CONFERENCE IDC CLOUD COMPUTING

Le Cloud dans tous ses états

Le contrat Cloud : plus simple et plus dangereux

Les bons réflexes pour entrer dans un contrat Cloud en toute sécurité

Benjamin May
Avocat à la Cour
Associé, ARAMIS Société d'avocats

1/ Réflexions sur la nature du contrat Cloud

2/ Les sujets clés du contrat Cloud

- Périmètre du service et niveau d'engagement du prestataire
- Sécurité
- La problématique des transferts de données
- La localisation des données et des infrastructures à l'étranger, facteur de complications

Quelques réflexions sur la nature du contrat cloud

- **Des réalités diverses :** Mise à disposition à distance de matériel, par ex. datacenters (Infrastructure as a Service - IaaS), plateformes informatiques (Platform as a Service – PaaS) ou applications (Software as a Service – SaaS).

- **Plus simple :** Eviter d’avoir à gérer des ensembles contractuels lourds (licences, maintenance, achat/crédit-bail/location financière, intégration, etc.). Désormais, un seul contrat.

- **Plus dangereux :**
  - Contrat de prestation de services, non soumis à un régime légal supplétif (garanties, etc.)
  - Pas un contrat de maîtrise d’œuvre donc: pas d’obligation de résultat, pas d’obligation de conseil renforcée

    => un contrat où tout doit être écrit: clauses juridiques (obligation de résultat, obligation de conseil) et opérationnelles (intégrité des données, conformité des traitements, réactivité de la maintenance, disponibilité de l’espace disque, etc.)

- **Une approche juridique globale du contrat cloud : la notion de gardien de la chose**
  - Le client confie une chose au prestataire
  - Le prestataire s’oblige à la conserver, sans vol, perte ou détérioration (=> sécurité)
  - Le prestataire s’engage à la restituer à première demande (=> disponibilité)

Les analogies

- **Le contrat ASP (proche du SaaS)**

  = Accès à distance à une solution logicielle

  Différence : le contrat ASP n’implique pas forcément de migration et stockage de données du client par le prestataire

- **Le contrat d’outsourcing**

  = Prise en charge partielle ou totale du SI d’une entreprise

  Différence : Dans l’outsourcing, le client externalise une fonction interne (d’où la question du transfert de personnel : art. L. 1224-1 du code du travail)

Périmètre du service et vie du contrat

- Nécessité de bien décrire le service attendu
  - Ne pas se limiter à une expression de besoins fonctionnels
  - Définir les capacités de stockage et de traitement, la bande passante, etc.
  - Prendre en compte l'évolution du service : évolution des besoins du client, des logiciels mis à disposition, etc.

- Points d'attention particuliers :
  - Définir le processus de reprise des données et les événements déclencheurs
  - Si recours à des applications stratégiques / éditeurs vulnérables : mise en séquestre des codes sources pour que le client puisse continuer à exploiter l'application en cas de défaut du prestataire
  - Prévoir une garantie maison-mère ou une garantie bancaire à première demande si envoi d'informations sensibles dans le « cloud »

Continuité du service (restitution de la chose)

- Niveau de service
  - Indicateurs de qualité : définition (qualité et performance : temps de réponse «propre», hors impromptus de connexion), outils de mesure et droit d'audit
  - Prévoir des éléments préventifs et curatifs : audit des plans de back-up et de continuité, en essayant d'y avoir accès…

- La responsabilité de la connexion
  - Qui prend la responsabilité de la connexion, de sa performance et de sa sécurité ?
  - Conséquence sur le SLA : si le prestataire exclut toute responsabilité en matière de connexion, il n'est plus lié par aucun engagement de service
  - Premiers éléments de réponse :
    - Le prestataire peut prendre en charge la partie privée (accès via un réseau privé virtuel) et ne peut exclure sa responsabilité que pour la partie strictement publique (Internet)
    - Eléments annexes : Le prestataire peut mettre en œuvre des moyens pour sécuriser l'accès; par exemple, prévoir des procédures d'alerte (détection immédiate des défauts de connexion) et une redondance en cas de panne
    - Prévoir un audit technique et contractuel des solutions de connexions

Sécurité (conservation de la chose)

- Besoin de transparence
  - Informations techniques : localisation du serveur, serveur dédié/mutualisé, etc.
  - Le prestataire doit indiquer les prestations qu'il sous-traite (hébergement, réseau, éditeurs, etc.). Quels engagements de performance et de sécurité le prestataire a-t-il obtenu ?
  - Sécurité physique (climatisation, surveillance, etc.) et logique (anti-virus, cryptage, etc.)

