AYI NEDJIMI Consultants

Souveraineté Cloud : Protéger les Données Sensibles en

Catégorie : Cloud Security Lecture : 11 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet souveraineté cloud : CLOUD Act, FISA 702, Schrems II, SecNumCloud 3.2, EUCS, offres souveraines françaises (OVHcloud, Scaleway.

2.1 CLOUD Act : quand le droit américain s'applique partout

Le **Clarifying Lawful Overseas Use of Data Act** (CLOUD Act), adopté en mars 2018, est la pierre angulaire du problème de souveraineté. Cette loi permet aux autorités américaines (FBI, DOJ, agences fédérales) d'exiger la production de données détenues par un fournisseur cloud américain, **indépendamment de la localisation géographique des données**. En clair : si vos données sont hébergées chez AWS dans la région eu-west-3 (Paris), le gouvernement américain peut légalement contraindre Amazon à les transmettre via un mandat ou une assignation. Guide complet souveraineté cloud : CLOUD Act, FISA 702, Schrems II, SecNumCloud 3.2, EUCS, offres souveraines françaises (OVHcloud, Scaleway. Ce guide couvre les aspects essentiels de souverainete cloud donnees sensibles france : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

Les implications sont considérables :

- **Extraterritorialité absolue** : la localisation des données (France, Allemagne, Japon) est juridiquement sans effet. Seule compte la nationalité du fournisseur cloud.
- **Gag orders** : les autorités peuvent exiger la confidentialité de la demande d'accès. Le fournisseur cloud ne peut pas informer son client que ses données ont été saisies.
- **Périmètre large** : couvre les données de contenu (emails, fichiers, bases de données) ET les métadonnées (logs, journaux d'accès, informations de connexion).
- **Pas de limite aux données personnelles** : couvre également les données commerciales, les secrets industriels, la propriété intellectuelle.

Le CLOUD Act prévoit un mécanisme de contestation (« motion to quash ») que le fournisseur cloud peut invoquer si la demande crée un conflit avec le droit étranger. En pratique, cette protection est **largement illusoire** : Microsoft a publiquement déclaré n'avoir jamais réussi à bloquer une demande CLOUD Act pour un client non-américain. Le rapport de transparence 2025 de Google indique que 94 % des demandes CLOUD Act sont honorées dans un délai de 30 jours.

2.2 FISA Section 702 : la surveillance de masse des non-Américains

La **Section 702 du Foreign Intelligence Surveillance Act** est encore plus préoccupante que le CLOUD Act. Renouvelée en avril 2024 jusqu'en 2026, cette loi autorise la NSA à collecter massivement les communications de non-Américains à des fins de renseignement, **sans mandat individuel**. Les programmes de surveillance PRISM et Upstream opèrent sous cette autorité légale.

Contrairement au CLOUD Act qui nécessite une procédure judiciaire (même expéditive), FISA 702 opère via des **directives secrètes** émises par la Foreign Intelligence Surveillance Court (FISC), un tribunal secret dont les décisions ne sont pas publiées. Les fournisseurs cloud américains sont légalement contraints de coopérer et n'ont aucun moyen de s'y opposer publiquement.

