréquemment la possibilité de déterminer et de modifier les modèles d'exploitation, les technologies employées, les fournisseurs de prestations internes et externes au groupe ainsi que d'autres facteurs essentiels (autorité sur le concept).

Lors du choix d'un prestataire, il convient donc de tenir compte en particulier des éléments suivants:

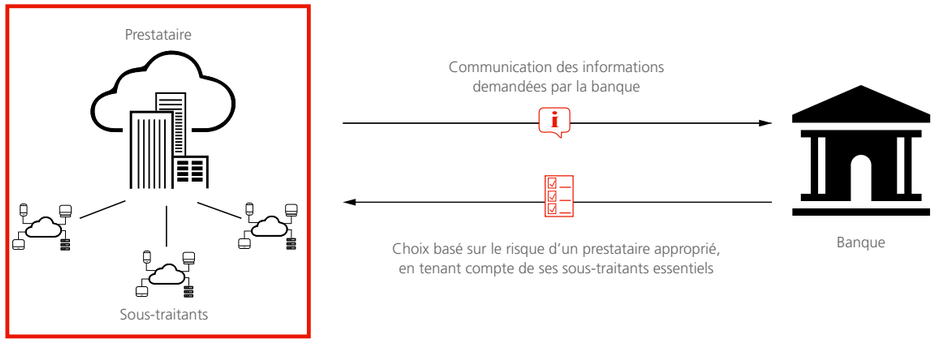
- capacité de ce prestataire de remplir ses obligations contractuelles,
- stabilité économique,
- juridiction dont il relève.

Outre ces critères tenant aux prestations, il convient de vérifier si le prestataire est disposé à respecter les obligations essentielles résultant du droit des marchés financiers et des prescriptions légales sur la protection des données.

Graphique 1

Choix du prestataire et des sous-traitants, changements les concernant

Obligations des prestataires envers la banque



Le prestataire doit mettre les informations demandées à la disposition de la banque et informer cette dernière de tout éventuel engagement ou remplacement d'un sous-traitant essentiel. La banque, en cas de désaccord, peut résilier son contrat avec le prestataire, puis rapatrier ou transférer à un nouveau prestataire les fonctions et prestations externalisées ainsi que les informations protégées.

Source: Association suisse des banquiers (ASB) 2019

Lors du choix d'un prestataire et de ses sous-traitants, il convient d'être extrêmement attentif à la confidentialité et à la sécurité des données, qui doivent faire partie intégrante de la procédure de vérification préalable (*due diligence*).

La banque doit être préalablement informée de tout engagement ou remplacement d'un sous-traitant essentiel (voir graphique 1). En outre, il lui appartient de prendre toutes dispositions appropriées pour être en mesure de rapatrier ou de transférer à un nouveau prestataire les fonctions et prestations externalisées ainsi que les informations protégées. A cet effet, elle peut par exemple prévoir un délai de résiliation suffisamment long ou une option de prolongation avec maintien du modèle d'exploitation existant.

B) Respect du secret bancaire sur le cloud

> But des recommandations formulées dans le Guide:
> le **secret bancaire** est **respecté** et les **données protégées** à tout moment, y compris sur le cloud.

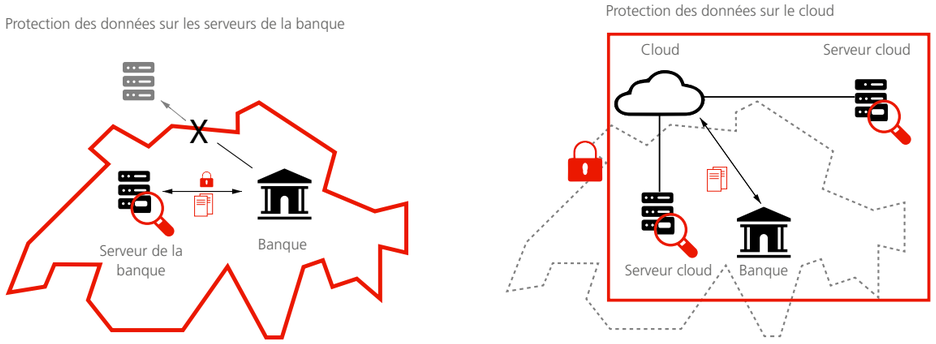
Dès lors que des données d'identification de clients (*Client Identifying Data*, CID) ou des données personnelles sont traitées dans le cadre des prestations de cloud computing, il y a lieu de respecter le secret bancaire ainsi que les lois sur la protection des données.

A l'heure actuelle, les banques en Suisse appliquent le principe «*over the border out of control*»: dès lors que des données sont stockées à l'étranger, elles échappent au contrôle des tribunaux suisses. En conséquence, les CID ne sont pas stockées à l'étranger et il est impossible d'y accéder depuis l'étranger. Le maintien d'un principe aussi absolu rendrait impossible le recours au cloud.

Le Guide met donc l'accent sur le traitement des CID soumises au secret bancaire en vertu de l'art. 47 LB. Il définit à cet égard des mesures techniques, organisationnelles et contractuelles visant à limiter le risque que le prestataire et ses sous-traitants accèdent à des CID (voir graphique 2).

Graphique 2

Le secret bancaire sur le cloud



Protection des données garantie et respect du secret bancaire. «*Over the border out of control*»: en pratique, le contrôle sur les données s'arrête aux frontières de la juridiction.

Protection des données garantie et respect du secret bancaire grâce à des mesures techniques, organisationnelles et contractuelles.

Source: Association suisse des banquiers (ASB) 2019

Protection des données des clients sur le cloud

Mesures techniques

- **Anonymisation**: l'anonymisation consiste à modifier de manière irréversible des attributs personnels (p. ex. le nom et d'autres éléments d'identification d'une personne) de telle sorte qu'ils ne puissent plus être rattachés à la personne concernée. Dès lors, les données ne sont/contiennent plus des CID et/ou des données personnelles.
- **Pseudonymisation**: la pseudonymisation consiste à remplacer des attributs personnels par un nom d'emprunt appelé pseudonyme. La règle de rattachement à la personne concernée doit faire l'objet d'une protection adéquate, sous le contrôle de la banque en Suisse. Tout accès doit être protégé conformément au principe du *need to know* et faire l'objet d'une journalisation permettant de le retracer.

- **Cryptage**: le cryptage consiste à transformer un texte clair[4] en un texte codé à l'aide d'une clé de cryptage. Dès lors, les informations initiales ne sont lisibles que si l'on dispose de la clé de cryptage. Cette dernière peut être à la disposition du prestataire ou conservée par ses soins, mais la banque doit en contrôler l'accès et la protéger des personnes non autorisées. Le processus de cryptage et la puissance de la clé de cryptage doivent tenir compte des normes de sécurité en vigueur, afin que le cryptage puisse être considéré comme cryptographiquement sûr. Toute transmission de CID doit être cryptée.

