Cybersécurité dans le Cloud : Loi SREN vs EUCS ?

La Certification SecNumCloud menacée par la nouvelle version du Schéma Européen de Certification de Cybersécurité des Services Cloud ?

Protection des données de santé vs disparition des éléments de souveraineté dans la dernière version de l'EUCS

Eléonore SCARAMOZZINO, Avocate

constellation • law

SOMMAIRE

Cybersécurité dans le Cloud : Loi SREN vs EUCS ?

La Certification SecNumCloud menacée par la nouvelle version du Schéma Européen de Certification de Cybersécurité des Services Cloud ?

Protection des données de santé vs disparition des éléments de souveraineté dans la dernière version de l'EUCS

Par Eléonore Scaramozzino, Avocat, Constellation Avocats

Version du 20.04.2024

L'autorisation de la Cnil pour la création de l'entrepôt de données EMC2 dont les données du SNDS seront hébergées par Microsoft[i], se trouverait-elle confirmée par la dernière version du schéma européen de certification des services cloud, EUCS (European Union Cybersecurity Certification Scheme for Cloud Services) ? La version discutée le 15 et 16 avril par le groupe d'experts européen, dans son niveau d'exigences les plus élevé, a supprimé la sécurité juridique visant à protéger contre l'extraterritorialité des législations non européennes pour les données sensibles et stratégiques et leurs traitements associés. Cette suppression des éléments de souveraineté, qui n'a pas fait l'objet d'une communication officielle, intervient dans un contexte de prolongation du programme d'espionnage de la section 702 de la loi sur la surveillance du renseignement étranger (FISA). Comme l'avait jugé la Cour de Justice de l'Union européenne dans ses arrêts Schrems I[ii] et Schrems II[iii], cette section 702 permet à l'administration américaine d'accéder aux données des ressortissants européens sans mandat, hébergées chez les hyperscalers américains (Microsoft, Amazon, Google).

Afin d'éviter une fragmentation du marché intérieur, l'EUCS a pour vocation de se substituer aux certifications nationales (SecNumCloud pour la France, C5 en Allemagne) au sein de l'UE. En voulant

harmoniser la certification de la sécurité des services du Cloud, au nom du marché intérieur, et éviter la multiplication de souveraineté étatique pour le Cloud, qui conduirait à une fragmentation du marché intérieur, l'UE ne semble pas prendre la mesure des réels enjeux pour la souveraineté numérique européenne, pour la sécurité de ses data et le marché du cloud

Si la section 702 de la FISA reste pour les américains un outil efficace en matière de sécurité nationale, la souveraineté numérique doit rester pour l'Union Européenne, un instrument de protection pour ses données sensibles et stratégiques.

La discussion sur EUCS intervient en parallèle à l'adoption par le Parlement de la loi sur la Sécurité et la Régulation de l'Espace Numérique (SRNE). Les articles 31 et 32 (ex articles 10 Bis A et 10 Bis B) introduisent la certification SecNumCloud. A l'issue du passage devant le Conseil Constitutionnel, la loi sera notifiée à la Commission européenne qui devra se prononcer sur sa conformité avec la certification EUCS. Au cours du débat parlementaire, la Commission avait déjà émis des critiques sur sa compatibilité avec le droit européen, et tout particulièrement le Digital Service Act (DSA) [iv].

I- La loi SREN introduit des mesures protégeant les acteurs européens du Cloud

Le Parlement a adopté la loi SREN, qui anticipe certaines règles du règlement européen sur les données (Data Act)[v], entré en vigueur en janvier 2024 et applicable à partir de septembre 2025. Cette loi vise à renforcer la protection en ligne des citoyens et adapter le droit national aux récentes évolutions de la régulation européenne du domaine numérique, le DSA (Data Service Act[vi]) et le DMA (Digital Market Act ou règlement sur les marchés numériques[vii]). Sur le marché du cloud, elle ambitionne de restaurer l'équité commerciale et assurer l'interopérabilité des services sur ce marché. En effet, cette loi intègre notamment des dispositions **c**oncernant les fournisseurs de cloud et les entreprises de services cloud afin de limiter les pratiques anticoncurrentielles dans le secteur du cloud**.** Au cours du débat parlementaire, la loi SREN a été renforcée sur la sécurité de l'hébergement des données sensibles, dont les données de santé. Cependant, cette protection contre toute application extraterritoriale des lois extra-européennes, permettant l'accès des puissances étrangères, telles que les Etats-Unis avec la loi FISA, et la Chine, est menacée par les discussions sur **le projet de certification EUCS, pour European Union Cybersecurity Scheme for Cloud Services,** élaboré par l'ENISA, l'agence européenne pour la cybersécurité**.** La loi SNREM a fait l'objet d'une saisine du Conseil Constitutionnel.

