Qui détient les clés de vos données ?

Trois niveaux de chiffrement : ce que chacun protège, et ce qu'il coûte

	1. Clé gérée par le fournisseur le chiffrement par défaut	2. Clé gérée par vous, chez lui dans son service de clés	3. Clé détenue hors du fournisseur gestionnaire externe ou chiffrement avant l'envoi
Qui détient la clé ?	Le fournisseur, de bout en bout.	Vous la gérez (renouvellement, révocation, journaux), mais elle reste chez lui.	Vous, ou un tiers que vous choisissez.
Le fournisseur peut-il lire ?	Oui, techniquement.	Oui, techniquement : la clé est dans son infrastructure.	Pas sans votre clé, que vous pouvez lui refuser.
Face à une réquisition	Il peut livrer vos données en clair.	Pas de vraie protection juridique : il garde l'accès à la clé.	Sans votre accord, il ne peut livrer que du chiffré, hors noms de fichiers, destinataires et dates.
Ce que ça coûte	Rien : c'est inclus.	Un peu d'administration, et le risque de tout bloquer si la clé est révoquée par erreur.	Des fonctions en moins (recherche, aperçus, intelligence artificielle), un service de clés à tenir : s'il tombe, vos données sont inaccessibles.
Pour quelles données ?	Publiques et internes.	Restreintes, quand vous voulez maîtriser la clé.	Confidentielles, quand la loi d'un pays étranger est un risque réel.

La bonne question

Pas « un administrateur peut-il accéder ? », mais : est-ce que je le sais, est-ce que je peux le refuser, et en ai-je la trace ?

Les accès du personnel

Exigez des journaux des accès du fournisseur et, pour le plus sensible, votre accord préalable. Les grands fournisseurs le proposent sur certaines offres.

La clé ne protège pas tout

Elle protège la confidentialité, pas la disponibilité. Si le service s'arrête, seule une sauvegarde chez un tiers vous sauve.