- Déterminer les conditions d'archivage
  - Durée de conservation selon les délais de prescription et des obligations légales :
    - Cinq ans : actes commerciaux, salaires
    - Dix ans : documents comptables
    - Trois, six ou dix ans en matière fiscale

  - Conditions de conservation :
    - Documents spécifiques : par ex. conditions de validité des factures électroniques (factures signées électroniquement ou transmises par EDI; art. 289 V et 289 bis du CGI)
    - La conservation des données signées électroniquement peut être impactée par le Cloud

Les transferts de données (1/4) : enjeux

- L'impact de l'aspect réglementaire français
  - Secret bancaire ou médical
  - Loi Informatique et Libertés, applicable notamment aux données des salariés
  - Droit social : l'employeur est tenu de consulter le comité d'entreprise en cas d'introduction d'une nouvelle technologie dans l'entreprise (art. L.2323-13 du code du travail)

- L'impact de l'aspect réglementaire étranger
  - La localisation des données peut entraîner l'application de lois de police étrangères, même si l'on stipule un autre droit applicable au contrat

Les transferts de données (2/4) : la loi Informatique et Libertés

- Statut de responsable de traitement vs. sous-traitant
  - Le responsable traitement : personne qui détermine les finalités et les moyens du traitement, doit respecter les droits des personnes concernées, les formalités CNIL
- En théorie, le prestataire est sous-traitant du client
- Risque si le prestataire est qualifié de responsable du traitement :
  - Entraîne un certain nombre de droits sur l'exploitation des données
  - Risques pour le client : risque de responsabilité au titre du transfert de données irrégulier à un responsable de traitement (formalités, droits des personnes concernées notamment + risque pénal en cas de transfert irrégulier hors UE)
  - Risque pour le prestataire : la qualification de responsable l'expose à un fort risque de non-conformité

=> Orienter la rédaction du contrat pour éviter que le prestataire puisse devenir responsable du traitement

Les transferts de données (3/4) : la loi Informatiques et Libertés

- L'obligations de sécurité pèse sur le responsable du traitement
  - Le responsable du traitement, est « *tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* »
  - Le sous-traitant doit se conformer aux instructions du responsable du traitement
  - Le contrat « *comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement* »

- Sanctions pénales et pouvoirs de contrôle étendus de la CNIL (art. 45 s.)

Les transferts de données (4/4) : la loi Informatique et Libertés

- La loi s'applique au client et/ou au prestataire, quelles que soient les stipulations du contrat, dès lors que les critères d'application sont remplis

- Application territoriale de la loi
  - Est « *établi* » en France, « *le responsable d'un traitement qui exerce une activité sur le territoire français* »
  - Idem si le responsable du traitement est établi hors UE et « *recourt à des moyens de traitement situés sur le territoire français* »

- Transferts de données à l'étranger : quel risque ?
  - Intra-UE : informations sur la déclaration CNIL + information de la personne concernée si transfert à destination d'un responsable de traitement
  - Hors UE dans des pays de niveau de protection suffisant : même régime qu'intra-UE
  - Hors UE dans des pays n'offrant pas un niveau de protection suffisant : autorisation CNIL sur présentation du contrat de transfert (sous-traitant ou responsable du traitement) + dans certains cas autorisation de la personne concernée (art. 69)
    - Attention aux données des salariés : la CNIL exige une sélection, toutes les données ne pouvant pas être transférées sans nécessité (notamment NIR, coordonnées bancaires, situation familiale, etc.)
      (Guide CNIL pour les employeurs et les salariés)

Les complications liées au contexte transnational

- **Loi applicable et juge compétent**
  - A défaut de choix des parties, rattachement principal des contrats de prestation de services : pays du prestataire

- **Exécution des jugements**
  - En UE : le jugement acquiert force exécutoire dans l'Etat membre d'exécution sous réserve de l'accomplissement de formalités : copie authentique de la décision et certificat du caractère exécutoire de la décision (art. 41 du Règlement 44/2001)
  - Hors UE : procédure d'exequatur

- **Les problèmes posés**
  - Agir en France ou à l'étranger?
  - Quid en cas de faillite du prestataire et/ou de saisie de serveurs par des créanciers?

  => Pas de solution miracle, mais la transparence est vivement conseillées: où sont les données, quel est l'état du prestataire (liste des sûretés, informations sur les modifications de l'actionnariat, alerte sur le niveau d'activité, etc.)

MERCI DE VOTRE ATTENTION