www.jusletter.ch

Wolfgang Straub

Cloud Computing – check-list pour la rédaction de contrats

Les services basés sur le cloud computing sont variés et comprennent des services gratuits sur Internet jusque à des solutions réelles d'externalisation informatique. Les règles contractuelles sont par conséquent également variées. L'auteur présente une liste de points à inclure dans un contrat afin de fournir une aide lors de projets complexes.

Catégories d'articles: Contributions
Domaines juridiques: Informatique et droit; Contrats innomés; Protection des données

Proposition de citation: Wolfgang Straub, Cloud Computing – check-list pour la rédaction de contrats, in: Jusletter 14 juillet 2014

ISSN 1424-7410, http://jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

[Rz 1] Les services du cloud computing soulèvent une grand variété de questions, dont certaines peuvent être réglées par des contrats, pour d'autres ce n'est pas le cas. L'élaboration d'un contrat devrait toujours être précédée par une analyse des intentions des deux cocontractants, ainsi qu'une analyse des opportunités et risques juridiques, techniques et économiques. Le document présent est à considérer comme un complément à une démarche systématique[1], qui contient les éléments comme suit : Définition des services à délocaliser (outsourcing), analyse des exigences juridiques et des ressources, définition des critères pour la sélection du prestataire, définition des compétences. Le présent check-list est un outil pour le commettant[2]. Il est confectionné pour des services complexes. Cependant, elle ne prétend pas d'être complète[3]. Si le contrat est imposé par le prestataire, elle peut aider à localiser des risques potentiels et ainsi de prendre la décision, si le risque est justifiable ou non[4].

[Rz 2] Le présent document représente une traduction du check-list initialement publié en allemand.[5] Elle ne correspond pas 1 à 1 à la version originale qui est parfois un peu plus détaillée – cela va sans se dire, que les deux versions sont des aides de travail. Ils ne

---

1 Voir STRAUB WOLFGANG, Cloud Verträge – Regelungsbedarf und Vorgehensweise, in: PJA 7/2014, p. 905 ss.

2 Dans la version française nous utilisons le terme commettant pour le « client » du fournisseur/prestataire des services cloud. Ceci contrairement au « client », qui serait dans ce cas-là, le client du commettant. Cette distinction est importante, parce qu'il y a un certain nombre de « commettants », qui offrent leurs service, qu'ils achètent bien entendu chez un prestataire cloud, aux clients privés ou commerciaux.

3 Des check-lists supplémentaires se trouvent dans les guides EUROCLOUD, http://switzerland.eurocloud.org/publikationen.html. Voir notamment la liste détaillée de questions concernant la sécurité contenu dans ‚Leitfaden Risk & Compliance, chapitre 6, p. 28 ss. Pour une check-list concernant des audits voir HALPERT BEN (éd.), Auditing Cloud Computing: A Security and Privacy Guide, Hoboken NJ 2011, p. 175 ss. Voir aussi le check-list de l'association Swiss ICT concernant les contrats d'externalisation, www.modellvertraege.ch, le check-list 'Outsourcing Contracts Control Review' du Switzerland Chapter de la Information Systems Audit and Control Association, http://www.isaca.ch et le check-list du préposé des données du canton de Zurich, https://dsb.zh.ch/internet/datenschutzbeauftragter/de/themen/weitere_themen/outsourcing.html. Pour les entités publiques souhaitant d'utiliser des cloud services se posent des questions supplémentaires. Voir UNITE DE PILOTAGE INFORMATIQUE DE LA CONFEDERATION, Commentaire sur la stratégie d'informatique en nuage des autorités suisses, https://www.egovernment.ch/fr/umsetzung/e-government-schweiz-2008-2015/cloud-computing-schweiz/ et EUROCLOUD Leitfaden Cloud Computing – Öffentliche Auftragsvergabe, http://switzerland.eurocloud.org/publikationen.html. Lors de projets informatiques au sein de la Confédération, une analyse des besoins de protection (SCHUBAN) préalable est nécessaire. Voir https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/prozesse-methoden/p041-schutzbedarfsanalyse_schuban.html. Au niveau départemental, parfois des check-lists supplémentaires concernant l'architecture et la sécurité informatique doivent être prises en compte.

