Contrats, Certifications, Réglementations :

une composante juridique à la transformation vers le Cloud

La transformation de services dans les entreprises et leur passage dans le Cloud est une des principales tendances de l'IT. 80% des entreprises ont des projets de déploiements de services dans le Cloud sur les 12 prochains mois et 70 à 80% devraient, selon Gartner, adopter les services du Cloud public.

La gestion des données et son cadre contractuel, juridique et règlementaire n'est pas un nouveau problème inhérent au Cloud. Cependant, ces services apportent une nouvelle composante avec la gestion déléguée des données qui complexifie le sujet, en particulier pour le Cloud public où la gestion des données est confiée pour tout ou partie à un tiers. Au-delà des aspects métiers et budgétaires, ces transformations d'entreprise doivent donc intégrer les sujets contractuels et règlementaires.

Une relation contractuelle à établir

La première étape est de réfléchir à la protection et à la confidentialité des données de l'entreprise, en amont de la migration, pour éviter des accès et modifications non autorisés. La Commission Nationale de l'Informatique et des Libertés (CNIL) a édité sept recommandations pour une entreprise :

1. Identifier clairement les données et les traitements qui passeront dans le Cloud ;
2. Définir ses exigences de sécurité technique et juridique ;
3. Conduire une analyse de risques pour identifier les mesures de sécurité essentielles ;
4. Identifier le type de Cloud pertinent pour le traitement envisagé ;
5. Choisir un prestataire présentant des garanties suffisantes ;
6. Revoir la politique de sécurité interne ;
7. Surveiller les évolutions dans le temps.

Le respect de la confidentialité des données et les moyens déployés pour en assurer l'intégrité sont deux points majeurs dans la contractualisation avec un fournisseur Cloud. Les clauses générales et particulières doivent également être explicitement définies dans les contrats d'hébergement d'informations. Les responsabilités de chacun (entreprise, prestataires et sous-traitants) et les engagements de services associés doivent être définis, même avec des partenaires de confiance. Les types de clauses suivantes, publiées par la CNIL, peuvent aider dans la définition d'un contrat de services Cloud.

Eléments de responsabilités	Points à préciser dans le contrat
Traitement des données	- Moyens de **protection des données personnelles**, **moyens de traitement** et la liste des **sous-traitants éventuels**. - P**rocédures** et **moyens** mis à disposition pour l'**accès aux données** et le **signalement de failles de sécurité**.
Localisation et transfert des données	- Localisation et transfert des données - **Moyens de protection** des données, en cas d'hébergement en zone hors UE Objectif : assurer la **visibilité sur les pays hébergeant les serveurs** du prestataire et la possibilité de l'entreprise de **limiter les transferts vers les pays dont la sécurité n'est pas suffisante.**
Garanties de mise en œuvre	- **Délai minimum de conservation des données** suivant le type d'information stocké - **Moyens de destruction ou de restitution des données** - Selon les typologies de contrats, possibilité pour l'entreprise de **réaliser des audits de gestion**. - Engagement du prestataire sur **le devoir de coopération avec les autorités** de protections des données compétentes.
Formalités auprès des autorités	- Engagement du prestataire sur sa coopération avec les autorités de protection des données (formalités administratives pouvant être effectuées **au nom du client** par le prestataire ou **au nom du prestataire** s'il est **responsable conjoint du traitement**.)
Sécurité et confidentialité des données	- **Obligations du** prestataire - **Politiques et mesures de sécurité retenues** - **Engagements de services**. **Certifications demandées** à définir par contrats.

Les clauses de résiliation et de réversibilité des données font partie de la contractualisation avec un prestataire Cloud et ne doivent pas être négligées. Elles sont d'autant plus importantes qu'elles doivent s'assurer de **l'appartenance des données**, de leur **réversibilité** et de leur **transférabilité** vers de nouveaux services.

Des services Cloud certifiés

Des fournisseurs de services certifiés

Les fournisseurs de services Cloud adoptent depuis quelques années une démarche de certification de leurs offres qui complètent les obligations contractuelles établies avec leurs clients.

Les deux principales certifications concernent la sécurité des données, avec la norme ISO 27001 et le management des informations client, avec la certification SSAE 16 (anciennement SAS 70). Ces deux certifications complémentaires assurent un cadre normatif fort pour la gestion externalisée des données. Google, pour ses Google Apps, et Amazone, pour ses Amazone Web Services, ont tous deux reçus ces certifications après un travail de mise en conformité.

"ISO 27001, published by the International Organization for Standardization (ISO), specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks."

