Risques liés à la sécurité des données et à la conformité en 2026 : Souveraineté des données en Europe

Même Le marché le plus réglementé au monde découvre encore que les contrats ne prévalent pas sur la loi — et que l'architecture reste la meilleure protection.

L'Europe dispose de l'écosystème de souveraineté des données le plus mature au monde. **Le RGPD a fixé la norme mondiale. NIS 2 et DORA renforcent les exigences en matière de résilience opérationnelle. Le Data Act est entré en vigueur en septembre 2025, suivi des obligations des modèles d'IA à usage général (GPAI) prévues par l'AI Act européen en août 2025.** Les organisations européennes se distinguent par le plus haut niveau de compréhension parmi les pays interrogés : 80 % se disent « bien » ou « très bien » informées des enjeux liés aux exigences en matière de souveraineté.

Mais la maturité n'a pas éliminé le risque. Un tiers des répondants européens ont subi un incident lié à la souveraineté au cours des 12 derniers mois. Le problème de confiance envers les fournisseurs persiste : 44 % évoquent des inquiétudes concernant les garanties de souveraineté des fournisseurs, freinant l'adoption de solutions cloud européennes. Les évolutions géopolitiques — notamment les changements de politique aux États-Unis — ravivent des questions que l'arrêt Schrems II était censé avoir tranchées depuis des années. Ce résumé synthétise les principaux enseignements européens d'une enquête menée au Canada, au Moyen-Orient et en Europe.

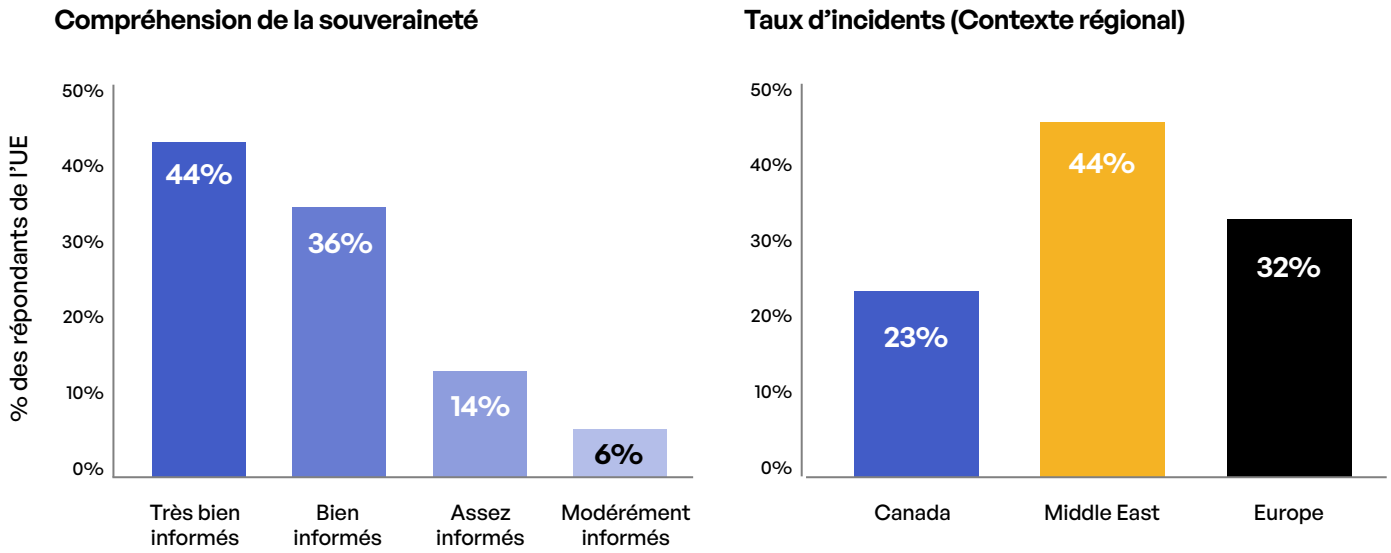
44% **des organisations européennes interrogées mettent en avant leurs inquiétudes liées aux garanties de souveraineté des fournisseurs comme un frein — le niveau le plus élevé de toutes les régions étudiées, remettant en cause l'idée selon laquelle « il suffit d'utiliser des centres de données situés dans l'union européens ».**

La maturité réglementaire n'a pas permit de combler l'écart en matière d' incidents

