Swiss Banking

Guide «cloud»

Novembre 2025
Guide de l'ASB
3e édition

Table des matières

Remarque:
Les modifications apportées en rapport à la deuxième édition sont signalées par un astérisque (*) dans le Guide légal et réglementaire et figurent à la fin du document. Les simples adaptations rédactionnelles sans incidence matérielle ne sont pas signalées.

Avant-propos

La transition numérique se poursuit irrésistiblement dans le secteur financier, conférant une importance croissante aux prestations de cloud computing. Dans cette troisième édition du guide «cloud» de l'Association suisse des banquiers (ASB), nous nous penchons sur les évolutions et les défis liés au recours à la technologie du cloud par les banques et les maisons de titres.

Les nouvelles technologies favorisent la compétitivité du secteur financier suisse: selon la situation des banques et des maisons de titres concernées, les prestations de cloud computing peuvent générer pour elles, d'une part, des gains d'efficience, des avantages en termes de coûts et une sécurité accrue, mais aussi, d'autre part, la possibilité de développer des services innovants et de les commercialiser de manière rapide et flexible. Par ailleurs, la résilience de l'infrastructure des banques et des maisons de titres ainsi que la confiance dans son bon fonctionnement jouent un rôle essentiel. Mais les prestations de cloud computing peuvent également comporter des risques, par exemple celui de créer des dépendances par rapport à des tiers, et entraîner des pertes de contrôle en cas d'utilisation inappropriée.

Quelle que soit la technologie mise en œuvre, il y a des exigences légales et réglementaires à respecter. Celles-ci concernent notamment le secret professionnel tel que prévu par la loi sur les banques (LB) et la loi sur les établissements financiers (LEFin), la protection et la sécurité des données ainsi que la résilience, par exemple en relation avec des données critiques au sens de la circulaire 2023/1, «Risques et résilience opérationnels – banques», de l'Autorité fédérale de surveillance des marchés financiers (FINMA).

L'interprétation de ces prescriptions, et en particulier leur mise en œuvre au moyen de mesures techniques et organisationnelles (en abrégé MTO) appropriées, peuvent être plus ou moins complexes selon le modèle d'affaires et d'exploitation. C'est pourquoi dès 2019, un groupe de travail placé sous la direction de l'ASB a élaboré un guide légal et réglementaire (ci-après le «Guide») pour les banques et les maisons de titres qui recourent à des prestations de cloud computing. L'objet de ce Guide est de formuler des recommandations auxquelles les établissements pourront se référer pour l'acquisition et la mise en œuvre de prestations de cloud computing.

Afin d'intégrer les évolutions légales et réglementaires intervenues depuis sa première publication, par exemple en matière de réglementation des risques opérationnels, le Guide a été mis à jour.

Le Guide est structuré en 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 et les maisons de titres, met en lumière les principes pertinents selon l'ASB ainsi que les aspects réglementaires majeurs en relation avec le recours à des prestations de cloud computing par les banques et les maisons de titres, et propose des pistes de solutions. La deuxième partie expose les recommandations légales et réglementaires de l'ASB au regard du droit suisse.

Définir puis mettre en œuvre des mesures techniques et organisationnelles appropriées, qui concrétisent et rendent opérationnelles les exigences légales et de politique commerciale concernant l'utilisation des technologies du cloud, constitue également un enjeu crucial pour les banques et les maisons de titres qui

recourent à des prestations de cloud computing. Il appartient à chaque établissement de relever ce défi à titre individuel, en tenant compte de sa situation spécifique.

Le présent document ne prétend pas à l'exhaustivité. Il est mis à jour et complété au vu des évolutions technologiques et juridiques. Chaque nouvelle version du Guide fait l'objet d'une publication.

Management Summary

- Le **recours à la technologie du cloud** est un **facteur critique de succès** pour la Suisse et pour sa place financière. Il est indispensable que les banques et les maisons de titres aient une vision claire des exigences légales et réglementaires qui s'imposent à elles et soient en mesure de les concrétiser et de les rendre opérationnelles au moyen de mesures techniques et organisationnelles appropriées.
- Le présent document constitue un **guide juridiquement non contraignant,** conçu comme un outil pratique d'interprétation en cas de recours à des prestations de cloud computing par les établissements. Il se focalise sur les quatre domaines suivants:
  - **suivi (gouvernance, y compris gestion des risques):** choix du prestataire de services de cloud computing et de ses sous-traitants, accord en cas de changement de sous-traitants
  - **traitement des données:** traitement de données bancaires de client.e.s
  - **autorités et procédures:** transparence et coopération entre les établissements et les prestataires de services de cloud computing 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
- Le Guide propose aux établissements des pistes de solutions concrètes en réponse aux principales problématiques légales et réglementaires. Il appartient néanmoins à **chaque établissement** de gérer l'aspect véritablement clé en ce qui concerne le recours au cloud, à savoir l'évaluation des risques et la définition subséquente de mesures techniques et organisationnelles appropriées.

Les prestations de cloud computing en pratique

Utilité et avantages des prestations de cloud computing

La transition numérique se poursuit irrésistiblement dans le secteur financier, conférant une importance croissante aux prestations de cloud computing. Selon la situation des banques et des maisons de titres concernées, les prestations de cloud computing peuvent générer pour elles, d'une part, des gains d'efficience et des avantages en termes de coûts, mais aussi, d'autre part, la possibilité de développer des services innovants et de les commercialiser de manière rapide et flexible. En outre, des prestataires spécialisés dans le cloud computing permettent le cas échéant d'améliorer la sécurité de l'infrastructure des banques et des maisons de titres. Les prestations de cloud computing constituent donc un facteur critique de succès pour la place financière suisse.

Les clientes et les clients des banques sont nombreux à utiliser des prestations de cloud computing au quotidien, sans toujours s'en rendre compte. 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 peut fonctionner aussi pour des établissements hautement spécialisés exerçant des activités complexes. Mais quelle que soit la technologie mise en œuvre, il y a des exigences légales et réglementaires à respecter.

La migration de l'infrastructure et des processus vers un cloud permet aux établissements d'accélérer la maturation commerciale de leurs produits et services innovants, d'où des gains de compétitivité. Elle leur permet également de bénéficier des nouvelles technologies, comme l'intelligence artificielle, sans avoir à réaliser de lourds investissements en matériel et en 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'offre de fonctionnalités cloud est généralement disponible en «self service» à des coûts variables, dans la mesure où seules sont facturées les prestations auxquelles il est directement fait appel. Les établissements ont ainsi davantage de latitude, par exemple, pour réagir aux fluctuations de leurs besoins, puisqu'ils peuvent activer en toute flexibilité les ressources informatiques nécessaires ou les désactiver le cas échéant.

Le fait de ne plus avoir à développer ou acquérir des compétences et des ressources dans le cadre de leur propre infrastructure informatique rend les prestations de cloud computing particulièrement attrayantes pour les petits établissements. Ces derniers ont désormais accès à des technologies autrefois réservées aux grandes entreprises et qui génèrent des économies d'échelle significatives.[1] Toutefois, il leur faut développer et optimiser de nouvelles compétences pour assurer une gestion et un suivi efficaces des prestations de cloud computing auxquelles ils recourent. L'utilisation du cloud permet aussi de satisfaire plus facilement 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 établissements suisses, de plus en plus, prennent conscience de l'utilisation de prestations de cloud computing. Par ailleurs, la concurrence règne désormais entre les prestataires nationaux et internationaux, ce dont on ne peut que se réjouir. Le recours croissant à des prestations de cloud computing contribuera à renforcer encore la place financière et l'écosystème financier en Suisse.

---

1 En raison des coûts marginaux, de nombreux établissements sont dans l'incapacité de mettre en place leur propre système de cloud au même prix que des prestataires spécialisés. Grâce au cloud, 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 (grand) logiciel pour y apporter des corrections.

Le **cloud computing** est un modèle de traitement des données qui, par le biais d'un ré-seau, permet d'accéder aisément, à tout moment et en tout lieu, à un pool partagé de res-sources informatiques configurables (p. ex. réseaux, serveurs, systèmes de stockage, ap-plications et services). Ces ressources peuvent être mises à disposition rapidement, moyennant un minimum de tâches d'administration et de faibles interactions avec les four-nisseurs 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]

Considérations de fond à propos du recours à des prestations de cloud computing

Il convient dans un premier temps qu'en fonction de son modèle d'affaires et d'exploitation ainsi que de sa stratégie, l'établissement fixe les objectifs de politique commerciale qu'il poursuit en recourant à des prestations de cloud computing. Dans un second temps, il est recommandé d'identifier et de clarifier les conditions légales et réglementaires y relatives. Ensuite, il y a lieu de concrétiser les conclusions de ces deux étapes dans des prescriptions internes, y compris des prescriptions concernant les mesures techniques et organisationnelles[4] qui régiront le choix, la mise en œuvre et le contrôle des prestations de cloud computing.[5] Ces prescriptions sont typiquement élaborées et/ou appliquées dans le cadre de projets cloud à l'échelle de l'établissement, qui impliquent de nombreuses parties prenantes et une forte division du travail. Une gouvernance contraignante, qui définit clairement les tâches, les compétences et les responsabilités (y compris en matière de contrôle), assure une bonne utilisation du cloud à l'issue du projet.