"SSAE 16's certification, developed by the American Institute of Certified Public Accountants (AICPA), represents that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related

En parallèle des certifications majeures, les fournisseurs de services Cloud tendent vers l'adoption de normes spécifiques pour le stockage et les services en ligne, avec par exemple Les normes **PCI-DSS** (paiement en ligne sécurisé) et **NEN 70** (pour le secteur médical).

Des compétences certifiées

La certification des offres Cloud passe également par la certification des ressources manageant ces technologies. Ces certifications très souvent « propriétaires » sont de plusieurs natures :

- **Les fondamentaux du Cloud**
  Ces formations généralistes permettent d'acquérir les fondamentaux du Cloud par une approche business et technique.
- **La sécurité des données**
  Ces formations sont généralement indépendantes des technologies pour assurer un cursus complet.
- **Les technologies propriétaires**
  Elles sont à destination des administrateurs des services Cloud, pour assurer un haut niveau d'expertise sur l'administration et l'utilisation de services propriétaires.

TOP 10 Cloud's certifications
CIO.com

1- CCSK -- Cloud Security Alliance
2- Cloud U -- Rackspace
3- CompTIA Cloud esentials -- CompTIA
4- Cloud Certified Professionnal --CloudSchool.com
5&6- IBM Certified Cloud Solution Architect v1 and v3 - IBM
7- Google Certified Deployment Specialist -- Google
8- Salesforce.com Certified Professional -- Salesforce.com
9- VMware Certified Professional - Vmware
10- Red Hat Certificate of Expertise in Infrastructure-as-a-Service -- Red Hat

Des règlementations étatiques complexes

La gestion des données et leur territorialité est une des questions juridiques les plus complexes dans les Systèmes d'Information. Différentes lois et conventions ont été établies par et entre les pays pour assurer, entre autres, la protection du pays et la préservation de leurs patrimoines sensibles (culturel, scientifique, militaire).

La gestion de la territorialité de la donnée s'est complexifiée avec son externalisation dans le Cloud. La localisation devant se faire selon les contraintes réglementaires étatiques, il est indispensable de connaitre la nature des données pour respecter le cadre juridique.

De plus, certains pays et unions de pays ont interdit le transfert de données, personnelles et professionnelles, vers des pays n'ayant pas le même niveau de sécurité. Des règlementations ont été établies (notamment vers les Etats-Unis) pour assurer les échanges tout en garantissant la sécurité des données. Le respect de ces réglementations par les fournisseurs de services doit être assuré dans le cadre d'une transformation d'entreprise vers le Cloud.

Réglementations étatiques

En France, un décret en date du 2 Novembre 2011, complété par un arrêté du Journal Officiel du 3 Juillet 2012, fait état de la « protection du potentiel scientifique et technique » de la France. Cette mesure juridique définit deux axes différents et complémentaires de protection :

- La protection des activités et des informations définit un cadre juridique à la protection des informations sensibles, quel que soit l'endroit où elles sont manipulées. Elle inclut les processus de vérification des zones scientifiques et techniques protégées.
- La protection des lieux établit également de nouvelles « **Zones à Régime Restrictif** ». Cette exigence, concernant l'accès aux zones hébergeant des informations sensibles, se matérialise par une demande d'autorisation, émise par le ministère de tutelle, obligatoire pour toute opération sur les données.

Aux Etats-Unis, la règlementation International Traffic in Arms Regulation (**ITAR**) a été actée en 1976, pendant la guerre froide, pour implémenter un système d'embargo sur les armes sur les pays membres du « Council for Mutual Economic Assistance ». ITAR sert aujourd'hui à contrôler l'exportation et l'importation de toutes technologies ou données techniques pouvant servir à des fins militaires, par exemple les équipements aéronautiques, les engins explosifs et les systèmes informatiques, équipements ou logiciels, servant ou pouvant servir à contrôler des équipements militaires. L'export ou l'import de matériels ou d'informations nécessite une autorisation émise par le Département d'Etat des Etats-Unis, exception faite du cas où le partage est fait avec des entreprises ou citoyens américains.

