

Contrat d'outsourcing et contrats informatiques

Les nouvelles exigences légales et réglementaires à intégrer; les aspects juridiques à couvrir dans les clauses contractuelles

- > Circulaire FINMA Outsourcing, Nouvelle LPD, Circulaire FINMA Risques et résilience opérationnels
- > Analyse de certaines clauses contractuelles types, mise à jour de la documentation contractuelle
- > Impact de l'Intelligence Artificielle dans ce type de contrats
- > Contrats Cloud (SaaS, IaaS, PaaS) : importance des clauses de réversibilité; quels points à traiter et négocier en cas de sortie de contrat, etc. ?



Thierry Demiéville,
Senior Legal Counsel

Titulaire d'un Master en droit avec mention de l'Université de Fribourg, d'un LL.M en droit commercial et des sociétés (Queen Mary University of London), d'un CAS en digital finance law et d'un CAS en compliance in financial services de l'Université de Genève, Thierry Demiéville est un juriste spécialisé dans les questions de droit bancaire, abordant les problématiques dans une perspective transversale, sous l'angle juridique, compliance et de la finance numérique, avec 20 ans d'expérience dans le domaine financier. Il a notamment été responsable juridique auprès de Flow Bank SA, Senior Legal Officer auprès de la Lloyds TSB Bank, succursale de Genève, Sous-Directeur au sein du Service juridique de la Compagnie Bancaire Helvétique, responsable juridique & compliance auprès d'IG Bank SA, Directeur-Adjoint au sein du Service juridique de la Banque Cramer & Cie SA, juriste au Registre central auprès de BNP Paribas Private Bank (Suisse) et Sous-Directeur au sein du Fichier central (représentant juridique du service) de Mirabaud & Cie.

8.30 Introduction

- Définition de la « gestion des contrats »
- Rappel de la liberté contractuelle
- Exigences légales et réglementaires
- Grande variété de contrats dans le domaine financier
- Focus sur certains contrats: contrat d'outsourcing, contrat informatique
- Impact des nouvelles technologies dans le domaine contractuel : intelligence artificielle (IA)

LE CONTRAT D'OUTSOURCING

8.40 Définition du contrat d'outsourcing

- **Fonction essentielle externalisée**
- > Exemples d'outsourcings
- **Transfert de grandes quantités de CID («Mass CID») au prestataire de services**
- > Définition du concept de « grandes quantités de CID »

8.55 Conditions de la Circulaire FINMA 2018/3 Outsourcing applicables au contrat d'outsourcing - Rappel des exigences et derniers développements

- **Inventaire des fonctions externalisées**
- **Exigences vis-à-vis du prestataire de services**
- Capacités professionnelles
- Garantie d'un exercice durable de la fonction / garantie d'une réintégration ordonnée de la fonction externalisée ou d'un transfert à un autre prestataire (réversibilité)
- Répartition des compétences et responsabilités entre l'institution financière et le prestataire de services
- Surveillance régulière du prestataire de services
- > Evaluation périodique de l'efficacité des contrôles de sécurité mis en place par le prestataire
- > Evaluation périodique des niveaux de service convenus dans les « Service Level Agreements » (SLA)
- **Audit et surveillance:** par la FINMA; par l'institution financière; par la société d'audit de l'institution financière
- **Exigences en matière de sécurité**
- Adéquation des mesures
- Continuité de la fonction externalisée en cas d'urgence (« Business continuity / Disaster recovery »)
- **Transfert d'une fonction essentielle à l'étranger**
- Garantie du droit d'accès et d'inspection à l'étranger
- Garantie de la capacité d'assainissement et de liquidation de la banque
- > Accès aux informations nécessaires en tout temps
- **Exigences vis-à-vis de la sous-traitance**
- Devoir d'informer la banque en cas de recours ou de changement de sous-contractant exerçant des fonctions essentielles
- Possibilité pour la banque de mettre un terme au contrat d'outsourcing en cas de refus de recours ou de changement de sous-contractant
- Transfert au sous-contractant des obligations et des garanties nécessaires au respect de la circulaire outsourcing
- **Obligation de confidentialité**

9.40 Loi fédérale sur la protection des données (LPD) du 25 septembre 2020

Rappel de certaines exigences et derniers développements concernant la nouvelle LPD dans le cadre d'un outsourcing impliquant un transfert de CID

- **Obligations du responsable du traitement**
- Devoir d'informer (art. 19 et 20 LPD)
- Analyse d'impact relative à la protection des données personnelles (art. 22 et 23 LPD): conditions, exceptions
- Annonce des violations de la sécurité des données (art. 24 LPD)
- **Sécurité et protection des données (art. 7 et 8 LPD et art. 3 OPDo)** - Mise en œuvre de mesures organisationnelles et techniques appropriées
- > Protection des données dès la conception et par défaut (« Privacy by design & by default »)
- > Gestion des accès aux données et des identités : système d'autorisation, sélection des personnes ayant accès aux données, principe du « need-to-know », authentification
- > Chiffrement des données, pseudonymisation et anonymisation
- **Exigences de la nouvelle LPD vis-à-vis de la sous-traitance (art. 9 LPD)**
- Vérification par le responsable du traitement de la capacité du sous-traitant de garantir la sécurité des données
- Autorisation préalable requise du responsable du traitement afin que le sous-traitant puisse lui-même sous-traiter à un tiers le traitement des données
- Respect par le sous-traitant des mêmes obligations générales que le responsable du traitement
- **Communications de données personnelles à l'étranger**
- Communication vers un Etat disposant d'une législation assurant un niveau de protection « adéquat »
- Communication vers un Etat ne disposant pas d'une législation assurant un niveau de protection « adéquat »