En résumé, on retiendra que le choix, l'acquisition et la mise en œuvre de prestations de cloud computing constituent un processus très fractionné en termes de répartition des tâches, qui se caractérise par une multitude de conditions-cadres liées à la politique commerciale et à la situation de l'établissement lui-même ainsi qu'à des éléments extérieurs.

D'un point de vue juridique, la gestion des prestataires est primordiale; les conditions-cadres légales et réglementaires applicables dépendent en particulier du modèle opérationnel cible *(target operating model)* de l'établissement, des caractéristiques du prestataire (prestataire de services de cloud computing), ainsi que de la nature des données concernées, du lieu de leur traitement et de l'accès à ces données – par exemple en cas de travaux de maintenance. Le principe est que les conditions-cadres sont d'autant plus strictes que les données concernées sont sensibles et que leur traitement présente un lien avec l'étranger.

---

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

4 La définition et la mise en place de mesures techniques et organisationnelles appropriées ne sont pas des questions juridiques.

5 Concernant les données personnelles, ce processus a été expressément prévu par exemple à l'art. 7, al. 2 de la loi révisée sur la protection des données (LPD).

De manière générale, tout prestataire de services de cloud computing doit respecter les conditionscadres applicables à l'établissement qui le mandate et qui lui transfère dès lors les obligations lui incombant. Il est donc important, d'une part, que cet établissement dispose d'une organisation suffisamment mature en matière de données, y compris pour ce qui concerne la gestion des données et des risques et son suivi granulaire et, d'autre part, que le prestataire fasse preuve de la flexibilité requise.

Principales pistes de solutions proposées par l'ASB dans le Guide

Nonobstant d'éventuelles obligations légales et réglementaires, le présent Guide formule des recommandations juridiquement non contraignantes auxquelles les établissements pourront se référer pour l'acquisition et la mise en œuvre de prestations de cloud computing. Il propose également des interprétations du droit applicable en relation avec les prestations de cloud computing. Il se focalise sur quatre domaines:

- **suivi (gouvernance, y compris gestion des risques):** choix du prestataire de services de cloud computing et de ses sous-traitants, accord en cas de changement de sous-traitants
- **traitement des données:** traitement de données bancaires de client.e.s
- **autorités et procédures:** transparence et coopération entre les établissements et les prestataires de services de cloud computing 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

Le présent Guide propose des pistes de solutions concrètes pour répondre aux exigences réglementaires. En cela, il constitue une contribution importante de l'ASB en faveur de la place financière suisse. Les établissements désireux d'utiliser le Guide doivent toutefois le faire en tenant compte de leur taille ainsi que de la complexité et de l'organisation de leur modèle d'affaires et de leurs processus, selon une approche fondée sur le risque et proportionnée.

A) Choix du prestataire et des sous-traitants, changements les concernant[6]

But des recommandations formulées dans le Guide:
l'établissement dispose à tout moment des principales informations requises pour pouvoir choisir un prestataire de services de cloud computing, y compris des informations sur les sous-traitants essentiels dudit prestataire.

6 Voir à ce sujet le chapitre II:5 du Guide.

A des fins d'efficacité et de compétitivité, les prestataires de services de cloud computing 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).

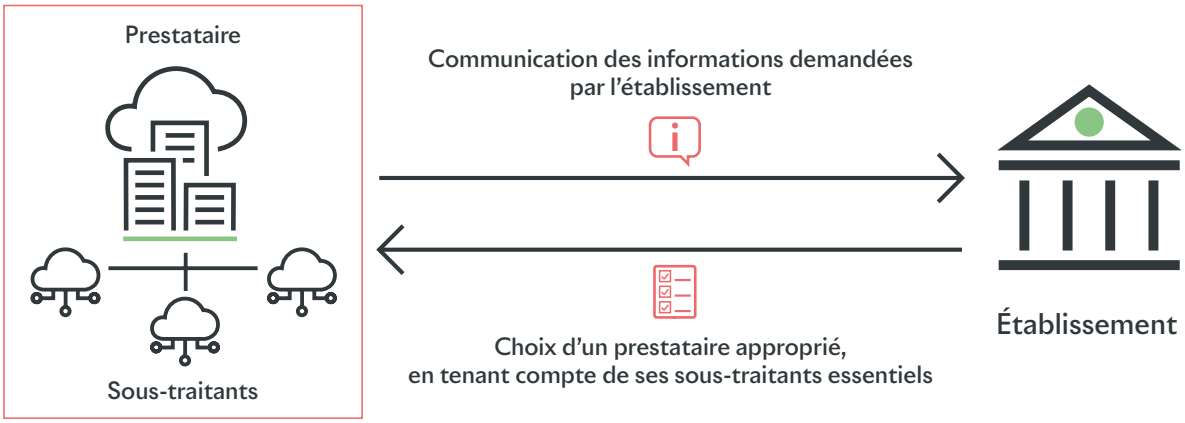
Lors du choix d'un prestataire, il convient donc de tenir compte en particulier des éléments suivants:

- capacité du prestataire de remplir ses obligations contractuelles, notamment au moyen de mesures techniques et organisationnelles appropriées;
- stabilité économique;
- législation à laquelle le prestataire est soumis.

Outre les critères tenant aux prestations, il convient de vérifier si le prestataire est disposé à et en mesure de s'engager contractuellement à respecter les obligations essentielles résultant du droit des marchés financiers et des prescriptions légales sur la protection des données, en prenant les mesures techniques et organisationnelles requises.

Graphique 1

Choix du prestataire et des sous-traitants, changements les concernant
Obligations des prestataires envers l'établissement



Le prestataire devrait mettre les informations demandées à la disposition de l'établissement et il est tenu en particulier d'informer ce dernier de tout éventuel engagement ou remplacement d'un sous-traitant essentiel. L'établissement, 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 éventuelles données données bancaires de client.e.s.

Source: Association suisse des banquiers (ASB) 2025

Lors du choix d'un prestataire et de ses sous-traitants, il convient d'accorder une grande importance à la sécurité des données (c'est-à-dire à leur confidentialité, leur intégrité, leur disponibilité et leur traçabilité), qui doit faire partie intégrante de l'examen de diligence *(due diligence)*.

En particulier, l'établissement doit être préalablement informé de tout changement concernant un sous-traitant essentiel (cf. graphique 1).[7] 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 données bancaires de client.e.s. Comptent notamment parmi ces dispositions un délai de préavis raisonnable, une option de prolongation avec maintien du modèle d'exploitation existant ainsi qu'une liberté de choix quant aux interfaces et aux formats d'exportation de données.

B) Respect du secret bancaire[8] sur le cloud[9]

But des recommandations formulées dans le Guide:
le respect des prescriptions légales et réglementaires concernant **le secret bancaire doit être assuré à tout moment y compris sur le cloud, au moyen de mesures techniques et organisationnelles appropriées.**

Dès lors que des données bancaires de client.e.s 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 la loi sur la protection des données.[10]

Le Guide se focalise sur le traitement de données relevant du secret bancaire, appelées en l'occurrence «données bancaires de client.e.s». Il envisage à cet égard diverses mesures techniques, organisationnelles et contractuelles appropriées pour limiter le risque que le prestataire de services de cloud computing et ses sous-traitants accèdent à des données bancaires de client.e.s (cf. graphique 2).

---

7 Voir à ce sujet la Circ.-FINMA 18/3, «Outsourcing. Externalisations dans le secteur des banques, des entreprises d'assurance et de certains établissements financiers au sens de la LEFin», chiffre marginal 33, ainsi que l'art. 9, al. 3 LPD.

8 Le Guide traite du secret bancaire à titre d'exemple. Les développements y relatifs sont transposables par analogie, notamment, au secret professionnel au sens de l'art. 69 de la loi sur les établissements financiers (LEFin). En ce qui concerne les données bancaires de client.e.s, l'art. 162 du Code pénal (secret des affaires) et – dès lors que ces données peuvent être qualifiées de données personnelles – l'art. 62 LPD (devoir de discrétion) s'appliquent à titre subsidiaire.

