

À L'ATTENTION DES RSSI, DPO ET RESPONSABLES CONFORMITÉ

La souveraineté des données est une architecture, pas une clause contractuelle

Vos données. Votre juridiction. Votre contrôle.

Le défi

La France est allée plus loin que presque tout autre État européen dans l'imposition de la souveraineté numérique, et le niveau d'exigence en matière de conformité continue de s'élever. Une commission d'enquête parlementaire, ouverte le 10 mars 2026 et conduite par le député Philippe Latombe, a établi que 93 % du cloud public utilisé en France est hébergé par AWS, Azure ou Google Cloud – ce qui signifie que les données des administrations, des hôpitaux et des collectivités locales, y compris les dossiers médicaux, les données fiscales et les fichiers de police, reposent majoritairement sur une infrastructure contrôlée par les États-Unis. Les questions centrales de cette commission sont désormais celles auxquelles toute organisation régulée en France doit pouvoir répondre : où les données sont-elles physiquement hébergées, les clauses contractuelles permettent-elles un rapatriement en cas de crise géopolitique, et les modèles tarifaires créent-ils un verrouillage technologique ?

Au-delà de cette commission d'enquête, la doctrine fondatrice de souveraineté française, « Cloud au Centre », impose aux administrations publiques, aux opérateurs d'importance vitale (OIV) et aux opérateurs de services essentiels (OSE) de recourir à des « clouds de confiance » certifiés selon le référentiel SecNumCloud 3.2 de l'ANSSI, lequel plafonne à 24 % la participation étrangère au capital, précisément pour empêcher qu'une entité de droit américain ne détienne un contrôle suffisant pour être contrainte de divulguer des données en vertu du CLOUD Act américain. En avril 2026, la DINUM (Direction interministérielle du numérique) a demandé à chaque ministère de produire un plan d'élimination des dépendances numériques non européennes d'ici l'automne 2026 – un mandat couvrant les systèmes d'exploitation, les outils collaboratifs, l'infrastructure cloud et l'IA, concernant environ 2,5 millions d'agents publics. Dans le cadre de la loi Informatique et Libertés et du contrôle exercé par la CNIL, les garanties contractuelles et la localisation des centres de données sur le territoire national ne suffisent plus à répondre à la question que se posent désormais les régulateurs, les législateurs et les acheteurs publics français : qui contrôle réellement l'infrastructure, et pouvez-vous le prouver ?

La solution

Kiteworks délivre la souveraineté des données comme une architecture, et non comme une clause contractuelle – exactement l'exigence qui sous-tend le plafond de participation étrangère de SecNumCloud et le mandat d'élimination des dépendances de la DINUM. Déployez votre infrastructure en mode mono-tenant, sur site, dans votre propre cloud, ou en tant que cloud privé hébergé par Kiteworks, en France ou dans la juridiction de votre choix, chiffrée avec des clés que vous seul détenez. Parce qu'aucun client Kiteworks ne partage d'infrastructure, d'environnements d'exécution ni d'accès au plan de contrôle avec un autre client, et parce que Kiteworks ne détient jamais vos clés de chiffrement, cette architecture reflète le même principe que le plafond de participation étrangère de SecNumCloud : la souveraineté se définit par qui contrôle les données et l'infrastructure qui les traite, et non simplement par l'emplacement d'un centre de données.

Gouvernez chaque envoi, chaque partage et chaque téléchargement grâce aux règles de géo-restriction du Data Policy Engine, appliquées en temps réel sur l'ensemble des canaux. Démontrez-le grâce à une piste d'audit complète et sans limitation, transmise en direct à votre SIEM, avec des options d'hébergement évaluées FedRAMP et IRAP – le type de preuve concrète et en temps réel que la CNIL, l'ANSSI et la commission Latombe poussent désormais les organisations françaises à produire.

Pourquoi la souveraineté est désormais un enjeu de conseil d'administration en France

33 %	des organisations ont subi un incident de souveraineté au cours de la dernière année.
6,11 Md€	d'amendes RGPD cumulées à l'échelle de l'UE à ce jour.
93 %	du cloud public français est hébergé par AWS, Azure ou Google Cloud – commission d'enquête parlementaire française, 2026.
Automne 2026	date limite pour que chaque ministère français soumette un plan d'élimination des dépendances numériques non européennes.

