AYI NEDJIMI Consultants

Cloud Compliance : Guide RGPD, HDS et SecNumCloud 2026

Catégorie : Cloud Security Lecture : 9 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide conformité cloud complet : exigences RGPD hébergement données UE, certification HDS santé, qualification SecNumCloud ANSSI et directive NIS 2.

La conformité réglementaire dans le cloud est devenue un enjeu stratégique majeur pour les organisations européennes en 2026. Le renforcement continu du cadre réglementaire, avec le RGPD appliqué depuis huit ans, la directive NIS 2 entrée en vigueur, la certification HDS renforcée et la qualification SecNumCloud de l'ANSSI en pleine expansion, crée un environnement juridique exigeant que chaque architecte cloud et responsable sécurité doit maîtriser. La complexité est amplifiée par la dimension multi-cloud : les obligations de conformité s'appliquent indépendamment du provider choisi, mais les mécanismes techniques d'implémentation varient significativement entre AWS, Azure et GCP. Les enjeux ne sont plus uniquement techniques mais aussi géopolitiques, avec la question de la souveraineté numérique et de l'immunité aux législations extraterritoriales qui influence directement le choix des providers et des architectures. Ce guide détaille chaque cadre réglementaire applicable, les exigences techniques correspondantes et les stratégies d'implémentation pragmatiques pour atteindre et maintenir la conformité dans les environnements cloud publics.

Résumé exécutif

Guide de conformité cloud complet : exigences RGPD, certification HDS, qualification SecNumCloud, directive NIS 2 et stratégies d'implémentation pour les environnements cloud publics AWS, Azure et GCP.

Retour d'expérience : nous avons accompagné un établissement de santé dans sa migration vers Azure avec certification HDS. Le projet a nécessité neuf mois de travail incluant l'audit de l'architecture existante, la définition du schéma de classification des données, la mise en place du chiffrement avec BYOK, la configuration des contrôles d'accès renforcés et la documentation de conformité. Le coût de la non-conformité (amendes CNIL potentielles, perte de la certification HDS, risque réputationnel) dépassait largement l'investissement de mise en conformité, estimé à moins de cinq pour cent du budget cloud annuel. Face à la complexité croissante des environnements cloud hybrides et multi-cloud, les organisations doivent adopter des stratégies de sécurité adaptées aux spécificités de chaque fournisseur tout en maintenant une cohérence globale. Les équipes sécurité sont confrontées à des défis inédits : surfaces d'attaque dynamiques, configurations éphémères, gestion des identités à grande échelle et conformité réglementaire multi-juridictionnelle. Ce guide technique présente les approches éprouvées en environnement de production, les erreurs fréquentes à éviter et les stratégies de durcissement prioritaires. Chaque recommandation est issue de retours d'expérience concrets en entreprise et a été validée sur des architectures cloud de production à grande échelle.

Conformité RGPD dans le cloud : exigences et implémentation

Le **Règlement Général sur la Protection des Données** impose des obligations spécifiques lorsque des données personnelles sont traitées dans le cloud public. La première obligation est la *licéité du transfert* : les données personnelles de résidents européens doivent être traitées dans des conditions conformes au RGPD, ce qui inclut le choix de régions de stockage dans l'UE et l'évaluation de l'impact des législations extraterritoriales (Cloud Act américain notamment) sur les providers. Les **clauses contractuelles types** (SCC) encadrent les transferts hors UE mais leur suffisance est régulièrement remise en question par les autorités de protection des données.

L'implémentation technique du RGPD dans le cloud couvre la **cartographie des traitements** de données personnelles dans chaque service cloud (S3, RDS, Cosmos DB, BigQuery...), le **chiffrement** avec des clés contrôlées par le client via KMS (BYOK ou HYOK), la mise en oeuvre du **droit à l'effacement** avec des procédures de suppression vérifiables, la **pseudonymisation** et la **minimisation des données**, et la tenue d'un **registre des traitements** à jour. Les services de classification automatique des données comme *Amazon Macie*, *Azure Purview* et *Cloud DLP* facilitent l'identification des données personnelles dans les services cloud. Consultez ANSSI pour les engagements RGPD d'AWS et CIS Benchmarks pour la conformité Azure. Notre article sur Securite Aws Hardening Compte Services détaille les stratégies de chiffrement cloud. L'ANSSI fournit des recommandations complémentaires via Azure Defender for Cloud.

Certification HDS : hébergement de données de santé

La **certification HDS** (Hébergeur de Données de Santé) est obligatoire en France pour tout organisme hébergeant des données de santé à caractère personnel pour le compte de tiers. Elle couvre deux périmètres : l'hébergement d'infrastructure physique et l'hébergement infogéré. Les exigences techniques incluent la **sécurité physique** des datacenters (contrôle d'accès biométrique, vidéosurveillance, détection d'intrusion), la **gestion des accès** avec authentification forte et traçabilité complète, le **chiffrement** des données au repos et en transit, la **continuité d'activité** avec PRA/PCA documentés et testés, et la **notification des incidents** avec des délais de communication définis.

Les trois majors cloud providers disposent de la certification HDS pour leurs régions françaises et européennes. Cependant, la **responsabilité partagée** implique que la certification du provider ne couvre que l'infrastructure : le client doit mettre en oeuvre les contrôles de sécurité applicatifs, de gestion des accès et de protection des données conformes au référentiel HDS. La documentation de conformité doit démontrer la maîtrise de l'ensemble de la chaîne, depuis l'infrastructure certifiée du provider jusqu'aux contrôles applicatifs du client. Les audits HDS vérifient cette complétude et sanctionnent les lacunes dans la chaîne de responsabilité. Notre guide sur Cloud Logging Centralisation Monitoring détaille les aspects spécifiques de la sécurité Azure applicable à l'hébergement de données de santé.

Qualification SecNumCloud de l'ANSSI

La qualification *SecNumCloud* de l'ANSSI représente le niveau le plus élevé de certification de sécurité cloud en France. Elle impose des exigences techniques, organisationnelles et juridiques strictes qui vont au-delà des certifications internationales. Les exigences clés incluent la **localisation des données** exclusivement sur le territoire français, la **souveraineté capitalistique** de l'opérateur (contrôle majoritaire européen), l'**immunité aux législations extraterritoriales** (notamment le Cloud Act américain), des **contrôles de sécurité renforcés** alignés sur le niveau élevé de l'ISO 27001 avec des compléments spécifiques, et un processus d'**audit approfondi** par l'ANSSI.

En 2026, la qualification SecNumCloud est devenue un critère déterminant pour les marchés publics, les opérateurs d'importance vitale (OIV) et les opérateurs de services essentiels (OSE). La stratégie "Cloud au Centre" de l'État français impose SecNumCloud pour les données sensibles des administrations. Les offres qualifiées sont encore limitées : **3DS Outscale**, **OVHcloud** et **Scaleway** pour les providers français, avec des offres de "cloud de confiance" développées par Thales (S3NS avec Google) et Orange-Capgemini (Bleu avec Microsoft) en cours de qualification. L'architecture hybride combinant un cloud SecNumCloud pour les données sensibles avec un cloud hyperscaler pour les workloads non sensibles constitue l'approche pragmatique adoptée par la plupart des organisations concernées. Notre article sur Cnapp Protection Cloud Native Applications explore les stratégies de sécurité multi-cloud applicables à ces architectures hybrides. Les recommandations de Azure Defender for Cloud de l'ANSSI guident les choix architecturaux pour les organisations soumises à SecNumCloud.

Certification	Périmètre	Exigences clés	Obligatoire pour
RGPD	Données personnelles	Consentement, chiffrement, effacement, DPO	Toute organisation traitant des données UE
HDS	Données de santé	Certification ISO 27001+, continuité, notification	Hébergeurs de données de santé FR
SecNumCloud	Cloud souverain	Souveraineté, immunité extraterritoriale	OIV, OSE, administrations FR
NIS 2	Cybersécurité	Gouvernance risques, notification incidents, supply chain	Entités essentielles et importantes UE
PCI DSS	Données de paiement	Segmentation, chiffrement, monitoring, scan	Organisations traitant des paiements
SOC 2	Contrôles opérationnels	Sécurité, disponibilité, intégrité, confidentialité	Fournisseurs de services cloud

Directive NIS 2 et obligations cloud

La directive **NIS 2**, transposée dans les droits nationaux européens, élargit considérablement le périmètre des organisations soumises à des obligations de cybersécurité. Elle distingue les *entités essentielles* (énergie, transport, santé, finance, eau, infrastructure numérique) des *entités*

importantes (industrie manufacturière, services postaux, gestion des déchets, chimie, alimentation) avec des obligations différenciées. Les obligations communes incluent la **gouvernance des risques** avec une politique de sécurité documentée et approuvée par la direction, la **gestion des incidents** avec notification sous 24 heures pour l'alerte précoce et 72 heures pour le rapport détaillé, la **sécurité de la supply chain** incluant les fournisseurs cloud, et la **continuité d'activité** avec des plans testés régulièrement.

L'impact sur les environnements cloud est significatif. Les organisations soumises à NIS 2 doivent évaluer et documenter les risques liés à leur utilisation du cloud, inclure les cloud providers dans leur gestion des risques fournisseurs, mettre en place des mécanismes de détection et de réponse aux incidents dans les environnements cloud, et démontrer la capacité à maintenir les services essentiels en cas d'incident cloud. La **responsabilité de la direction** est engagée personnellement en cas de non-conformité, avec des amendes pouvant atteindre dix millions d'euros ou deux pour cent du chiffre d'affaires mondial. Notre guide sur Cspm Cloud Security Posture Management détaille les implications de NIS 2 pour la sécurité des organisations. Le Azure Defender for Cloud de l'ANSSI fournit les orientations nationales pour la transposition de NIS 2.