Mesures organisationnelles

- Surveillance appropriée par la banque des opérations du prestataire et de ses sous-traitants
- Audit des normes de sécurité et de confidentialité du prestataire au moyen de rapports indépendants établis sur la base de normes d'audit reconnues.

Mesures contractuelles

- Identification appropriée des mesures techniques et organisationnelles dans le contrat
- Obligation du prestataire d'imposer les mesures techniques et organisationnelles essentielles à ses sous-traitants dès lors que ces derniers traitent des CID
- Engagement contractuel du prestataire de respecter la confidentialité
- Prise en compte du caractère sensible des données et responsabilité du prestataire à cet égard
- Surveillance de la mise en œuvre et du respect des mesures techniques, organisationnelles et contractuelles par le prestataire et audit par une société d'audit reconnue
- Accord entre le prestataire et l'établissement sur la marche à suivre par l'un ou par l'autre en cas de demandes des autorités ou de procédures ayant pour objet la remise ou la transmission d'informations protégées traitées dans le cadre du cloud computing.

4 Série de mots formant un texte et/ou un message non crypté.

C) Transparence et coopération entre les établissements et les prestataires en ce qui concerne les mesures administratives et judiciaires

But des recommandations formulées dans le Guide:
le prestataire et la banque déterminent d'un commun accord une marche à suivre lorsque des autorités étrangères demandent la communication d'informations protégées.

Des demandes des autorités ou des procédures peuvent avoir pour objet la remise ou la transmission d'informations protégées traitées sur le cloud. Par ailleurs, des lois étrangères peuvent également prévoir la remise de données par le prestataire de services de cloud computing.

Le Guide préconise que le prestataire et la banque conviennent d'une marche à suivre pour traiter les demandes des autorités ayant pour objet la remise ou la transmission d'informations protégées.

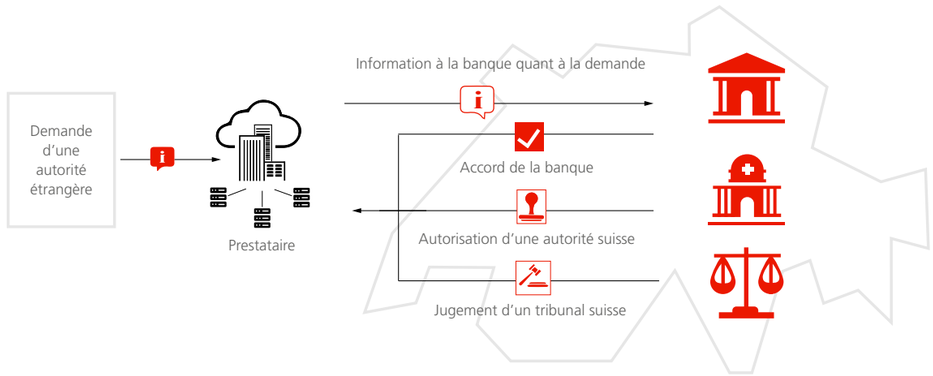
Dans la mesure où le droit le permet, les informations protégées ne doivent être transmises à des autorités étrangères qu'avec l'accord préalable écrit de la banque, en vertu d'un jugement du tribunal suisse compétent ou sur la base d'une autorisation de l'autorité suisse compétente (voir graphique 3).

Dans la mesure où le droit le permet, il appartient au prestataire d'informer la banque en temps utile lorsque des autorités étrangères formulent une demande portant sur la transmission ou la communication d'informations protégées sur le cloud. Il lui appartient également de lui accorder les droits nécessaires pour conduire la procédure et de l'aider à traiter les demandes des autorités étrangères.

Graphique 3

Demande d’une autorité étrangère

Communication d’informations protégées sous certaines conditions



Le prestataire et la banque doivent convenir de la marche à suivre en cas de demandes d’autorités étrangères ayant pour objet la communication d’informations protégées traitées sur le cloud. Les informations protégées ne peuvent être communiquées que conformément aux dispositions légales en vigueur et avec l’accord écrit de la banque, en vertu d’un jugement du tribunal suisse compétent ou sur la base d’une autorisation de l’autorité suisse compétente.

Source: Association suisse des banquiers (ASB) 2019

D) Contrôle (audit) des prestations de cloud computing et des moyens mis en œuvre

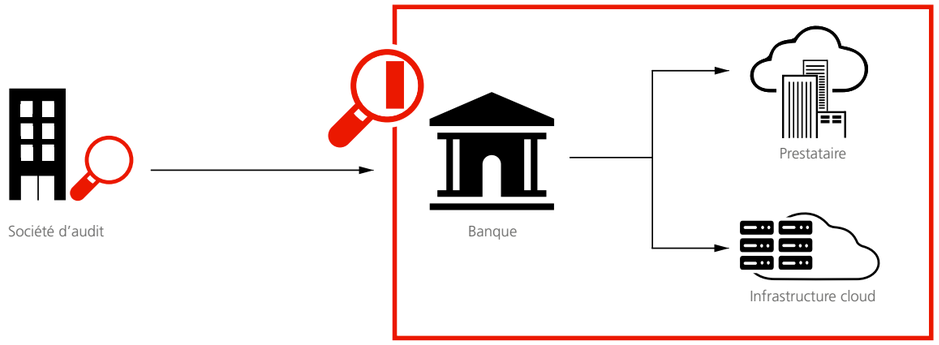
But des recommandations formulées dans le Guide:
à des fins de contrôle (audit), les tiers concernés ont **accès** à tout moment aux **données sur le cloud**.

En général, les prestataires fournissent des prestations de cloud computing à un grand nombre de clients à partir de centres de calcul hautement sécurisés. Le contrôle (audit) des infrastructures utilisées nécessite un haut niveau de spécialisation.

Graphique 4

Contrôle (audit) sur le cloud

Le contrôle des infrastructures cloud nécessite un haut niveau de spécialisation.



Lors de l’audit de la banque, il convient de s’assurer que la société d’audit dispose au minimum d’un accès logique à l’infrastructure cloud.