9 Voir à ce sujet les chapitres III:10 et IV du Guide.

10 Si les données bancaires de client.e.s sont des données personnelles, elles sont également soumises aux dispositions du droit applicable en matière de protection des données.

Définitions[11]

Données bancaires de client.e.s
Toutes les informations soumises au secret bancaire conformément à l'art. 47 LB. Chaque établissement définit lui-même, dans le cadre de ses exigences de politique commerciale et légales, quelles informations concrètes relèvent de la notion de données bancaires de client.e.s.

Données personnelles au sens de la loi sur la protection des données (LPD)
Toutes les informations concernant une personne physique identifiée ou identifiable.[12]

Lien avec l'étranger et *foreign lawful access*[13]

Selon le modèle d'exploitation de l'établissement et les technologies mises en œuvre, il peut arriver que les prestataires de services de cloud computing auxquels cet établissement fait appel présentent un lien avec l'étranger. Tel est le cas par exemple lorsqu'un prestataire fait partie d'un groupe étranger, a son siège à l'étranger ou traite à l'étranger des données bancaires de client.e.s.

Lors de l'acquisition de prestations de cloud computing, l'établissement concerné doit convenir de mesures techniques et organisationnelles appropriées avec le prestataire, afin de garantir la confidentialité des données bancaires de client.e.s chez ce prestataire et d'assurer par exemple leur protection contre les cybercriminels.

Si le prestataire présente un lien avec l'étranger, il n'est toutefois pas exclu que le droit étranger applicable de ce fait autorise des autorités étrangères à ordonner la communication de données bancaires de client.e.s. En pareil cas, les autorités étrangères peuvent traiter ces données conformément au droit applicable dans leur pays, par exemple dans le cadre de leurs investigations ou de leurs procédures. Or il peut arriver que les dispositions étrangères ne prévoient pas une protection appropriée des données au sens où on l'entend en Suisse, ni des droits comparables (p. ex. restrictions en matière d'accès aux données et de transmission des données, voies de recours).

Pour des raisons pratiques, on peut raisonnablement considérer en cas de doute que le lien avec l'étranger est susceptible de conduire à l'application de lois étrangères, et donc de permettre aux autorités étrangères d'accéder aux données de manière certes légale au regard de leur propre droit, mais illégale au regard du droit suisse applicable aux établissements suisses *(foreign lawful access)*.

---

11 Choix de notions non exhaustif.

12 Art. 5, let. a LPD.

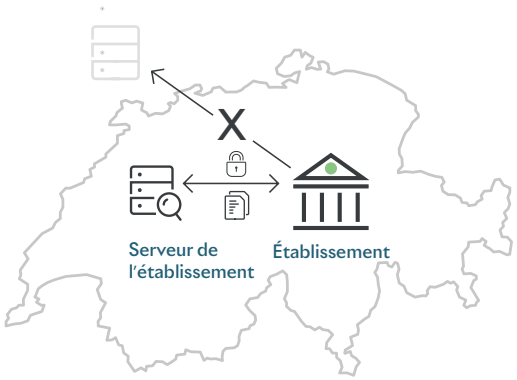
13 Voir à ce sujet le chapitre III:10, chiffre marginal 51, ainsi que le chapitre IV du Guide.

Si des mesures techniques et organisationnelles appropriées garantissent selon une probabilité proche de la certitude soit qu'il n'y aura aucune transmission de données, soit que les données transmises ne permettront pas à des tiers non autorisés (au sens du droit suisse) d'identifier directement ou indirectement des personnes protégées par le secret bancaire, il n'y a pas divulgation enfreignant le secret.[14] En revanche, si des mesures techniques et organisationnelles appropriées ne permettent d'empêcher selon une probabilité proche de la certitude ni la transmission de données, ni l'identification des personnes concernées, il y aurait lieu de demander le consentement des personnes concernées ainsi que, si nécessaire, l'autorisation des autorités compétentes, et de justifier ainsi la divulgation des données à des autorités étrangères (cf. graphique 3).[15]

Graphique 2

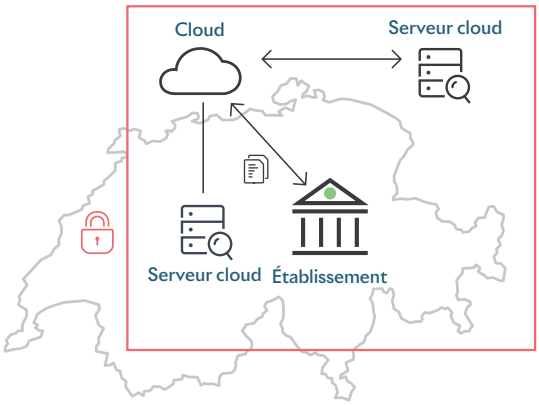
Le secret bancaire sur le cloud

Protection des données sur les serveurs de l'établissement



Protection des données garantie et respect du secret bancaire. En pratique, le contrôle sur les données s'arrête aux frontières de la juridiction.

Protection des données sur le cloud



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

Source: Association suisse des banquiers (ASB) 2025

14 En vertu du droit de la protection des données également, ces données ne constituent pas des données personnelles selon la méthode dite relative. Cela a été confirmé judiciairement. Cf. ATF 136 II 508 – Logistep ainsi que l'arrêt de la Cour de justice de l'Union européenne (CJUE) du 19 octobre 2016 dans l'affaire C-582/14 – Patrick Breyer contre Bundesrepublik Deutschland. Voir en outre le considérant 26 du 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), pour le cas où celui-ci serait applicable: *«Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement […].»*

15 Voir à ce sujet le chapitre IV du Guide.

Protection des données bancaires de client.e.s sur le cloud[16]

Mesures techniques possibles[17]

Des mesures techniques appropriées peuvent avoir pour effet que les données traitées sur le cloud ne répondent plus à la qualification de données bancaires de client.e.s. Tel est le cas des données anonymisées. Il en va de même, du point de vue de la ou du destinataire des données, des données bancaires de client.e.s pseudonymisées ou cryptées, par exemple lorsque le ou la destinataire ne dispose pas d'un tableau de concordance des pseudonymes ou de la possibilité de décrypter les données cryptées.[18]

- **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 que, selon une probabilité proche de la certitude, plus personne ne puisse les rattacher à la personne concernée.
- **Pseudonymisation:** la pseudonymisation consiste à remplacer des attributs personnels par un nom d'emprunt appelé pseudonyme de telle sorte que, selon une probabilité proche de la certitude, l'établissement puisse les rattacher à la personne concernée, mais pas la ou le destinataire des données.
- **Cryptage:** le cryptage est la principale forme de pseudonymisation. Il consiste à transformer un texte clair[19] 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.

Mesures organisationnelles possibles

- Surveillance appropriée par l'établissement des mesures opérationnelles prises par le prestataire de services de cloud computing et par 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 possibles[20]

- Identification appropriée des mesures techniques et organisationnelles dans le contrat
- Obligation du prestataire de services de cloud computing de convenir de mesures techniques et organisationnelles appropriées avec ses sous-traitants
- Engagement contractuel du prestataire à respecter la confidentialité au moyen de prescriptions concrètes concernant les mesures techniques et organisationnelles

---

16 Voir par exemple aussi l'annexe C du rapport de la Chancellerie fédérale de mars 2025 intitulé «Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale» (2e édition), qui donne un aperçu sommaire des risques et des mesures d'atténuation correspondantes.

17 Voir à ce sujet le chapitre III:10.2 du Guide, chiffres marginaux 38 ss.

18 Voir à ce sujet la note de bas de page 14.

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

20 Certains établissements considèrent que les mesures contractuelles font partie des mesures organisationnelles. Quoi qu'il en soit, les mesures techniques et organisationnelles ne sont généralement pas des questions ou des prescriptions juridiques.

- 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 l'établissement et le prestataire 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 de données bancaires de client.e.s traitées sur le cloud
- Accord entre l'établissement et le prestataire sur la marche à suivre par l'un ou par l'autre dans le cadre de l'identification et de l'évaluation des violations de la confidentialité par des cybercriminels et autres

Corrélations entre les prescriptions légales, les prescriptions concernant les mesures techniques et organisationnelles et ces mesures elles-mêmes[21]

Dans le contexte des prescriptions concernant les mesures techniques et organisationnelles, le législateur et le régulateur parlent souvent d'une «approche fondée sur le risque».[22] Ils ne visent pas ainsi le manquement à des prescriptions légales ou réglementaires fondé sur un «risque calculé» – bien au contraire.

