

La législation des clouds au sein de l'entreprise

Introduction

Les données générées par les entreprises sont de plus en plus nombreuses, qu'elles soient sensibles ou non, à propos de clients, d'employés, ou encore d'avancées sur un produit ou un service. Le cloud va permettre à l'entreprise d'assurer la protection et la sécurisation fiable de ses informations sans altérer leur intégrité, grâce à un prestataire qualifié.

Cependant, seulement 5% des TPE et PME possède un cloud. Les risques leurs semblent trop importants, notamment lorsqu'il est question d'offres standardisées accompagnées de contrat d'adhésion. En effet, les clients ne peuvent pas négocier. Les nouvelles lois de la RGPD qui seront effectives le 25 mai 2018 auront pour but de pallier les fuites d'informations considérables. Les mesures de protection des données seront harmonisées et ce au sein des 27 pays de l'Union Européenne. Le droit à l'oubli sera rendu possible par la suppression totale des données.

Dans ce document, il sera présenté ce qu'il est nécessaire de savoir pour développer ce type de système d'information en toute sécurité et selon la réglementation européenne de la protection des données :

**Comment la nouvelle législation de la RGPD
va accroître la sécurité des données stockées dans le cloud d'une entreprise ?**

I/ Définition et fonctionnement

Le cloud computing correspond à l'externalisation de diverses tâches¹ qui ne sont pas toujours maîtrisées par l'entreprise, faute de moyens humains, matériels et/ou financiers qui initialement prenaient effet dans l'enceinte de l'entreprise.

Cette technique doit répondre à plusieurs critères définis par la NIST :

- Païement "à l'usage" | Les coût sont réduits et maîtrisés, car ils sont calculés selon la consommation
- Simplicité et flexibilité d'un service à la demande et virtualisation des ressources | l'accessibilité aux données est sécurisées, disponible à tout moment au sein de n'importe quel endroit, sur différents devices (téléphones, tablettes ...)

Ce service présente des avantages en plus de ceux présentés dans les critères précédents:

- Cela permet de réduire les pertes d'argent liées aux matériels (en particuliers informatiques) non-performants
- Le cloud computing rentre dans une démarche écologique : la consommation d'énergies est réduite après optimisation de son utilisation
- Ces tâches déléguées, les salariés peuvent se concentrer sur leurs réelles missions, et ainsi, apporter une plus-value à l'entreprise

Pour externaliser ces services auprès d'un tiers, un contrat sera rédigé entre les deux parties qui sont l'entreprise et le prestataire.

Il obligera le second à respecter la confidentialité des données dont ils détiendra la gestion. Ce contrat va également permettre à l'entreprise de se protéger sur le plan légal qui se consolide de plus en plus, notamment en cas de problème informatique. Il faudra pour cela, transférer les responsabilités grâce aux différentes clauses du contrat.

3 types : les clouds hybrides, privés ou publics.

3 modèle : SaaS : « Software as a Service » logiciel en ligne, PaaS : « Platform as a Service » plateforme de développement d'applications en ligne, IaaS : « Infrastructure as a Service » infrastructures de calcul et de stockage en ligne.

¹ Exemple de tâches : stockage de données, d'outils informatiques de logiciels d'édition en ligne, ...

II/ Risques et réglementations

a) Risques

On peut noter que le cloud est soumis à plusieurs types de risques. Ces derniers sont en lien direct avec les données. Leur contrôle et protection est plus que jamais, nécessaire. Vous devez, à tout moment, connaître leur localisation et leur traitement, surtout si votre prestataire de cloud fait usage de sous-traitants. Multiplier la sous-traitance, accroît le risque de détournement des données. Même lorsque les données sont exportées sur des liens chiffrés (VPN, https...), celles-ci restent toutefois traitées en clair par le prestataire de Cloud computing.

Il existe également des risques techniques qui vont des problèmes de réseaux au crash du serveur de l'entreprise prestataire.

b) Réglementation

L'étude des services Cloud réalisée par Netskope en 2016 montre que les applications utilisées par les entreprises ne répondent pas aux nouvelles normes de la RGPD, en affichant pas que les clients sont propriétaires de la données. Seulement 24.6% d'entre-elles sont activement en train de se préparer à répondre aux nouvelles conditions. La France et l'Allemagne ont déjà un avantage sur cette mise à niveau : une partie des règles existent déjà dans les droits des deux pays.

En France, la CNIL recommande déjà depuis 2012, un régime de cotraitance pour les entreprises souscrivant à un service de cloud computing.

La RGPD impose désormais ce régime. C'est le point le plus important de ce nouveau règlement car il implique le remaniement de nombreux contrats. Cela signifie que chaque parti a des responsabilités² et la transparence entre les deux est le maître-mot.

² Selon l'article 26 du règlement qui explique que les "responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement".

Un document sera donc rédigé, en mentionnant les conditions de partage des finalités du traitement, les mesures techniques et organisationnelles mise en place pour effectuer le traitement, les politiques de sécurité, la personne s'assurant du respect effectifs des droits, les conditions d'intervention d'un sous-traitant auprès du sous-traitant, les conditions de confidentialités, la localisation des données et leur parcours de vie (destruction, ...), et enfin le partage des risques et responsabilités entre les responsables conjoints.

D'un côté les éditeurs de services devront s'assurer de fournir l'ensemble des fonctionnalités requises à leurs clients. De l'autre les clients, que sont les entreprises, devront contrôler les usages des applications en choisissant celles répondant aux critères imposés par la RGPD. Ensemble, ils doivent choisir des solutions adaptées au statut de l'entreprise et non pas satisfaisant pour le grand public.

