LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Santé
et de la Sécurité sociale

Réponse commune de Madame la Ministre de la Santé et de la Sécurité sociale et de Madame la Ministre de la Digitalisation à la question parlementaire n° 4718 du 7 septembre 2026 de l'honorable Députée Madame Liz Braz.

L'Agence nationale des informations partagées dans le domaine de la santé (Agence eSanté), ci-après l'Agence, exerce les missions définies à l'article 60*ter* du Code de la sécurité sociale, sous l'autorité conjointe des ministres ayant dans leurs attributions la Santé et la Sécurité sociale. Les modalités de mise en place du dossier de soins partagé, ci-après le DSP, sont fixées par le règlement grand-ducal modifié du 6 décembre 2019 précisant les modalités et conditions de mise en place du dossier de soins partagé**.**

Dans les éléments qui suivent, le terme « prestataire informatique » désigne les sociétés fournissant des logiciels ou des services d'hébergement aux professionnels de santé ; le terme « prestataire de soins » désigne les professionnels et établissements de santé.

- Quelles autorités sont actuellement chargées de contrôler la sécurité, la résilience et les infrastructures d'hébergement des prestataires privés qui traitent, hébergent ou sauvegardent des données de santé pour le compte de médecins et d'autres professionnels de santé ? Existe-t-il des aspects de ces infrastructures qui ne font actuellement l'objet d'aucun contrôle préalable ou périodique par une autorité publique ?

En vertu de l'article 4 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la CNPD est l'autorité de contrôle compétente au sens du règlement (UE) 2016/679 (« RGPD »). À ce titre, elle est chargée de surveiller l'application du RGPD et de veiller au respect de ses dispositions, y compris des obligations en matière de sécurité des traitements prévues à l'article 32 du RGPD.

Du point de vue de la protection des données à caractère personnel, le RGPD impose tant au responsable du traitement qu'au sous-traitant de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

À cet égard, l'article 32, paragraphe 1, du RGPD vise notamment la capacité à garantir « la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement », ainsi que la capacité à rétablir la disponibilité des données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique. Il prévoit également la mise en place d'une procédure visant à tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles mises en œuvre pour assurer la sécurité du traitement.

Du point de vue de la cybersécurité, la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité (ci-après « loi NIS2 ») est entrée en vigueur le 10 mai 2026 et s'applique d'office aux entités de taille moyenne ou large dans les secteurs de la santé, des infrastructures numériques et de gestion des services TIC (B2B). L'Institut luxembourgeois de Régulation (ILR) est l'autorité compétente pour assurer la supervision de la cybersécurité. Les entités de petite taille ou de taille micro ne tombent pas *d'office* dans le champ d'application de la loi NIS2, mais suivant l'article 11, paragraphe 1, point 5°, de la loi NIS2 l'autorité compétente peut identifier une telle entité comme entité essentielle.

- Ces prestataires sont-ils soumis, avant de pouvoir proposer de tels services aux professionnels de santé, à un agrément, une certification, une homologation ou un audit de sécurité obligatoire portant spécifiquement sur l'hébergement de données de santé ? Dans l'affirmative, quelle autorité délivre cet agrément ou cette certification, selon quels critères et avec quelle périodicité les contrôles sont-ils renouvelés ?

Du point de vue de la protection des données, le RGPD ne prévoit pas, en tant que condition préalable à l'exercice d'une activité de sous-traitance un agrément, une homologation ou une certification obligatoire spécifique aux hébergeurs de données de santé.

Le RGPD prévoit, à ses articles 40 et 41, la possibilité d'élaborer des codes de conduite destinés à contribuer à la bonne application du RGPD, ainsi que, à ses articles 42 et 43, des mécanismes de certification permettant notamment de démontrer la conformité des opérations de traitement effectuées par les responsables du traitement et les sous-traitants.

Le recours à ces instruments n'est toutefois pas obligatoire en vertu du RGPD et ces mécanismes ne sont par ailleurs pas spécifiques au secteur de la santé ou à l'hébergement de données de santé.

Lorsqu'un professionnel de santé est, le cas échéant, tenu de réaliser une analyse d'impact relative à la protection des données en vertu de l'article 35, paragraphe 3 du RGPD, son sous-traitant doit lui apporter l'assistance nécessaire à sa réalisation, conformément à l'article 28, paragraphe 3, lettre f), du RGPD.

Du point de vue du RGPD, aucune de ces entités n'est soumise à un contrôle préalable ou périodique. Tout contrôle éventuel, en ce qui concerne le volet applicable à la protection des données, intervient le cas échéant *a posteriori*, le RGPD ayant substitué au système de formalités préalables un principe de responsabilité (voir considérant 89 du RGPD et articles 5, paragraphes 2 et 24 du RGPD) et impliquant ainsi un contrôle exercé *a posteriori*.