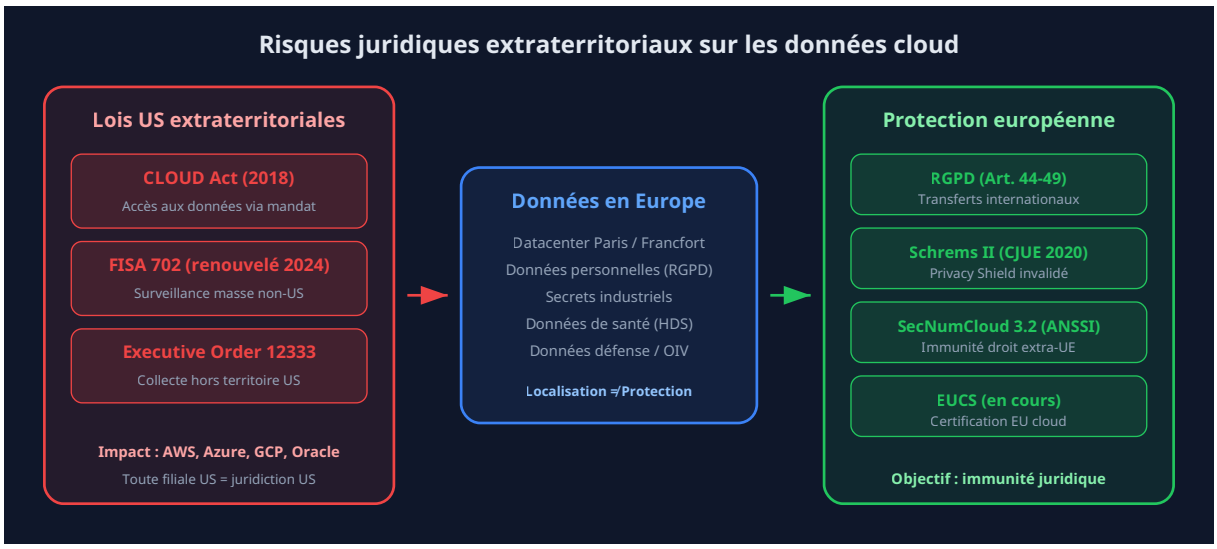
C'est précisément FISA 702 qui a motivé la **décision Schrems II** de la CJUE. La Cour a estimé que le niveau de surveillance autorisé par cette loi était incompatible avec les droits fondamentaux garantis par la Charte européenne (articles 7 et 8 : respect de la vie privée et protection des données personnelles). Le chiffrement des données, même avec des clés gérées par le client, ne constitue pas une garantie suffisante : les autorités américaines peuvent exiger les clés de déchiffrement ou contraindre le fournisseur à implémenter des backdoors.

2.3 Schrems II et le Data Privacy Framework

Notre avis d'expert
La sécurité cloud-native nécessite un changement de paradigme complet. Les outils et approches conçus pour les data centers traditionnels ne fonctionnent pas dans un monde de microservices, d'infrastructure as code et de déploiement continu. Il faut repenser la sécurité pour l'agilité.

L'arrêt **Schrems II** (CJUE, 16 juillet 2020, C-311/18) a invalidé le Privacy Shield et imposé aux organisations européennes de vérifier, au cas par cas, que le pays destinataire offre un niveau de protection « essentiellement équivalent » au droit européen avant tout transfert de données personnelles. Pour les États-Unis, la Cour a conclu que cette équivalence n'existait pas, en raison de FISA 702.

Le **Data Privacy Framework** (DPF), adopté par la Commission européenne en juillet 2023, tente de résoudre ce problème en s'appuyant sur un décret présidentiel américain (Executive Order 14086) qui encadre l'accès aux données européennes par les agences de renseignement. Cependant, un décret présidentiel peut être révoqué par le président suivant -- il n'a pas la force contraignante d'une loi. L'association noyb de Max Schrems a déjà déposé un recours devant la CJUE, et de nombreux juristes considèrent un arrêt « Schrems III » comme inévitable.



Le débat central autour de l'EUCS concerne le **niveau High** et les exigences de souveraineté. La France, soutenue par l'Italie et l'Espagne, pousse pour inclure des exigences d'immunité au droit extra-européen similaires à SecNumCloud 3.2. L'Allemagne, les Pays-Bas et les pays nordiques s'y opposent, arguant que cela exclurait les hyperscalers américains et créerait un protectionnisme technologique. En 2026, le compromis n'est toujours pas trouvé -- le niveau High de l'EUCS pourrait inclure une exigence de « localisation et contrôle européens » sans aller jusqu'au critère capitalistique de SecNumCloud.

3.3 HDS, NIS 2 et DORA : exigences sectorielles

Au-delà de SecNumCloud, plusieurs réglementations sectorielles imposent des contraintes spécifiques sur l'hébergement cloud :

Réglementation	Secteur	Exigences cloud	Statut 2026
HDS (Hébergeur de Données de Santé)	Santé	Certification HDS obligatoire, hébergement en France, auditabilité	Applicable, révision en cours
NIS 2	Entités essentielles et importantes	Gestion des risques supply chain cloud, notification incidents 24h	Transposition en cours
DORA	Secteur financier	Registre des prestataires ICT, tests de résilience, stratégie multi-cloud	Applicable depuis jan. 2025
RGPD	Toutes organisations	TIA obligatoire pour transferts hors UE, mesures supplémentaires	Applicable, sanctions renforcées
LPM / IGI 1300	Défense, OIV	Cloud qualifié SecNumCloud obligatoire pour données Diffusion Restreinte	Applicable

La doctrine « Cloud au centre » de l'État français (circulaire du Premier ministre, 2021, actualisée en 2023) impose l'utilisation de **cloud qualifié SecNumCloud** pour les données de sensibilité « diffusion restreinte » et supérieure. Les administrations et les opérateurs d'importance vitale (OIV) sont les premiers concernés, mais la tendance s'étend progressivement au secteur privé via NIS 2 et les attentes des donneurs d'ordre publics.