Les prescriptions légales et réglementaires applicables doivent être respectées dans tous les cas, au moyen de mesures techniques et organisationnelles appropriées et spécifiques à chaque établissement.

C'est pour définir les mesures techniques et organisationnelles appropriées que s'applique l'approche fondée sur le risque: cette approche considère qu'en fonction du modèle d'affaires et d'exploitation propre à l'établissement concerné ainsi que de sa stratégie, la probabilité qu'un risque se réalise et l'ampleur des dommages résultant d'une violation du droit sont plus importantes dans certains scénarios que dans d'autres.

L'approche fondée sur le risque se traduit par le fait que les mesures techniques et organisationnelles appropriées, une fois définies puis correctement mises en œuvre, ne doivent pas obligatoirement envisager et prévenir tous les scénarios imaginables en théorie, mais seulement ceux dont la réalisation, dans le cas d'espèce, est prévisible selon le cours nor-mal des choses et l'expérience générale de la vie et peut être évitée si l'on respecte ses obligations. Si un scénario non prévisible au sens indiqué ci-dessus se réalise, et si ce scénario n'a pas pu être évité en dépit de mesures techniques et organisationnelles appropriées et correctement mises en œuvre, l'établissement et/ou les personnes décisionnaires ne devraient pas pouvoir en principe se voir reprocher un comportement (pénalement) répréhensible.[23]

---

21 Voir à ce sujet le chapitre III:10.2, chiffre marginal 37 du Guide.

22 Voir par exemple le rapport explicatif relatif à l'ordonnance sur la protection des données (OPDo) du 31 août 2022, pp. 11, 18 s., 23, 28.

23 Cf. ATF 135 IV 56, consid. 2.1. Il existe diverses méthodes d'évaluation de la probabilité de réalisation d'un risque et de l'ampleur des dommages résultant d'une violation du droit.

Exclure totalement tous les risques n'est ni possible en pratique, ni exigé par la loi. Le critère devrait être que dans le cas d'espèce, les risques prévisibles propres à l'établissement ont été gérés ès qualités par les personnes compétentes au moyen de mesures techniques et organisationnelles appropriées et que dès lors, les obligations de diligence ont été respectées.

C) Transparence et coopération entre les établissements et les prestataires en ce qui concerne les mesures administratives et judiciaires[24]

But des recommandations formulées dans le Guide:[25]
le prestataire de services de cloud computing et l'établissement déterminent d'un commun accord une marche à suivre lorsque des autorités étrangères demandent la communication de données bancaires de client.e.s.

Des demandes des autorités ou des procédures peuvent avoir pour objet la remise ou la transmission de données bancaires de client.e.s traitées sur le cloud. Par ailleurs, des lois étrangères peuvent prévoir la communication de données par les prestataires de services de cloud computing.

Le Guide préconise que le prestataire et l'établissement conviennent d'une marche à suivre pour traiter les demandes des autorités ayant pour objet la remise ou la transmission de données bancaires de client.e.s.

Si, en cas de demande de remise ou de transmission de données bancaires de client.e.s, une autorité suisse compétente en l'espèce (p. ex. un tribunal suisse compétent) s'appuie sur un fondement juridique suffisant et clair issu du droit suisse (y compris les traités ratifiés par la Suisse), on parle de *lawful access*. Il convient alors de vérifier si la remise ou la transmission des données entre effectivement dans le champ du fondement juridique invoqué.

En revanche, si une autorité étrangère s'appuie sur un fondement juridique issu de son propre droit, on parle de *foreign lawful access*. La remise ou la transmission de données bancaires de client.e.s peut être

24 Voir à ce sujet le chapitre IV du Guide.

25 Les mêmes recommandations pourraient être pertinentes notamment dans le cadre d'autres secrets professionnels ou en cas de secrets commerciaux. Les questions relatives au droit de la protection des données demeurent réservées et ne sont pas traitées ici.

illégale au regard de la législation suisse (p. ex. lorsque les informations concernées sont protégées par le secret bancaire) alors qu'elle est légale au regard de la législation étrangère. Dans ce cas, comme indiqué supra, des mesures techniques et organisationnelles appropriées, préalablement mises en œuvre, doivent permettre selon une probabilité proche de la certitude soit d'empêcher la transmission de données bancaires de client.e.s, soit de ne transmettre que des informations ne permettant pas à des tiers non autorisés (au sens du droit suisse) d'identifier directement ou indirectement des personnes protégées par le secret bancaire. Si cela devait s'avérer impossible, il y aurait lieu d'examiner si la remise ou la transmission de données concernée peut être justifiée par le consentement[26] de l'établissement, le consentement[27] des personnes concernées, la décision d'un tribunal suisse compétent et/ou l'autorisation de l'autorité suisse compétente donnée aux autorités étrangères (cf. graphique 3).[28]

Dans tous les cas et dans la mesure où le droit le permet, le prestataire de services cloud devrait informer l'établissement en temps utile lorsque des autorités étrangères formulent une demande ayant pour objet la remise ou la transmission de données bancaires de client.e.s. S'il n'y est pas autorisé en vertu de la législation invoquée par l'autorité étrangère concernée, il lui appartient de s'assurer par lui-même que la demande de cette dernière est légale au regard de cette même législation et de la contester si tel n'est pas le cas.[29] Lorsqu'il conteste une demande, le prestataire demande des mesures provisoires visant à suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente se prononce sur son bien-fondé. Il ne divulgue pas les données bancaires de client.e.s demandées tant qu'il n'est pas obligé de le faire en vertu des règles de procédure applicables.[30]

Il appartient également au prestataire de services cloud d'accorder à l'établissement les droits nécessaires pour conduire la procédure et de l'aider à traiter les demandes des autorités étrangères.n.

---

26 Le consentement peut prendre différentes formes et être documenté de différentes manières, c'est une question de gestion des risques et de propension au risque dans la perspective d'une éventuelle procédure probatoire.

27 Voir note de bas de page 26.

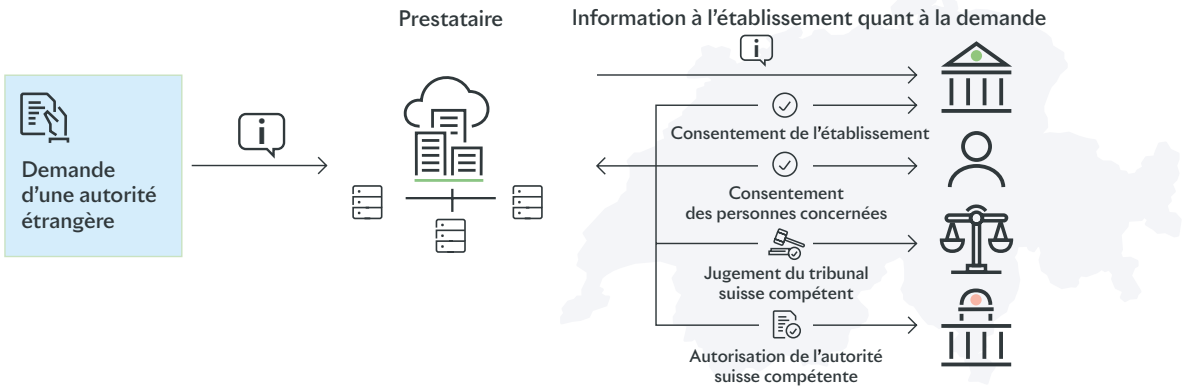
28 En relation avec les demandes d'autorités étrangères, que les informations concernées soient qualifiées de données bancaires de client.e.s et/ou de données personnelles, d'autres prescriptions sont pertinentes, notamment l'art. 42c de la loi sur la surveillance des marchés financiers (LFINMA) et l'art. 271 du Code pénal (CP). Voir les développements y relatifs au chapitre IV du Guide.

29 Par analogie avec les clauses 15.1. Notification et 15.2. Contrôle de la légalité et minimisation des données de la décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil. .

30 Voir note de bas de page 29.

Graphique 3

Demande d'une autorité étrangère
Communication de données bancaires de client.e.s sous certaines conditions



Le prestataire et l'établissement doivent convenir de la marche à suivre en cas de demandes d'autorités étrangères ayant pour objet la communication de données bancaires de client.e.s traitées sur le cloud. Si la communication de données bancaires de client.e.s ne peut être empêchée selon une probabilité proche de la certitude au moyen de mesures techniques et organisationnelles, elle ne peut intervenir que conformément aux dispositions légales en vigueur et selon le cas avec le consentement de l'établissement, le consentement des personnes concernées, en vertu d'un jugement du tribunal suisse compétent et/ou sur la base d'une autorisation de l'autorité suisse compétente.

