



Cloud Act — *Risques*

Analysez l'exposition de votre infrastructure aux lois extraterritoriales américaines.

Cloud Act (2018)

FISA 702 · EO 12333

SecNumCloud

Le lieu de stockage ne suffit pas. Ce qui détermine l'exposition, c'est la **juridiction du fournisseur** : toute entité soumise au droit américain — maison mère, filiale ou technologie sous licence — peut être contrainte de livrer vos données, où qu'elles soient hébergées.

REPÈRES

Critère = juridiction, pas localisation

FISA 702 prolongé (2024)

Test du « contrôle » de la maison mère

DPF ≠ bouclier (appel CJUE, oct. 2025)

EXPOSITION PAR SCÉNARIO D'HÉBERGEMENT

SCÉNARIO D'HÉBERGEMENT	POURQUOI C'EST (OU NON) EXPOSÉ	RISQUE
Hyperscaler US, région US AWS / Azure / GCP, données aux États-Unis	Fournisseur sous juridiction US et données sur le sol américain : accès direct (Cloud Act, FISA 702, EO 12333).	Élevé
Hyperscaler US, région UE Mêmes acteurs, données en Europe	Le critère est la juridiction du fournisseur, pas le lieu de stockage : la maison mère US reste contraignable.	Élevé
Filiale « souveraine » d'un groupe US Entité UE dédiée (ex. AWS European Sovereign Cloud)	La séparation opérationnelle n'annule pas l'obligation légale de la maison mère US (test du « contrôle »).	Élevé
« Cloud de confiance » sous licence US Techno US opérée par une entité UE (ex. Bleu, S3NS)	Opéré par une société UE pour viser l'immunité, mais s'appuie sur une technologie sous licence US : protection réelle débattue.	Modéré
Fournisseur 100 % UE Aucun lien capitalistique ni opérationnel avec les US	Hors juridiction américaine : ni le Cloud Act ni FISA 702 ne s'appliquent.	Faible
Fournisseur UE qualifié SecNumCloud Qualification ANSSI (v3.2)	Droit européen exclusif, lois extraterritoriales contractuellement exclues : effet bouclier visé.	Faible



MESURE TECHNIQUE : LE CHIFFREMENT À CLÉS MAÎTRISÉES

L'EDPB (reco. 01/2020) retient le **chiffrement avec des clés détenues hors de l'infrastructure du fournisseur** comme mesure de référence. Il réduit fortement l'exposition — mais ne l'annule pas si le prestataire peut être contraint et a accès aux clés.



DEUX IDÉES REÇUES À ÉCARTER

« **Mes données sont en Europe, donc protégées** » : une région UE d'un acteur US reste exposée via sa maison mère. « **Le Data Privacy Framework me couvre** » : le DPF ne neutralise ni le Cloud Act ni FISA 702, et il est contesté (appel devant la CJUE le 31 oct. 2025) — un « Schrems III » est jugé probable.

Cartographier votre exposition ?

Le Coq Numérique audite vos dépendances cloud et trace un plan de souveraineté.

[Voir nos ressources →](#)



Le Coq Numérique

www.lecoqnumerique.fr/ressources

Sources : ANSSI (SecNumCloud) · EDPB · CNIL · RGPD.
Document informatif — ne se substitue pas à un avis juridique.