Le **contrôle des clés de chiffrement** est le pilier technique de la souveraineté cloud. Sans contrôle des clés, le chiffrement n'offre aucune protection contre un fournisseur contraint de coopérer avec une autorité étrangère. Trois modèles sont possibles :

- **Provider-Managed Keys (PMK)** : le fournisseur cloud gère les clés. Aucune souveraineté -- le provider peut déchiffrer à tout moment. Acceptable uniquement pour les données C0.
- **Customer-Managed Keys (CMK)** : le client apporte ses propres clés dans le KMS du cloud (BYOK). Le client contrôle la rotation et la révocation, mais le provider a accès à la clé en mémoire lors du déchiffrement.
- **Hold Your Own Key (HYOK) / External KMS** : la clé ne quitte jamais le HSM du client. Le cloud effectue les appels de chiffrement/déchiffrement vers le KMS externe. Souveraineté maximale mais impact performance et compatibilité limitée avec certains services managés.

```
# Architecture HYOK avec Thales CipherTrust Manager
# Le HSM Thales contrôle les clés, le cloud ne les voit jamais

# 1. Configuration CipherTrust Manager (on-prem ou cloud souverain)
ciphertrust_manager:
  hsm_partition: "souverain-prod"
  key_policy:
    exportable: false          # Clé non-exportable
    rotation_period: "90d"
    allowed_operations:
      - encrypt
      - decrypt
      - wrap
      - unwrap

# 2. Intégration avec le cloud via External Key Manager
# Pour GCP (Cloud EKM) :
gcloud kms ekm-connections create sovereign-ekm \
  --location=europe-west9 \
  --service-directory-service="projects/my-proj/locations/europe-west9/namespaces/ekm/
services/ciphertrust" \
  --hostname="ciphertrust.sovereign.example.fr" \
  --server-certificates-pem-file=ciphertrust-cert.pem

# 3. Création d'une clé externe
gcloud kms keys create sovereign-key \
  --keyring=sovereign-ring \
  --location=europe-west9 \
  --purpose=encryption \
  --protection-level=external \
  --external-key-uri="ciphertrust://keyid/sovereign-prod-aes256"
```

5.3 Réseau et localisation des données

La **localisation des données** est une exigence réglementaire pour certaines catégories (santé HDS, données Diffusion Restreinte) et une bonne pratique de souveraineté pour toutes les données sensibles. Au-delà du stockage, la localisation concerne également le transit réseau : les données ne doivent pas transiter par des infrastructures hors UE, même temporairement.

- **Résidence des données** : choisir des régions cloud françaises (Paris, Marseille) ou européennes. Configurer les *data residency controls* (GCP Organization Policy, Azure Policy, AWS SCP) pour interdire le déploiement de ressources hors régions autorisées.
- **Backbone réseau** : vérifier que le backbone du fournisseur ne fait pas transiter les données par des points de présence hors UE. Les interconnexions privées (AWS Direct Connect, Azure ExpressRoute, GCP Cloud Interconnect) offrent un contrôle du chemin réseau.
- **DNS souverain** : utiliser des résolveurs DNS européens pour éviter les fuites de métadonnées vers des serveurs DNS américains.

6. Migration vers un cloud souverain

6.1 Évaluation et cartographie préalable

La migration vers un cloud souverain commence par un **inventaire exhaustif** des workloads et données existants. Pour chaque application, il faut évaluer :

- **Sensibilité des données** : classification C0 à C3 selon la matrice définie.
- **Dépendances techniques** : services managés utilisés (bases de données, IA/ML, serverless), APIs propriétaires, intégrations tierces.
- **Contraintes réglementaires** : obligation HDS, LPM, RGPD, NIS 2, DORA selon le secteur.
- **Criticité métier** : impact en cas d'indisponibilité, RTO/RPO requis.
- **Coût de migration** : effort de refactoring, tests, formation des équipes.

Cette évaluation permet de construire une **matrice de décision** qui identifie les workloads candidats à la migration souveraine (données C2-C3, contraintes réglementaires fortes) et ceux qui peuvent rester sur des clouds non qualifiés (données C0-C1, applications non critiques).

