Le cloud est aujourd'hui devenu incontournable dans presque tous les aspects de l'informatique d'entreprise. Il joue un rôle clé dans l'activité de l'entreprise et doit être considéré comme une nouvelle norme. La protection des données, et en particulier la sauvegarde, l'archivage et la reprise après incident, arrivent actuellement en tête de la liste des cas d'utilisation du cloud. Mais avant de signer votre contrat de cloud public, avez-vous pris soin de lire et négocier toutes ses clauses ? Ou les interminables paragraphes pleins de jargon juridique vous ont-ils poussé à cliquer sur « j'accepte » un peu trop vite ?

Il est bon que votre service juridique lise l'intégralité du document, mais voici déjà trois points importants que vous devez garder en tête en recourant aux services d'un fournisseur de cloud.

1. OÙ SERONT RÉELLEMENT SITUÉES VOS DONNÉES ?

DIFFICULTÉ : la Directive sur la protection des données de l'Union européenne déjà en application ainsi que le Règlement général sur la protection des données (GDPR) à venir interdisent de stocker en dehors de l'UE des données pouvant permettre d'identifier un individu, sauf si le destinataire dispose d'une certification Privacy Shield (Bouclier de protection des données) ou de règles d'entreprise contraignantes ou si un accord de transfert des données conforme aux dispositions approuvées par la Commission européenne est conclu entre l'exportateur et le destinataire des données extérieur à l'UE. Certains fournisseurs de cloud peuvent traiter et stocker vos données n'importe où si vous ne pensez pas à choisir l'endroit où elles doivent être stockées. Il est difficile de vérifier si les données sont réellement traitées dans les datacenters que le fournisseur de cloud affirme utiliser. Sans compter que certains fournisseurs ne précisent même pas l'emplacement de leurs datacenters.

CONSEIL : sachez quelles données vous stockez dans le cloud. S'il est essentiel pour vous d'avoir la garantie que vos données sont stockées à un endroit précis, négociez avec le fournisseur de cloud pour que l'emplacement exact du datacenter soit mentionné dans votre contrat de cloud.

2. LA DISPONIBILITÉ VAUT-ELLE AUSSI POUR VOS DONNÉES ?

DIFFICULTÉ : les fournisseurs de cloud soulignent souvent à quel point leurs systèmes sont redondants et tolérants aux pannes, mais vous devez quand même faire preuve de diligence raisonnable. Un fournisseur de cloud s'engagera à rétablir l'accès à vos services cloud conformément aux accords de niveau de service, mais bien souvent il n'ira pas jusqu'à garantir l'intégrité de vos données ou à endosser la responsabilité en cas de pertes de données. La plupart des fournisseurs de cloud vous laissent la responsabilité de prendre des mesures pour assurer le niveau de sécurité, la protection et la sauvegarde appropriés de vos données.

CONSEIL : ne partez pas du principe que vos données sont à l'abri dans le cloud simplement parce que le service a été conçu pour être durable à 99,999999999 %. Il ne s'agit pas d'un accord de niveau de service et cela ne garantit ni la disponibilité, ni l'accès à vos données. Il est donc important d'avoir toujours des copies de sauvegarde de vos données sensibles dans un autre cloud ou localement sur une appliance de sauvegarde et de récupération des données pour les cas de pannes.

3. COMMENT SONT TRAITÉES VOS DONNÉES APRÈS LA CESSATION DU SERVICE ?

DIFFICULTÉ : le non-paiement n'est que l'une des raisons pour lesquelles votre fournisseur de cloud peut résilier votre contrat. Il peut aussi invoquer un manquement grave, le non-respect des politiques d'utilisation acceptables ou celui des droits de propriété intellectuelle. Le problème, c'est que l'action d'un seul utilisateur peut donner au fournisseur le droit de mettre fin à tout le service. Après une résiliation, de combien de temps disposez-vous pour récupérer vos données avant que le fournisseur de cloud ne les supprime ? Beaucoup de fournisseurs suppriment les données immédiatement ou peu de temps après, en général 30 jours plus tard.

CONSEIL : efforcez-vous de bien cerner ce qui peut être une cause de résiliation de contrat de service, surtout ce qui est défini comme des motifs valables. Négociez une période suffisante pour récupérer vos données à la résiliation du contrat, voire demandez d'être prévenu avant la suppression des données. Pensez également à garder des copies de sauvegarde dans un autre cloud ou dans une appliance locale de sauvegarde.

Avant de choisir la solution de cloud la mieux adaptée à vos données, effectuez une analyse complète des risques. Si vous réalisez que les risques sont si importants que de nombreux points du contrat doivent être négociés avant de pouvoir confier vos données à ce service cloud, c'est peut-être que ce cloud public n'est pas la meilleure solution pour ce type de données. Un cloud privé sur site ou une appliance locale de sauvegarde pourraient peut-être mieux convenir.

À PROPOS DE VERITAS TECHNOLOGIES LLC

Veritas Technologies LLC permet aux organisations d'exploiter au mieux leurs informations grâce à des solutions conçues pour les grands environnements complexes et hétérogènes. Veritas travaille aujourd'hui avec 86 % des entreprises du classement Fortune 500, améliorant la disponibilité et la visibilité de leurs données pour renforcer leur compétitivité.

Veritas (France) SAS
Tour Égée
17 avenue de l'Arche
92400 Courbevoie
France
Tél. : +33 1 70 82 92 92
www.veritas.com/fr

Vous trouverez sur notre site web les adresses et numéros de téléphone de nos agences locales.
https://www.veritas.com/about/contact.html

V0352FR 03/17