Mesures pour la protection des acteurs européens du Cloud

Le titre 3 de la SREN, "installe des mesures importantes pour la protection des acteurs européens du Cloud, en s'attaquant à plusieurs pratiques déloyales des grands acteurs américains du Cloud. Ces mesures permettent de réduire la dépendance des organisations aux hyperscalers (Amazon, Micorsoft, Google). L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) est chargée de l'application de ces mesures.

La Loi SREN prévoit en effet de

Encadrer les frais de transfert et de migration des données entre les plateformes Cloud :	Concernant les frais de transfert, ils seront facturés **selon une tarification fixée par arrêté de la SENUM** après proposition de l'Arcep. Le non-respect de cette tarification pourra entraîner des amendes jusqu'à 3% du CA mondial, et jusqu'à 5% en cas de récidive. Les fournisseurs de cloud ne pourront plus facturer de frais de transfert de données supérieurs aux frais réels.
Obliger les services Cloud à être interopérables :	Les opérateurs de cloud devront garantir l'interopérabilité et la portabilité des données entre les différentes solutions concurrentes sur le marché. L'Arcep définira les règles à cet égard.
¨Plafonner les crédits Cloud**.**	Les avoirs commerciaux, utilisés par les entreprises pour fidéliser leurs clients et critiqués par certains comme moyen de captation de clientèle, **seront limités à un an maximum.**
Etre transparents sur les mesures prises pour empêcher l'accès illégal aux données de leurs clients.	Les fournisseurs de cloud devront également publier des informations relatives aux juridictions dont dépendent leurs infrastructures et décrire les mesures de protection mises en œuvre.

Mesures de sécurité complémentaires pour les données de santé

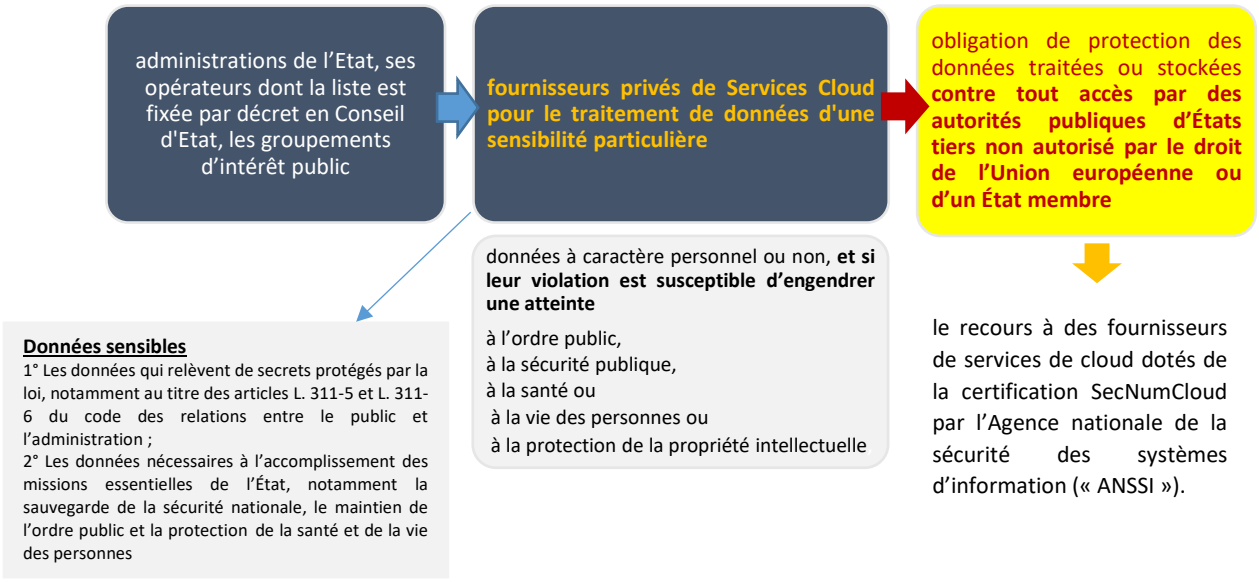
Le texte a été amendé par le Sénat et l'Assemblée nationale sur la question de l'hébergement des données sensibles. L'activité des **Sénateurs et des députés** a permis d'adopter, au chapitre III relatif à la protection des données stratégiques et sensibles sur le marché de l'informatique en nuage », deux

articles additionnels (article 10 bis A et article 10 bis B, devenu dans le texte final les articles 31 et 32) visant à renforcer les exigences de sécurité relatives à l'hébergement des données de santé.

