Le stockage dans le cloud

Par stockage dans le cloud ou stockage en ligne, on entend un espace de stockage accessible uniquement via Internet. Or, toutes les solutions de cloud ne se valent pas en termes de protection et de sécurité des données. Voici donc quelques règles à suivre pour protéger vos données stockées dans le cloud.

Pour vous protéger,

- **choisissez une solution de cloud adaptée.** Les services de cloud étrangers posent souvent des problèmes d'un point de vue de la protection des données.
- **renforcez la sécurité de votre compte.** Utilisez un mot de passe fort (https://www.ebas.ch/fr/4-proteger-les-acces-internet/) et activez si possible l'authentification à deux facteurs, comme pour l'e-banking.
- **ne transmettez vos données que de façon chiffrée.** Choisissez un service utilisant un mode de transmission chiffré (https).
- **chiffrez vos données avant de les stocker.** Il est difficile de s'assurer que les données sont effectivement chiffrées par le service de cloud. Mieux vaut donc le faire vous-même.
- **gardez une copie de vos données sur un support local.** Procédez régulièrement à des sauvegardes locales pour vos données stockées dans le cloud. En règle générale, il est impossible de vérifier que vos données sont correctement sauvegardées par le fournisseur du service.
- **protégez tous les dispositifs accédant aux données stockées dans le cloud.** Reportez-vous pour cela à nos « 5 règles pour votre sécurité numérique » (https://www.ebas.ch/fr/5-regles-pour-votre-securite-numerique/) .

Les services de cloud tels que Dropbox, iCloud, Securesafe ou Google Drive vous permettent de stocker vos données sur des serveurs centralisés via Internet. Dans la pratique, vous transférez ni plus ni moins vos données à des tiers. Cela pose donc naturellement des questions de sécurité et de protection des données.

Le pays du fournisseur de cloud

Le choix du epays du fournisseur de cloud est déterminant. À partir du moment où vos données sont stockées à l'étranger, elles sont soumises à une autre réglementation concernant la protection des données. Il faut savoir par ailleurs que nombre de données circulant sur Internet sont systématiquement enregistrées et analysées par les services de renseignements.

Au regard de la loi, le stockage et la conservation des données étant considérés comme une forme de traitement des données, ces services sont soumis eux aussi à la réglementation sur la protection des données.

Le recours aux services de cloud s'avère donc problématique lorsqu'il s'agit de stocker des données personnelles particulièrement sensibles de tiers. Selon le contexte, on peut facilement en arriver à enfreindre la loi locale sur la protection des données ou le règlement européen sur la protection des données (le fameux RGPD), ce dernier étant plus strict encore.

Sont considérées comme particulièrement sensibles, les données personnelles concernant :

- les convictions ou activités religieuses, philosophiques, politiques ou syndicales.
- la santé, la sphère intime ou l'appartenance ethnique.

- les mesures d'aide sociale.
- les poursuites et les sanctions administratives ou pénales.

Afin d'éviter tout conflit potentiel avec la loi sur la protection des données, préférez toujours les fournisseurs suisses.

La sécurisation du compte

L'accès à votre espace de stockage en ligne se fait *via* le navigateur, en vous connectant à votre compte depuis la page d'accueil de votre fournisseur, ou grâce à un programme (ou une application) précédemment installé sur votre dispositif, et qui vous permet d'accéder au service.

L'accès représente donc un point crucial car un mot de passe faible laisse le champ libre aux hackers potentiels. Il convient donc d'appliquer absolument nos 6 règles pour créer un mot de passe fort (https://www.ebas.ch/fr/4-proteger-les-acces-internet/) . Afin de mieux sécuriser l'accès à votre compte, préférez si possible l'authentification à deux facteurs, comme pour les services d'e-banking.

Si vous utilisez un smartphone ou une tablette pour accéder à vos données, leur sécurité en cas de perte ou de vol de l'appareil dépend de la manière dont vous avez sécurisé l'accès à votre dispositif et au service de cloud. Plus d'informations à ce sujet sont disponibles ici (https://www.ebas.ch/fr/4-proteger-les-acces-internet/) . De même, l'accès via des réseaux non sécurisés – comme certains réseaux wifi (https://www.ebas.ch/fr/les-reseaux-sans-fil-wifi-wlan/) par exemple – représente un risque non négligeable.

Une transmission sécurisée des données

Choisissez un service qui transmette vos données sous forme chiffrée afin d'empêcher tout accès non autorisé par des personnes tiers pendant leur transfert.

Dans votre navigateur, vous pouvez vous en assurer en vérifiant la présence au début de la barre d'adresse de « https:// » et l'affichage du symbole du cadenas (https://www.ebas.ch/fr/le-controle-du-certificat/) . Si vous utilisez un programme ou une application pour accéder à votre espace de stockage, vous devez vérifier dans les paramètres que la transmission des données est bien chiffrée.

Un stockage sécurisé des données

En stockant vos données sur le nuage, vous les confiez en pratique à des tiers. C'est pour cette raison qu'il convient d'accorder une attention toute particulière à la protection et au chiffrement des données.

Les principales solutions de cloud offrent aujourd'hui la possibilité de stocker les données sous une forme chiffrée. Si le fonctionnement est généralement simple et pratique, la fiabilité du système est en revanche difficile à vérifier. La méthode la plus sûre est donc de prendre en charge vous-même le cryptage et le décryptage de vos données, au moins pour les données sensibles.

Une sauvegarde correcte

Difficile aussi de vérifier la bonne sauvegarde des données par le fournisseur de cloud... Mieux vaut donc effectuer vous-même des sauvegardes locales régulières des données que vous stockez en ligne. Pour en savoir plus, cliquez ici (https://www.ebas.ch/fr/1-sauvegarder-les-donnees/) .

Des dispositifs sûrs

La présence d'un logiciel malveillant sur votre dispositif met également en danger les données que vous stockez en ligne. Reportez-vous pour cela à nos « 5 règles pour votre sécurité numérique » (https://www.ebas.ch/fr/5-regles-pour-votre-securite-numerique/) .

Les services de cloud

Il existe une foule de fournisseurs de cloud dans le monde. Voici quelques exemples :

Services de cloud étrangers :

- Dropbox (https://www.dropbox.com)
- Google Drive (https://www.google.com/drive)
- Apple iCloud (https://www.apple.com/chde/icloud)
- Microsoft OneDrive (https://onedrive.live.com)

Solutions de cloud avec stockage des données en Suisse :

- MyDrive (https://www.mydrive.ch)
- Securesafe (https://www.securesafe.com)
- Speicherbox (https://www.speicherbox.ch)

Le stockage dans le cloud ou stockage en ligne consiste en une sauvegarde des données sur des serveurs centralisés via l'Internet public. L'avantage ? Économiser les espaces de stockage locaux et permettre l'accès aux données stockées depuis n'importe quel lieu et n'importe quel dispositif connecté, même simultanément.

Mais la transmission de données personnelles à des tiers comporte parfois des problèmes de sécurité et pose la question de la protection de ces données. Le choix de la solution de cloud est donc décisif.