FICHE PRATIQUE N°1

Cloud

JANVIER 2016

SÉCURITÉ : LES 10 BONNES QUESTIONS À SE POSER

Alors que le recours à des solutions SaaS s'impose de plus en plus dans les habitudes des entreprises, quels points vérifier avant de se lancer ? Quelles sont les questions à se poser et quelles garanties vérifier avant de choisir son fournisseur ? Pour vous aider dans votre réflexion, nous vous donnons ci-dessous les points clés à vérifier auprès des prestataires de services Cloud...

COMMENT EST ASSURÉE LA SÉCURITÉ DES DONNÉES ?

En fonction de la nature des données confiées au prestataire SaaS (données personnelles, sensibles, stratégiques, etc.), l'exigence en termes de sécurité ne sera pas la même.

Les principaux points qui seront à vérifier et pour lesquels l'éditeur devra apporter des réponses précises seront les suivants :

Où sont localisées les données client ?

L'entreprise qui envisage de souscrire à un abonnement SaaS devra en amont s'assurer du lieu exact où sont localisées ses données, surtout s'il s'agit de données stratégiques, et vérifier que le prestataire ne les transfère pas à l'étranger sans son accord. Cela évitera la mauvaise surprise d'une réquisition judiciaire des données par des autorités étrangères ou l'hébergement dans des pays dans lesquels les niveaux de sécurité ne sont pas optimums. **La localisation des données doit donc être précisée contractuellement.**

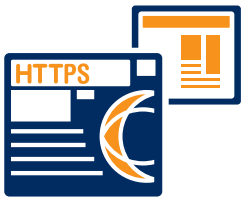
Soyez par exemple vigilants avec les « cloud publics » pour lesquels il n'y a généralement aucun engagement sur la localisation des données.

Comment la confidentialité des données est-elle gérée ?

Le prestataire doit être en mesure de garantir la confidentialité des données qui lui sont confiées, avec par exemple **une architecture étanche et des protocoles d'accès sécurisés.**

Veillez également à ce que le prestataire garantisse qu'il n'utilisera pas vos données à d'autres fins que celles prévues dans le contrat.

CROISSANCE MARCHÉ DU CLOUD EN FRANCE EN 2014*



POUR 82% DES EXPERTS COMPTABLES LE SAAS EST SYNONYME DE SÉCURITÉ**

La réversibilité des données est-elle cadrée contractuellement ?

La réversibilité (ou portabilité) est la possibilité de pouvoir obtenir une copie de l'intégralité des données dans un format couramment utilisé, qui permet au client de **pouvoir changer de solution sans perte d'information.**

L'éditeur SaaS devra mentionner le format que prendra la restitution des données, afin de permettre à l'entreprise de s'assurer qu'il ne s'agit pas d'un format propre à l'éditeur qui pourrait rendre complexe la migration vers une autre solution.

Qu'advient-il des données à l'issue du contrat ?

Afin de garantir la sécurité de ses données, l'entreprise doit vérifier la durée de conservation de ses données à l'issue de son contrat ainsi que la destruction effective et sécurisée de celles-ci.

Chez Cegid par exemple, les données sont conservées 60 jours après la fin du contrat puis elles sont effacées.

Sources : *IDC - ** « Baromètre du Cloud Cegid/La Profession Comptable »

FICHE PRATIQUE N°1

Cloud

JANVIER 2016

QUELLES GARANTIES QUANT À LA SÉCURITÉ PHYSIQUE DES LOCAUX ?

Outre des mesures de sécurité que l'on pourrait qualifier de purement informatiques, il est essentiel que les locaux où seront stockées vos applications et vos données soient eux-mêmes sécurisés : **sécurité des accès, mais également autonomie de l'infrastructure** afin qu'une simple coupure de courant ne puisse pas mettre en péril l'accès des utilisateurs à leurs applications.

Les niveaux de sécurité peuvent varier en fonction des prestataires, voire des datacenters d'un même prestataire. C'est pourquoi il est essentiel de **vérifier les garanties que présente le prestataire** afin que l'infrastructure du data center ne puisse constituer en elle-même une potentielle faille de sécurité: protection du site et sécurité des accès, sécurité électrique et système de climatisation, protection du réseau (pare-feu, antivirus, détection d'intrusion, etc.)...

Vérifiez également que l'ensemble des éléments du datacenter sont redondés. Très concrètement, cela signifie que tout problème technique rencontré aura immédiatement une solution grâce à un autre élément qui viendra prendre la relève de l'élément défectueux et cela, sans perturber l'utilisation du service. En effet un élément non redondé constitue une faille de sécurité pour l'ensemble du data center : on parlera ainsi de **politique « No SPOF » (No Single Point Of Faillure).** C'est notamment la politique appliquée dans les datacenters qui hébergent les solutions SaaS du groupe Cegid.

Un bon indicateur quant à la qualité des process est l'existence de **certifications de type ISO 27001**, qui établit des spécifications de pointes concernant la sécurité des Systèmes d'Informations.

UN OBJECTIF : SÉCURISER VOTRE ACTIVITÉ

Choisir un partenaire pérenne, s'assurer qu'il sera en mesure de vous garantir la sécurité de vos données et de l'infrastructure qui les protège sont des préalables essentiels. **C'est l'assurance de ne pas risquer d'arrêt d'exploitation dans l'utilisation de votre solution qui pourrait pénaliser votre activité.**

Mais quelles que soient les garanties qui vous sont données, vous accédez à votre solution au travers de votre propre infrastructure Télécom. C'est donc un des points de vigilance important. L'exploitation d'une solution de production « cœur de métier » doit disposer de la bande passante nécessaire et ne pas risquer d'être ralentie par d'autres flux internet quotidiens (visionnages de vidéos, mails, téléchargements...).

Le prestataire doit vous fournir des prérequis techniques nécessaires au bon fonctionnement de la solution, et vous communiquer les débits minimums recommandés. De l'ultra sécurisé VPN à la ligne ADSL dédiée, l'infrastructure télécom devra être déterminée en fonction de la criticité des données hébergées, de la typologie d'application utilisée, ou du nombre d'utilisateurs.

Autant de mesures au service de la sécurisation des données et de l'activité !

Les bonnes questions à se poser ou à poser à son prestataire :

1. Est-ce que j'opte pour un partenaire pérenne ?
2. Quelles sont les mesures de sécurité mises en place ?
3. La localisation des données est-elle bien précisée dans mon contrat ?
4. La propriété des données est elle bien encadrée par mon contrat ?
5. La réversibilité des données est-elle cadrée contractuellement ?
6. La confidentialité des données est-elle garantie ?
7. Les documents contractuels sont-ils simples et sans multiples renvois ?
8. Quels sont les prérequis techniques au bon fonctionnement de la solution ?
9. Toutes ces informations vous sont-elles fournies dans le cadre de la contractualisation ?
10. Alors ...Quand est-ce-que je me lance ?

GARDIENNAGE 24/7
AVEC RONDES POUR LES DATACENTERS DU CLOUD PRIVÉ CEGID EN FRANCE

QUALITÉ DES PROCESS
CERTIFIÉ ISO 27001

99%
TAUX DE DISPONIBILITÉ GARANTI

avea Services
13 rue de la Loire - BP 83411
44234 St Sébastien s/ Loire Cedex
Tél. : 02 51 72 99 72
infos@avea.fr
www.avea.fr
CegidPartner

Cegid - 01/2015

Cegid, 52 quai Paul Sédallian
69279 Lyon CEDEX 09
Tél. 0 811 884 888 (coût d'un appel local) • www.cegid.fr/experts

Cegid
Cloud Services & Software