4 Pour le niveau de responsabilité des organes de la direction et du conseil d'administration lors de projets d'externalisation de l'informatique voir STRAUB WOLFGANG, Verantwortung für Informationstechnologie – Gewährleistung, Haftung und Verantwortlichkeitsansprüche, Zurich / St. Gall 2008, N. 572ss et 627. Pour les banques le circulaire 2008/21 «Risques opérationnels banques» (actuellement en cours de révision) doit être respecté. Voir notamment annexe 3, N. 5ss.

5 STRAUB WOLFGANG Cloud Computing – check-list pour la rédaction de contrats, jusletter 14 juillet 2014

remplacent dans aucun cas une démarche professionnelle ou la consultation de personnes spécialisée, avant de signer un contrat pour le cloud computing.

1. Conditions cadres

1.1. Contractants

1.1.1. *Information concernant l'hébergeur respectivement le prestataire des services* et ses sous-traitants, notamment clarifier la question „où" (géographiquement) les services sont fournis. Cela influence les lois applicables.

1.1.2. Informations relatives aux *certifications du prestataire* et de se sous-traitants. Garantie, que ces certifications seront à maintenir pendant toute la durée du contrat.

1.1.3. *Informations portants sur le commettant,* notamment la question des sites concernés et les services abonnés. Cela influence les lois applicables.

1.2. Documents faisant partie intégrante du contrat

1.2.1. Une liste de parties constituantes du contrat avec une hiérarchie claire des différentes composantes. Éviter l'utilisation de liens (URL) qui peuvent être modifiés unilatéralement par le prestataire.

1.2.2. Faire *attention* à la forme d'éventuels avenants au contrat. Éviter des droits unilatéraux. Définir précisément la forme de déclarations, qui changent la situation juridique.

1.3. Définitions et références aux standards

1.4. Obligations accessoires

1.4.1. *Obligation d'information et de collaboration* (p.ex. en cas de restrictions des services non perceptibles pour le commettant). Définir la forme d'une réclamation éventuelle.

1.4.2. *Obligation de soutenir des prestataires tiers du commettant.*

2. Contenu des prestations

2.1. Principes de base

2.1.1. *Liste et description détaillée de tous les centres de calculs* qui seront impliqués. (localisation, certifications etc.)

2.1.2. *Description des sites* depuis lesquels un accès sur les données sera possible.

2.1.3. *Spécifications des logiciels* (et de leurs versions), mises à disposition par le prestataire (fonctionnalités, options etc.).

2.1.4. Déclaration de *prestations livrées par des tiers* (p.ex. infrastructure ou logiciels). Déclaration d'éventuelles licences et services (avec Service Level Agreement).

2.1.5. *Droits d'utilisation des logiciels*. Si des logiciels appartenant à des tiers seront utilisés dans le cadre des services cloud, il faut prévoir d'acquérir les droits correspondants. Une exploitation de logiciels licenciés par le commettant dans le cadre des services cloud peut nécessiter des licences supplémentaires.

2.1.6. Réglementation des *droits de la propriété intellectuelle* si des développements seront faites spécifiquement pour le commettant.

2.1.7. *Conditions techniques*, p.ex. possibilité d'importer ou exporter des données. Description des interfaces entre fournisseur et commettant.

2.1.8. *Possibilité de migrer* des logiciels ou des données sur d'autres plateformes.

2.1.9. *Concept de formation* des utilisateurs (et administrateurs) ainsi que la documentation pour les utilisateurs à fournir.

2.2. Périmètres de responsabilité

2.2.1. Définition des *responsabilités du commettant* (p.ex. maîtrise des données)

2.2.2. Définition des *responsabilités du prestataire* (prestations, réalisation, mesures protectrices etc.)

2.2.3. *Règles de délimitation* concernant les responsabilités des sous-traitants

2.3. Droit d'instruction

2.3.1. Est-ce que le *droit d'instruction du commettant* est défini de manière précise?

2.3.2. Quoi faire si des *instructions* du commettant sont – dans la perspective du prestataire – *incompatibles avec les lois applicables* sur la protection des données?

2.3.3. Quand et sous quelle forme, des infractions à des normes impératives du droit ou à des devoirs contractuels doivent-elles être communiqué au commettant. (*data breach notification*)

2.4. Migration

2.4.1. Description d'un éventuel *projet de migration* (procédure, organisation, procédure d'escalade).

2.4.2. Description du *processus de la réception* du projet.

2.5. Description des services

2.5.1. *Description des services et définition du „Service Level Agreement"* (SLA; accord sur la qualité de service) – p.ex. définition d'un taux de disponibilité, de bandes passantes minimales, temps de réponse, Support Levels, Recovery Time Objectives. Si possible définir des „Key Performance Indicators" pour mesurer la satisfaction du client.