Source: Association suisse des banquiers (ASB) 2019

Le respect des prescriptions légales, réglementaires et contractuelles applicables au prestataire doit faire l’objet de contrôles réguliers, en particulier pour ce qui concerne les exigences en matière d’externalisation, de protection des données et de sécurité des informations. Ces contrôles doivent pouvoir être demandés et réalisés par l’établissement, par sa société d’audit interne et/ou externe, ou encore par la FINMA. Les audits groupés (*pool audits*) réalisés par plusieurs établissements ou par leurs sociétés d’audit, ainsi que les audits indirects ou de suivi, sont autorisés.

Il n’est pas impératif de contrôler sur place les infrastructures informatiques servant à la fourniture des prestations de cloud computing, à l’exception des mesures de sécurité physique. Un accès logique[5] est suffisant. Le contrôle des sous-traitants essentiels par l’établissement peut s’effectuer indirectement, par le biais du contrôle du prestataire.

5 Contrôle d’accès technique et/ou interaction avec le matériel informatique via un accès à distance, par opposition à l’accès physique qui suppose des interactions avec le matériel informatique dans l’environnement physique.

Guide légal et réglementaire

pour les

banques et négociants en valeurs mobilières qui recourent à des prestations de cloud computing relevant de l'externalisation réglementée par la FINMA

Table des matières

Chapitre I: Dispositions générales

1 Objet et but, champ d'application et caractère non contraignant

1 L'objet du présent Guide est de formuler des recommandations auxquelles les établissements et les prestataires pourront se référer pour l'acquisition et la mise en œuvre de prestations de cloud computing. Il s'agit d'un outil d'interprétation destiné aux professionnels et qui vise à clarifier les prescriptions légales et réglementaires, en particulier sur les quatre thèmes clés suivants:

- **gestion et suivi**: choix du prestataire et de ses sous-traitants, accord en cas de changement de sous-traitants (chapitre II)
- **traitement des données**: traitement de données concernant les clients des banques et secret bancaire (chapitre III)
- **autorités et procédures**: transparence et coopération entre les établissements et les prestataires en ce qui concerne les mesures administratives et judiciaires (chapitre IV)
- **audit**: contrôle des prestations de cloud computing et de l'infrastructure de type cloud utilisée pour fournir ces prestations (chapitre V)

Le présent Guide intègre également des interprétations visant à remédier aux incertitudes juridiques ou à l'absence de jurisprudence quant aux difficultés liées au recours à des prestations de cloud computing. Ces difficultés étant parfois inédites, les interprétations correspondantes n'ont pas été établies en concertation avec tous les services compétents. Les établissements désireux d'utiliser le présent Guide peuvent toutefois prendre en compte leur taille ainsi que la complexité de leur modèle d'affaires, selon une approche basée sur les risques et proportionnée.

2 Le présent Guide porte sur les prestations de cloud computing fournies par des prestataires sur commande des établissements et qui, en tant qu'externalisation de fonctions essentielles, relèvent de la Circ.-FINMA 18/3.

3 Le présent Guide est non contraignant et ne constitue pas une norme d'autorégulation au sens de la Circ.-FINMA 08/10.

2 Définitions

4 Aux fins du présent Guide, on entend par:

a) «**Annexe 3 de la Circ.-FINMA 08/21**»: l'annexe 3, intitulée «Traitement des données électroniques de clients», de la circulaire 2008/21 de la FINMA.
b) «**CID**»: les données d'identification du client (*Client Identifying* Data) au sens de l'annexe 3 de la Circ.-FINMA 08/21, Cm[1] 52.
c) «**Circ.-FINMA 18/3**»: la circulaire 2018/3 de l'Autorité fédérale de surveillance des marchés financiers, intitulée «*Outsourcing* – banques et assureurs. Externalisations dans le secteur des banques et des entreprises d'assurance», date de publication de la version en vigueur: 21 septembre 2017.
d) «**Circ.-FINMA 08/21**»: la circulaire 2008/21 de l'Autorité fédérale de surveillance des marchés financiers, intitulée «Risques opérationnels – banques. Exigences de fonds propres et exigences qualitatives relatives aux risques opérationnels dans le secteur bancaire», date de publication de la version en vigueur: 20 novembre 2008.
e) «**Circ.-FINMA 08/10**»: la circulaire 2008/10 de l'Autorité fédérale de surveillance des marchés financiers, intitulée «Normes d'autorégulation reconnues comme standards minimaux», date de publication de la version en vigueur: 20 novembre 2008.
f) «**clients**»: les clients d'un établissement.
g) «**cloud**» ou «**cloud computing**»: les modèles de service tels que définis par le National Institute of Standard and Technology (NIST)[2] ou la European Union Agency for Network and Information Security (ENISA)[3], à savoir les modèles «Infrastructure as a Service» (IaaS), «Platform as a Service» (PaaS) et «Software as a Service» (SaaS), qui peuvent être mis à disposition dans le cadre de modèles de fourniture de type cloud privé, cloud public ou cloud hybride.
h) «**données personnelles**»: comme défini par les lois sur la protection des données applicables au cas d'espèce. La notion de «données personnelles» inclut celle de «données à caractère personnel» et toutes notions analogues telles que définies par les lois applicables sur la protection des données.

1 «Cm»: abréviation de «chiffre marginal» ou «chiffres marginaux».
2 https://csrc.nist.gov/publications/detail/sp/800-145/final.
3 https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

i) «**établissement**»: toute banque et tout négociant en valeurs mobilières au sens de la Circ.-FINMA 18/3, Cm 5.
j) «**grandes quantités de CID**»: les quantités de CID telles que définies à l'annexe 3 de la Circ.-FINMA 08/21, Cm 53.
k) «**Guide**»: les principes et recommandations formulés dans le présent document.
l) «**informations protégées**»: les CID, les données personnelles ainsi que les autres informations et données qualifiées de confidentielles par l'établissement.
m) «**LB**»: la Loi fédérale sur les banques et les caisses d'épargne (Loi sur les banques), RS 952.0.
n) «**LBVM**»: la Loi fédérale sur les bourses et le commerce des valeurs mobilières (Loi sur les bourses), RS 954.1.
o) «**LPD**»: la Loi fédérale sur la protection des données (Loi sur la protection des données), RS 235.1.
p) «**OB**»: l'Ordonnance sur les banques et les caisses d'épargne (Ordonnance sur les banques), RS 952.02.
q) «**OBVM**»: l'Ordonnance sur les bourses et le commerce des valeurs mobilières (Ordonnance sur les bourses), RS 954.11.
r) «**prestataire**»: le fournisseur des prestations de cloud computing, qui est extérieur à l'établissement et au groupe dont fait éventuellement partie l'établissement.
s) «**prestations de cloud computing**»: les modèles de service fournis par le prestataire en matière de cloud computing, sur commande de l'établissement.
t) «**secret bancaire**»: le secret protégé par l'art. 47 LB.
u) «**sous-traitants essentiels**»: les sous-traitants qui, dans le cadre de la fourniture des prestations de cloud computing par le prestataire, (i) assurent des fonctions essentielles au sens de la Circ.-FINMA 18/3 ou (ii) sont considérés comme essentiels par l'établissement.
v) «**traitement**»: les opérations relatives à des données personnelles telles que définies dans la Loi fédérale sur la protection des données et dans les lois applicables sur la protection des données.