Certification SecNumCloud pour l'hébergement des données sensibles par les administrations de l'Etat et leurs opérateurs

Article 31 (ex art 10Bis A)

création d'une obligation de stockage immunisé contre l'accès des autorités des puissances étrangères non autorisées



Apport de la CMP

Alors que le périmètre initial de cette disposition se limitait aux administrations de l'Etat et à leurs opérateurs, figurant dans la liste annexée au projet de loi de finances. Le texte de compromis élaboré lors de la Commission mixte paritaire étend désormais ce périmètre aux groupements d'intérêt public (GIP), qui exercent une mission d'intérêt général et dont beaucoup manipulent des données sensibles. Le contenu de cette liste sera établi par un décret en Conseil d'Etat.

Dérogation temporaire

Le texte issu de la Commission Mixte Paritaire limite la capacité de dérogation temporaire. En effet, il est prévu que cette dérogation devra toutefois être rendue publique. Elle devra faire l'objet d'un avis motivé du Parlement et ne pourra excéder un délai de 18 mois[viii] après qu'une offre « considérée comme acceptable » a été rendue disponible en France. Les modalités pour les projets déjà engagés seront définies dans un décret en Conseil d'Etat. Ainsi, le HDH, en qualité de GIP, devra sélectionner un acteur certifié SecNumCloud, et non pas seulement HDS, cependant, comme le GIP plateforme de données de santé s'est déjà engagé avec Microsoft, il peut solliciter une dérogation temporaire.

Le décret en Conseil d'Etat précisera notamment :

- les critères de sécurité et de protection, y compris en termes de détention du capital, des données (d'une sensibilité particulière).
- les conditions dans lesquelles une dérogation motivée et rendue publique peut être accordée sous la responsabilité du ministre dont relève le projet déjà engagé et après validation par le Premier ministre, et fixe éventuellement les critères selon lesquels une telle offre peut être considérée comme acceptable.

Protection supplémentaire pour l'archivage des données de santé

Cet article apporte des modifications à l'article L.1111-8 du Code de la Santé Publique (**CSP**) qui impose le recours à un hébergeur certifié ou agréé en cas d'externalisation de l'hébergement de données de santé recueillies à l'occasion d'activité de prévention, de diagnostic, de soin ou de suivi social et médico-social, dans des conditions propres à garantir leur confidentialité et leur sécurité.

Lors des discussions du projet de loi à l'Assemblée nationale, il était proposé d'imposer aux fournisseurs de services de cloud d'être certifiés SecNumCloud, à compter du 1er juillet 2024, pour l'hébergement des données de santé. Le texte finalement adopté à l'issue de la Commission Mixte Paritaire (CMP) inscrit dans la loi les évolutions prochaines du référentiel « hébergeur de données personnelles de santé » (« **HDS** ») introduites par le ministère de la santé et de la prévention.

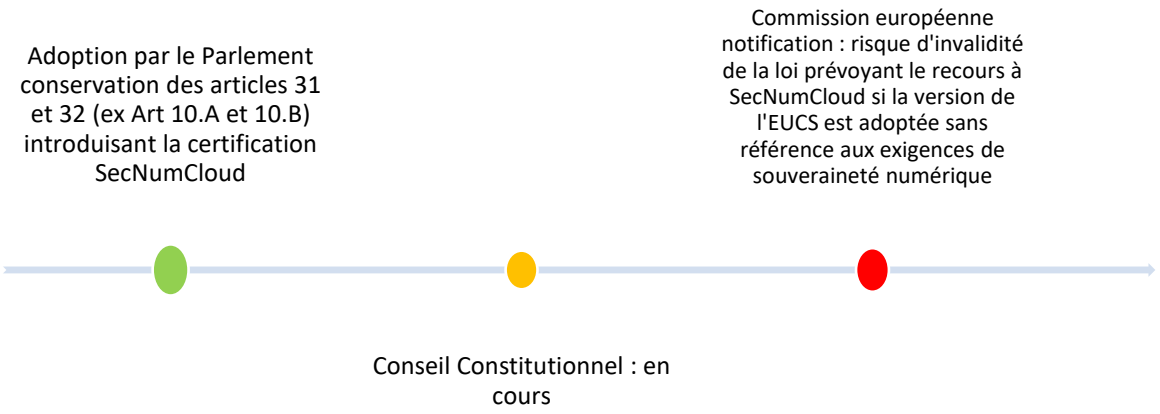
Le référentiel doit préciser « les obligations de l'hébergeur en matière de stockage de ces données sur le territoire » d'un État membre de l'Union européenne ou de l'espace économique européen ainsi que, dans le contrat entre le prestataire et le client, « les mesures prises face aux risques de transfert ou d'accès non autorisé de ces données par des États tiers » à l'Union européenne ou l'EEE.