Source: Association suisse des banquiers (ASB) 2025

D) Contrôle (audit) des prestations de cloud computing et des moyens mis en œuvre[31]

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 clientes et de clients à partir de centres de calcul hautement sécurisés. Le contrôle (audit) des infrastructures utilisées nécessite un haut niveau de spécialisation.

Le respect des prescriptions légales, réglementaires et contractuelles applicables au prestataire devrait faire l'objet de contrôles réguliers, en particulier pour ce qui concerne les exigences en matière d'externali-

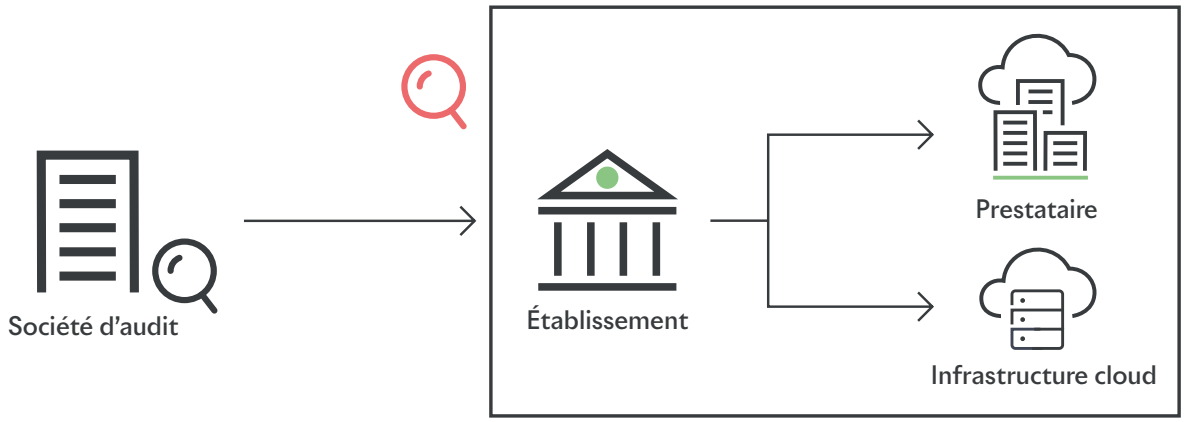
31 Voir à ce sujet le chapitre V du Guide.

sation, de protection des données et de sécurité des informations. Ces contrôles devraient pouvoir être demandés et réalisés par l'établissement, par sa société d'audit externe ou 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[32] est suffisant. Le contrôle des sous-traitants essentiels par l'établissement peut s'effectuer indirectement, par le biais du contrôle du prestataire (cf. graphique 4).

Graphique 4

Contrôle (audit) sur le cloud
Le contrôle des infrastructures cloud nécessite un haut niveau de spécialisation



Lors de l'audit de l'établissement, 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) 2025

32 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 les maisons de titres 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 professionnel.le.s 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 bancaires de client.e.s[1] (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)

Au fil des expériences faites par les différents établissements, les questions juridiques initiales ont été clarifiées; la discussion à propos du cloud s'est donc déplacée vers des questions non juridiques autour des prescriptions concernant la mise en place de mesures techniques et organisationnelles appropriées. Celles-ci concrétisent et rendent opérationnelles les exigences légales, réglementaires et de politique commerciale propres à chaque établissement, qui reflètent les divers modèles d'affaires et d'exploitation. A cet effet, les établissements désireux d'utiliser le présent Guide peuvent prendre en compte leur taille ainsi que la complexité de leur modèle d'affaires, selon une approche fondée sur le risque 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 autorégulation.

1 Le Guide se focalise sur le traitement de toutes les données relevant du secret bancaire, appelées en l'occurrence «données bancaires de client.e.s».

2 Définitions

(4)* Aux fins du présent Guide, on entend par:

a. **«Circ.-FINMA 18/3»:** la circulaire 2018/3 de l'Autorité fédérale de surveillance des marchés financiers, intitulée «Outsourcing. Externalisations dans le secteur des banques, des entreprises d'assurance et de certains établissements financiers au sens de la LEFin», date de publication de la version en vigueur: 21 septembre 2017.
b. **«Circ.-FINMA 23/1»:** la circulaire 2023/1 de l'Autorité fédérale de surveillance des marchés financiers, intitulée «Risques et résilience opérationnels – banques. Gestion des risques opérationnels et garantie de la résilience opérationnelle», date de publication de la version en vigueur: 7 décembre 2022.
c. **«clientes et clients»:** les clientes et les clients d'un établissement.
d. **«cloud» ou «cloud computing»** les modèles de service tels que définis par le National Institute of Standard and Technology (NIST)[2] ou l'Agence de l'Union européenne pour la cybersécurité (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.[4]
e. **«CP»:** le code pénal suisse, RS 311.0.
f. **«données bancaires de client.e.s»:** toutes les informations soumises au secret bancaire conformément à l'art. 47 LB. Chaque établissement définit lui-même, dans le cadre de ses exigences de politique commerciale et légales, quelles informations concrètes relèvent de la notion de données bancaires de client.e.s.
g. **«données critiques»:** les données au sens de la Circ.-FINMA 23/1, chiffre marginal 7.
h. **«données personnelles»:** les données définies comme telles dans la loi sur la protection des données. La notion de «données personnelles» inclut celle de «données à caractère personnel».[5]
i. **«établissement»:** les banques et les maisons de titres au sens de la Circ.-FINMA 18/3, chiffre marginal 5.
j. **«Guide»:** les principes et recommandations formulés dans le présent document.
k. **«LB»:** la loi fédérale sur les banques et les caisses d'épargne (loi sur les banques), RS 952.0.
l. **«LEFin»:** la loi fédérale sur les établissements financiers (loi sur les établissements financiers), RS 954.1.
m. **«LFINMA»:** la loi sur l'Autorité fédérale de surveillance des marchés financiers (loi sur la surveillance des marchés financiers), RS 956.1.

---

2 The NIST Definition of Cloud Computing (2011)

3 European Network and Information Security Agency (ENISA), Cloud Computing Security Risk Assessment (2009)

4 «Cloud» ou «cloud computing» intègre aussi par exemple le modèle «Function-as-a-Service» (FaaS).

5 Telle que définie dans le 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), pour le cas où celui-ci serait applicable.

n. **«LPD»:** la loi fédérale sur la protection des données (loi sur la protection des données), RS 235.1.
o. **«LSI»:** la loi fédérale sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information), RS 128.
p. **«OB»:** l'ordonnance sur les banques et les caisses d'épargne (ordonnance sur les banques), RS 952.02.
q. **«obligation d'annonce»:** les obligations d'annonce au sens de l'art. 24 LPD, des art. 74a ss LSI, de la Communication FINMA sur la surveillance 05/2020 «Obligation de signaler les cyber-attaques selon l'art. 29, al. 2 LFINMA»[6] et de la Circ.-FINMA 23/1, chiffre marginal 81.
r. **«OEFin»:** l'ordonnance sur les établissements financiers, RS 954.11.
s. **«prestataire»:** le fournisseur des prestations de cloud computing, qui est extérieur à l'établissement et au groupe dont fait éventuellement partie l'établissement.
t. **«prestations de cloud computing»:** les modèles de service fournis par le prestataire en matière de cloud computing, sur commande de l'établissement.
u. **«secret bancaire»[7]:** le secret protégé par l'art. 47 LB.
v. **«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.
w. **«traitement»:** les opérations relatives à des données personnelles telles que définies dans la loi sur la protection des données.[8]

6 Dans sa communication sur la surveillance 03/2024 du 7 juin 2024, la FINMA précise certains points concernant l'obligation de signaler les cyberattaques.

7 Le présent Guide traite du secret bancaire à titre d'exemple. Les développements y relatifs sont transposables par analogie, notamment, au secret professionnel au sens de l'art. 69 LEFin. En ce qui concerne les données bancaires de client.e.s, l'art. 162 CP (secret des affaires) et – dès lors que ces données peuvent être qualifiées de données personnelles – l'art. 62 LPD (devoir de discrétion) s'appliquent à titre subsidiaire.

8 Voir aussi la définition figurant dans le règlement général sur la protection des données, pour le cas où celui-ci serait applicable.

Chapitre II: suivi (gouvernance, y compris gestion des risques)

Fondements juridiques

- Art. 3 et 47 LB, art. 12 OB
- Art. 2, 5, 6, 9, 41 ss. et 69 LEFin, art. 66 et 68 OEFin
- LPD
- Circ.-FINMA 23/1
- 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 donc résulter d'un processus structuré.

(6)* Dans l'analyse des risques[9] préalable à cette décision, 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 données, en particulier des données bancaires de client.e.s, traitées dans le cadre desdites prestations.

