

# Bien choisir son hébergement et son cloud

Localisation des données, réversibilité, sauvegardes : les questions à poser avant de signer.

10 min de lecture · Niveau Intermédiaire · [cyberionis.fr/ressources/choisir-hebergement-cloud](https://cyberionis.fr/ressources/choisir-hebergement-cloud)

Externaliser dans le cloud ne fait pas disparaître votre responsabilité : vous restez comptable de vos données vis-à-vis de vos clients et du RGPD. Le bon choix d'hébergement se joue sur quelques critères concrets, avant la signature.

## 1. Les questions à poser au prestataire

- Où sont physiquement stockées les données ? (Un hébergement en France ou dans l'UE simplifie la conformité RGPD)
- Quelles sauvegardes sont incluses, avec quelle fréquence et quelle durée de rétention ?
- Quel engagement de disponibilité (SLA) et quelles compensations en cas de panne ?
- Comment récupère-t-on ses données si l'on part ? (réversibilité, formats standards, frais de sortie)
- Quelles certifications ? (ISO 27001, HDS pour les données de santé, SecNumCloud pour le plus sensible)

## 2. Le partage des responsabilités

En cloud, la sécurité est partagée : le fournisseur sécurise l'infrastructure, vous restez responsable de la configuration, des comptes, des droits d'accès et de vos données. La majorité des fuites de données « cloud » proviennent d'erreurs de configuration côté client, pas du fournisseur.

- MFA sur tous les comptes d'administration cloud
- Chiffrement des données sensibles
- Sauvegardes indépendantes du fournisseur pour les données critiques
- Alertes de facturation pour détecter les dérives (ou les usages frauduleux)

## 3. Souveraineté et dépendance

Selon la sensibilité de votre activité, la question du droit applicable aux données (Cloud Act américain vs hébergeurs européens comme OVHcloud ou Scaleway) et celle de la dépendance à un fournisseur unique méritent d'être posées dès le départ — il est bien plus coûteux d'y répondre après la migration.

## 4. Migrer sans se rater

- Commencer par le moins critique : le site web ou un outil secondaire essuie les plâtres, pas la facturation
- Migrer avec un double-run : l'ancien système reste opérationnel jusqu'à validation complète du nouveau
- Tester la charge et les sauvegardes AVANT la bascule, pas après
- Documenter la nouvelle architecture au fil de l'eau : comptes, configurations, dépendances
- Prévoir la formation des équipes — la meilleure migration échoue si personne ne sait s'en servir

- Négocier la réversibilité dès le contrat d'entrée : c'est au moment où le fournisseur veut vous gagner qu'on obtient les meilleures conditions de sortie

#### BON À SAVOIR

*Le coût du cloud se pilote : dimensionnez au réel (pas « au cas où »), éteignez les environnements de test la nuit, activez les alertes de facturation dès le premier jour, et faites une revue trimestrielle des ressources — les machines oubliées qui tournent pour rien sont LE grand classique de la facture cloud qui enfle.*

---

## L'essentiel à retenir

- 01 Vérifier la localisation des données et la conformité RGPD
- 02 Lire le SLA et les conditions de réversibilité avant de signer
- 03 Activer la MFA sur tous les accès d'administration
- 04 Conserver une sauvegarde des données critiques hors du fournisseur
- 05 Activer les alertes de facturation dès le premier jour
- 06 Documenter la configuration pour ne pas dépendre d'une seule personne

## Questions fréquentes

### Cloud ou serveur dans nos locaux : comment trancher ?

Le serveur local garde du sens pour des besoins spécifiques (gros volumes locaux, logiciel métier ancien, connexion Internet fragile) — à condition d'assumer ce qui va avec : sauvegardes, redondance, sécurité physique, maintenance. Pour la plupart des TPE/PME, le cloud offre un niveau de résilience impossible à égaler en interne à budget équivalent. La vraie question n'est pas idéologique : c'est « qui assure les sauvegardes, la disponibilité et la sécurité, et pour combien ? »

### Un hébergeur français est-il obligatoire pour être conforme RGPD ?

Non : le RGPD demande un hébergement UE ou un mécanisme de transfert valide, pas un drapeau français. Un hébergeur européen simplifie l'analyse (pas de question de droit extraterritorial américain) ; un hébergeur américain avec datacenters UE reste possible via les mécanismes en vigueur, mais votre analyse doit suivre leurs évolutions juridiques. Pour les données sensibles ou le secteur public, les qualifications type SecNumCloud tranchent le débat.

### Le fournisseur cloud sauvegarde déjà — pourquoi sauvegarder encore ?

Ses sauvegardes le protègent LUI (panne de son infrastructure), pas VOUS : elles ne couvrent généralement ni votre suppression accidentelle au-delà d'une courte rétention, ni le piratage de votre compte, ni sa défaillance commerciale. La règle : pour toute donnée critique, une sauvegarde que vous contrôlez, hors du fournisseur. Même Microsoft recommande une sauvegarde tierce de Microsoft 365.

### Comment éviter d'être prisonnier d'un fournisseur (vendor lock-in) ?

Privilégier les formats et standards ouverts, documenter l'architecture, éviter de bâtir le cœur du métier sur des services propriétaires sans équivalent, et tester réellement l'export des données une fois par an. Le lock-in n'est pas toujours un mal absolu (les services intégrés font gagner du temps) — mais il doit être un choix conscient et chiffré, pas une découverte au moment de partir.

## Pour aller plus loin

ANSSI — SecNumCloud et les offres qualifiées — [cyber.gouv.fr/produits-services-qualifies](https://cyber.gouv.fr/produits-services-qualifies)

CNIL — l'informatique en nuage — [www.cnil.fr/fr/definition/cloud-computing](https://www.cnil.fr/fr/definition/cloud-computing)

### Un projet cloud ou d'infrastructure ?

Choix, migration, sécurisation, supervision : Cyberionis conçoit des infrastructures sobres et qui durent.  
[contact@cyberionis.fr](mailto:contact@cyberionis.fr) · 06 64 90 07 74 · [cyberionis.fr](https://cyberionis.fr)