Du point de vue de la cybersécurité, la loi NIS2 ne prévoit aucun mécanisme d'agrément ou de certification en amont de la fourniture du service.

En ce qui concerne l'attestation de conformité pour la connexion au DSP, en application de l'article 11, paragraphe 2, du règlement grand-ducal du 6 décembre 2019, un programme informatique ne peut établir de connexion à l'application DSP que s'il est conforme aux critères de connexion inclus dans les référentiels d'interopérabilité de la plateforme électronique nationale d'échange et de partage de données de santé, ci-après la plateforme, et s'il obtient l'attestation de conformité correspondante.

La procédure comporte une phase d'analyse et de tests, qui vérifie la conformité des échanges du programme avec la plateforme aux règles d'interopérabilité définies pour le DSP, puis une phase de tests et de contrôle de la connexion effective à la plateforme. L'attestation est délivrée par l'Agence sur la base des résultats des tests de conformité prévus par le règlement.

L'attestation porte sur le programme informatique pour ce qui concerne ses échanges avec la plateforme et elle atteste que ces échanges respectent les règles d'interopérabilité définies pour le DSP. Elle ne porte ni sur la qualité, la sécurité ou la robustesse intrinsèques du programme informatique, ni sur les fonctionnalités qu'il offre à ses utilisateurs, ni sur l'infrastructure d'hébergement, les dispositifs de

sauvegarde ou les modalités de continuité d'activité du professionnel de santé ou de son prestataire informatique, qui ne font pas partie des critères de connexion.

L'attestation reste valable tant qu'aucune modification n'affecte la validité des tests réalisés ou l'une des conditions de sa délivrance. En application de l'article 11, paragraphe 3, du même règlement, toute modification du programme informatique susceptible d'avoir un impact sur les critères de connexion, de même que toute mise à jour des référentiels d'interopérabilité, est communiquée par écrit et sans délai ; l'Agence et le professionnel de santé ou son sous-traitant conviennent alors d'un plan d'évolution et, le cas échéant, des tests de conformité à repasser pour le maintien de l'attestation. Le règlement ne prévoit pas de renouvellement périodique de l'attestation.

- Lorsqu'un prestataire fait lui-même appel à un sous-traitant ou à un fournisseur de services cloud pour héberger ou sauvegarder des données de santé, quelles obligations d'information lui incombent à l'égard du professionnel de santé concerné ? Celui-ci doit-il être informé de l'identité du sous-traitant, de la nature des données qui lui sont confiées ainsi que du lieu de leur hébergement ? Une autorisation préalable du professionnel de santé est-elle requise ?

Lorsque le prestataire agit en qualité de sous-traitant au sens du RGPD et entend lui-même recourir à un autre sous-traitant, l'article 28, paragraphe 2, du RGPD prévoit qu'il ne peut recruter celui-ci sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement.

En cas d'autorisation écrite générale, le sous-traitant doit informer le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, afin de lui donner la possibilité d'émettre des objections.

Le Comité européen de la protection des données précise à cet égard, dans ses Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, que, pour permettre au responsable du traitement d'évaluer et d'autoriser le recours à un sous-traitant ultérieur, il doit disposer des informations nécessaires concernant les sous-traitants envisagés, notamment leur localisation, les activités qu'ils réaliseront et les garanties mises en œuvre.

En outre, conformément à l'article 28, paragraphe 4, les mêmes obligations en matière de protection des données que celles fixées dans le contrat entre le responsable du traitement et le sous-traitant doivent être imposées au sous-traitant ultérieur et le sous-traitant initial demeure pleinement responsable devant le responsable du traitement.

Du point de vue de la cybersécurité, la loi NIS2 prévoit que l'entité essentielle ou importante doit appliquer des mesures afin d'assurer la sécurité de la chaîne d'approvisionnement (article 12, paragraphe 2, point 4°). Dans le cadre de l'approche basée sur les risques, il revient à l'entité NIS2 d'estimer la quantité et la qualité des informations ou garanties nécessaires pour assurer la sécurité de ses services selon les risques posés par une sous-traitance ou un fournisseur.

- Quelles obligations s'appliquent lorsque des données de santé sont confiées à un fournisseur de services cloud, notamment en matière de localisation des données, chiffrement, contrôle des accès et transferts éventuels hors du Luxembourg ou de l'Union européenne ? Le fait que les données soient chiffrées modifie-t-il les obligations applicables en matière d'information, de sous-traitance ou de contrôle ?

Dans la mesure où les données hébergées dans le cloud constituent des données à caractère personnel, les dispositions du RGPD sont applicables. Le RGPD ne fixe toutefois pas de prescriptions techniques

uniformes imposant, en tant que telles, des mesures spécifiques en matière de localisation des données, de chiffrement ou de contrôle des accès.

En matière de sécurité des données personnelles, l'article 32 du RGPD impose au responsable du traitement et au sous-traitant de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Le RGPD cite expressément, parmi les mesures susceptibles d'être appropriées, la pseudonymisation et le chiffrement des données à caractère personnel, ainsi que des mesures permettant d'assurer la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement.

Lorsque le recours à un fournisseur de services cloud implique un transfert de données à caractère personnel vers un pays tiers ou une organisation internationale, les dispositions du chapitre V du RGPD, et notamment ses articles 44 et suivants, sont applicables.

Le chiffrement constitue une mesure de sécurité susceptible d'être mise en œuvre conformément à l'article 32, paragraphe 1, point a), du RGPD.

Le chiffrement ne modifie toutefois pas, en tant que tel, la qualification des données comme données à caractère personnel et ne soustrait pas le traitement au champ d'application du RGPD.

Les obligations applicables en matière d'information, de sous-traitance et de contrôle demeurent dès lors applicables.

Du point de vue de la cybersécurité, la loi NIS2 prévoit que l'entité essentielle ou importante doit appliquer des mesures afin d'assurer la sécurité de la chaîne d'approvisionnement (article 12, paragraphe 2, point 4°). Dans le cadre de l'approche basée sur les risques, il revient à l'entité NIS2 d'estimer la quantité et la qualité des informations ou garanties nécessaires pour assurer la sécurité de ses services selon les risques posés par une sous-traitance ou un fournisseur.

- Les autorités compétentes disposent-elles actuellement d'une vue d'ensemble des prestataires et sous-traitants intervenant dans l'hébergement des données de santé au Luxembourg, comprenant notamment les fournisseurs cloud utilisés, la localisation des infrastructures principales et de sauvegarde ainsi que les éventuelles chaînes de sous-traitance ?

La CNPD ne dispose pas d'un registre central recensant l'ensemble des responsables du traitement de données personnelles, des sous-traitants, des sous-traitants ultérieurs et des fournisseurs cloud actifs dans le domaine de la santé au Luxembourg. Une telle centralisation d'information et la réalisation d'une cartographie générale nécessiteraient par ailleurs à minima une base légale intégrant notamment une obligation de notification en amont au régulateur.

Suivant l'article 11, paragraphe 4, de la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité les entités essentielles et importantes tombant dans le champ d'application de la loi sont tenues de s'auto-enregistrer auprès de l'ILR.

- Quelles exigences minimales sont actuellement imposées aux prestataires en matière de sauvegarde, redondance géographique, séparation des sauvegardes, restauration après incident et continuité des activités ? Existe-t-il notamment une obligation de garantir qu'une cyberattaque affectant l'infrastructure principale ne puisse simultanément compromettre les sauvegardes nécessaires à sa restauration ?

Le RGPD ne fixe pas de prescriptions techniques uniformes imposant, en tant que telles, ni une architecture particulière de sauvegarde ou une redondance géographique déterminée. Il impose en

revanche la mise en œuvre de mesures techniques et organisationnelles appropriées, déterminées notamment au regard des risques et de l'état des connaissances.

Ainsi, l'article 32, paragraphe 1, points b) et c), impose la mise en œuvre de mesures techniques et organisationnelles appropriées permettant notamment d'assurer de manière constante la disponibilité et la résilience des systèmes et services de traitement des données personnelles ainsi que « des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ». Le point d) exige en outre une procédure visant à tester et évaluer régulièrement l'efficacité de ces mesures.

Du point de vue de la cybersécurité, l'article 12 de la loi NIS2 impose aux entités essentielles ou importantes d'appliquer des mesures de sécurité. Cependant, les entités tombant dans les secteurs infrastructures numériques et gestion de service TIC doivent appliquer les mesures plus précises prévues par le règlement européen (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateaux de services de réseaux sociaux, et les prestataires de services de confiance.

- Les professionnels de santé disposent-ils actuellement d'un registre, label ou autre moyen officiel leur permettant de vérifier, avant de confier les données de leurs patients à un prestataire, que celui-ci ainsi que son infrastructure d'hébergement répondent à un niveau de sécurité déterminé et régulièrement contrôlé ?

Le recours à ces instruments n'est pas obligatoire en vertu du RGPD. Il appartiendrait au législateur national d'instaurer un régime spécifique d'agrément ou de certification, par exemple à l'instar de la législation française. En effet, l'article L. 1111-8 du Code français de la santé publique exige que l'hébergeur de données de santé dispose d'un certificat de conformité délivré par les organismes de certification accrédités par l'instance française d'accréditation ou l'instance nationale d'accréditation d'un autre État membre de l'Union européenne.

La loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité ne prévoit pas de registre public permettant de vérifier un certain niveau de sécurité ou de disponibilité des infrastructures.

L'Agence publie en outre sur son site internet, en application de l'article 11, paragraphe 2, du règlement grand-ducal du 6 décembre 2019, la liste des programmes informatiques et des établissements de soins ayant obtenu une attestation de conformité pour leur connexion à la plateforme. Elle publie également la liste des logiciels labellisés dans le cadre du dispositif SONS.

Ces listes attestent de la conformité des échanges des logiciels avec la plateforme et les services concernés. Elles ne constituent pas une évaluation des logiciels dans leur ensemble, ni de l'infrastructure d'hébergement, des sauvegardes ou de la continuité d'activité du prestataire informatique.

- Lorsqu'un prestataire proposant des services aux professionnels de santé fait état contractuellement ou commercialement d'un taux de disponibilité, d'une redondance de ses infrastructures ou d'une garantie de continuité de service, quelles dispositions permettent de garantir que ces indications correspondent effectivement aux services et données médicales confiés au prestataire et non uniquement à la disponibilité technique du centre de données ou de l'infrastructure sous-jacente ? Quelle autorité est compétente pour contrôler de telles affirmations ?

La question du respect, par un prestataire, d'un engagement contractuel relatif à un taux de disponibilité, à une redondance ou à une garantie de continuité de service relève, en premier lieu, des relations contractuelles entre les parties et ne relève pas, en tant que telle, des compétences de la CNPD. Par ailleurs, l'article 28, paragraphe 3, point h), du RGPD impose que le contrat conclu avec le sous-traitant prévoie que celui-ci mette à la disposition du responsable du traitement de données personnelles toutes les informations nécessaires pour démontrer le respect de ses obligations et permette la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur mandaté par lui, et contribue à ces audits.

Le responsable du traitement dispose ainsi, indépendamment des pouvoirs de contrôle de la CNPD, d'outils contractuels et juridiques lui permettant de vérifier que le sous-traitant respecte effectivement les obligations qui lui incombent en matière de protection des données. En cas de litige portant exclusivement sur l'exécution d'un engagement contractuel, il appartient en principe aux parties de mettre en œuvre les voies de recours prévues par le droit applicable, le cas échéant devant les juridictions compétentes.

Du point de vue de la protection des données, ces engagements peuvent néanmoins présenter une pertinence lorsque leur non-respect est susceptible d'entraîner un manquement aux obligations découlant du RGPD, notamment de son article 32 concernant la disponibilité, la résilience et la capacité de restauration des données.

Du point de vue de la cybersécurité, la loi NIS2 ne prévoit pas de registre public permettant à vérifier un certain niveau de sécurité ou de disponibilité des infrastructures.

- Au vu des enseignements de l'incident récent, le Gouvernement considère-t-il le dispositif actuel suffisant ou envisage-t-il la création d'un régime spécifique d'agrément ou de certification des prestataires et hébergeurs de données de santé, assorti d'exigences minimales obligatoires, d'audits réguliers et d'une transparence sur les sous-traitants et infrastructures cloud utilisés ?

En ce qui concerne le cadre applicable aux acteurs connectés à la plateforme, l'article 10, paragraphe 2, du règlement grand-ducal modifié du 6 décembre 2019 impose au professionnel de santé et, le cas échéant, à son sous-traitant connectés à la plateforme la mise en œuvre de mesures techniques et organisationnelles de sécurité comprenant au minimum :

- un système d'authentification fort ;
- une gestion de l'identification unique des patients et des professionnels de santé, le système d'identification lui-même étant fourni par l'Agence au titre de l'article 10, paragraphe 1er du règlement grand-ducal susmentionné ;
- un contrôle des accès ;

- une procédure de gestion des incidents pour tout événement, anomalie ou incident ayant ou pouvant avoir un impact sur la sécurité de la plateforme, incluant une coopération avec l'Agence ;
- une sensibilisation du personnel utilisant une application de la plateforme.

Ces mesures minimales visent la sécurité de la connexion et des échanges avec la plateforme.

Concernant l'incident de cybersécurité récent, le prestataire concerné a informé l'Agence de l'incident le 27 août 2026. L'Agence a procédé à des vérifications sur ses propres systèmes et sur les interfaces entre le logiciel concerné et la plateforme. Les systèmes de l'Agence n'ont pas été l'objet de cet incident. Des mesures préventives ont été prises et l'Agence a demandé au prestataire à être informée des conclusions de ses analyses concernant les interfaces avec la plateforme.

Luxembourg, le 2 novembre 2026

La Ministre de la Santé
et de la Sécurité sociale

(s.) Martine Deprez