Mon avis : la superposition des cadres réglementaires (RGPD, HDS, SecNumCloud, NIS 2, PCI DSS) crée une complexité de conformité qui dépasse les capacités de la plupart des équipes de sécurité. L'automatisation de la vérification de conformité via les outils CSPM et les frameworks de compliance-as-code est devenue indispensable. Les organisations qui traitent la conformité comme un projet ponctuel plutôt qu'un processus continu se retrouvent systématiquement en difficulté lors des audits de renouvellement.

Comment assurer la conformité RGPD dans le cloud public ?

La conformité RGPD dans le cloud public requiert une approche structurée couvrant les dimensions juridique, organisationnelle et technique. **Dimension juridique** : formalisez les accords de traitement des données (DPA) avec chaque cloud provider, évaluez les transferts hors UE via des analyses d'impact de transfert (TIA), mettez en place les clauses contractuelles types pour les transferts nécessaires et documentez la base légale de chaque traitement. **Dimension organisationnelle** : nommez un DPO avec une expertise cloud, tenez un registre des traitements incluant les services cloud utilisés, définissez les procédures de réponse aux droits des personnes (accès, effacement, portabilité) et formez les équipes sur les spécificités RGPD dans le cloud. **Dimension technique** : choisissez des régions UE pour le stockage des données personnelles, chiffrez avec des clés contrôlées par le client (BYOK), activez les services de classification automatique des données, configurez le logging pour la traçabilité des accès et mettez en place des mécanismes d'effacement vérifiable. Notre article sur Gcp Security Bonnes Pratiques Audit 2026 fournit des recommandations complémentaires sur le chiffrement des données cloud.

Pourquoi la qualification SecNumCloud est-elle stratégique ?

La qualification SecNumCloud est devenue un enjeu stratégique qui dépasse la simple conformité technique pour plusieurs raisons. **Premièrement, l'obligation réglementaire** : la doctrine "Cloud au Centre" de l'État français et les orientations de l'ANSSI imposent SecNumCloud pour les données sensibles des administrations, des OIV et des OSE, créant un marché captif pour les offres qualifiées. **Deuxièmement, la confiance client** : dans les secteurs sensibles (santé, défense, finance), la qualification SecNumCloud est de plus en plus exigée dans les appels d'offres privés comme garantie de souveraineté et de sécurité. **Troisièmement, la protection juridique** : l'immunité aux législations extraterritoriales exigée par SecNumCloud protège les données contre les réquisitions judiciaires de pays tiers, un risque concret avec le Cloud Act américain et les lois équivalentes. **Quatrièmement, le positionnement concurrentiel** : les fournisseurs de services qualifiés SecNumCloud disposent d'un avantage différenciant sur un marché européen de plus en plus sensible à la souveraineté numérique. L'investissement dans la qualification SecNumCloud représente un choix stratégique à long terme pour les organisations qui opèrent dans l'écosystème de confiance français et européen.

Quelles sont les exigences HDS pour l'hébergement de données de santé ?

Les exigences HDS structurent la sécurité de l'hébergement de données de santé autour de six domaines complémentaires. La **sécurité physique** exige des datacenters avec contrôle d'accès multi-facteur, vidéosurveillance continue, détection d'intrusion et protection contre les risques environnementaux. La **gestion des accès** impose une authentification forte pour tous les accès administratifs, une traçabilité complète des opérations, une revue périodique des droits et une séparation des rôles. Le **chiffrement** doit couvrir les données au repos et en transit avec des algorithmes conformes aux recommandations de l'ANSSI et une gestion rigoureuse des clés. La **disponibilité** requiert un PRA/PCA documenté, testé annuellement et capable de restaurer les services dans les délais contractuels. La **notification des incidents** impose des délais de communication définis (à l'ARS dans les 24 heures pour les incidents graves) et une procédure de gestion des incidents documentée. La **réversibilité** garantit au client la possibilité de récupérer ses données dans un format exploitable en fin de contrat. L'ensemble de ces exigences doit être démontré lors de l'audit de certification, renouvelé tous les trois ans avec des audits de surveillance intermédiaires.

À retenir : la conformité cloud en France repose sur quatre piliers réglementaires : le RGPD pour les données personnelles, la certification HDS pour les données de santé, la qualification SecNumCloud pour la souveraineté et NIS 2 pour la cybersécurité des entités essentielles. L'automatisation de la vérification de conformité via le CSPM et la documentation continue des contrôles sont indispensables pour maintenir la conformité dans la durée.

Votre architecture cloud est-elle conforme aux exigences RGPD de localisation des données, ou des traitements de données personnelles s'effectuent-ils encore hors de l'Union européenne ?

Sources et références : CISA · Cloud Security Alliance

Perspectives et prochaines étapes

Le cadre réglementaire européen du cloud continue d'évoluer avec le schéma européen de certification de cybersécurité pour les services cloud (EUCS) en cours de finalisation, qui harmonisera les exigences de sécurité cloud au niveau européen. Les investissements dans les offres de cloud souverain se poursuivent avec l'émergence de solutions combinant les technologies des hyperscalers avec la gouvernance européenne. Les organisations doivent anticiper ces évolutions en structurant leur approche de conformité cloud sur des frameworks extensibles capables d'intégrer de nouvelles exigences sans refonte complète de leur architecture de contrôles.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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