(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. En conséquence, après la phase d'acquisition *(«change the bank»),* il y a lieu de structurer suffisamment l'organisation et les processus pour assurer le bon fonctionnement de la prestation de cloud computing

9 Par exemple, il y a lieu d'analyser les risques liés à la sécurité des données ou aux aspects opérationnels.

(«run the bank»), en prenant des mesures techniques et organisationnelles appropriées ainsi qu'en instaurant des systèmes adéquats de documentation[10], de contrôle et de gouvernance.

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 la législation sur la protection des données[11], dès lors que les prestations de cloud computing incluent le traitement de données bancaires de client.e.s 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 devrait coopérer 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 devrait déterminer les droits et obligations des parties et des tiers intéressés, y compris en ce qui concerne leur mise en œuvre.

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

(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 répondre aux besoins en termes de mesures techniques et organisationnelles ainsi que d'obligations contractuelles, de sa stabilité économique, des ordres juridiques dont lui et ses sous-traitants relèvent et d'autres critères déterminants.[12] Les sous-traitants essentiels sont

---

10 En particulier, lorsqu'un contrat de services renvoie à des annexes au moyen de liens informatiques, il serait bon que les établissements téléchargent les annexes valables à la date de conclusion du contrat et les conservent.

11 La loi et l'ordonnance sur la protection des données ainsi que le règlement général sur la protection des données, pour le cas où celui-ci serait applicable.

12 Dès lors qu'il y a traitement de données personnelles, les obligations de contrôle prévues dans la LPD, par exemple dans le cadre d'une analyse d'impact relative à la protection des données personnelles ou d'une sous-traitance, doivent être respectées. Leur teneur et leur étendue sont à déterminer au cas par cas, en tenant compte du modèle d'affaires et d'exploitation de l'établissement concerné.

à intégrer dans cette évaluation. Le prestataire devrait 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 devrait prendre en compte la volonté de ce dernier de respecter les obligations résultant du droit des marchés financiers[13] et des prescriptions légales sur la protection des données, ainsi que l'organisation du modèle d'exploitation. Si le prestataire et ses sous-traitants sont amenés à traiter des données bancaires de client.e.s de l'établissement ou d'autres données personnelles, la sécurité des données (c'est-à-dire leur confidentialité, leur intégrité, leur disponibilité et leur traçabilité) constitue un critère de choix décisif et doit faire partie intégrante de l'examen de diligence *(due diligence*[14]*)*.

(17)* Tout changement concernant le prestataire (p. ex. société du groupe relevant d'un autre ordre juridique) devrait être soumis à l'accord préalable de l'établissement, celui-ci pouvant être donné par écrit ou de toute autre manière probante. Peuvent être exemptées d'accord préalable les restructurations internes au groupe au sein du même ordre juridique et qui n'ont pas d'impacts significatifs sur les relations entre les parties, les critères et les risques. A la demande de l'établissement, le prestataire devrait 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 définis dans la Circ.-FINMA 3/18.[15] 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 l'engagement d'un nouveau sous-traitant essentiel et pouvoir mettre fin à la fourniture des prestations par le 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 et une liberté de choix quant aux interfaces et aux formats d'exportation de données, afin que les fonctions et prestations externalisées ainsi que les données bancaires de client.e.s 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 le niveau de criticité des fonctions externalisées et des données bancaires de client.e.s.

---

13 Y compris les dispositions appropriées en matière de confidentialité.

14 Il faut définir des critères clairs pour évaluer la manière dont le prestataire gère les données critiques et les vérifier avant de signer le contrat (voir Circ.-FINMA 23/1, chiffre marginal 82).

15 Cf. Circ.-FINMA 3/18, chiffre marginal 33.

6 Centres de données et centres d'exploitation

(19)* On redoute parfois que le recours à des prestations de cloud computing rende impossible de déterminer les lieux où les données sont traitées (ubiquité des données). Du point de vue des établissements, la confiance des clientes et des clients quant à la gestion de leurs données est un enjeu crucial.

(20) Le prestataire devrait 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)* Au moins lorsque le prestataire traite des données personnelles ou lorsque ses sous-traitants sont à qualifier de sous-traitants essentiels, tout transfert de site dans un autre ordre juridique pendant la durée du contrat devrait faire l'objet d'une procédure définie dans ledit contrat et, selon la protection requise au cas par cas, être soumis à l'accord préalable de l'établissement.[16] 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)* D'autres exigences visant à prévenir l'accès de tiers aux données font l'objet des développements ci-après.

16 En ce qui concerne l'accord, l'option de prolongation et, le cas échéant, la fin du contrat, les principes cités au chiffre marginal 18 s'appliquent.

Chapitre III: données et sécurité des données

Fondements juridiques

- Art. 47 LB
- Art. 69 LEFin
- Circ.-FINMA 23/1
- 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 secret bancaire, il convient de respecter aussi les dispositions de la Circ.-FINMA 23/1 relatives aux données critiques. Il appartient à l'établissement de procéder à une identification et une classification des données bancaires de client.e.s traitées dans le cadre des prestations de cloud computing.

(24)* L'objectif est de 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 mesures techniques et organisationnelles complémentaires (y compris contrôles).

(25)* Il convient d'examiner à cet effet si et dans quelle mesure les clientes et les clients ont été informés d'une externalisation du traitement de données bancaires de client.e.s à un prestataire en Suisse ou à l'étranger ou, le cas échéant, s'ils ont donné leur accord à cette externalisation.[17]

(26)* Les modifications significatives apportées pendant la durée du contrat à la classification des données bancaires de client.e.s externalisées doivent faire l'objet d'un suivi et les mesures requises doivent être prises préalablement aux externalisations concernées.

17 Voir à ce sujet le chapitre III:10 ci-après.

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

(27)* Le prestataire devrait permettre à l'établissement de vérifier[18] les lieux de traitement (en particulier de stockage) des données bancaires de client.e.s ainsi que de contrôler ces lieux au moyen de mesures techniques et organisationnelles. L'établissement devrait aussi être en mesure de respecter ses obligations de transparence envers les clientes et les clients et, dès lors, de connaître avec toute la précision requise les lieux de traitement des données bancaires de client.e.s , en particulier les lieux de stockage.

(28)* Par ailleurs, l'établissement devrait être préalablement informé des flux de données bancaires de client.e.s qui se situent dans la sphère du prestataire et, le cas échéant, de ses sous-traitants. Au besoin, il y a lieu de définir l'architecture sous-jacente à ces flux de données au moyen de mesures techniques et organisationnelles suffisamment précises, puis de la fixer par contrat.

(29)* Entrent dans le champ du chiffre marginal ci-dessus la définition et la mise en œuvre d'un concept d'accès[19] par le prestataire. Ce dernier devrait communiquer à l'établissement, sur simple demande, les autorisations d'accès octroyées. Il lui incombe également de surveiller et répertorier de manière appropriée les accès à des données bancaires de client.e.s.

(30)* Tout concept d'accès devrait définir le but de l'accès de manière suffisamment restrictive et indiquer dans quels cas précis l'accès à des systèmes qui traitent des données bancaires de client.e.s 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.

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

(31)* De manière générale, des mesures techniques et organisationnelles appropriées visant à protéger les données bancaires de client.e.s de l'établissement devraient être proposées par le prestataire, puis fixées par contrat. Dans ce cadre, les normes techniques internationales et locales[20] doivent être respectées. En outre, le prestataire devrait convenir de mesures techniques et organisationnelles appropriées avec ses sous-traitants.

(32)* Le prestataire devrait s'assurer que dès lors qu'ils ont accès à des données bancaires de client.e.s, ses employé.e.s et ceux/celles de ses sous-traitants s'engagent formellement à respecter la confidentialité et soient dûment informé.e.s, formé.e.s et surveillé.e.s au moyen de mesures

18 Les exigences relatives à une telle vérification sont énoncées au chapitre V ci-dessous.

19 Concernant les données bancaires de client.e.s.

20 P. ex. normes de l'Organisation internationale de normalisation (ISO) et du National Institute of Standards and Technology (NIST) (règles de l'art).

appropriées.[21] Un tel engagement des employé.e.s est considéré comme suffisant lorsqu'il est pris envers le prestataire ou ses sous-traitants dans le cadre du contrat de travail. Il est recommandé aux prestataires de respecter les prescriptions légales sur la protection des données et d'attirer expressément l'attention de leurs employé.e.s opérant en Suisse sur le secret bancaire ainsi que des autres obligations légales applicables en matière de confidentialité et sur la peine encourue en cas de violation.