10.25 Pause-café

10.45 Circulaire FINMA 2023/1 Risques et résilience opérationnels - banques

Survol de certaines exigences de cette Circulaire dans le cadre d'un outsourcing impliquant un transfert de CID

- Données critiques
- Fonctions critiques
- Stratégies, politiques et directives/procédures internes : haute direction, direction, services
- Gestion des risques TIC : établissement d'un inventaire
- Gestion des cyberrisques : processus critiques
- Gestion des risques des données critiques : mesures additionnelles de protection des données critiques en cas de transfert ou de stockage à l'étranger et d'externalisation
- Business continuity management (BCM) : exigences concernant le « disaster recovery plan » (DRP) en cas de processus critiques externalisés
- Garantie de la résilience opérationnelle : coordination des composantes d'une gestion globale des risques incluant la gestion des externalisations

11.10 Contenu des directives et procédures internes à mettre en place dans le cadre d'un outsourcing

- Rôles et responsabilités internes
- Sélection du prestataire de services
- « Risk Assessment »
- Monitoring des fonctions externalisées
- Description des informations à inclure dans un contrat d'outsourcing
- Protection des données
- Annexes aux directives et procédures : inventaire des fonctions externalisées et « incident report »

11.25 Exigences spécifiques vis-à-vis des clients de l'institution financière

- Levée du secret bancaire (art. 47 LB)
- Devoir de transparence

11.35 Documentation/Preuve exigée dans la pratique par les auditeurs afin de s'assurer de la conformité du contrat d'outsourcing aux exigences légales et réglementaires

- Rapports ISAE, ISO et SOC (ISAE 3402, ISO 27001, SOC 1, etc.)
- Cartographie des risques
- Inventaire des fonctions externalisées
- Documentation/clause attestant que les sous-traitants se conforment aux exigences réglementaires
- Documentation/clause attestant que les mesures réglementaires de sécurité sont respectées

LES CONTRATS INFORMATIQUES

11.55 Définition du contrat informatique

- Pas de définition légale

12.00 Quelques catégories de contrats informatiques

• Catégories de contrats « standard »

- Contrat de maintenance
- Contrat de licence
- Contrat de développement de logiciel
- Contrat d'intégration

• Catégories de contrats basés sur le modèle du «Cloud computing» : description, exemples, points d'attention

- Modèles de déploiement cloud: cloud public, cloud privé, cloud hybride, cloud communautaire
- Contrat SaaS (Software as a Service) :
 - Contrat IaaS (Infrastructure as a Service)
 - Contrat PaaS (Platform as a Service)
 - Contrat FaaS (Function-as-a-Service)
 - Contrat DaaS (Desktop as a Service)
 - Contrat SaaS (Storage as a Service)

12.35 Déjeuner

14.00 Structure contractuelle d'un contrat informatique

• Corpus contractuel

• Différentes phases

- Phase d'implémentation/développement
- Phase de tests (user acceptance testing, UAT)
- Phase de pré-production (« staging »)

- Phase de mise en production ou « Go Live »

• Analyse de certaines clauses types

- Clause sur l'objet des prestations fournies
- Clause sur les « fees »
- Clause sur les droits de propriété intellectuelle
- Clause de responsabilité et d'indemnisation
- Clause de confidentialité et de protection des données
- Durée et fin du contrat
- Principes généraux

• **Spécificités de résiliation des contrats cloud** : types de résiliations, clauses de réversibilité (étendue du droit d'accès aux données, portabilité des données, modalités de transfert)

- Droit applicable et juridiction

15.00 Pause-café

PROBLÉMATIQUES COMMUNES

15.20 Impact de l'Intelligence Artificielle dans le domaine contractuel et plus spécifiquement dans les contrats d'outsourcing et informatiques

• Contrats avec les prestataires de services d'IA

• Importance de certaines clauses dans un contrat IA

- Clauses de protection des données : protection par un accord de traitement des données (« Data Processing Agreement »)

- Clauses relatives aux obligations de confidentialité

- Clauses de droits de la propriété intellectuelle (PI) : titularité des droits de PI, droits de PI sur les résultats (« output ») générés par le système IA, utilisation des données pour l'entraînement du système IA, clause d'indemnisation, Background IP, Foreground IP, etc.

- Obligations contractuelles liées à la réglementation IA et aux conditions générales (en particulier « Terms of use ») des prestataires de services d'IA

> Impacts du « EU AI Act »

> Exigences en droit suisse

> Conditions générales des prestataires de services d'IA

15.50 Implications et coordination des départements / services concernés de l'institution financière dans le cadre des contrats d'outsourcing et informatiques

- Le service juridique
- Le service compliance
- Le service informatique : Service cybersécurité, Chief Information Security Officer (CISO)
- Le service des risques
- Le Data Protection Officer (DPO)
- Le service des opérations
- Le service « Vendor Management »

16.05 Mise à jour, modifications et archivage de la documentation contractuelle

• Echéances contractuelles : renouvellement du contrat, résiliation du contrat

• Modifications contractuelles : formelles et matérielles

• Archivage de la documentation contractuelle : durée de conservation, forme de conservation

16.30 Fin du séminaire

INFORMATION & INSCRIPTION

Tel: +41 22 849 01 11

Fax: +41 22 849 01 10

info@academyfinance.ch

Academy & Finance SA

Rue Neuve-du-Molard 3, 1204 Genève

www.academyfinance.ch

PRIX

980 CHF (+ TVA 8.1%)

Inscriptions supplémentaires de la même société : -50%

Je m'inscris au séminaire "Contrat d'outsourcing et contrats informatiques" le 14 mars 2025.

Je participerai dans la salle Je participerai online sur Zoom

Nom et prénom

Fonction

Société.....

Adresse

Code postal et ville

Tel Email.....

Date Signature