Commission nationale de l'informatique et des libertés

Délibération n° 2025-098 du 16 octobre 2025 portant avis sur un projet de décret portant modification de certaines dispositions relatives à l'hébergement de données de santé à caractère personnel

NOR : *CNIX2602740V*

N° de demande d'avis : *25013418*	**Thématiques** : *hébergement de données de santé ; territorialité ; transferts*
Organisme(s) à l'origine de la saisine : *Ministère du Travail, de la Santé, des Solidarités et des Familles*	**Fondement de la saisine** : *article L. 1111-8 du code de la santé publique*

L'essentiel :

1. Le projet de décret, pris en application des dispositions de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique et de l'article L. 1111-8 du code de la santé publique, précise les obligations pesant sur les hébergeurs de données de santé en matière de souveraineté.

2. La CNIL accueille favorablement le renforcement des exigences prévues par l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel.

3. En outre, elle estime que l'actualisation des exigences réglementaires quant aux mentions du contrat d'hébergement constitue un apport bienvenu dans la perspective d'une plus grande transparence à l'égard des personnes concernées.

La Commission nationale de l'informatique et des libertés,

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données ou RGPD) ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (« loi informatique et libertés ») ;

Vu le code de la santé publique, notamment son article L. 1111-8 ;

Sur la proposition de M. Vincent Lesclous, commissaire, et les observations de M. Damien Milic, commissaire du Gouvernement,

Adopte la délibération suivante :

I. – **La saisine**

A. – *Le contexte*

La loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (« loi SREN ») contient diverses dispositions visant à assurer la protection des données stratégiques et sensibles sur le marché de l'informatique en nuage.

En particulier, l'article 32 de la loi SREN modifie le IV de l'article L. 1111-8 du code de la santé publique, relatif aux conditions de l'hébergement des données de santé à caractère personnel, pour y intégrer des obligations en matière de souveraineté.

Ainsi, cet article prévoit des obligations pour l'hébergeur de données de santé quant à la territorialité de l'hébergement et quant au contenu du contrat d'hébergement, en particulier concernant les mesures prises face aux risques de transfert de ces données ou d'accès non autorisé à celles-ci par des Etats n'appartenant pas à l'Union européenne ou à l'Espace économique européen (ci-après « Etat tiers »).

B. – *L'objet de la saisine*

Le projet de décret soumis à la CNIL pour avis par le ministère du travail, de la santé, des solidarités et des familles (délégation au numérique en santé) précise la portée des nouvelles obligations pesant sur les hébergeurs de données de santé.

A cette fin, le projet de décret prévoit :

– l'obligation pour l'hébergeur de données de santé, le cas échéant ses sous-traitants, d'héberger les données de santé à caractère personnel exclusivement sur le territoire d'un Etat membre de l'Union européenne ou partie à l'accord sur l'Espace économique européen ;

– les fondements des transferts de données, au sens du chapitre V du RGPD, en cas d'accès à distance aux données de santé depuis un Etat tiers ;
– les informations devant figurer dans le contrat d'hébergement concernant les transferts résultant d'un accès à distance, les réglementations extra-européennes applicables qui impliqueraient un transfert de données à caractère personnel ou un accès non autorisé à ces données au sens de l'article 48 du RGPD, les mesures mises en œuvre pour atténuer les risques liés à ces transferts et les risques résiduels demeurant malgré ces mesures, ainsi que les modalités d'exercice des droits par les personnes concernées ;
– l'obligation pour l'hébergeur de données de santé d'assurer la tenue à jour et la publicité de la cartographie des transferts de données de santé en dehors de l'Union européenne, des éventuels accès à distance à ces données et des risques d'accès non autorisé à ces données.

II. – **L'avis de la CNIL**

A. – *Sur les apports du projet de décret par rapport à la réglementation en vigueur*

De manière générale, le projet de décret reprend les exigences déjà prévues par l'arrêté du 11 juin 2018 tel que modifié par l'arrêté du 26 avril 2024 (ci-après « référentiel HDS »), en particulier les exigences n° 28 à 31, qu'il complète en exigeant expressément l'insertion de certains éléments dans le contrat d'hébergement.