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 la cliente ou le client le délie du secret bancaire au sens de l'art. 47 LB.[22] Tel serait en particulier le cas si l'établissement arrivait à la conclusion qu'une divulgation de données bancaires de client.e.s à des tiers non autorisés ne pouvait être évitée, selon une probabilité proche de la certitude, au moyen de mesures techniques et organisationnelles appropriées. Dans ce cas, l'établissement risquerait de se voir imputer une violation intentionnelle ou par négligence du secret bancaire en recourant aux prestations de cloud computing.

(34)* Selon le présent Guide, dès lors que l'établissement a prévu des mesures techniques, organisationnelles et contractuelles appropriées en matière de sécurité des données bancaires de client.e.s traitées dans le cadre des prestations de cloud computing afin d'exclure, selon une probabilité proche de la certitude, toute divulgation des données bancaires de client.e.s à des tiers non autorisés, il n'a pas besoin d'être délié du secret bancaire par la cliente ou 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 techniques, organisationnelles et contractuelles possibles[23]

(35)* Il y a violation du secret professionnel du banquier dès lors que des données bancaires de client.e.s sont effectivement divulguées à des personnes non autorisées, intentionnellement ou par négligence, et que cette divulgation est causée par l'établissement.[24] L'art. 47, al. 1 LB définit une infraction matérielle, la seule possibilité que des personnes non autorisées prennent connaissance de données bancaires de client.e.s ne constitue pas une violation du secret bancaire.

---

21 Cf. Circ.-FINMA 23/1, chiffre marginal 80.

22 Voir note de bas de page 7.

23 Certains établissements considèrent que les mesures contractuelles font partie des mesures organisationnelles. Quoi qu'il en soit, les mesures techniques et organisationnelles ne sont généralement pas des questions ou des prescriptions juridiques.

24 Cf. ATF 6B_1403/2017 du 8 août 2017.

(36)* Lorsque, dans le cadre des prestations de cloud computing, le prestataire et ses sous-traitants ne prennent pas effectivement connaissance de données bancaires de client.e.s traitées sur le cloud, il n'y a 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 à des données bancaires de client.e.s.

(37)* Les mesures à prendre résultent des dispositions légales et réglementaires applicables au cas d'espèce.[25] Toutefois, l'appréciation du caractère approprié de ces mesures n'est pas une question juridique et devrait 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 données bancaires de client.e.s, ainsi qu'au regard de la probabilité que le risque se réalise et de la gravité de ce risque pour les droits des clientes et des clients concernés.

Peut également être pris en compte le fait qu'en fonction du modèle d'affaires et d'exploitation propre à l'établissement concerné ainsi que de sa stratégie, la probabilité qu'un risque se réalise et l'ampleur des dommages résultant d'une violation du droit sont plus importantes dans certains scénarios que dans d'autres. Des mesures techniques et organisationnelles appropriées ne doivent donc pas obligatoirement envisager et prévenir tous les scénarios imaginables en théorie, mais seulement ceux dont la réalisation, dans le cas d'espèce, est prévisible selon le cours normal des choses et l'expérience générale de la vie et peut être évitée si l'on respecte ses obligations.[26] Il faut faire preuve à cet égard de toute la diligence requise dans chaque cas particulier.

Sont présentés ci-après quelques exemples de mesures possibles.[27]

(38)* **Mesures techniques appropriées pour protéger les données bancaires de client.e.s**

Des mesures techniques appropriées peuvent avoir pour effet que l'établissement n'est plus tenu de classifier les données traitées sur le cloud comme données bancaires de client.e.s. Ainsi, les données anonymisées ne répondent pas à la qualification de données bancaires de client.e.s. Il en va de même, du point de vue de la ou du destinataire des données, des données bancaires de client.e.s pseudonymisées et/ou cryptées, par exemple lorsque le ou la destinataire ne dispose pas d'un tableau de concordance des pseudonymes et/ou de la possibilité de décrypter les données cryptées.[28]

---

25 Cf. aussi Circ.-FINMA 23/1, chiffre marginal 79.

26 Cf. ATF 135 IV 56, consid. 2.1. Cette approche est appelée aussi «approche fondée sur le risque». Il existe diverses méthodes d'évaluation de la probabilité de réalisation d'un risque et de l'ampleur des dommages résultant d'une violation du droit.

27 Voir par exemple aussi l'annexe C du rapport de la Chancellerie fédérale de mars 2025 intitulé «Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale» (2e édition), qui donne un aperçu sommaire des risques et des mesures d'atténuation correspondantes.

28 En vertu du droit de la protection des données également, ces données ne constituent pas des données personnelles selon la méthode dite relative. Cela a été confirmé judiciairement. Cf. ATF 136 II 508 – Logistep ainsi que l'arrêt de la Cour de justice de l'Union européenne (CJUE) du 19 octobre 2016 dans l'affaire C-582/14 – Patrick Breyer contre Bundesrepublik Deutschland. Voir aussi le considérant 26 du règlement général sur la protection des données, pour le cas où celui-ci serait applicable: *«Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement [...].»*

Sont considérées comme des procédés techniques appropriés pour assurer une protection adéquate des données bancaires de client.e.s, en particulier, les mesures de sécurité ci-après.

(39)* Anonymisation: Les données anonymisées avec une probabilité proche de la certitude (technique irréversible) ne répondent plus à la qualification de données bancaires de client.e.s et/ou de données personnelles. Elles ne sont donc pas soumises aux exigences formulées dans la présente section.

(40)* Pseudonymisation: S'agissant de données bancaires de client.e.s, la règle de rattachement aux personnes concernées devrait faire l'objet d'une protection adéquate, sous le contrôle de l'établissement. En particulier, les droits d'utilisation du tableau de concordance devraient être restreints sur la base du principe du *need to know* et les accès devraient faire l'objet d'une journalisation permettant de les retracer.

(41)* Cryptage: S'agissant de données bancaires de client.e.s, 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 données bancaires de client.e.s dans le cadre des prestations de cloud computing. L'établissement devrait évaluer, sur la base d'une analyse des risques et notamment au regard de la classification des données bancaires de client.e.s, les procédures appropriées pour assurer le contrôle de la clé de cryptage.

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. Cela se détermine en fonction de l'état de la technique (règles de l'art).

Toute transmission de données bancaires de client.e.s devrait en principe être cryptée. Le processus de cryptage et la puissance de la clé de cryptage doivent tenir compte des normes de sécurité en vigueur, afin que la transmission puisse être considérée comme cryptographiquement sûre.

(42)* **Mesures organisationnelles visant à protéger les données bancaires de client.e.s**

Les mesures opérationnelles prises par le prestataire et ses sous-traitants devraient pouvoir être surveillées par l'établissement de manière appropriée.

L'audit obligatoire des normes de sécurité et de confidentialité du prestataire devrait se faire au moyen de rapports indépendants établis sur la base de normes d'audit reconnues.[29]

(43)* **Mesures contractuelles visant à protéger les données bancaires de client.e.s**

En règle générale, les mesures contractuelles reprennent les mesures techniques et organisationnelles convenues. 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 de convenir de mesures techniques et organisationnelles appropriées avec ses sous-traitants;

29 Par exemple les normes d'audit des contrôles en place ISAE 3000 ou SOC2.

- l'engagement contractuel du prestataire à respecter la confidentialité au moyen de prescriptions concrètes concernant les mesures techniques et organisationnelles;
- 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 ainsi que leur audit par une société d'audit reconnue;
- les accords prévus au chapitre IV (Autorités et procédures) ainsi que ceux concernant la marche à suivre dans le cadre de l'identification et de l'évaluation des violations de la confidentialité par des cybercriminels et autres.[30]

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 employé.e.s du prestataire et de ses sous-traitants traitent sur le cloud des données bancaires de client.e.s en texte clair, c'est-à-dire sans cryptage ni/ou 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) 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 aux prestations de cloud computing d'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[31]. Par ailleurs, l'établissement se voit généralement reconnaître le droit de donner des instructions[32] 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 les 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.[33]

---

30 Dans ce cas, les textes applicables varient selon les données concernées (objet de la protection), de sorte que les clarifications requises, les délais et les seuils d'annonce à respecter ainsi que les autorités compétentes varient également. Cf. p. ex. l'art. 24 LPD, la Communication FINMA sur la surveillance 05/2020 «Obligation de signaler les cyberattaques selon l'art. 29, al. 2 LFINMA», la Circ.-FINMA 23/1, chiffre marginal 81, ainsi que les art. 74a ss LSI. Il convient de noter dans le contrat avec le prestataire que ces obligations de signaler ne concernent pas exclusivement les données bancaires de client.e.s.