Chapitre II: Gestion et suivi (gouvernance)

Fondements juridiques

- Art. 3 et 47 LB, art. 12 OB
- Art. 10 et 43 LBVM, art. 19f OBVM
- LPD
- Circ.-FINMA 08/21, notamment son annexe 3
- Circ.-FINMA 18/3

3 Décision de recourir à des prestations de cloud computing

5 Le cloud computing se caractérise par la grande diversité des prestations proposées, qui peuvent être aussi bien des infrastructures et des services hautement standardisés que des solutions spécifiques. La décision de recourir à des prestations de cloud computing doit[4] donc résulter d'un processus structuré.

6 Lorsque cette décision intervient sur la base d'une analyse préalable des risques[5], il convient de prendre en compte non seulement les opportunités et les risques inhérents au recours aux prestations de cloud computing, mais aussi le caractère essentiel de ces prestations au sens de la Circ.-FINMA 18/3 ainsi que la qualification des informations protégées, notamment des CID, à traiter dans le cadre desdites prestations.

4 Le présent document est un guide qui formule des recommandations, de sorte que les termes «doit» ou «doivent» sont à entendre non pas comme des impératifs, mais comme des suggestions de bonnes pratiques.
5 Par exemple, il y a lieu d'analyser les risques liés à la sécurité des données ou au droit applicable.

7 S'agissant de l'analyse des risques, l'établissement intègre dans son évaluation les risques susceptibles de résulter d'un manquement dans la fourniture des prestations de cloud computing, ou encore d'une défaillance totale ou partielle des prestations de cloud computing ou du prestataire.

8 Si le recours aux prestations de cloud computing, leur acquisition ou leur cessation comporte des risques, ces derniers doivent faire l'objet de mesures appropriées visant à les atténuer. Ces mesures sont mises en œuvre, adaptées et surveillées dans le cadre de la gestion des risques aussi longtemps que l'établissement recourt aux prestations de cloud computing.

4 Responsabilités et rôles

9 Selon la réglementation applicable à l'établissement, il peut y avoir lieu de respecter certaines prescriptions du droit des marchés financiers, voire le secret bancaire et les lois sur la protection des données dès lors que les prestations de cloud computing incluent le traitement de CID ou de données personnelles.

10 Pour l'attribution des responsabilités et la définition des rôles, les modèles de service et de fourniture doivent être pris en compte. A cet effet, le prestataire doit contribuer de manière appropriée et dans toute la mesure requise et mettre les informations pertinentes à la disposition de l'établissement. Idéalement, cette coopération intervient dès la procédure d'offre.

11 Si le prestataire fait appel à des sous-traitants pour fournir les prestations de cloud computing, il convient d'en tenir dûment compte en définissant les responsabilités et les rôles des sous-traitants essentiels.

12 (Le contrat entre l'établissement et le prestataire doit déterminer les droits et obligations des parties et des autres intéressés, y compris en ce qui concerne leur mise en œuvre.

5 Choix et changement du prestataire et des sous-traitants essentiels

13 A des fins d'efficacité et de compétitivité, les prestataires, en particulier ceux proposant des prestations de cloud computing hautement standardisées, se réservent fréquemment la liberté de déterminer et de modifier les modèles d'exploitation, les technologies employées, les fournisseurs de prestations internes et externes au groupe ainsi que d'autres facteurs essentiels (autorité sur le concept).

14 Il est dans l'intérêt de l'établissement de sélectionner le prestataire approprié au regard de sa capacité de remplir ses obligations contractuelles, de sa stabilité économique, de la juridiction dont il relève et d'autres critères essentiels. Les sous-traitants essentiels sont à intégrer dans cette évaluation. Le prestataire doit contribuer de manière appropriée à la collecte des informations demandées par l'établissement à cet effet.

15 L'évaluation des risques éventuels comprend notamment l'identification des mesures d'atténuation ainsi que des personnes responsables de leur mise en œuvre.

16 Par ailleurs, outre les critères tenant aux prestations, le choix du prestataire doit prendre en compte la volonté de ce dernier de respecter les obligations résultant du droit des marchés financiers[6] et des prescriptions légales sur la protection des données, ainsi que l'organisation de son modèle d'exploitation. Si le prestataire et ses sous-traitants sont amenés à traiter des CID de l'établissement ou d'autres données personnelles, la confidentialité et la sécurité des données constituent un critère décisif et font partie intégrante de la procédure de vérification préalable (*due diligence*). Cela vaut notamment pour tous les types d'activités donnant accès à de grandes quantités de CID[7].

6 Y compris le secret bancaire.
7 Voir les exigences formulées dans la Circ.-FINMA 08/21, en particulier à l'annexe 3.

17 Tout changement de prestataire est soumis à l'accord préalable de l'établissement, lequel peut être donné par écrit ou de toute autre manière probante. Peuvent être exemptées de cette obligation les restructurations internes au groupe au sein de la même juridiction et qui n'ont pas d'impacts significatifs sur les relations existant entre les parties, les critères et les risques. A la demande de l'établissement, le prestataire doit accepter de prévoir des règles équivalentes pour le cas où l'entreprise qui le contrôle ou qui contrôle un de ses sous-traitants essentiels serait amenée à changer.

18 Tout engagement de nouveaux sous-traitants essentiels ou tout remplacement d'un sous-traitant essentiel doit s'effectuer conformément aux principes fixés dans la Circ.-FINMA 03/18[8]. Un accord contractuel fixant les critères d'engagement des sous-traitants essentiels, dès lors qu'il incombe au prestataire d'en garantir le respect et de prouver à l'établissement qu'il sera exécuté, peut offrir à l'établissement un surcroît de sécurité. Toutefois, dans tous les cas, l'établissement doit être informé par le prestataire préalablement à tout engagement d'un nouveau sous-traitant essentiel et pouvoir résilier le contrat qui le lie au prestataire dans un délai donné, le cas échéant pour juste motif. En pareil cas, il appartient à l'établissement de prendre toutes dispositions appropriées, en particulier de se réserver un délai de préavis raisonnable et de s'assurer un soutien approprié de la part du prestataire à l'issue du contrat, voire des options de prolongation avec maintien du modèle d'exploitation existant, afin que les fonctions et prestations externalisées ainsi que les informations protégées puissent être rapatriées ou transférées à un nouveau prestataire. A cet égard, les effets dits de verrouillage (*lock-in*) doivent être pris en compte, de même que le volume, le nombre et la criticité des fonctions externalisées et des informations protégées.