2.5.2. Définition de *fenêtres d'entretien* (plages horaires) pour la maintenance (durés maximale d'interruptions, forme, conditions et délai pour l'annonce de la maintenance).

2.5.3. *Incident Management, Problem Management et support.* Description des processus. Ne pas oublier des détails comme p.ex. la disponibilité d'une hotline et la langue de celle-ci.

2.5.4. *Service Level Monitoring*: Comment est-ce que l'accomplissement du SLA est mesuré (p.ex. méthodologie et périodicité) ? Est-ce qu'il y a la possibilité d'une vérification par des tiers (audit) ?

2.5.5. *Service Level Management* (p.ex. pénalités, malus, droit de résiliation du contrat).

2.5.6. *Release Management* pour les logiciels (description du cycle de vie pour les release, possibilité de refuser un release, conditions de maintenance pour des individualisations etc.).

2.5.7. Eventuellement cycle de renouvellement de l'équipement informatique (*Hardware*).

2.6. Change Management

2.6.1. Conditions pour des *modifications des prestations sur demande du commettant.*

2.6.2. Conditions pour des *modifications des prestations sur demande du prestataire.*

2.6.3. Description du *processus d'adaptation des services*

3. Rémunérations

3.1. Rémunérations

3.1.1. *Prix à forfait* (p.ex. pour des paquets standard)

3.1.2. *Tarif se basant sur l'utilisation*

3.1.3. *Tarif horaire et conditions pour des travaux supplémentaires* non inclus dans les forfaits

3.2. Couts supplémentaires

3.2.1. Dépenses et frais supplémentaires

3.2.2. Impôts (notamment TVA)

3.3. Possibilité d'adaptation des rémunérations

3.3.1. Possibilité d'augmenter ou diminuer les tarifs/prix selon *l'utilisation des services*.

3.3.2. *Rabais* (p.ex. pour des prestations évolutives)

3.3.3. Rémunération dégressive avec la durée du contrat (p.ex. prestations infrastructure)

3.3.4. *Indexation* (p.ex. taux horaires)

3.3.5. *Couts pour l'entretien de modifications individuelles* sur des logiciels.

3.3.6. Eventuellement un *Benchmarking* de certaines prestations.

3.4. Mesure des prestations consommées

3.5. Délais, modalités du calcul et de la facturation

3.5.1. *Début et fin* des rémunérations (correspondant à l'utilisation effective).

3.5.2. *Modalités du calcul et de la facturation.* Coordonner la période de décompte avec le Service Level Management (payement de bonus/malus)

3.6. Demeure de payements et résolution d'éventuels désaccords concernant obligations financières

3.6.1. Conséquences en cas d'une demeure du commettant (p.ex. intérêts moratoires, rétention de prestations, résiliation du contrat)

3.6.2. *Possibilité d'un dépôt sur un compte bloqué*, réglementation contractuelle du processus d'escalade concernant la restitution du dépôt

3.6.3. *Droit de compensation* d'obligations réciproques

3.6.4. *Interdiction retenir ou effacer des données* du commettant

4. Sécurité et protection des données

4.1. Protection des données

4.1.1. Est-ce que le prestataire doit traiter dans le cadre de ces prestations des *donnés concernant des personnes physiques ou morales*? Quels sont les données qui seront crées dans le cadre des services? Y-a-t-il des données sensibles ou des profils de la personnalité au sens de la loi sur la protection des données? Définition du but et de l'étendue de la création, du traitement et de l'utilisation des données, notamment le cercle des personnes concernées et des personnes ayant accès aux donnés, la durée de l'utilisation, l'archivage et l'effacement des données.

4.1.2. *Compliance avec les lois applicables sur la protection des données* du côté du commettant et du prestataire ainsi que de ses sous-traitants. Au sein d'un groupe de sociétés il est parfois nécessaire de respecter les normes de protection de données de plusieurs ordres juridiques.