31 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.»*

32 Circ.-FINMA 3/18, chiffre marginal 21.

33 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 peut être évalué 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 à prendre résultent également des dispositions légales et réglementaires applicables au cas d'espèce.[34]

(49) Les mesures techniques et organisationnelles 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 employé.e.s 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 luiwmême.
- L'établissement est particulièrement attentif aux accords prévus au chapitre IV (Autorités et procédures).

(50)* Comme indiqué *supra*, le traitement de données bancaires de client.e.s en texte clair par des employé.e.s du prestataire et de ses sous-traitants ne constitue pas en soi une divulgation à des tiers non autorisés et donc une violation du secret bancaire par l'établissement.

(51)* On pourrait supposer qu'il y a divulgation de données bancaires de client.e.s à des personnes non autorisées lorsque des tiers extérieurs à la sphère du prestataire, par exemple des autorités étrangères, prennent connaissance de ces données en raison du recours aux prestations de cloud computing par l'établissement. Le lien avec l'étranger pourrait conduire à l'application de lois étrangères, et donc permettre aux autorités étrangères d'accéder aux données de manière certes légale au regard de leur propre droit, mais illégale au regard du droit suisse applicable aux établissements suisses (*foreign lawful access)*. Si des mesures techniques et organisationnelles appropriées, préalablement mises en œuvre, permettent selon une probabilité proche de la certitude soit d'empêcher la transmission de données bancaires de client.e.s, soit de la limiter aux informations ne permettant pas à des tiers non autorisés (au sens du droit suisse) d'identifier directement ou indirectement des personnes protégées par le secret bancaire, il n'y a pas d'acte commis intentionnellement ou par négligence et donc pas de violation punissable du secret bancaire.[35]

---

34 Cf. aussi Circ.-FINMA 23/1, chiffre marginal 79.

35 En cas de simple possibilité d'accéder à des données bancaires de client.e.s, l'hypothèse d'une tentative punissable de divulgation à des personnes non autorisées est donc caduque.

10.4 Obligations d'information de l'établissement

(52)* En vertu des prescriptions légales sur la protection des données, tout traitement de données personnelles dans le cadre des prestations de cloud computing entraîne une obligation d'information des personnes concernées, qui peut être remplie au moyen de la déclaration générale de confidentialité de l'établissement. 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.

(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 de la cliente ou du client, des accords contractuels, des dispositions du droit du mandat et du principe de bonne foi. Peuvent servir de points de référence, notamment, le positionnement sur le marché et la communication de l'établissement sur les mandats antérieurs confiés à des prestataires.

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

(54)* L'établissement devrait pouvoir accéder à tout moment, depuis la Suisse, aux données bancaires de client.e.s qui sont stockées et traitées à l'étranger ou en Suisse. Le prestataire devrait 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.[36]

(55)* Le prestataire devrait s'engager à restituer à tout moment les données bancaires de client.e.s 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[37] et des connaissances[38] requis à cet effet. En pareil cas, le prestataire devrait retransférer les données bancaires de client.e.s dans un format standardisé et exploitable par une machine laissé au choix de l'établissement.

---

36 Voir la Circ.-FINMA 18/3, chiffre marginal 31 pour les externalisations essentielles.

37 Par exemple la clé de cryptage.

38 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.

(56) Si le prestataire met en œuvre des solutions propriétaires entraînant des effets de verrouillage *(lock-in),* il devrait se déclarer prêt à assister l'établissement en cas de migration vers d'autres solutions ou d'octroi de licences sur les solutions propriétaires.[39]

Chapitre IV: autorités et procédures

Fondements juridiques

- Art. 271 CP
- Art. 273 CP
- Art. 47 LB
- Art. 16 s. LPD
- Traités internationaux en matière d'entraide judiciaire
- Circ.-FINMA 23/1
- Art. 42c LFINMA

(57)* Le prestataire doit convenir avec l'établissement de la marche à suivre en cas de demandes des autorités ayant pour objet la remise ou la transmission de données bancaires de client.e.s traitées sur le cloud.[40] Sauf dispositions légales impératives contraires, le prestataire doit prendre envers l'établissement l'engagement contractuel de respecter les mesures techniques et organisationnelles énoncées aux chiffres marginaux 58-60 ci-après.

(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 données de client.e.s traitées sur le cloud à des autorités étrangères ou à d'autres parties situées à l'étranger que conformément aux dispositions légales et réglementaires applicables et selon le cas (i) avec le consentement

39 Selon le domaine d'application, des textes étrangers peuvent prévoir des prescriptions légales supplémentaires sur ces aspects. C'est le cas par exemple du règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données).

40 Les mêmes principes pourraient s'appliquer notamment dans le cadre d'autres secrets professionnels ou en cas de secrets commerciaux. Les questions relatives au droit de la protection des données demeurent réservées et ne sont pas traitées ici.

préalable de l'établissement[41], (ii) avec le consentement préalable des personnes concernées[42], (iii) en vertu d'un jugement du tribunal suisse compétent, et/ou (iv) 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 données bancaires de client.e.s. 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 à la communication de données bancaires de client.e.s 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 ainsi que des clientes et des clients de ce dernier.[43] En outre, il appartient au prestataire de s'assurer par lui-même que la demande de divulgation est légale au regard de la législation invoquée par l'autorité étrangère concernée et de la contester si tel n'est pas le cas. Lorsqu'il conteste une demande, le prestataire demande des mesures provisoires visant à suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente se prononce sur son bien-fondé. Il ne divulgue pas les données bancaires de client.e.s demandées tant qu'il n'est pas obligé de le faire en vertu des règles de procédure applicables.[44]

(61)* Le prestataire doit également 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 de données bancaires de client.e.s et sont susceptibles d'avoir un impact sur le prestataire ainsi que sur ses sous-traitants[45] ou sur les sociétés de son groupe[46].

(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 marginal 10.[47]

---

41 Le consentement peut prendre différentes formes et être documenté de différentes manières, c'est une question de gestion des risques et de propension au risque dans la perspective d'une éventuelle procédure probatoire.

42 Voir note de bas de page 41.

43 Voir chapitres II et III, en particulier les développements concernant le secret bancaire et la transparence prévue par le droit relatif à la protection des données.

44 Par analogie avec les clauses 15.1. Notification et 15.2. Contrôle de la légalité et minimisation des données de la décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil.

45 Sous-traitants ayant accès à des données bancaires de client.e.s.

46 Voir note de bas de page 37.

47 Voir chiffre marginal 37.

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. 61 et 63 LEFin
- Circ.-FINMA 23/1, chiffres marginaux 71-82, ainsi que les points d'audit concernant la gestion des risques des données critiques
- Circ.-FINMA 18/3

(63) En général, les prestataires fournissent des prestations de cloud computing à un grand nombre de clientes et de clients[48] à partir de centres de calcul hautement sécurisés. 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 clientes et clients doivent être prises en compte.

(64) Le respect des obligations transférées au prestataire par contrat (y compris les mesures techniques et organisationnelles) et résultant des exigences légales et réglementaires (notamment en matière d'externalisation, de protection des données et de sécurité des informations) devrait 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.

(65) Les contrôles devraient pouvoir être demandés et réalisés par l'établissement, par sa société d'audit externe ou par la FINMA.[49] 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.

48 Cloud public.

49 Voir la Circ.-FINMA 18/3, chiffre marginal 26 pour les externalisations essentielles.

(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 et doit donc être convenu par contrat avec le prestataire.

Le Guide légal et réglementaire a été modifié comme suit, avec effet à compter de novembre 2025:

Chiffres marginaux modifiés	1, 3, 4, 6, 8, 9, 14, 16, 17, 18, 19, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30,31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, 48, 50, 51, 52, 54, 55, 57, 58, 59, 60, 61 et 69
Fondements juridiques (encadré) adaptés aux	chapitres II, III, IV, V
Terminologie adaptée dans les	chiffres marginaux 1, 4, 6, 9, 16, 18, 23, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 50, 51, 54, 55, 57, 58, 59, 60 et 61 ainsi que dans les notes de bas de page 19, 35 et 45
Notes de bas de page modifiées	9, 13, 15, 19, 35, 45 et 46
Nouvelles notes de bas de page	1, 2, 3, 6, 7, 8, 10, 11, 12, 14, 16, 18, 20, 21, 22, 23, 25, 26, 27, 28,30, 34, 36, 39, 40, 41, 42, 44, 47 et 49
Autres	Suppression du titre du chapitre III:10.5 (avant le chiffre marginal 53); adaptation du titre des chapitres II, III:10.2 et III:10.4

Association suisse des banquiers
Aeschenplatz 7
Case postale 4182
CH-4002 Bâle
office@sba.ch
www.swissbanking.ch