6.2 Stratégies de migration

Quatre stratégies de migration sont envisageables, en fonction de la complexité et des dépendances de chaque workload :

Stratégie	Description	Complexité	Cas d'usage
Rehost (Lift & Shift)	Migration à l'identique vers IaaS souverain	Faible	VMs, workloads legacy, bases de données IaaS
Replatform	Adaptation minimale pour exploiter les PaaS souverains	Moyenne	Conteneurisation Kubernetes, bases managées
Refactor	Réécriture pour éliminer les dépendances propriétaires	Élevée	Applications utilisant des services propriétaires (Lambda, Cosmos DB)
Hybride	Données sensibles en souverain, compute sur hyperscaler	Variable	Applications nécessitant des services IA/ML avancés

6.3 Éviter le vendor lock-in

La souveraineté implique la **réversibilité** : la capacité de changer de fournisseur cloud sans perte de données ni interruption majeure. Pour minimiser le vendor lock-in :

- **Conteneurisation** : empaqueter les applications dans des conteneurs Docker/OCI, orchestrés par Kubernetes. Kubernetes est disponible sur tous les clouds et fournisseurs souverains.
- **APIs ouvertes** : privilégier les APIs S3-compatible pour le stockage objet, PostgreSQL/MySQL pour les bases de données, plutôt que les services propriétaires (DynamoDB, Cosmos DB).
- **Infrastructure as Code** : utiliser Terraform/OpenTofu avec des modules abstraits qui encapsulent les différences entre fournisseurs.
- **Formats ouverts** : stocker les données dans des formats ouverts (Parquet, Avro, JSON) plutôt que des formats propriétaires.
- **Clause de réversibilité contractuelle** : exiger du fournisseur un plan de réversibilité documenté avec un SLA d'assistance à la migration sortante.

7. Cas d'usage sectoriels

7.1 Santé : HDS et données de santé

Le secteur de la santé est le plus avancé en matière d'exigences de souveraineté cloud en France. La certification **HDS (Hébergeur de Données de Santé)** est obligatoire pour tout hébergement de données de santé à caractère personnel. En 2026, la convergence entre HDS et SecNumCloud se précise : l'ANSSI travaille à un référentiel unifié qui intègrerait les exigences HDS dans le périmètre SecNumCloud, simplifiant la conformité pour les établissements de santé.

Les cas d'usage critiques incluent le **Health Data Hub** (entrepôt national de données de santé), qui a été contraint de migrer depuis Microsoft Azure vers une infrastructure souveraine suite à une décision du Conseil d'État. Les hôpitaux et les GHT (Groupements Hospitaliers de Territoire) migrent progressivement vers des clouds HDS+SecNumCloud pour le dossier patient informatisé (DPI), l'imagerie médicale et les entrepôts de données cliniques.

7.2 Secteur financier : DORA et résilience

Le règlement **DORA**, applicable depuis janvier 2025, impose aux entités financières une gestion rigoureuse des prestataires ICT cloud. Les banques et assurances françaises sont tenues de maintenir un **registre d'information** détaillé de leurs prestataires cloud, d'évaluer les risques de concentration (dépendance excessive à un seul provider) et de disposer d'une **stratégie de sortie** documentée pour chaque prestataire critique. La tendance est à la diversification multi-cloud avec au moins un fournisseur souverain qualifié pour les workloads les plus sensibles (systèmes de paiement, données KYC, reporting réglementaire).

7.3 Secteur public et défense

Le secteur public français est le principal moteur de la demande de cloud souverain. La **doctrine « Cloud au centre »** impose l'utilisation de cloud qualifié SecNumCloud pour toutes les données de sensibilité « diffusion restreinte » et supérieure. Les ministères, les collectivités territoriales et les établissements publics migrent progressivement vers des offres souveraines, avec une priorité donnée aux applications de gestion RH, financière et aux systèmes d'information critiques.

Pour la **défense et les OIV**, les exigences sont encore plus strictes : cloud privé dédié, homologation spécifique, personnel habilité, infrastructure physiquement isolée. Le ministère des Armées développe son propre cloud de défense, tandis que les OIV s'appuient sur des offres SecNumCloud renforcées par des mesures de sécurité physique et organisationnelle supplémentaires.