Extension du référentiel HDS aux Services d'Archivage numérique

Le référentiel HDS est applicable aux services d'archivage numérique des données de santé à l'issue de leur durée de conservation, au sens du Règlement de protection des données personnelles. Jusqu'à présent, l'archivage est soumis à une procédure d'agrément spécifique par le ministère de la culture.

Le texte prévoit enfin que ces dispositions deviendront applicables au plus tard le 1er juillet 2025, la date doit être précisée par un décret.

Les étapes de la loi SREN : un risque de non-conformité avec le droit européen (l'EUCS)



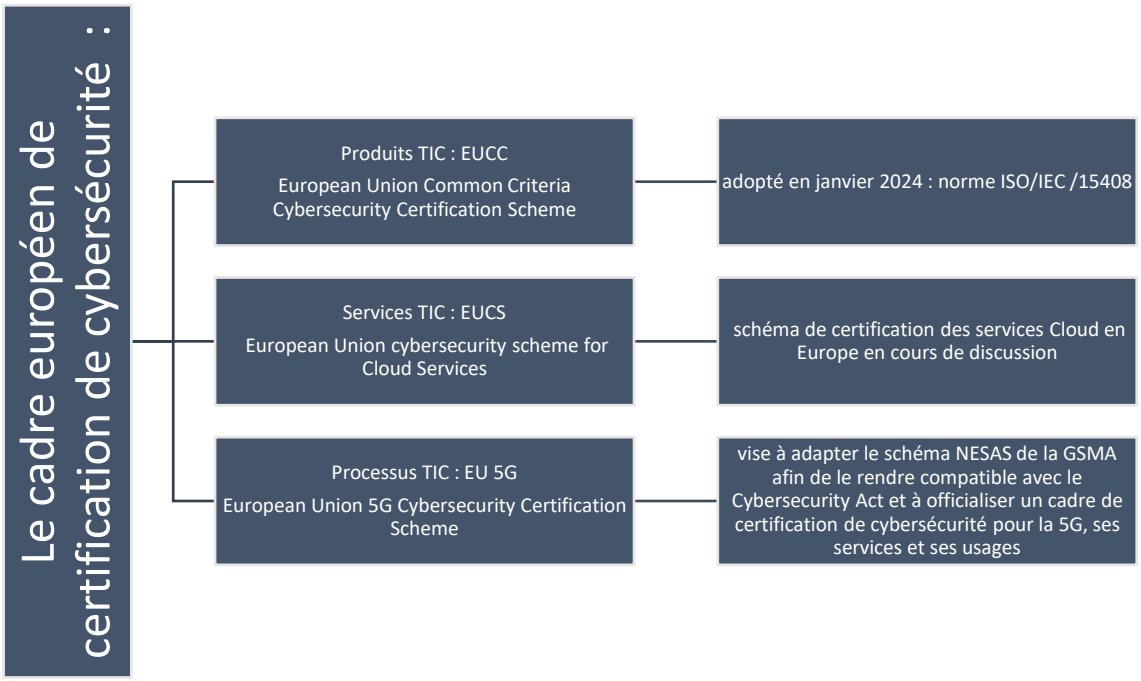
II-Certification SecNumCloud vs Certification EUCS

Cadre européen de certification de cybersécurité

Le règlement (UE) 2019/881 du Parlement européen et du conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité) donne mandat à l'ENISA pour contribuer à réduire la fragmentation du marché intérieur et parvenir à un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, y compris en aidant activement les États membres et les institutions, organes et organismes de l'Union à améliorer la cybersécurité.

Le cadre européen de certification de cybersécurité (Titre III, Cadre de certification de cybersécurité) est établi

> « *afin d'améliorer les conditions de fonctionnement du marché intérieur en renforçant le niveau de cybersécurité au sein de l'Union et en permettant de disposer, au niveau de l'Union, d'une approche harmonisée en ce qui concerne les schémas européens de certification de cybersécurité, en vue de créer un marché unique numérique pour les produits TIC, services TIC et processus TIC* .
>
> *2. Le cadre européen de certification de cybersécurité prévoit un mécanisme visant à établir des schémas européens de certification de cybersécurité et à attester que les produits TIC, services TIC et processus TIC qui ont été évalués conformément à ces schémas satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services qui sont offerts par ces produits, services et processus ou accessibles par leur intermédiaire tout au long de leur cycle de vie*. » (art 46)



Adoption d'un schéma européen de certification de cybersécurité

La Commission publie un programme de travail glissant de l'Union pour la certification européenne de cybersécurité qui recense les priorités stratégiques pour les futurs schémas européens de certification de cybersécurité[ix]. La Commission tient dûment compte des avis du GECC (groupe européen de certification de cybersécurité[x]) et du groupe des parties prenantes[xi] pour la certification de cybersécurité sur le projet de programme de travail glissant de l'Union. Le programme de travail glissant de l'Union est mis à jour au moins tous les trois ans, et plus souvent si nécessaire

La Commission peut demander à l'ENISA de préparer un schéma candidat ou de réexaminer un schéma européen de certification de cybersécurité existant inclus ou non dans le programme de travail glissant de l'Union (art 48). L'ENISA prépare un schéma candidat et consulte toutes les parties prenantes concernées. Pour chaque schéma candidat, l'ENISA crée un groupe de travail ad hoc, afin qu'il lui fournisse des conseils et des compétences spécifiques.

L'ENISA coopère étroitement avec le GECC et tient le plus grand compte de l'avis non contraignant du GECC avant de transmettre à la Commission le schéma candidat. La Commission peut adopter des actes

d'exécution prévoyant un schéma européen de certification de cybersécurité pour les produits TIC, services TIC et processus TIC.

Coexistence entre le schéma de certification de cybersécurité au niveau national et au niveau européen

Les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC et processus TIC couverts par un schéma européen de certification de cybersécurité cessent de produire leurs effets à partir de la date fixée dans l'acte d'exécution. Les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC et processus TIC qui ne sont pas couverts par un schéma européen de certification de cybersécurité continuent à exister[xii]. Les États membres s'abstiennent d'instaurer de nouveaux schémas nationaux de certification de cybersécurité pour les produits TIC, services TIC et processus TIC qui sont déjà couverts par un schéma européen de certification de cybersécurité en vigueur. Les États membres informent la Commission et le GECC de leur intention éventuelle d'élaborer de nouveaux schémas nationaux de certification de cybersécurité

EUCC : European Union Common Criteria Cybersecurity Certification Scheme

La Commission européenne a déjà adopté le 31 janvier 2024, l'EUCC European Union **Common Criteria** Cybersecurity Certification Scheme, qui correspond aux common criteria de la norme IS/IEC 15408, qui vise à fournir un ensemble harmonisé de règles et procédures, pour certifier la cybersécurité des produits matériels et logiciels ainsi que des services et processus informatiques au sein de l'UE. L'objectif de l'EUCC est **d'**aider les organisations à démontrer leur conformité avec des normes de cybersécurité reconnues, augmentant ainsi la confiance des clients et partenaires. Ce schéma de certification vise à créer un marché unique pour les produits et services de cybersécurité, facilitant ainsi le commerce et la coopération transfrontaliers dans l'UE. Ainsi, les produits seront conformes au Cybersecurity Act, s'ils sont conformes aux exigences de l'EUCC, dans la conception des services, l'analyse des risques et la gestion de la cybersécurité. En tant qu'Autorité Nationale de Certification de Cybersécurité (ANCC), l'ANSSI sera en charge de délivrer les certifications pour le niveau élevé et de surveiller la bonne application du schéma EUCC en France. L'agence française indique cependant que les certificats SOG-IS existants pourront être réévalués en certificats EUCC dès lors que les nouvelles exigences seront respectées.

EUCS : European Union Cybersecurity Certification Scheme for Cloud Services

Depuis 2020, les 27 tentent de se mettre d'accord sur cette certification l'EUCS pour « European Union Cybersecurity Certification Scheme for Cloud Services » prévue par le règlement européen du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications[xiii]. Le futur référentiel européen de cybersécurité du cloud est un ensemble d'exigences techniques de cybersécurité, qui doit être adoptée en 2024. Elle vise à remplacer les certifications cloud nationales existantes (France SecNumCloud, Allemagne C, Espagne ENS) afin d'harmoniser totalement la sécurité cloud dans l'UE.

Le projet de certification EUCS, élaboré par l'ENISA doit promouvoir la sécurité du cloud à travers un processus visant à renforcer l'indépendance de l'Europe, face à aux hyperscalers américains. Il s'inspire des schémas nationaux existants. L'objectif de ce texte est de créer une certification cloud destinée à évaluer la sécurité des fournisseurs de services cloud à l'échelle européenne.

Le projet européen de certification cloud EUCS prévoit trois niveaux de certifications possibles. Ces niveaux de sécurité différents seraient adaptés en fonction des usages et du niveau de sensibilité des données à héberger :

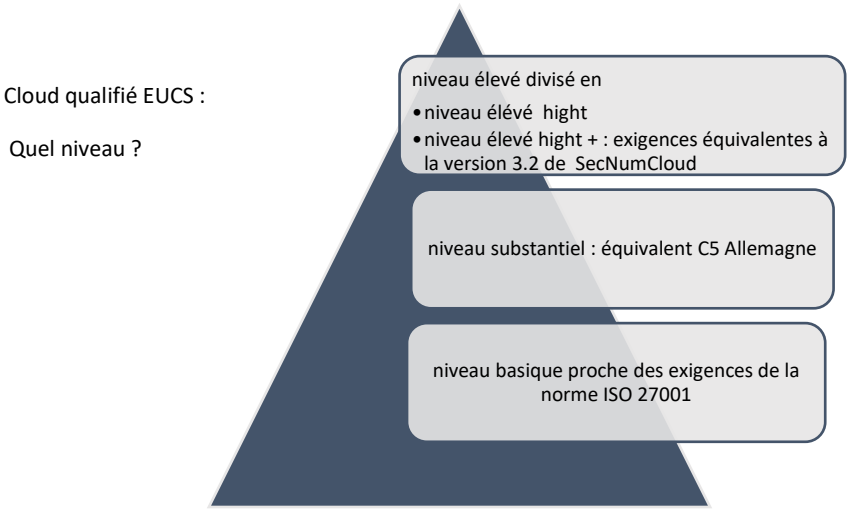


Schéma de certification des services cloud : discussion sur la dernière version

La France avec son référentiel SecNumCloud fait figure de référence dans la conception de la certification cloud européenne EUCS. La France, l'Italie ou encore l'Espagne se positionnent en faveur d'une protection stricte des données européennes et donc contre le principe d'application extraterritoriale des lois étrangères pour les données sensibles. Cette volonté d'inclure des exigences de souveraineté au sein de la certification européenne de services cloud EUCS ne fait pas l'unanimité.

Emmenés par les Pays-Bas, 12 autres pays européens – dont l'Allemagne – s'opposent à une version du texte qui contiendrait de trop fortes exigences de souveraineté.

SecNumCloud : *référentiel de sécurité français le plus exigeantau niveau UE*	version précédente de l'EUCS (high level +)	nouvelle version du texte discutée la 15 et 16 avril 2024 par le comité d'experts nationaux (high level+)
Plusieurs critères imposant que les fournisseurs, dont les sièges sociaux sont situés hors UE, ne soient pas soumis à leurs lois nationales, comme le Cloud Act (**Clarifying Lawful Overseas Use of Data Act)** , la FISA (Foreign Intelligence Surveillance Act, section 702 permettant au gouvernement américain de procéder à une surveillance ciblée des ressortissants étrangers vivant en dehors des US sans avoir besoin d'obtenir de mandat) pour les US, permettant à des puissances non européennes d'avoir accès aux données hébergées par ces derniers. Il s'agit d'une protection juridique, qui impose l'immunité de l'application extraterritoriale des lois extra européennes. Pour la CNIL , le référentiel SecNumCloud 3.2 fournit une réponse aux exigences de la CJUE en matière de protection des données dans le cloud. **A terme, la certification SecNumCloud sera remplacée par la certification EUCS**.	**La version précédente de l'EUCS** obligeait les entreprises n'étant pas basée dans un pays membre de l'UE à mettre en place une coentreprise avec une société européenne, ou de coopérer directement avec une entreprise locale chargée de l'hébergement et du traitement des données.	suppression de cette exigence plus d'exclusivité aux entreprises européennes pour traiter les données européennes les plus sensibles (données de santé, mais données stratégiques) Les seuls critères retenus sont purement techniques, sans prendre en compte l'aspect juridique. Obligation de transparence : fournir des informations sur le lieu de stockage et le traitement des données des clients et les lois applicables, ainsi que des détails sur les employés des fournisseurs de services cloud et les processus automatisés et manuels impliqués dans la gestion et l'exploitation du service. ***Avec cette version « dégradée » qui ne reprend pas le critère de la localisation des données, l'immunité à l'extraterritorialité des lois étrangères:***

		les entreprises et les administrations publiques européennes **sont privées d'un outil indispensable pour protéger la confidentialité de leurs données sensibles et stratégiques** à l'encontre des ingérences d'acteurs non européens. les Etats membres pourront-ils imposer des exigences de sécurité complémentaire pour des données sensibles telles que les données de santé, dès lors que cette version est la certification EUCS du plus haut niveau ?

Lundi 15 et Mardi 16 avril, le groupe d'experts nationaux s'est réuni à l'ENISA (Agence européenne de Cybersécurité) pour négocier le projet EUCS (European Union Cybersecurity Scheme for Cloud Services), qui vise à établir les critères pour délivrer une certification cloud harmonisée dans tous les Etats membres de l'UE.

La dernière version en discussion supprimait la condition d'immunité aux lois extraterritoriales, comme le prévoit le référentiel français SecNumCloud. L'abandon de l'exigence de souveraineté pour les acteurs, souhaitant bénéficier de la future certification, est porté notamment par les Pays-Bas, l'Allemagne et une douzaine d'autres Etats membres. En effet, la clause, qui a trait à certains critères de souveraineté, reste la plus discutée. Le niveau hight +, prévoyant une immunité à l'extraterritorialité des lois des puissances étrangères, imposant l'accès aux données des entreprises à leurs administrations.

Les oppositions à la version allégée du EUCS fondées sur la capacité de protéger des données européennes sensibles et stratégiques

Une coalition de plusieurs entreprises européennes regroupant notamment Orange, Airbus et Deutsche Telekom, fournisseurs et utilisateurs de Cloud européen, a adressé une lettre ouverte aux autorités de leurs pays et à la Commission européenne. Elle alerte sur les risques d'une suppression de la souveraineté dans le schéma de certification européenne de cybersécurité dans le cloud (EUCS).

En France, le **Cigref**, association loi 1901, regroupant de grandes entreprises et administrations publiques françaises, a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Le 11 avril, il a publié un communiqué de presse intitulé « *EUCS, le déclin d'une ambition : lettre ouverte à la Présidence de la Commission Européenne* », déplorant une situation « *qui*

va à l'encontre de l'ambition d'autonomie stratégique et technologique de l'Union européenne ». Il appelle la Commission européenne à prendre des mesures immédiates pour clarifier et renforcer la protection des données non personnelles sensibles et stratégiques au sein de l'EUCS. Le schéma de certification devrait pouvoir offrir **la garantie raisonnable** que les données les plus critiques puissent être sécurisées contre toute forme d'ingérence étrangère. Il s'agit d'un enjeu de sécurité et d'indépendance de l'Union Européenne et de son économie.

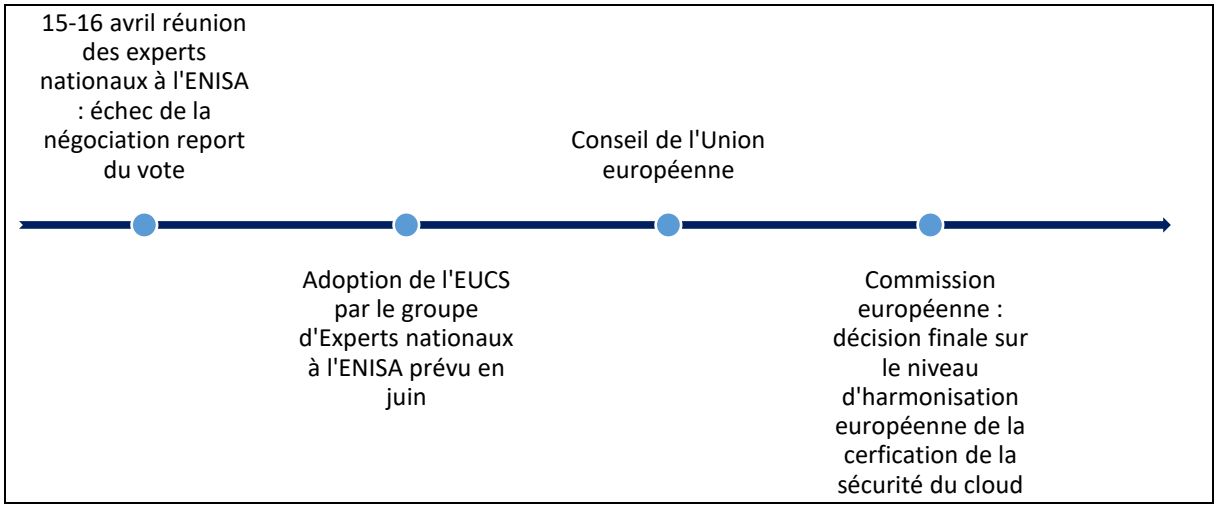
La certification SecNumCloud et notamment l'exigence de l'hébergement des données de santé par un hébergeur non soumis à l'ingérence d'une puissance étrangère risque d'être considérée non conforme à la Certification EUCS (European Union Cybersecurity Certification Scheme for Cloud Services).