4.1.3. *Soumission du prestataire ainsi que ses sous-traitants aux lois et obligations applicables au commettant* (p.ex. secret professionnel protégeant des clients du commettant)

4.1.4. Définition d'un *point de contact commun pour toutes les questions de la protection des données* (y inclure des éventuels sous-traitants), p.ex. un conseiller à la protection des données indépendant selon l'art. 11a al. 5 let. e LPD

4.1.5. Obligation du prestataire de *répondre aux droits de personnes concernés* (p.ex. droit d'information, droit à la correction d'informations incorrectes ou le blocage de données)

4.1.6. *Transmission du secret professionnel* et de l'interdiction d'exploitation des données pour son propre compte aux sous-traitants et employés qui pourront avoir accès aux données.

4.1.7. *Certifications du prestataire* et se sous-traitants et maintien de la certification.

4.1.8. *Certification du commettant*, obligation du prestataire de soutenir de commettant lors d'une recertification.

4.1.9. *Mesures technique et organisationnelles* pour éviter d'éventuelles infractions au droit de la protection des données (p.ex. séparation des données de différents commettants, limitation des droits d'accès, journal d'accès).

4.1.10. *Interdiction d'un transfert des données et du traitement* soit chez un sous-traitant soit à l'étranger sans accord préalable (par écrit) du part du commettant.

4.1.11. Eventuellement *des dispositifs spécifiques* pour des données qui sont soumises à des lois ou prescriptions particulières (p.ex. secret professionnel).

4.1.12. Obligation d'informer immédiatement le commettant en cas de certains types d'incidents, p.ex. infraction aux dispositions sur la protection des données (*data breach notification*)

4.1.13. Il faut définir les obligations et les libertés du prestataire au cas où une *autorité publique étrangère demande l'accès aux données* du commettant ou de ses clients (p.ex. obligation du prestataire d'épuiser tous les moyens juridique pour défendre les données du commettant, déclaration du prestataire de ne pas livrer des données *sponte sua*).

4.1.14. *Conséquences en cas d'infractions* à la loi sur la protection des données (p.ex. obligation d'informer le commettant, peine reconventionnelle, droit du commettant de résilier le contrat avec effet immédiat).

4.2. Sécurité des informations

4.2.1. *Standards* applicables et *certifications*

4.2.2. *Concept de sécurité*. Description du processus et des responsabilités lors de la définition et de l'actualisation du concept de sécurité et pour la protection des données.

4.2.3. Description des *processus, des rôles et des responsabilités* (dans le concept de sécurité).

4.2.4. *Description de l'architecture de sécurité* (p.ex. séparation des environnements pour le développement, le testing et la production ainsi que les redondances et les mesures techniques).

4.2.5. Description d'éventuelles *méthodes de cryptage* et gestion des clés pour les dispositifs de stockage et du transfert des données entre le commettant et le prestataire.

4.2.6. Description détaillé des *processus d'authentification* pour l'accès aux services ainsi de la gestion des utilisateurs; possibilité d'un audit des logs.

4.2.7. *Logging*: Définition des donnés et des activités qui sont à enregistrer dans des fichiers log ainsi que les personnes, qui ont accès à ces fichiers.

4.2.8. *Précautions pour éviter des risques et des catastrophes* (p.ex. redondances comprenant de domaines différentes); description des processus et des niveaux de services pour le backup et le disaster recovery.

4.2.9. Obligations du prestataire en cas de *graves problèmes de sécurité ou en cas de catastrophes* ; p.ex. à quel moment le prestataire peut- ou doit-il prendre des mesures de manière autonome (avec ou sans information du commettant)?

4.2.10. Description des *tests de sécurité* à entreprendre chez le prestataire (audits, penetration testing etc.)

4.3. Sauvegarde, archivage et radiation de données

4.3.1. Etendue, forme et périodicité *de sauvegarde des données*

4.3.2. *Compliance* avec des prescriptions légales sur la conservation et l'archivage de documents et de données (p.ex. dans le contexte du droit fiscal et de la comptabilité); définition des processus et données concernés ainsi que la durée de l'archivage. À ne pas oublier les droits d'accès du commettant à ses données et le processus pour la retransmission des données à la fin du contrat.

4.3.3. Eventuellement le prestataire peut mettre à disposition des outils *E-Discovery* en cas de procédures judiciaires à l'étranger.

4.3.4. *Stockage des supports des données* (répartition spatiale, indentification, cryptage, droit et possibilités d'accès)

4.3.5. *Interdiction d'exploitation* et *exclusion d'un droit de retenir des données* du commettant, notamment en cas d'un retard dans les paiements du commettant ou en cas d'une insolvabilité du prestataire.

