_swissprivacy.law

On Cloud Number Nine : un bref survol des enjeux juridiques et règlementaires du cloud banking

Philipp Fischer et Marine Largant, le 12 novembre 2020

Alors que de plus en plus d'entreprises recourent à une infrastructure *cloud*, que ce soit pour le stockage ou le traitement de données, il peut être utile de rappeler les trois axes principaux qu'une banque doit prendre en compte en amont du lancement d'un projet de coopération avec un prestataire de services *cloud*.

Les principaux enjeux qu'une banque doit considérer dans le choix d'un *cloud service provider* (« CSP »), la revue des processus internes et la négociation contractuelle avec le CSP, sont les suivants :

1. Droit règlementaire : Circulaire FINMA Outsourcing 2018/03 (« Circulaire Outsourcing ») et Annexe 3 de la Circulaire FINMA Risques opérationnels 2008/21 (« Circulaire Risques Opérationnels »);
2. Droit de la protection des données : Loi fédérale sur la protection des données (« LPD », cf. également la nouvelle version adoptée en septembre 2020 : « nLPD ») et Règlement général de l'UE sur la protection des données (« RGPD ») si applicable ;
3. Secret bancaire et dispositions analogues : Article 47 de la loi fédérale sur les banques (« LB »), article 69 de la loi sur les établissements financiers (« LEFin »), article 162 du code pénal (« CP ») et autres dispositions légales protégeant la confidentialité de certaines informations.

Le Guide « Cloud » de l'Association suisse des banquiers (« ASB ») illustre de manière didactique comment ces normes générales et abstraites doivent être transposées dans le cadre de projets impliquant le recours à un *cloud*.

A. Droit règlementaire

La Circulaire Outsourcing s'applique aux banques et maisons de titres suisses, ainsi qu'aux succursales suisses de banques et maisons de titres étrangères. A compter du 1er janvier 2021, le champ d'application de la Circulaire Outsourcing sera élargi aux directions de fonds (et aux SICAV autogérées qui sont traitées par analogie aux directions de fonds), ainsi qu'aux gestionnaires de fortune collective.

Dans une perspective matérielle, la Circulaire Outsourcing règlemente l'externalisation d'une fonction essentielle, à savoir une « fonction dont dépend de manière significative le respect des objectifs et des prescriptions de la législation sur la surveillance des marchés financiers » (Circulaire Outsourcing, N 4). Selon la pratique de la FINMA, toute externalisation impliquant la transmission à un prestataire de services d'une grande quantité de *client-identifying data* (CID) tombe *ipso facto* sous le coup de la Circulaire Outsourcing.

L'application de la Circulaire Outsourcing déclenche une série d'obligations, dont les principales sont résumées ci-après :

- Choix, instruction et contrôle du CSP (y compris *due diligence* documentée);
- Tenue d'un inventaire des externalisations de fonctions essentielles ;
- Extension du système de contrôle interne à la fonction externalisée ;
- Conclusion d'un contrat avec le CSP qui contient notamment les dispositions suivantes :
    - Droit pour la banque de donner des instructions au CSP et d'en contrôler l'exécution ;
    - Exigences en matière de sécurité de l'information, y compris un dispositif propre à assurer la continuité de la fonction externalisée en cas d'urgence ;
    - Droit d'accès et d'audit intégral, permanent et sans entraves au bénéfice (i) de la banque, (ii) de son auditeur prudentiel et (iii) de la FINMA sur la fonction externalisée, à la fois auprès du CSP et de ses sous-traitants ; en cas de transfert à l'étranger (ce qui est souvent le cas lors du recours à un *cloud*), le CSP doit garantir que ces droits puissent s'exercer dans le pays de destination ;
    - Lorsque le CSP fait appel à des sous-traitants pour exécuter tout ou partie d'une *fonction essentielle*, le contrat doit permettre à la banque (i) d'être informée suffisamment tôt du recours, respectivement du changement de sous-traitants et (ii) d'avoir la possibilité de mettre un terme au contrat d'externalisation si elle refuse le recours au sous-traitant. Ces sous-traitants doivent par ailleurs souscrire aux mêmes obligations que le CSP.

Les exigences de l'Annexe 3 de la Circulaire Risques Opérationnels doivent également être prises en compte lorsque le recours au CSP implique la transmission de *client-identifying data* à ce dernier.

B. Droit de la protection des données

Si des données personnelles (y compris des *client-identifying data*) sont rendues accessibles

au CSP, le projet d'externalisation doit également être revu à la lumière de la LPD (et potentiellement du RGPD), ce qui implique la prise en compte notamment des points suivants :

- Devoir d'information à l'égard des personnes concernées (*e.g.*, clients, employés);
- Conclusion d'un contrat de sous-traitance (*data processing agreement*) avec le contenu minimal prévu par les articles 28 RGPD, 10a LPD et 9 nLPD ;

Lorsque des données personnelles sont accessibles dans un Etat ne disposant pas d'une législation assurant un niveau « adéquat » de protection des données personnelles (*e.g.*, les Etats-Unis), des mesures de protection supplémentaires doivent être mises en œuvre, la plus utilisée étant les « Clauses-Modèles » de la Commission européenne. La validité de ces clauses est toutefois incertaine depuis l'arrêt *Schrems II* de la Cour de Justice de l'UE du 16 juillet 2020 (cf. swissprivacy.law/17/), de sorte que d'autres garanties doivent être envisagées.

Les contraintes liées à la protection des données peuvent être significativement réduites si seules des données pseudonymisées ou cryptées sont remises au CSP, en prêtant toutefois attention au risque de *reverse engineering* et donc de divulgation indirecte de données personnelles.

C. Secret bancaire et secret commercial

La compatibilité avec le secret bancaire doit être analysée pour chaque projet qui implique la mise à disposition de *client-identifying data* au CSP, typiquement lorsque les spécificités de la prestation ne permettent pas la pseudonymisation ou le cryptage.

Si la transmission est limitée à un CSP situé en Suisse (hypothèse peu réaliste compte tenu du *business model* des CSP), l'obtention d'une levée du secret bancaire par le client ne sera en principe pas nécessaire vu que le CSP est lui-même soumis au secret bancaire en vertu de l'art. 47 al. 1 let. a LB. Le Guide « Cloud » de l'ASB adopte le même raisonnement en cas de transmission de *client-identifying data* à un CSP localisé *en-dehors de Suisse*, alors même que la protection pénale du secret bancaire est limitée par le principe de territorialité. En pratique, nombreuses sont les banques qui demandent une levée du secret bancaire dans cette dernière hypothèse, l'un des éléments-clés étant de s'assurer que cette renonciation au secret bancaire est octroyée sur une base dûment informée.

D. Conclusions

D'un point de vue juridique, le lancement d'un projet de *cloud banking* doit être revu dans la

perspective de la relation contractuelle avec le CSP, tout en gardant à l'esprit les droits des personnes dont les données seront confiées au CSP (*e.g.*, respect du devoir d'information prévu en droit de la protection des données, obtention éventuelle d'une levée du secret bancaire). D'un point de vue règlementaire, les exigences supplémentaires découlant des circulaires de la FINMA doivent être prises en compte, notamment lors de la négociation du contrat conclu avec le CSP.

Proposition de citation : Philipp FISCHER / Marine LARGANT, *On Cloud Number Nine* : un bref survol des enjeux juridiques et règlementaires du cloud banking, 12 novembre 2020 *in* www.swissprivacy.law/27