Au final, l'EUCS permet à des puissances étrangères d'avoir accès aux données sensibles, mais également de favoriser la concurrence des hyperscalers américains. Dans son avis n°23-A-08 du 29 juin 2023 portant sur le fonctionnement concurrentiel de l'informatique en nuage (cloud), l'Autorité de la concurrence relève que « *Amazon, Microsoft et Google auraient capté 80% de la croissance des dépenses en infrastructures et applications de services cloud public en France en 2021. Au cours des prochaines années, la concentration du marché français pourrait ainsi se poursuivre, à leur bénéfice. (…) Ces caractéristiques du secteur favorisent et renforcent la position des fournisseurs en place. Elles appellent à une vigilance particulière sur l'évolution de la structure concurrentielle du marché et les pratiques susceptibles d'être mises en œuvre par les hyperscalers*. [xiv]»

La disparition de la protection juridique dans la dernière version de l'EUCS, témoigne de fortes pressions des entreprises américaines, considérant que les restrictions sont de nature à nuire à la compétitivité et à l'innovation. Cette harmonisation se heurte aux spécificités d'utilisation du Cloud dans les Etats membres.

Les différentes étapes

Pour EUCS



La France a obtenu un report du vote au mois de juin. Ce report permettra-t-il d'obtenir du Conseil de l'Union européenne des réponses sur la possibilité de conserver son référentiel SecNumCloud ?

A suivre ….

Pour toute information complémentaire ou question vous pouvez contacter directement l'auteur

Eléonore Scaramozzino
Avocat
Constellation Avocats
escaramozzino@constellation.law

constellation • law

[i] Voir Entrepôt de données EMC2 : La CNIL se serait-elle résignée, https://escaramozzino.legal/2024/03/20/entrepot-de-donnees-emc2-la-cnil-se-serait-elle-resignee
[ii] CJUE, 6 octobre 2015, C-392/14, Maximilian Schrems vs Data Protection Commissioner.
[iii] CJUE, 16 juillet 2020, C-311/18, Data Protection Commissionner c. Facebook Ireland Ltd, Maximillian Schrems
[iv] Règlement UE 2022/2065 du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE
[v] Règlement (UE) 2023/2854 du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données)
[vi] Règlement UE 2022/2065 du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE
[vii] Règlement UE 2022/1925, relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828

[viii] Dans son amendement le Député Philippe Latombe prévoyait une dérogation limitée à 12 mois pour ne pas que l'exception devienne la règle.
[ix] Article 47 du règlement (UE) 2019/881
[x]Article 62 du règlement (UE) 2019/881 : groupe européen de certification de cybersécurité : « *2-Le GECC est composé de représentants d'autorités nationales de certification de cybersécurité ou de représentants d'autres autorités nationales compétentes. Un membre du GECC ne peut représenter plus de deux États membres* ».
[xi] Article 22 du Règlement (UE) 2019/881 du parlement européen et du conseil du 17 avril 2019 relatif à l'ENISA : Groupe des parties prenantes pour la certification de cybersécurité : « Le groupe des parties prenantes pour la certification de cybersécurité se compose de membres sélectionnés parmi des experts reconnus représentant les parties prenantes concernées. La Commission, à la suite d'un appel transparent et ouvert, sélectionne, sur la base d'une proposition de l'ENISA, les membres du groupe des parties prenantes pour la certification de cybersécurité en assurant un équilibre entre les différents groupes de parties prenantes ainsi qu'un équilibre approprié entre les hommes et les femmes et un équilibre géographique. »
[xii] Article 57 du règlement (UE) 2019/881
[xiii] Règlement (UE) 2019/881 du parlement européen et du conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité)
[xiv] Autorité de la Concurrence, Avis n°23-A-08 du 29 juin 2023 portant sur le fonctionnement concurrentiel de l'informatique en nuage (« cloud »). p.6