La compréhension des enjeux de la souveraineté en Europe est solide et largement partagée. 44 % se disent « très bien informés », 36 % « bien informés », seuls 6 % se situant au niveau le plus bas. La conformité au RGPD est quasi universelle. **La préparation à NIS 2 et DORA est bien avancée, la plupart des organisations étant en « phase de mise en oeuvre » ou « principalement conformes ».**

Et pourtant, 32,3 % des répondants européens ont été confrontés à un incident de souveraineté l'an dernier — un taux supérieur à celui du Canada (23,3 %), mais inférieur à celui du Moyen-Orient (44,4 %). Les incidents les plus fréquents sont les transferts transfrontaliers non autorisés, investigations des autorités de régulation, violations de données ayant des implications en matière de souveraineté et défaillances de conformité chez des prestataires ou partenaires tiers. Le message est clair : la maturité réglementaire réduit, mais n'élimine pas les incidents. L'écart restant est d'ordre opérationnel, non pas un manque d'information—et le combler exige une architecture adaptée, pas par davantage de campagnes de sensibilisation.

La maturité réglementaire en Europe n'a pas éliminé les incidents — un tiers des répondants en signale encore un



Niveau de compréhension de la souveraineté parmi les répondants européens (à gauche) et taux d'incidents dans le contexte régional (à droite)

L'intérêt business : la souveraineté comme atout concurrentiel européen

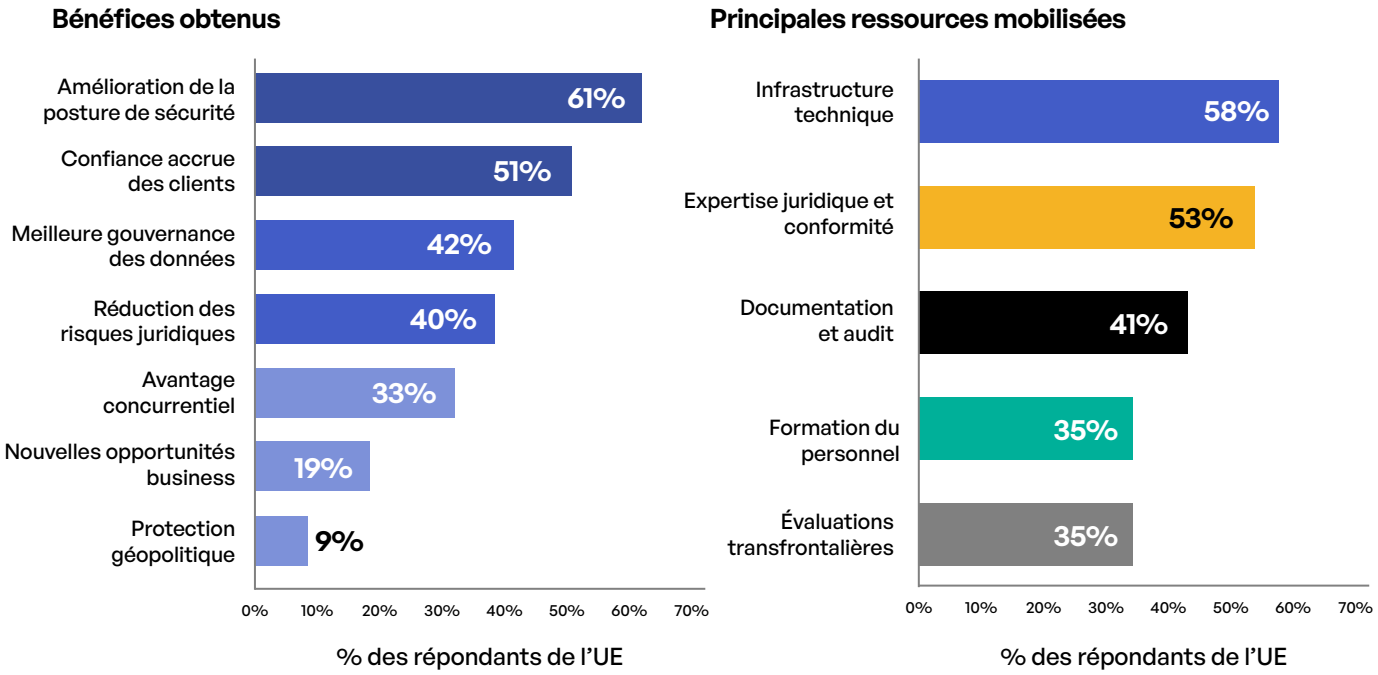
Les participants européens à l'étude associent la souveraineté à une véritable valeur ajoutée. **L'amélioration de la posture de sécurité arrive en tête (61 %), suivie par la confiance accrue des clients (51 %), une meilleure gouvernance des données (42 %), la réduction des risques juridiques (40 %) et l'avantage concurrentiel (33 %).** Ces données mettent en avant la souveraineté non comme une contrainte réglementaire, mais comme un facteur de différenciation sur un marché européen sensible à la réglementation.