8 Circ.-FINMA 03/18, Cm 33.

6 Centres de données et centres d'exploitation

19 On redoute parfois que le recours à des prestations de cloud computing entraîne une perte de contrôle sur les données traitées et qu'il devienne impossible de déterminer les lieux où celles-ci sont stockées et traitées (ubiquité des données). Du point de vue des établissements, la confiance des clients quant à la gestion de leurs données est un enjeu crucial.

20 Le prestataire doit informer l'établissement des sites où se trouvent les infrastructures de cloud computing qu'il utilise ou peut utiliser (centres de données) et à partir desquels il exploite le cloud (centres d'exploitation), ainsi que de tout transfert desdits sites pendant la durée du contrat. Ces renseignements incluent l'identification des personnes (morales), notamment le prestataire et ses sous-traitants essentiels, qui exploitent, possèdent ou contrôlent de toute autre manière les centres de données et d'exploitation.

21 Lorsque le prestataire traite des informations protégées, tout transfert de site dans une autre juridiction pendant la durée du contrat doit faire l'objet d'une procédure définie dans ledit contrat et, selon la protection requise au cas par cas, peut être soumis à l'accord préalable de l'établissement. Il appartient alors au prestataire de préciser les risques inhérents au transfert de site et de communiquer à l'établissement toutes les informations susceptibles d'éclairer sa décision, en particulier quant aux mesures de sécurité envisagées.

22 L'accord préalable doit pouvoir être refusé par l'établissement sans indication de motifs. S'il est donné, il appartient à l'établissement de prendre toutes dispositions appropriées, en particulier de se réserver un délai de préavis raisonnable et de s'assurer un soutien approprié de la part du prestataire à l'issue du contrat, voire des options de prolongation avec maintien du modèle d'exploitation existant, afin que les fonctions et prestations externalisées ainsi que les informations protégées puissent être rapatriées ou transférées à un nouveau prestataire. A cet égard, les effets dits de verrouillage (*lock-in*) doivent être pris en compte, de même que le volume, le nombre et la criticité des fonctions externalisées et des informations protégées. Les autres exigences visant à prévenir l'accès de tiers aux données font l'objet des développements ci-après.

Chapitre III: Données et sécurité des données

Fondements juridiques

- Art. 47 LB
- Art. 43 LBVM
- Annexe 3 de la Circ.-FINMA 08/21
- Circ.-FINMA 18/3
- LPD

7 Classification des données et des informations

23 Afin d'assurer une application irréprochable des prescriptions légales sur la protection des données et de garantir le respect du secret bancaire, il appartient à l'établissement de procéder à une classification des informations protégées traitées dans le cadre des prestations de cloud computing.

24 Cette classification par niveaux de confidentialité vise à permettre à l'établissement et, au besoin, au prestataire, de déterminer les prescriptions légales et réglementaires applicables en matière de traitement de données, de flux de données et de concepts d'accès, ainsi que d'apprécier l'opportunité de procéder à des contrôles supplémentaires.

25 Est à prendre en compte comme critère de classification le fait que les clients ont été informés ou pas d'une externalisation du traitement de CID à un prestataire de services de cloud computing en Suisse ou à l'étranger et dans quelle mesure ils ont été informés ou, le cas échéant, le fait qu'ils ont donné leur accord à cet effet[9].

9 Voir à cet égard le chapitre III:10 ci-après.

26 Les modifications significatives apportées pendant la durée du contrat à la classification des informations protégées externalisées doivent faire l'objet d'un suivi et les mesures requises doivent être prises préalablement aux externalisations concernées.

8 Lieux de stockage et flux de données, concept d'accès

27 Le prestataire doit permettre à l'établissement de vérifier que les lieux de traitement de CID et, le cas échéant, d'autres informations protégées répondent aux exigences y relatives, ainsi que d'effectuer des contrôles sur place. L'établissement doit aussi avoir la possibilité de respecter ses obligations de transparence envers les clients et, dès lors, de connaître avec toute la précision requise les lieux de traitement des informations protégées, en particulier les lieux de stockage.

28 Par ailleurs, l'établissement doit être préalablement informé des flux de données concernant des informations protégées qui se situent dans la sphère du prestataire et, le cas échéant, de ses sous-traitants. Au besoin, il y a lieu de définir contractuellement, avec une précision suffisante, l'architecture sous-jacente à ces flux de données.

29 Entrent dans le champ du paragraphe ci-dessus la définition et la mise en œuvre d'un concept d'accès[10] par le prestataire. Ce dernier doit communiquer à l'établissement, sur simple demande, les autorisations d'accès octroyées[11]. Il lui incombe également de surveiller et répertorier de manière appropriée les accès à des informations protégées, en particulier des CID.

30 Tout concept d'accès doit définir de manière suffisamment restrictive le but de l'accès et indiquer dans quels cas précis l'accès à des systèmes qui traitent des informations protégées est possible et/ou autorisé. Concrètement, ces «cas précis» incluent par exemple les cas d'urgence ou les défaillances critiques de l'infrastructure de type cloud auxquelles il n'est pas possible de remédier par d'autres moyens.

10 Pour les accès à des informations protégées.
11 Voir note 8.

9 Mesures techniques et organisationnelles générales en matière de sécurité des données

31 De manière générale, il appartient au prestataire de proposer à l'établissement, puis de mettre en œuvre conformément aux accords conclus avec ce dernier, toutes mesures techniques et organisationnelles appropriées en vue d'assurer la sécurité des informations protégées qui lui sont confiées à des fins de traitement. Dans ce cadre, les normes internationales et locales doivent être respectées. Les sous-traitants du prestataire, le cas échéant[12], doivent également être tenus d'appliquer ces mesures, de même que le personnel engagé par le prestataire et ses sous-traitants.

32 Il appartient au prestataire de s'assurer que dès lors qu'ils ont accès à des informations protégées, y compris des CID, ses propres collaborateurs et ceux de ses sous-traitants s'engagent formellement à respecter la confidentialité et soient dûment informés et formés. Un tel engagement des collaborateurs est considéré comme suffisant lorsqu'il est pris envers le prestataire ou ses sous-traitants dans le cadre du contrat de travail. Est également considéré comme suffisant le fait que dans ce cadre, l'obligation de confidentialité soit conforme aux prescriptions légales sur la protection des données, même si le secret bancaire n'est pas explicitement mentionné comme objet de l'engagement. Il est toutefois recommandé aux prestataires d'attirer expressément l'attention des collaborateurs opérant en Suisse sur le secret bancaire et sur la peine encourue en cas de violation. Il en va de même en ce qui concerne la violation du secret commercial et la peine encourue[13].