La CNIL accueille très favorablement ce renforcement des obligations prévues par le référentiel HDS, qui apparaît de nature à accroître la transparence vis-à-vis des personnes concernées ainsi qu'à renforcer la maîtrise des données de santé par les parties au contrat d'hébergement vis-à-vis du risque d'accès extra-européen.

B. – *Sur les dispositions relatives à la territorialité de l'hébergement des données de santé et au risque d'accès à distance*

Le 2° de l'article 1er du projet de décret précise la portée des exigences de l'article L. 1111-8 du code de la santé publique relative à la territorialité de l'hébergement des données de santé. Ainsi, lorsque l'activité d'hébergement de données de santé implique leur stockage, il doit intervenir exclusivement sur le territoire d'un Etat membre de l'Union européenne ou partie à l'accord sur l'Espace économique européen, sans préjudice des cas d'accès à distance depuis un Etat tiers.

Le ministère a précisé que cette obligation n'a pas pour objet d'obliger les responsables de traitement de données de santé à caractère personnel d'héberger leurs traitements exclusivement sur des offres issues d'acteurs économiques européens, mais vise à les orienter vers des offres immunes de tout risque d'accès extra-européen.

Cet article prévoit également que, dans l'hypothèse où la prestation proposée par l'hébergeur ou l'un de ses sous-traitants impliquerait un accès à distance à ces données depuis un Etat tiers, cet accès doit nécessairement être fondé sur une décision d'adéquation de la Commission européenne ou, à défaut, sur l'une des garanties appropriées prévues par l'article 46 du RGPD.

La CNIL accueille favorablement ces obligations en ce qu'elles ont pour objet d'assurer une protection renforcée des données de santé vis-à-vis d'acteurs extra-européens, tant dans le cadre de la prestation principale de stockage des données que dans le cadre des accès nécessaires à cette prestation.

Concernant les exigences de souveraineté et d'immunité des données de santé par rapport aux lois extra-européennes, la CNIL réitère son soutien à l'objectif annoncé par le ministère de faire converger les exigences de la certification HDS avec celles prévues par la qualification SecNumCloud.

C. – *Sur les mentions devant figurer dans le contrat d'hébergement relatives à la souveraineté des données*

Le 2° ainsi que les *b* et *c* du 3° de l'article 1er du projet de décret prévoient que le contrat d'hébergement de données de santé doit comporter :

– les informations relatives à l'encadrement des éventuels accès à distance aux données de santé depuis un Etat tiers, y compris le détail et la documentation des garanties appropriées, au sens de l'article 46 du RGPD, mises en place pour encadrer l'accès à distance en l'absence de décision d'adéquation, ainsi que les éventuelles autres mesures permettant d'assurer un niveau adéquat de protection des données ;
– la liste des réglementations extra-européennes susceptibles d'entraîner un transfert ou un accès non autorisé aux données de santé, les mesures mises en œuvre pour atténuer les risques qu'un tel transfert ou accès se réalise ainsi que les risques résiduels demeurant malgré ces mesures ;
– en l'absence de telles réglementations, une indication en ce sens ainsi que les justifications permettant d'en attester.

La CNIL accueille favorablement ces nouvelles mentions qui complètent et renforcent les exigences du référentiel HDS quant au contenu du contrat d'hébergement et permettent ainsi de garantir la maîtrise, par les parties au contrat, des différentes situations susceptibles de porter atteinte à la souveraineté des données.

D. – *Sur les droits des personnes*

Le *a* du 3° de l'article 1er du projet de décret prévoit que le contrat d'hébergement doit mentionner les modalités d'exercice des droits d'accès, de rectification, d'effacement et de portabilité des données, ainsi que de limitation du traitement et d'opposition au traitement lorsque ceux-ci sont applicables.

La CNIL accueille favorablement cette modification qui contribue à l'effectivité de l'exercice de leurs droits par les personnes concernées, en garantissant que les parties à la prestation d'hébergement des données de santé ont bien prévu les mesures appropriées pour permettre cet exercice.

Les autres dispositions du projet de décret n'appellent pas d'observations de la part de la CNIL.

La présidente,
M.-L. DENIS