Le déficit de confiance envers les fournisseurs : le défi majeur de la souveraineté en Europe

84% des répondants signalent leurs inquiétudes face à la capacité réelle de leurs fournisseurs cloud à garantir la souveraineté. Les aveux de grands fournisseurs américains sur les limites d'accès aux données ont transformé ce sujet en problème concret. L'arrêt Schrems a confirmé que les engagements contractuels ne peuvent pas neutraliser les législations étrangères. La conséquence est structurelle : les organisations européennes ne peuvent pas déléguer leur souveraineté à la seule garantie d'un fournisseur. Elles ont besoin de contrôles au niveau de l'architecture — conservation des clés de chiffrement au sein de la juridiction locale , politiques d'accès appliquées au niveau de la couche infrastructure, et journaux d'audit prouvant la localisation des données et l'identité des personnes y ayant accédé.

Les ressources nécessaires à mettre en place restent toutefois conséquentes. Les évolutions de l'infrastructure technique arrivent en tête (58 %), devant le renforcement de l'expertise juridique et conformité (53 %) ainsi que la documentation et de l'audit (41 %). Côté budget, 28 % des répondants européens déclarent consacrer plus de 5 millions d'euros par an à la souveraineté, et 31 % entre 1 et 5 millions d'euros. Parmi les organisations de plus de 10 000 salariés, plus de 70 % figurent parmi les plus haut niveaux de dépenses .Les investissements se concentrent sur les domaines de contrôle mesurable : maîtrise de la localisation des données, garde des clés de chiffrement, automatisation des politiques d'accès et journaux d'audit exportables pour répondre aux exigences des régulateurs et des clients entreprises.

La souveraineté génère une valeur business claire — à un coût opérationnel conséquent



La conformité souveraineté un vrai avantage commercial(à gauche) principales ressources mobilisées (à droite)

Le rapport coût-bénéfice est favorable aux organisations qui considèrent la souveraineté comme une discipline opérationnelle continue, et non comme un projet ponctuel de conformité. L'automatisation constitue le principal levier d'efficacité — 55 % prévoient d'investir dans l'automatisation de la conformité dans les deux prochaines années, ce qui en fait la stratégie la plus citée dans la région.

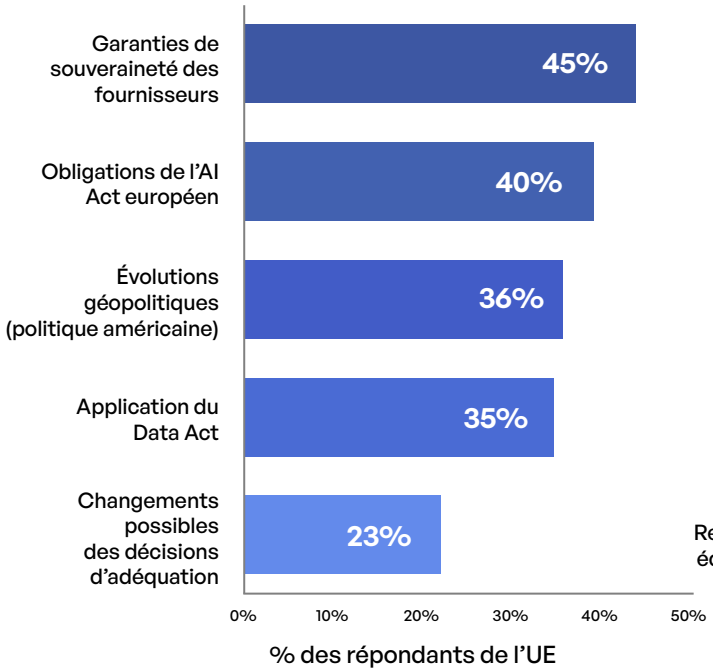
Un environnement sous tension : complexité réglementaire et incertitudes quand aux garanties des prestataires

Le risque autour de la souveraineté en Europe est particulièrement complexe, car il est superposé. **Les garanties de souveraineté des fournisseurs (44 %), l'AI Act européen (40 %), les évolutions de la politique américaine (36 %), la conformité au Data Act (34 %) et les possibles changements concernant les décisions d'adéquation (23 %) exigent une attention soutenue.** Aucune autre région affronte autant de fronts réglementaires à la fois.