10 Secret bancaire et mesures de sécurité

10.1 Remarques liminaires

33 Avant de recourir à des prestations de cloud computing, l'établissement doit impérativement vérifier s'il est nécessaire ou pas que le client le libère du secret bancaire au sens de l'art. 47 LB. Cet article s'appliquerait si l'établissement, en recourant aux prestations de cloud computing, violait intentionnellement ou par négligence le secret bancaire.

12 A cet égard, il convient de tenir compte du caractère essentiel des sous-traitants concernés.
13 Art. 162 CP.

34 Selon le présent Guide, dès lors que l'établissement a prévu des mesures de sécurité appropriées pour protéger les CID traitées dans le cadre des prestations de cloud computing, il n'a pas besoin d'être délié du secret bancaire par le client.

Le présent chapitre donne un aperçu de l'argumentation sur laquelle cette position est fondée, ainsi que des mesures de sécurité à prendre.

10.2 Mesures de sécurité techniques, organisationnelles et contractuelles

35 Il y a violation du secret bancaire dès lors que des CID sont effectivement divulguées à des personnes non autorisées, intentionnellement ou par négligence, et que cette divulgation est causée par l'établissement[14]. L'art. 47, al. 1 LB définit une infraction matérielle, la seule possibilité que des personnes non autorisées prennent connaissance de CID ne constitue pas une violation du secret bancaire.

36 Lorsque, dans le cadre des prestations de cloud computing, le prestataire et ses sous-traitants ne prennent pas effectivement connaissance des CID traitées sur le cloud, il n'y a donc pas révélation du secret au sens de l'art. 47, al. 1 LB. Toutefois, l'établissement doit avoir pris des mesures techniques, organisationnelles et contractuelles appropriées pour limiter le risque que le prestataire et ses sous-traitants accèdent aux CID.

37 Les mesures à envisager résultent de l'annexe 3 de la Circ.-FINMA 08/21, ainsi que des dispositions légales applicables en matière de protection des données. L'appréciation du caractère approprié de ces mesures doit s'effectuer au regard de l'état de la technique, des coûts de mise en œuvre, de la nature, de l'étendue, des circonstances et des buts du traitement des CID, ainsi qu'au regard de la probabilité que le risque se matérialise et de la gravité de ce risque pour les droits des clients concernés.

Sont présentés ci-après quelques exemples de mesures possibles.

14 Voir arrêt du Tribunal fédéral 6B_1403/2017 du 8 août 2017.

38 Mesures techniques de protection des CID:

Certaines mesures techniques peuvent avoir pour effet que les données traitées sur le cloud ne peuvent plus être qualifiées de CID. Cette définition[15] se fonde sur la notion de données personnelles au sens de la législation sur la protection des données. Ainsi, en vertu de la pratique juridique reconnue en Suisse, ne constituent pas des données personnelles respectivement des CID les données anonymisées, pseudonymisées ou cryptées que le destinataire ne peut rattacher à une personne donnée faute de disposer du tableau de concordance, de la règle de rattachement ou de la clé de cryptage.

Sont considérées comme des procédés techniques appropriés pour assurer une protection adéquate des CID, en particulier, les mesures de sécurité ci-après[16].

39 **Anonymisation**. Les données anonymisées (technique irréversible) ne peuvent plus être qualifiées de CID respectivement des données personnelles[17]. Elles ne sont donc pas soumises aux exigences formulées dans la présente section.

40 **Pseudonymisation**. S'agissant de CID, la règle de rattachement aux personnes concernées doit faire l'objet d'une protection adéquate, sous le contrôle de l'établissement en Suisse. En particulier, les droits d'utilisation du tableau de concordance doivent être restreints sur la base du principe du *need to know* et les accès doivent faire l'objet d'une journalisation permettant de les retracer.

41 **Cryptage**. S'agissant de CID, il convient de veiller à ce que l'accès à la clé de cryptage soit sous le contrôle de l'établissement et protégé des personnes non autorisées, même si ladite clé de cryptage est à la disposition du prestataire ou est conservée dans ses locaux et sert à crypter et décrypter automatiquement les CID dans le cadre des prestations de cloud computing. L'établissement doit évaluer, sur la base d'une analyse des risques et notamment au regard de la classification des CID, les procédures appropriées pour assurer le contrôle de la clé de cryptage.

15 Annexe 3 de la Circ.-FINMA 08/21, Cm 52.
16 Voir à cet égard l'annexe 3 de la Circ.-FINMA 08/21, Cm 20, ainsi que les définitions aux Cm 61 à 65.
17 Voir à cet égard l'annexe 3 de la Circ.-FINMA 08/21, Cm 64.

Le processus de cryptage et la puissance de la clé de cryptage doivent tenir compte des normes de sécurité en vigueur, afin que le cryptage puisse être considéré comme cryptographiquement sûr.

Toute transmission de CID doit être cryptée. Il est indispensable que le processus de cryptage et la puissance de la clé de cryptage soient conformes aux normes de sécurité en vigueur, afin que la transmission puisse être considérée comme cryptographiquement sûre.

42 Mesures organisationnelles de protection des CID:

Les opérations effectuées par le prestataire et ses sous-traitants doivent pouvoir être surveillées par l'établissement de manière appropriée.

L'audit obligatoire[18] des normes de sécurité et de confidentialité du prestataire doit se faire au moyen de rapports indépendants établis sur la base de normes d'audit reconnues[19].

43 Mesures contractuelles de protection des CID

Comptent notamment parmi les mesures contractuelles:

- l'identification appropriée des mesures techniques et organisationnelles dans le contrat conclu entre le prestataire et l'établissement, ainsi que l'obligation du prestataire d'imposer ces mêmes mesures à ses sous-traitants dès lors que ces derniers traitent des CID;
- l'engagement contractuel du prestataire de respecter la confidentialité;
- la prise en compte du caractère sensible des données et la responsabilité du prestataire à cet égard;
- la surveillance de la mise en œuvre et du respect des mesures techniques, organisationnelles et contractuelles;
- les accords prévus au chapitre IV (Autorités et procédures).

