

Souveraineté éducative : le coût caché de l'hébergement de vos contenus pédagogiques hors UE

CLOUD Act, FISA 702, Schrems II, SecNumCloud - pourquoi la localisation européenne ne suffit pas, et les quatre questions concrètes à poser à votre fournisseur cloud.

Guillaume Bouton - Cofondateur, directeur commercial, financier et innovation, ESSN SAS, Lyon

Où sont vraiment hébergés les contenus pédagogiques, les référentiels métier, les données apprenants, les copies d'évaluation et les enregistrements de classes virtuelles que produit votre organisme de formation ? Et qui peut, légalement, y accéder en dehors de votre contrôle ? La question revient à chaque appel d'offres public, à chaque audit Qualiopi sérieux, à chaque conversation avec un DPO conscient des dossiers en cours.

Beaucoup de directions de la formation répondent par deux raccourcis : « nos données sont en Europe » ou « notre fournisseur applique le RGPD ». Les deux réponses sont incomplètes au point d'être trompeuses. Voici pourquoi, et une grille concrète pour qualifier la souveraineté réelle d'un fournisseur cloud.

1. La localisation physique ne suffit plus depuis 2018

Le **CLOUD Act** américain - *Clarifying Lawful Overseas Use of Data Act*, loi H.R. 4943, adopté en mars 2018 - autorise les autorités fédérales américaines à exiger de toute entreprise relevant de leur juridiction la communication des données qu'elle stocke, que ces données soient physiquement situées aux États-Unis ou à l'étranger. Pour un OF hébergé chez un hyperscaler américain dont les datacenters sont à Francfort, Paris ou Dublin, la localisation européenne ne protège donc pas : le critère qui compte est la juridiction du fournisseur, pas l'emplacement du serveur.

À côté, la **Section 702 du Foreign Intelligence Surveillance Act (FISA 702)** autorise la surveillance ciblée de personnes non américaines situées hors des États-Unis, avec assistance obligatoire des fournisseurs. Elle a été renouvelée en avril 2024 par la loi *Reforming Intelligence and Securing America Act* (RISAA) pour deux ans, soit jusqu'en avril 2026. Combinés, ces deux textes exposent les contenus pédagogiques et les données apprenants d'un OF européen à une demande américaine, sans information préalable du responsable de traitement ni recours européen exploitable.

2. Schrems II : la porte rendue coûteuse à passer

L'arrêt **C-311/18 du 16 juillet 2020** - *Schrems II* - a invalidé la décision d'adéquation *Privacy Shield*, la CJUE estimant que le droit américain, notamment FISA 702, ne fournissait pas de protection essentiellement équivalente au RGPD. La Cour a maintenu les **clauses contractuelles types (CCT)**, mais avec une mise en garde : leur efficacité doit être évaluée au cas par cas pour chaque transfert. Un responsable de traitement ne peut se reposer sur la seule signature des CCT ; il doit conduire une analyse d'impact, déployer des mesures supplémentaires et tout documenter en cas de contrôle CNIL. La

documentation, le chiffrement bout en bout sans clé chez le fournisseur, la pseudonymisation forte et les audits récurrents finissent par effacer une grande partie du gain économique initial de l'hyperscaler.

3. SecNumCloud 3.2 : à quoi reconnaître un cloud réellement souverain

L'**ANSSI** publie depuis 2016 le référentiel **SecNumCloud**. Sa version courante, **3.2** (2022, mise à jour depuis), impose plus de **360 critères répartis sur 14 thèmes**, fondés sur l'ISO/IEC 27001 mais enrichis d'obligations prescriptives : durcissement, cloisonnement, authentification forte, chiffrement, audits PASSI, et surtout localisation des données dans l'UE assortie de garanties capitalistiques contre les lois extra-européennes.

Cette condition capitalistique distingue SecNumCloud des autres certifications : le prestataire ne doit pas être sous contrôle effectif d'une entité soumise à un droit extra-européen. Elle élimine de fait les hyperscalers américains du périmètre, même via des entités ou partenariats locaux - Microsoft-Bleu et Google-S3NS sont en cours de qualification, mais le débat reste ouvert. En mars 2026, l'ANSSI et le BSI allemand ont publié une déclaration commune posant les bases d'une doctrine franco-allemande harmonisée. Le marché du cloud souverain européen est estimé à 12,4 milliards d'euros en 2026, en croissance de 34 % sur un an.

« Le coût caché de l'hébergement hors UE n'est pas seulement juridique. Il est aussi opérationnel et stratégique : un OF qui pratique la commande publique ne peut pas indéfiniment expliquer à ses commanditaires qu'il dépend d'une chaîne d'hébergement soumise à un droit étranger. »

4. EUCS et NIS2 : ce que la réglementation prépare

L'**ENISA** développe depuis 2020 le schéma **EUCS** (*European Cybersecurity Certification Scheme for Cloud Services*), à quatre niveaux d'assurance. Il n'est pas encore adopté, bloqué depuis 2024 par le désaccord entre États voulant y intégrer des critères de souveraineté forts (dont la France) et ceux qui s'y opposent. En attendant, la **directive NIS2** (UE 2022/2555, transposition octobre 2024) et le **Data Act** (règlement UE 2023/2854, en vigueur depuis septembre 2025) permettent déjà d'exiger que les entités essentielles et importantes - dont une partie du secteur de la formation publique - s'appuient sur des fournisseurs certifiés EUCS une fois le schéma adopté. Pour un OF qui forme des publics relevant de la commande publique ou de secteurs régulés, ces évolutions arrivent dans la fenêtre 2026-2028.

5. Quatre questions concrètes à poser à votre fournisseur

1. Qui détient le capital de l'entité qui exploite le service ? Si une part significative relève du droit américain, le CLOUD Act s'applique, même contrat de droit français et datacenter à Paris. **2. Où sont localisées les opérations de support, maintenance et administration ?** Des accès root aux États-Unis ou en Inde rendent la donnée accessible depuis ces juridictions. **3. Le fournisseur est-il qualifié SecNumCloud 3.2, ou en cours documenté ?** La qualification vaut satisfaction de la condition capitalistique. **4. En cas de demande américaine, quel processus d'information du client ?** Le CLOUD Act prévoit des *gag orders* ; exigez les voies de recours activables. Une absence de réponse à plusieurs de ces questions est presque toujours disqualifiante.

Pour aller plus loin

Les alternatives existent : le cloud souverain européen est aujourd'hui assez mature pour accueillir l'essentiel des charges pédagogiques d'un OF - cours interactifs, évaluations, classes virtuelles, plateformes LMS. La question n'est pas technique, elle relève de la gouvernance d'achat et de la lecture des contrats. ESSN a fait dès sa création le choix d'une infrastructure 100 % européenne et de prestataires sous droit français ou européen, sans capital américain dominant. C'est le prérequis que nous portons avec le lancement d'U Hub, notre LCMS hébergé en France. Pour auditer votre propre chaîne d'hébergement avec les quatre questions ci-dessus, demandez la grille d'analyse complète.

Guillaume Bouton - Cofondateur, directeur commercial, financier et innovation, ESSN SAS. Cofondateur d'U Hub, LCMS hébergé en France, aligné sur le RGPD, NIS2 et l'article 50 du règlement IA (UE 2024/1689). Ingénieur commercial IT depuis 20 ans.

Tribune diffusée par E²SN dans le cadre du lancement de U Hub. Contact presse : contact@essn.fr