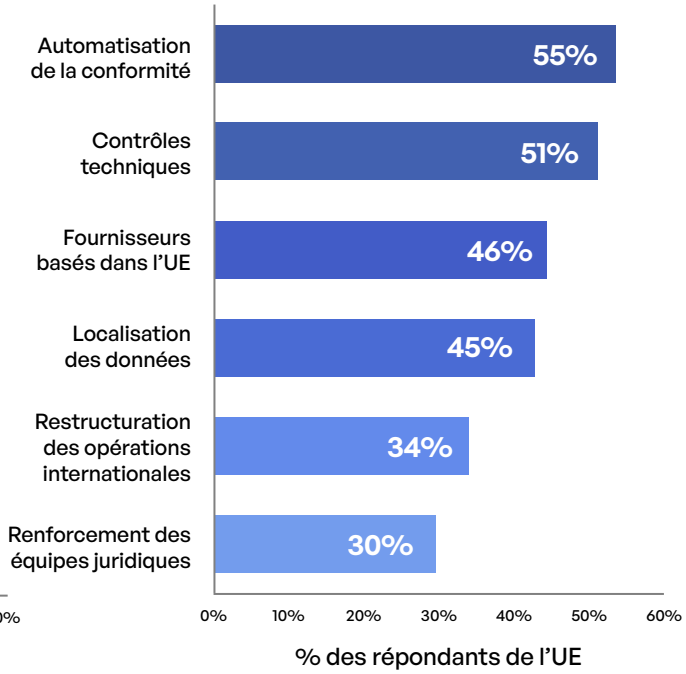
Les plans d'action reflètent cette complexité. L'automatisation de la conformité arrive en tête (55 %), suivie du renforcement des contrôles techniques (51 %), migration vers des fournisseurs européens (46 %), localisation des données (45 %), restructuration des opérations internationales (34 %) et du renforcement des équipes juridiques (30 %). Les organisations européennes ne réagissent pas à une menace unique — elles mettent en place des défenses multicouches pour répondre à une réglementation elle-même stratifiée. Les organisations qui réussiront seront celles qui intègrent la souveraineté dans leur architecture, plutôt que de l'ajouter à posteriori à une infrastructure existante par de simples seule politiques.

La superposition réglementaire et le déficit de confiance envers les fournisseurs définissent l'agenda de la souveraineté en Europe

Principales préoccupations et obstacles



Stratégies prévues pour les deux prochaines années



Principales préoccupations et obstacles (à gauche) stratégies souveraineté prévues pour les deux prochaines années (à droite)

Gouvernance de l'IA : se préparer à l'AI Act sous contrainte de souveraineté

34 % des répondants européens conservent toutes leurs données d'entraînement IA dans l'UE, et 34 % adoptent une approche mixte selon la sensibilité des données. Les mesures de protection sont largement adoptées : audits réguliers de l'IA en tête, suivis d'analyses d'impact pour les IA à haut risque (48 %), documentation relative aux obligations de transparence, gestion du consentement et évaluation des biais.

Les obligations GPAI de l'AI Act européen, entrées en vigueur en août 2025, ont formalisé ce que de nombreuses organisations mettaient déjà en place. Mais les 34 % qui utilisent une approche mixte doivent désormais renforcer leur classification de sensibilité, maintenant que l'application des règles est entrée en vigueur— « se baser sur la sensibilité » ne constitue pas un standard défendable si les critères de classification ne sont ni documentés ni auditables. Les organisations doivent s'assurer que la gouvernance des données IA s'inscrivent pleinement dans leur cadre global de démonstration de souveraineté, avec une documentation immédiatement prête pour des audits ou dans le cadre de GDPR.

Une souveraineté démontrable : la norme européenne

Les réglementations européennes exigent de plus en plus des preuves, et non de simples déclarations. On passe du « nous pensons être conformes » au « nous pouvons prouver où sont les données, comment les accès sont gérés, et les mécanismes permettant de visualiser. Les mouvements transfrontaliers sont existants». Cela implique trois éléments. Contrôle effectif de la localisation de données, maîtrise des clés de chiffrement et politiques d'accès empêchant les mouvements transfrontaliers non autorisés au niveau de l'architecture. Preuves : journaux d'audit exportables, logs de localisation des données et rapport de conformité sur la demande pour satisfaire régulateurs et clients. Capacité de réponse : des procédures testées pour les demandes d'accès aux données émanant des autorités publiques, en cas de défaillances de fournisseurs tiers, Transfer Impact Assessments (TIA) et scénarios de conformité Schrems II. Les organisations qui intègrent ces trois volets transforment la complexité réglementaire en avantage concurrentiel solide et crédible.