4.3.6. Processus pour la *radiation des données*

4.4. Audit et droit d'examen (vérification)

4.4.1. *Droits d'audit* du commettant chez le prestataire.

4.4.2. *Soutien du prestataire* lors d'un audit.

4.4.3. *Consultation d'experts tiers* dans le cadre d'un audit (notamment procédure de nomination de l'expert)

4.4.4. *Obligations du prestataire de maintenir des certifications.* Quelles sont les informations – résultant d'un audit dans le cadre d'une recertification – qui doivent être mises à disposition du commettant ?

4.4.5. Intégration du prestataire dans le *système de contrôle interne* du commettant.

4.4.6. Exécution du droit de *contrôle d'autorités publiques* (p.ex. FINMA, AFC etc.) auxquelles le commettant est soumis chez le prestataire et ses sous-traitants.

4.4.7. *Répartition des couts et efforts* dans le contexte des audits.

5. Garantie et responsabilité

5.1. **Répartition des sphères de risque et de responsabilité entre le commettant et le prestataire** (inclus de tiers et sous-traitants)

5.2. Responsabilité

5.2.1. *Fardeau de la preuve et calcul d'indemnisations*

5.2.2. Importance de la *culpabilité* en cas de dommages

5.2.3. *Exclusions de responsabilité*

5.2.4. Rapport entre *dommages-intérêts et peines conventionnelles*

5.2.5. Délais de prescription

5.3. **Garantie des droits du commettant** (notamment en cas d'éviction de de logiciels développés pour le commettant)

5.4. Assurances du prestataire

6. Durée de contrat et conditions de résiliation du contrat

6.1. Durée de contrat

6.1.1. *Entrée en vigueur* du contrat

6.1.2. *Durée du contrat*

6.2. Résiliation ordinaire du contrat

6.2.1. *Délai de préavis*

6.2.2. *Dates de résiliation*

6.2.3. *Forme* de la déclaration de résiliation

6.3. Résiliation extraordinaire du contrat

6.3.1. *Raisons de résiliation extraordinaire du contrat*

6.3.2. *Délai de préavis*

6.3.3. *Forme* de la déclaration de résiliation

6.4. Eventuelles options pour une résiliation à tout moment

6.4.1. *Modalités*

6.4.2. *Frais de résiliation*

6.5. Conséquences d'une résiliation

6.5.1. *Rémunération* (calcul d'une période entamée: *pro rata temporis*

6.5.2. *Transfert des données du commettant*

6.5.3. Description du *processus de la terminaison des services*

6.6. Backsourcing

6.6.1. *Obligation d'assistance lors d'une migration* (p.ex. migration de données du commettant)

6.6.2. *Planification* du backsourcing ou la migration à un nouveau prestataire

6.6.3. *Transfert* de données, documentations, interfaces et informations concernant le paramétrage etc.

6.6.4. *Condition pour une prolongation des services* en cas de retard de la transition

6.6.5. *Rémunération* de l'assistance du prestataire lors de la migration

7. Autres dispositions

7.1. Droit applicable et for

7.1.1. *Droit applicable*

7.1.2. *For et éventuellement procédure d'escalade*

7.2. Dispositions finales

7.2.1. *Succession juridique*

7.2.2. Droit du commettant de *révéler les conditions du contrat* à de tiers comme p.ex. le préposé à la protection des données

7.2.3. *Exigences formelles* pour des déclarations ou des modifications du contrat

7.2.4. *Signatures* → vérifier que tous les signataires ont le pouvoir de signer. Consulter si nécessaire le registre de commerce.

WOLFGANG STRAUB, dr. en droit, LL.M., est avocat à Berne et chargé de cours à l'Université de Berne (CAS ICT procurement).

Le présent check-list est issu de discussions nombreuses avec des collègues. Pour des contributions précieuses je remercie nommément CAROLINE GLOOR-SCHEIDEGGER, ADRIAN HÄSSIG, KARIN KOÇ, CHRISTIAN LAUX, CHRISTIAN LEUPI, DANIEL MARKWALDER, ROGER MAURON, PETER NEUENSCHWANDER, STEPHAN ROTHENBÜHLER, RENATE SCHERRER-JOST, JÜRG SCHNEIDER, CHRISTOPH STALDER, PETER TRACHSEL, FRIDOLIN WALTHER, MARIA WINKLER et ESTHER ZYSSET.