18 L'audit doit s'effectuer conformément aux prescriptions de l'annexe 3 de la Circ.-FINMA 08/21, principe 9.
19 Par exemple les normes d'audit des contrôles en place ISAE 3000 ou SOC2.

10.3 Cercle des personnes tenues au secret

44 Selon le modèle de service dans lequel s'inscrivent les prestations de cloud computing, il peut s'avérer nécessaire que des collaborateurs du prestataire et de ses sous-traitants traitent les CID en texte clair, c'est-à-dire sans cryptage ni pseudonymisation, et en prennent donc effectivement connaissance. La question se pose alors de savoir si le prestataire et ses sous-traitants doivent être qualifiés de personnes non autorisées au sens de l'art. 47, al. 1 LB. Précisons toutefois que les cryptages et décryptages entièrement automatisés effectués dans le cadre de la prestation de cloud computing ne sont pas à considérer comme des traitements de données en texte clair au sens du présent paragraphe.

45 Selon le présent Guide, le prestataire et ses sous-traitants ne sont pas des personnes non autorisées au sens de l'art. 47, al. 1 LB. Si l'établissement recourt à des prestations de cloud computing fournies par un prestataire, c'est fondamentalement qu'il a un intérêt réel à optimiser la qualité de ses services, ses coûts, ainsi que la sécurité des données. Le message du Conseil fédéral concernant la révision de la loi sur les banques considérait déjà expressément les prestataires de services informatiques comme des mandataires[20]. Par ailleurs, l'établissement se voit généralement reconnaître le droit de donner des instructions[21] au prestataire et à ses sous-traitants. Ces derniers répondent donc à la qualification de mandataires au sens de l'art. 47, al. 1 LB et peuvent être inclus dans le cercle des personnes tenues au secret.

46 Les prestataires et sous-traitants domiciliés à l'étranger sont également des mandataires et, dès lors, ils sont inclus dans le cercle des personnes tenues au secret. C'est conforme au sens et à la finalité de l'art. 47, al. 1 LB et la lettre de cette disposition ne l'exclut pas[22]. En outre, les prescriptions légales et réglementaires en vigueur à l'étranger peuvent également prévoir des mécanismes de protection efficaces.

20 Message du Conseil fédéral à l'Assemblée fédérale concernant la révision de la loi sur les banques, 13 mai 1970, FF 1970, 1197: «*En [...] soumettant les mandataires [au secret bancaire], on a voulu y englober en particulier les centres de calcul qui sont chargés par les banques du traitement électronique des informations.*»
21 Circ.-FINMA 03/18, Cm 21.
22 La nécessité d'une exclusion formelle résulte du principe de légalité prévu à l'art. 1 CP.

47 Les mesures de sécurité applicables doivent néanmoins prendre en compte l'accroissement du risque lié à un traitement des données en texte clair à l'étranger. Le caractère approprié de ces mesures est à évaluer en particulier au regard des risques spécifiques au pays concerné, en se demandant notamment, mais pas exclusivement, si la législation de ce pays assure une prévention adéquate des infractions à la protection des données.

48 Les mesures techniques, organisationnelles et contractuelles applicables résultent également de l'annexe 3 de la Circ.-FINMA 08/21, ainsi que des dispositions légales applicables en matière de protection des données.

49 Les mesures complémentaires énumérées ci-après peuvent être considérées comme appropriées au regard d'un risque accru encouru à l'étranger.

- Le traitement de données en texte clair par des collaborateurs du prestataire ou de ses sous-traitants est limité aux cas où la sécurité et la fiabilité du cloud computing l'exigent et soumis à des conditions temporelles et matérielles strictes.
- Les processus de traitement sont surveillés et enregistrés par le prestataire et l'établissement a la possibilité d'en contrôler le moment, la durée et l'étendue. En cas de soupçon de processus de traitement non autorisés, le prestataire est en mesure de mettre fin immédiatement aux traitements concernés.
- L'établissement reçoit des informations sur le traitement de la part du prestataire ou a la possibilité de s'informer lui-même.
- L'établissement est particulièrement attentif aux accords prévus au chapitre IV (Autorités et procédures).

50 Comme indiqué *supra*, le traitement de CID en texte clair par des collaborateurs du prestataire et de ses sous-traitants ne constitue pas en soi une violation du secret bancaire par l'établissement.

51 On peut supposer qu'il y a divulgation de CID à des personnes non autorisées lorsque des tiers extérieurs à la sphère du prestataire, comme par exemple des autorités étrangères, prennent connaissance de CID en raison du recours aux prestations de cloud computing par l'établissement. En pareil cas toutefois, dès lors que des mesures techniques, organisationnelles et contractuelles appropriées ont été prises en vue de protéger les CID, on peut se demander s'il est possible d'imputer à l'établissement une action ou une omission causale et intentionnelle ou négligente[23].

10.4 Obligations d'information résultant des prescriptions légales sur la protection des données

52 Tout traitement de données personnelles dans le cadre des prestations de cloud computing entraîne une obligation d'information résultant des prescriptions légales sur la protection des données, qui peut être remplie au moyen de la déclaration générale de confidentialité de l'établissement concerné. Conformément au principe de transparence, les informations doivent être formulées de manière simple et compréhensible. Il convient de préciser que les prescriptions légales sur la protection des données n'exigent pas d'indiquer qui sont les différents prestataires et leurs sous-traitants.

10.5 Autres obligations d'information

53 Les autres obligations d'information susceptibles de s'imposer sur d'autres fondements que les prescriptions légales sur la protection des données sont à apprécier au cas par cas. Cette appréciation s'effectue par exemple au regard des attentes du client, des accords contractuels, des dispositions du droit du mandat et du principe de bonne foi. Peuvent servir de points de référence, par exemple, le positionnement sur le marché et la communication de l'établissement sur les mandats antérieurs confiés à des prestataires.

23 En cas de simple possibilité d'accéder à des CID, l'hypothèse d'une tentative punissable de divulgation à des personnes non autorisées est caduque, puisqu'il s'agit d'un délit intentionnel.

AJUSTEMENT JUIN 2020

11 Mesures visant à garantir la disponibilité des données et leur restitution

54 L'établissement doit pouvoir accéder à tout moment, depuis la Suisse, aux informations protégées stockées et traitées à l'étranger ou en Suisse. Le prestataire doit s'engager à fournir les prestations de cloud computing de telle sorte qu'y compris en cas d'assainissement ou de liquidation de l'établissement, cet accès soit garanti à l'établissement, à une société succédante ou de défaisance et, le cas échéant, à la FINMA.