Cinq priorités pour 2026

1. Réduire l'écart de confiance vis à vis des fournisseurs par des choix d'architecture, pplutôt que par des mécanismes contractuels.

44% signalent des inquiétudes sur les garanties fournisseurs. La réponse n'est pas dans la promesse des fournisseurs — mais la conservation des clés de chiffrement dans la juridiction, des contrôles d'accès appliqués au niveau infrastructure et une localisation des données vérifiable. Les contrats ne peuvent pas primer sur la loi ; seule l'architecture permet de l'appliquer.

2. Prioritiser l'automatisation des processus de conformité pour absorber la complexité réglementaire.

55% l'envisagent déjà. Avec le Data Act et l'AI Act désormais en vigueur aux côtés de NIS 2 et DORA, la conformité manuelle devient ingérable à long terme. L'automatisation réduit la charge technique (58 %) tout en maintenant le niveau de preuve exigé par les régulateurs.

3. Se préparer dès maintenant aux obligations GPAI de l'AI Act.

40% citent l'AI Act comme une préoccupation majeure. Les organisations ayant anticipé en localisant leur données d'entrainement d'IA et mis en place des audits réguliers avant l'entrée en vigueur des obligations réglementaires sont en avance . Celles qui élaborent encore leur politique de données IA sont déjà en retard.

4. Elaborer et tester des plprocédures opérationelles relatives à Schrems II et aux demandes d'accès gouvernemental.

36% citent les évolutions géopolitiques comme une préoccupation. Les Transfer Impact Assessments doivent être à jour, le recours au DPF/ clauses contractuelles documentées SCC, et la réponse aux incidents de transfert transfrontalier doit être répétée — pas seulement planifiée.

5. Valoriser la souveraineté comme un atout stratégique auprès des clients

51% citent la 4 of 4 confiance accrue comme bénéfice et 33 % l'avantage concurrentiel. Sur un marché européen sensible à la réglementation, la capacité à démontrer la souveraineté à tout moment — via des preuves tangibles , et non de simples documents de politique — devient un prérequis pour les appels d'offres entreprises.

Kiteworks apporte une réponse concrète aux exigences de souveraineté des données

Selon ce rapport l'enjeu majeur de la souveraineté en Europe est la confiance vis-à-vis des fournisseurs un enjeu central— 44 % des participants évoquent des inquiétudes sur la capacité réelle de leurs fournisseurs cloud à garantir la souveraineté, et l'arrêt Schrems II a confirmé que les contrats ne peuvent pas prévaloir sur les lois étrangères. Le Réseau de données privé (Private Data Network) de Kiteworks est conçu pour combler ce déficit. Ses options de déploiement — sur site, cloud privé, hybride ou en hébergement dédié en single tenant — permettent aux organisations

de stocker leurs contenus sensibles exclusivement dans des infrastructures européennes, ndépendamment des fournisseurs dont le siège est aux Etats-Unis soumis au CLOUD Act. Kiteworks assure la conservation des clés de chiffrement dans la juridiction concernée , appliquant les mecanismes de géorepérage via des contrôles IP configurables et déploie une architecture zéro trust sur tous les canaux de communication : messagerie électronique, partage sécurisé de fichiers, transfert sécurisé de fichiers, SFTP et formulaires de données.

Sur un marché où le Data Act, l'AI Act, NIS 2 et DORA sont désormais tous en vigueur simultanément, Kiteworks propose des contrôles de conformité unifiés grâce à des journaux d'audit centralisés, un reporting automatisé et des modèles préconfigurés pour le RGPD, DORA, NIS 2 et PCI DSS. Ses journaux d'audit immuables fournissent les preuves exportables qui permettent e changement de paradigme: « nous pensons être conformes » au « nous pouvons prouver où sont les données, comment les accès sont gérés et comment les mouvements transfrontaliers sont empêchés ». Dans un environnement européen où les réglementations se superposent , cette capacité de démonstration transforme la souveraineté d'une contrainte de conformité en un avantage concurrentiel défendable.

Pour le rapport complet avec la méthodologie détaillée, les répartitions par secteur et l'analyse régionale, téléchargez-le maintenant.

Télécharger le rapport

Kiteworks