Comment Kiteworks délivre une souveraineté que vous pouvez prouver

■ Mono-tenant par conception

Infrastructure dédiée, sans bases de données, systèmes de fichiers, environnements d'exécution applicatifs ni systèmes d'exploitation partagés. Déployez sur site, dans votre propre cloud, ou en tant que cloud privé mono-tenant hébergé par Kiteworks, en France ou dans la juridiction de votre choix.

■ Clés de chiffrement détenues par le client

Grâce à l'intégration HSM, ni Kiteworks ni aucune partie cherchant à contraindre Kiteworks ne peut déchiffrer vos données – la même logique que celle qui sous-tend le plafond de 24 % de participation étrangère de SecNumCloud, appliquée au niveau de la détention des clés.

■ Contrôle de sortie par géo-restriction

Le Data Policy Engine bloque ou soumet à approbation les envois et partages, et peut bloquer purement et simplement les téléchargements, en fonction de la géolocalisation de l'utilisateur, des pays bloqués et des plages d'adresses IP.

■ Un seul plan de contrôle, pour tous les canaux

Le courrier électronique, le partage de fichiers, le SFTP, le MFT, les API et les agents d'IA sont tous régis par les mêmes politiques de sortie, de sorte qu'aucune brèche par canal ne permette aux données de s'échapper – répondant directement aux problématiques de verrouillage et de visibilité examinées par la commission Latombe.

■ Piste d'audit complète et sans limitation

Chaque action d'un utilisateur, d'un administrateur ou du système est enregistrée en temps réel et transmise en direct à votre SIEM, sans échantillonnage ni limitation en cas de forte charge.

■ Évaluée selon les référentiels gouvernementaux

FedRAMP High en cours de qualification, FedRAMP Moderate autorisé depuis 2017, et un hébergement évalué IRAP démontrent que l'architecture répond à des exigences de souveraineté de niveau gouvernemental – en complément, et non en remplacement, des offres de cloud souverain qualifiées SecNumCloud en France.

Copyright © 2026 Kiteworks. La mission de Kiteworks est de permettre aux organisations de gérer efficacement les risques liés à chaque envoi, partage, réception et utilisation de données privées. La plateforme Kiteworks offre aux clients un échange de données sécurisé qui assure la gouvernance, la conformité et la protection des données au sein d'un plan de contrôle unifié. Kiteworks unifie, suit, contrôle et sécurise les données sensibles circulant au sein, vers et en dehors de leur organisation, améliorant ainsi de façon significative la gestion des risques et garantissant la conformité réglementaire pour l'ensemble des échanges de données privées. Basée dans la Silicon Valley, Kiteworks protège plus de 100 millions d'utilisateurs finaux et des milliers d'entreprises et d'organismes publics dans le monde. protège plus de 100 millions d'utilisateurs finaux et des milliers d'entreprises et d'organismes publics dans le monde.

Où la souveraineté n'est pas négociable en France



Administration publique

Données des citoyens relevant du mandat de la DINUM imposant à chaque ministère un plan d'élimination des dépendances non européennes, et des exigences de la doctrine « Cloud au Centre » en matière de contrôle démontrable et localisé sur le territoire.



Défense et opérateurs critiques (OIV/OSE)

Données régies par le référentiel SecNumCloud 3.2 de l'ANSSI et par la loi de programmation militaire française, pour les opérateurs d'importance vitale et les opérateurs de services essentiels tenus de recourir à des « clouds de confiance ».



Services financiers

Données clients relevant du règlement européen sur la résilience opérationnelle numérique (DORA) et des lignes directrices de supervision de la CNIL.



Santé et sciences de la vie

Données des patients relevant du RGPD et des réglementations nationales sur les données de santé, ainsi que données de recherche soumises à des conditions de résidence.

Copyright © 2026 Kiteworks. La mission de Kiteworks est de permettre aux organisations de gérer efficacement les risques liés à chaque envoi, partage, réception et utilisation de données privées. La plateforme Kiteworks offre aux clients un échange de données sécurisé qui assure la gouvernance, la conformité et la protection des données au sein d'un plan de contrôle unifié. Kiteworks unifie, suit, contrôle et sécurise les données sensibles circulant au sein, vers et en dehors de leur organisation, améliorant ainsi de façon significative la gestion des risques et garantissant la conformité réglementaire pour l'ensemble des échanges de données privées. Basée dans la Silicon Valley, Kiteworks protège plus de 100 millions d'utilisateurs finaux et des milliers d'entreprises et d'organismes publics dans le monde. protège plus de 100 millions d'utilisateurs finaux et des milliers d'entreprises et d'organismes publics dans le monde.