Transfert de données entre pays

- Entre les membres de l'EEE, excepté les différentes réglementations étatiques, il n'existe pas de réglementation sur la protection des données. Cependant, 2 règlements définissent le cadre juridique en cas de **contentieux** n'étant pas résolus par la loi des parties (utilisée de manière privilégiée en cas de **litiges**) :

- **Rome I :** Parlement et Conseil Européen – 17 Juin 2008
- **Bruxelles I :** Conseil Européen – 22 Décembre 2000

Rome I :

« Les parties d'un contrat **choisissent la loi qui le régira** en totalité ou partie. […]
Lorsque les parties n'ont pas **choisi la loi applicable** aux contrats de vente de biens, de prestation de services, de franchise ou de distribution, elle sera déterminée sur la base du **pays de résidence du principal exécutant** du contrat. »

Bruxelles I :

« Le principe fondamental est que la **juridiction compétente** est celle de **l'État membre où le défendeur a son domicile**, quelle que soit sa nationalité. […]
Pour les personnes morales ou les sociétés, le domicile est défini en fonction du lieu de leur **siège statuaire**, de leur administration centrale ou de leur principal établissement. »

- Un cadre juridique « **Safe Harbor** » a été défini pour l'hébergement de données personnelles détenues par des entreprises de l'EEE par des **hébergeurs établis aux Etats Unis**. Il garantit le respect par l'hébergeur des principes de protection des données personnelles en vigueur dans les pays membres de l'EEE. Toute entreprise établie dans un pays membre de l'EEE peut faire héberger ses données par des entreprises établies aux Etats Unis ayant adhéré à « Safe Harbor », sans nécessiter d'autorisations préalables de l'autorité de protection des données personnelles de son pays. La certification Safe Harbor garantit en effet la prise en compte des exigences desdites autorités.

Le cadre Safe Harbor est une démarche auto-certifiante. Les membres doivent explicitement et annuellement accepter les principes suivants :

- **Notice** : Informer les clients des informations collectées, la raison de cette collecte et les moyens qu'ils ont pour limiter ces démarches ;
- **Choice** : Laisser le choix aux clients de divulguer certaines informations sur leurs usages des services et offrir la possibilité de changer ce choix si les informations collectées sont sensibles et/ou personnelles ;
- **Onward Transfer** : Veiller à ce que les sous-traitants utilisent les mêmes principes de protection des données que ceux indiqués dans le Safe Harbor, et notamment dans le cas de transfert d'information client ;
- **Access** : Donner les moyens aux clients d'accéder et de modifier leurs informations personnelles;
- **Security** : Définir et mettre en place des moyens de sécurité pour protéger les informations collectées ;

- **Data Integrity** : Prendre des mesures afin de s'assurer que l'information gérée est fiable, précise, complète, mise à jour et utilisée selon les fins prévues ;
- **Enforcement** : Conduire des audits de vérification de la conformité au Safe Harbor au sein du fournisseur de services, et s'assurer que ces principes soient respectés et appliqués par tous ses employés.

- Enfin, les « **Binding Corporate Rules** », développées par la CNIL, définissent un code de conduite à respecter et une mise en conformité avec la Directive européenne 95/46/CE interdisant le transfert de données vers des pays tiers à l'UE. Les entreprises concernées sont des multinationales réalisant des exports de données vers des pays ne garantissant pas le même niveau de protection des données qu'un pays de l'UE.

Un processus de reconnaissance mutuel entre 21 autorités[1] a également été mis en place garantissant l'acceptation automatique de BCR si celles-ci ont été jugées suffisantes par une entité.

En conclusion

La transformation d'une entreprise au travers des services Cloud comporte une part contractuelle et règlementaire importante, qui peut constituer un frein.

Google, Amazone, Microsoft, entre autres, ont pris les devants avec une véritable démarche et des certifications pour accompagner les entreprises dans ces évolutions.

Cela nécessite cependant un véritable accompagnement des entreprises en amont de la transformation pour définir « Qu'ai-je le DROIT de migrer dans le Cloud et comment pourrais-je PROTEGER mes informations? ».

Adrien Chodz'ko est ingénieur spécialisé en télécommunications et réseaux et en management des Systèmes d'Informations.
Après une première expérience réussie en tant que Responsable SI dans une PME du secteur du BTP, il a intégré Devoteam et travaille actuellement pour un grand industriel.
Pour lui, le conseil dans les Systèmes d'Information est un excellent moyen de mêler l'analyse métier et l'expertise technique.

Vincent Para est Senior Consultant au sein de Devoteam. Il a intégré le cabinet en 2009 une fois diplômé, et a travaillé sur les problématiques de développement durable (Green IT). Il se spécialise à présent dans la gestion des services IT et le management des DSI.

[1] Allemagne, Autriche, Belgique, Bulgarie, Chypre, Espagne, Estonie, France, Grande Bretagne, Irlande, Islande, Italie, Lettonie, Liechtenstein, Luxembourg, Malte, Norvège, Pays-Bas, République tchèque, Slovaquie, Slovénie