Les contrats de cloud computing : les clauses importantes du point de vue des clients

Au-delà des particularités propres à chaque contrat de "cloud computing" (Saas, Staas ou autre), les clients des prestataires doivent conserver à l'esprit plusieurs règles essentielles ainsi que l'idée selon laquelle le choix du prestataire et des conditions dans lesquelles les données seront, en pratique, stockées et transmises sont aussi importants que la nature des prestations ou les stipulations contractuelles.

En France, les entreprises, qui ne sont pas contraintes de conserver un « datacenter » en propre, s'orientent vers des services s'inscrivant dans le « cloud computing » qui leur permettent, pour résumer, de disposer d'une capacité de stockage et de services à la demande externalisés (SaaS ou Staas).

Le choix du prestataire est très important : seuls quelques grands comptes pourront négocier les contrats d'adhésion proposés par les géants du cloud computing (Salesforce, Amazon, Google, Microsoft, Cisco, EMC, Sage, etc.). Les PME pourront choisir des entreprises de moindre dimension présentant des garanties suffisantes, **pour tenter de négocier les clauses des contrats**.

Quel que soit le prestataire, il convient, avant de signer le contrat, de vérifier l'efficacité des clauses assurant la sécurité, l'intégrité et la disponibilité des données.[1]

1. Les clauses permettant de garantir la sécurité et l'intégrité des données

Il est primordial de savoir où sont physiquement stockées les données. **Une clause de localisation des données incluant une liste des pays hébergeant les serveurs du prestataire est donc indispensable.** Il convient, à tout le moins, de s'assurer que le transfert des données n'est possible qu'au sein des pays membres de l'Union européenne[i].

Il est à noter que la Commission européenne[2] considère que les Etats-Unis n'offrent pas – *les accords de « Safe harbor » étant considérés comme caducs* - un niveau de protection adéquat, le*Patriot Act* permettant d'accéder aux données hébergées par les prestataires américains, quel que soit le pays de stockage.

Même la conservation des données sur le sol européen ne serait pas un gage suffisant de sécurité**dès lors que le « data center » appartient à une société américaine**.

De même, le contrat de cloud computing doit prévoir la conservation des données dans le respect des lois en vigueur. L'attention doit être portée notamment sur les clauses relatives à :

- la durée de conservation des données, qui doit être limitée et raisonnable au regard des finalités pour lesquelles les données ont été collectées,

- la coopération du prestataire avec les autorités de protection de données (Google, à cet égard, n'est pas un exemple…),

- respect du droit d'accès et de modification des données.

Le respect de l'intégrité et de la confidentialité des données suppose que le contrat stipule des conditions propres à garantir qu'elles ne seront ni altérées (mesures physiques de protection, authentification et connexion sécurisée des utilisateurs, cryptographie des données, etc.), ni susceptibles d'être utilisées par le prestataire de façon illicite.

Une clause prévoyant le contrôle des mesures de protection par le biais **d'audits externes réguliers** serait précieuse.

2. Les clauses de responsabilité

Le client **demeure responsable du traitement des données qu'il a collectées**. Aussi, la question de la responsabilité en cas d'incident doit-elle figurer au contrat.

Une clause doit donc envisager clairement les responsabilités de chacun, par exemple en cas de vol ou de perte des données ou d'utilisation illicite des informations confiées, sans que la responsabilité du prestataire ne soit exclue ou trop limitée.

3. Les clauses permettant de garantir la disponibilité des données

Le contrat doit enfin envisager les moyens de **garantir une disponibilité des données pour le client**, que ce soit en cas de perte ou d'indisponibilité temporaire de celles-ci du fait du prestataire, ou à l'échéance du contrat.

Aussi **la clause de réplication est-elle incontournable.** Elle doit prévoir que les données seront dupliquées sur d'autres sites distants et/ou feront l'objet d'une restauration dans des délais et des modalités prédéfinis.

Enfin, une clause de réversibilité des données permettant d'organiser le retour des données chez le client ou leur transfert chez un autre prestataire sera nécessaire. Elle doit fixer les conséquences pratiques de la fin du contrat (remise d'une copie des données, modalités de transfert des données, délais, etc.).

C'est uniquement en s'assurant de la présence de telles clauses que le client est juridiquement garanti contre les risques liés aux solutions de cloud computing. Il convient toujours de garder à l'esprit qu'en l'absence de « précautions utiles […] pour préserver la sécurité des données »[ii], le responsable du traitement risque rien moins que 5 ans d'emprisonnement et 300.000 € d'amende[iii].

Pascal ALIX & Gwendoline PERFETTI,

VIRTUALEGIS, cabinet d'avocats

[1] CNIL, *Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing,* 25 juin 2012,

[2] Commission Européenne, *General Data Protection Regulation,* 25 janvier 2012.

[i] La loi du 6 août 2004 n'autorise les transferts hors UE qu'en cas de protection suffisante

[ii] Article 34 de la loi informatique et libertés

[iii] Article 226-17 du Code pénal