55 Le prestataire doit s'engager à restituer à tout moment les informations protégées à l'établissement, à une société succédante ou de défaisance ou à un prestataire succédant dans le cadre de l'assistance au terme du contrat, en cas d'assainissement ou de liquidation de l'établissement et sur instruction de l'établissement ou de la FINMA, pour autant qu'il dispose des moyens[24] et des connaissances[25] requis à cet effet. En pareil cas, le prestataire doit retransférer les informations protégées dans un format standardisé et exploitable par une machine.

56 Si le prestataire met en œuvre des solutions propriétaires entraînant des effets de verrouillage (*lock-in*), il doit se déclarer prêt à assister l'établissement en cas de migration vers d'autres solutions ou d'octroi de licences sur les solutions propriétaires.

24 Par exemple la clé de cryptage.
25 S'agissant notamment des prestations de cloud computing fournies dans le cadre d'IaaS ou de PaaS, il peut arriver que le prestataire ignore l'architecture choisie par l'établissement et/ou les composants que ce dernier utilise.

Chapitre IV: Autorités et procédures

Fondements juridiques

- Art. 271 CP
- Art. 273 CP
- Art. 47 LB
- Art. 6 LPD
- Traités internationaux en matière d'entraide judiciaire
- Annexe 3 de la Circ.-FINMA 08/21, Cm 20.

57 Il appartient au prestataire de convenir avec l'établissement de la marche à suivre en cas de demandes des autorités ayant pour objet la remise ou la transmission d'informations protégées traitées dans le cadre du cloud computing. Sauf dispositions légales impératives l'en empêchant, le prestataire doit prendre envers l'établissement les engagements contractuels énumérés aux Cm 57–60 ci-dessous.

58 Dans le cadre de procédures étrangères, le prestataire, ainsi que ses sous-traitants et les sociétés de son groupe, ne sont autorisés à transmettre ou communiquer des informations protégées traitées dans le cadre du cloud computing à des autorités étrangères ou à d'autres parties situées à l'étranger que conformément aux dispositions légales et réglementaires applicables et (i) avec l'accord préalable écrit de l'établissement, (ii) en vertu d'un jugement du tribunal suisse compétent ou (iii) sur la base d'une autorisation de l'autorité suisse compétente.

59 Le prestataire doit informer l'établissement en temps utile, avant de transmettre ou communiquer les informations protégées. Il doit également lui accorder les droits nécessaires pour conduire la procédure et l'aider à traiter les demandes d'autorités étrangères.

60 Si, en raison de dispositions légales impératives, le prestataire n'est pas en mesure d'informer l'établissement préalablement à la transmission ou la communication d'informations protégées à des autorités étrangères ou à d'autres parties situées à l'étranger, il lui appartient de prendre les mesures légales ou de protection appropriées dans le cadre de l'accord conclu et dans l'intérêt de l'établissement et des clients de ce dernier[26].

61 En outre, le prestataire doit fournir à l'établissement des informations générales sur le nombre (annuel), l'objet et le déroulement des procédures qui, selon les dispositions légales et réglementaires étrangères applicables, portent ou pourraient porter sur la transmission ou la communication d'informations protégées et sont susceptibles d'avoir un impact sur le prestataire ainsi que sur ses sous-traitants[27] ou sur les sociétés de son groupe[28].

62 Il appartient à l'établissement, le cas échéant avec la coopération appropriée du prestataire, d'évaluer les risques résultant de la possibilité, pour des autorités étrangères, de compromettre l'efficacité des mesures techniques, organisationnelles et contractuelles prises conformément au chiffre 10.

26 Voir chapitres II et III, en particulier les développements concernant le secret bancaire et la transparence.
27 Sous-traitants ayant accès à des informations protégées, en particulier des CID.
28 Voir note précédente.

Chapitre V: Contrôle (audit) des prestations de cloud computing et des moyens mis en œuvre

Fondements juridiques

- Art. 18 et 23 ss LB ainsi que les dispositions d'exécution de l'OB
- Art. 17 LBVM
- Circ.-FINMA 08/21
- Circ.-FINMA 18/3

63 En général, les prestataires fournissent des prestations de cloud computing à un grand nombre de clients à partir de centres de calcul hautement sécurisés[29]. Le contrôle (audit) des infrastructures utilisées nécessite un haut niveau de spécialisation; dans le même temps, les obligations de confidentialité de chaque prestataire envers ses autres clients doivent être prises en compte.

64 Le respect des obligations incombant au prestataire à titre légal et réglementaire (notamment en matière d'externalisation, de protection des données et de sécurité des informations) ou contractuel doit faire l'objet de contrôles réguliers, en sachant que l'efficacité des mesures prises suppose une coordination des contrôles entre le prestataire et l'établissement. Le prestataire doit coopérer de manière appropriée. La fourniture des prestations convenues par contrat peut également faire l'objet de contrôles.

29 Cloud public.

65 Les contrôles doivent pouvoir être demandés et réalisés par l'établissement, par sa société d'audit interne et/ou externe, ou encore par la FINMA. Les audits groupés (*pool audits*) réalisés par plusieurs établissements ou par leurs sociétés d'audit, ainsi que les audits indirects ou de suivi, dans le cadre desquels le contrôle et le reporting incombent à la société d'audit du prestataire ou à une société d'audit désignée par ses soins, sont autorisés, pour autant que la société d'audit dispose de l'indépendance et de la compétence technique requises. Il en va de même des audits demandés par la FINMA.

66 Il n'est pas impératif de contrôler sur place les infrastructures informatiques servant à la fourniture des prestations de cloud computing, à l'exception des mesures de sécurité physique. L'octroi d'un accès logique en faveur de l'établissement, de sa société d'audit ou de l'autorité compétente peut être considéré comme suffisant à cet effet. Le prestataire peut définir les modalités d'un tel droit d'accès directement avec l'autorité de surveillance.

67 S'agissant de prestations de cloud computing qui présentent un lien avec l'étranger, un accord contractuel prévoyant le droit, pour l'établissement, sa société d'audit, la société d'audit du prestataire et la FINMA, de réaliser un audit direct ou indirect du prestataire, répond à l'exigence d'une clarification adéquate des droits de contrôle.

68 Les principes ci-dessus valent aussi pour les sous-traitants essentiels du prestataire. Faute de contrat entre l'établissement et lesdits sous-traitants, ils résultent formellement du transfert des obligations contractuelles du prestataire à ses sous-traitants.

69 Le contrôle des sous-traitants essentiels peut s'effectuer indirectement, par le biais du contrôle du prestataire, mais un contrôle direct des sous-traitants essentiels peut être requis.

•SwissBanking

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Case postale 4182
CH-4002 Bâle

office@sba.ch
www.swissbanking.org