Si un problème survient de la protection des données, une déclaration de notification devra être faite par le responsable de traitement dans les 72 heures à la CNIL.

Un registre composé des réclamations des clients devra aussi être tenu.

L'entreprise doit toujours avoir le contrôle sur les données qu'elle collecte et traite, et doit donner son "opt-in" (accord) à l'éditeur de service pour que ce dernier puisse traiter les informations à gérer.

Ce nouveau règlement permet également au client du fournisseur de service de bénéficier du droit à l'oubli et de rompre son contrat.

Les sanctions seront plus lourdes. Les amendes pourront aller jusqu'à plus 4% du chiffre d'affaires mondial de l'entreprise, soit plus de 20 millions d'euros.

L'objectif de ces lourdes sanctions est de pouvoir sanctionner les grandes entreprises du GAFAM (Google, Amazon, FaceBook, Apple, Microsoft), qui sont connues pour ne pas respecter les règles.

III/ Préconisations

Le RGPD comprend des suggestions spécifiques sur les types d'actions de sécurité susceptibles d'être considérés comme « pertinents par rapport au risque », comme :

- Le cryptage des données personnelles
- La capacité d'assurer la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services qui traitent les données personnelles
- La possibilité de restaurer les données et d'assurer l'accès aux données en temps opportun en cas d'incident physique ou technique

Cet aspect du règlement pourrait également s'appliquer au partage de données entre plusieurs sociétés d'un même groupe ou appartenant au même réseau de distribution.

La CNIL et le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) proposent un mode d'emploi pour guider les entreprises. Voici un regroupement des différentes étapes proposées par les deux organismes :

- Identification des données et de leur traitement : selon le type de document, sa source, une réglementation peut lui être propre et obliger son hébergement dans des structures spécifiques

Quelles types de données sont concernées ?

- données à caractère personnel ?
 - données sensibles ?
 - données stratégiques pour l'entreprise ?
 - données utilisées dans les applications métiers ?
 - sont-elles susceptibles d'être convoitées par des cybercriminels ?
 - si oui, êtes-vous prêt à courir le risque d'être piraté ?
-
- Définir son projet en termes de technique et de juridiction : choisissez un hébergement adapté à vos données (plus ou moins sensibles), les contrats peuvent varier sur le degré de sécurité, de confidentialité, ou encore d'accessibilité
 - Effectuer une analyse des risques : une liste établie par l'ENISA (Agence Européenne chargée de la sécurité des réseaux et de l'information) référence les principaux risques ; vous pouvez également réaliser plusieurs tests d'intrusions dans le système du cloud afin de détecter d'éventuelles failles
 - Identifier le type en adéquation avec les besoins de l'entreprise
 - Choisir son prestataire après analyse et réflexion : il faut que votre prestataire soit à la hauteur de la sensibilité de vos données car l'entreprise endosse une responsabilité juridique vis-à-vis de celles-ci
 - Gérez le cycle de vie de l'information en tenant compte de toutes ces étapes (création, identification, stockage, utilisation, partage ou encore archivage etc.) y compris la mise en conformité et en audit, la portabilité et interopérabilité

Des entreprises comme Orange et Yahoo ce sont déjà fait hacker leurs systèmes d'informations sur le cloud. Parce que le risque zéro n'existe pas. Nous vous préconisons, si votre situation le permet de faire du "multi cloud", c'est-à-dire de vous externaliser auprès

de prestataires différents pour minimiser les pertes de données en cas de crash de l'un d'entre eux.

Vous pouvez demander à votre hébergeur d'effectuer une sauvegarde et/ou en garder une de votre côté. De plus, en cas de simple panne de connexion internet on peut envisager un verrouillage automatique pour bloquer tout accès non désiré aux données.

Conclusion

La RGPD a développé son règlement dans le but de limiter les fraudes notamment auprès des grandes entreprises. Il a pour but également de définir et de répartir les responsabilités entre les deux acteurs qui sont l'éditeurs de service et l'entreprise. Et enfin, il protège les citoyens, leurs données et les utilisations de ces dernières.

Sources :

CNIL. *Sécurité des données, nouvelle réglementation européenne 2018 : RGPD*. Disponible sur : <
https://www.cloudexpo-europe.fr/_media/Conferences-pdf/S%C3%A9curit%C3%A9-des-donn%C3%A9es,-nouvelles-r%C3%A8glementation-europ%C3%A9enne-2018---RGPD-SVDI.pdf >

CNIL. *Synthèse des réponses à la consultation publique sur le Cloud computing lancée par la CNIL d'octobre à décembre 2011 et analyse de la CNIL*. Disponible sur : <
https://www.cnil.fr/sites/default/files/typo/document/Synthese_des_reponses_a_la_consultation_publicue_sur_le_Cloud_et_analyse_de_la_CNIL.pdf >

GOURVENNEC, Yann. *GDPR : quels enjeux pour le cloud computing ?* Disponible sur <
<https://www.orange-business.com/fr/blogs/cloud-computing/actualites/rgpd-quels-enjeux-pour-le-cloud-computing-> >

LECANU, Guillaume. *[RGPD] Où sont stockées vos données ? Le Cloud pour les nuls*. Disponible sur : <
<https://koban.cloud/rgpd-stockees-vos-donnees-cloud-nuls/> >

WEIL, Tiffany. *RGPD : les applications Cloud sont-elles prêtes pour 2018 ?* Disponible sur <
<https://www.oodrive.fr/blog/reglementation/rgpd-les-applications-cloud-sont-elles-pretes-pour-2018/> >