8. Perspectives et recommandations

8.1 Tendances 2026-2028

Plusieurs tendances structurantes se dessinent pour les années à venir :

- **IA souveraine** : l'entraînement et l'inférence de modèles d'IA sur des données sensibles deviennent un cas d'usage majeur pour le cloud souverain. Les offres GPU souveraines (OVHcloud AI, NumSpot) se développent pour répondre à cette demande.
- **Edge souverain** : la souveraineté s'étend au edge computing, avec des micro-datacenters qualifiés déployés au plus près des utilisateurs (hôpitaux, usines, bases militaires).
- **Certification EUCS** : l'adoption du schéma européen, même avec un compromis sur le niveau High, harmonisera les exigences et facilitera le marché unique du cloud sécurisé.
- **Consolidation du marché** : le nombre de fournisseurs souverains se réduira par consolidation, avec l'émergence de 3 à 5 champions européens capables de rivaliser en fonctionnalités avec les hyperscalers.

8.2 Recommandations pratiques

Checklist souveraineté cloud

- **Classifier vos données** : identifier les données C2-C3 qui nécessitent un hébergement souverain. Ne pas tout migrer aveuglément.

- **Réaliser une TIA** (Transfer Impact Assessment) : évaluer les risques juridiques pour chaque transfert de données vers un cloud non européen.
- **Contrôler vos clés** : implémenter un modèle CMK ou HYOK pour les données sensibles. Le chiffrement sans contrôle des clés est illusoire.
- **Planifier la réversibilité** : conteneuriser, utiliser des APIs ouvertes, prévoir contractuellement la migration sortante.
- **Surveiller la conformité** : auditer régulièrement la posture cloud (CSPM), vérifier la localisation effective des données, monitorer les accès.
- **Former les équipes** : la souveraineté est aussi un enjeu humain. Les équipes doivent comprendre les enjeux juridiques et techniques.
- **Suivre l'évolution réglementaire** : EUCS, NIS 2, révision HDS -- le cadre évolue rapidement et impacte les choix d'hébergement.

Pour approfondir ce sujet, consultez notre outil open-source azure-sentinel-rules qui facilite les règles de détection Azure Sentinel.

Questions frequentes

Comment mettre en place Souveraineté Cloud dans un environnement de production ?

La mise en place de Souveraineté Cloud en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi Souveraineté Cloud est-il essentiel pour la securite des systemes d'information ?

Souveraineté Cloud constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Quelles sont les bonnes pratiques pour Souveraineté Cloud en 2026 ?

Les bonnes pratiques pour Souveraineté Cloud en 2026 incluent l'adoption d'une approche Zero Trust, l'automatisation des controles de securite, la mise en place d'une veille continue sur les vulnerabilites et l'integration des recommandations des organismes de reference comme l'ANSSI et le NIST.

Sources et références : CISA · Cloud Security Alliance

Points clés à retenir

- 6. Migration vers un cloud souverain
- 7. Cas d'usage sectoriels
- 8. Perspectives et recommandations
- Questions frequentes
- 9. Conclusion

9. Conclusion

La souveraineté cloud n'est ni un fantasme protectionniste ni un luxe réservé aux administrations. C'est une **nécessité stratégique** pour toute organisation manipulant des données sensibles dans un contexte géopolitique où l'extraterritorialité juridique américaine constitue un risque documenté et croissant. Le cadre réglementaire français et européen (SecNumCloud, EUCS, NIS 2, DORA) fournit des repères clairs, et l'écosystème des offres souveraines a atteint en 2026 un niveau de maturité suffisant pour répondre à la majorité des cas d'usage.

L'approche pragmatique recommandée est le **cloud hybride à géométrie variable** : héberger les données selon leur classification, en utilisant le cloud souverain qualifié pour les données sensibles et les hyperscalers (avec des mesures de protection appropriées) pour les workloads non critiques. Cette stratégie optimise le rapport protection/coût tout en préparant l'organisation à l'évolution inéluctable vers un renforcement des exigences de souveraineté. Dans un contexte où les données sont le nouvel actif stratégique, leur protection juridique et technique est un investissement, pas une contrainte.

Références et ressources externes

- ANSSI SecNumCloud — Référentiel et liste des prestataires qualifiés
- ENISA Cloud Security — Schéma de certification européen EUCS
- CNIL — Clauses contractuelles types — Cadre juridique pour les transferts hors UE
- Légifrance — Textes réglementaires français (LPM, Code de la santé publique)
- DINUM — Doctrine Cloud au centre — Stratégie cloud de l'État français

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr