Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 127/2023 du 8 septembre 2023

Objet :

- **un avant-projet de loi *de modification de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions et de modification de la loi du 29 janvier 2014 portant des dispositions relatives à la carte d'identité sociale et la carte ISI+*** (CO-A-2023-243)
- **un projet d'arrêté royal *modifiant l'arrêté royal du 26 février 2014 exécutant la loi du 29 janvier 2014 portant des dispositions relatives à la carte d'identité sociale et la carte ISI+*** (CO-A-2023-303)

Traduction[1]

Le Centre de Connaissances de l'Autorité de protection des données (ci-après "l'Autorité"), Présent.e.s: Mesdames Juline Deschuyteneer et Cédrine Morlière et Messieurs Yves-Alexandre de Montjoye et Bart Preneel ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après "la LCA") ;

Vu l'article 25, alinéa 3 de la LCA selon lequel les décisions du Centre de Connaissances sont adoptées à la majorité des voix ;

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, ci-après le "RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

[1] Pour la version originale validée collégialement, cf. la version néerlandaise du texte qui est disponible sur la version NL de la rubrique « avis » du site web de l'Autorité

Vu les demandes d'avis de Monsieur Frank Vandenbroucke, Vice-premier Ministre et Ministre des Affaires sociales et de la Santé publique (ci-après "le demandeur"), reçues le 11/06/2023 et le 07/07/2023 ;

Vu les explications de fond complémentaires, reçues les 26/07/2023 et 24/08/2023 ;

Émet, le 8 septembre 2023, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Le demandeur sollicite l'avis de l'Autorité concernant :
   - un avant-projet de loi *de modification de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions et de modification de la loi du 29 janvier 2014 portant des dispositions relatives à la carte d'identité sociale et la carte ISI+* (ci-après "l'avant-projet de loi") et
   - un projet d'arrêté royal *modifiant l'arrêté royal du 26 février 2014 exécutant la loi du 29 janvier 2014 portant des dispositions relatives à la carte d'identité sociale et la carte ISI+* (ci-après le "projet d'arrêté royal).

Contexte

2. L'avant-projet de loi vise tout d'abord à modifier l'article 5, 4°, b) de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions* (ci-après "la loi eHealth").

3. En vertu de l'article 5, 4° de la loi eHealth, la plate-forme eHealth est chargée, en vue de l'exécution de son objectif[2], de "*concevoir, gérer, développer et mettre gratuitement à la disposition des acteurs des soins de santé, sous forme standard, des services de base susceptibles d'aider les acteurs*(…)*"*. Un de ces services de base - faciliter l'échange électronique de données de santé entre acteurs des soins de santé - est "*un répertoire des références indiquant, avec l'accord des patients concernés, auprès de quels acteurs des soins de santé sont conservés quels types de données pour quels patients*".

[2] L'article 4 de la loi eHealth définit l'objectif de la plate-forme eHealth comme suit : "*La plate-forme eHealth a pour but d'optimaliser la qualité et la continuité des prestations de soins de santé et la sécurité du patient, de promouvoir la simplification des formalités administratives pour tous les acteurs des soins de santé et de soutenir la politique en matière de santé, et ce par des prestations de services et des échanges d'informations électroniques mutuels entre tous les acteurs des soins de santé, organisés avec les garanties nécessaires sur le plan de la sécurité de l'information et de la protection de la vie privée.*"

4. Il ressort de l'Exposé des motifs de l'avant-projet de loi que la modification du texte actuel susmentionné de l'article 5, 4°, b), de la loi eHealth en ce qui concerne le répertoire des références doit permettre :

- d'offrir une base légale, pas seulement pour le répertoire des références qui est tenu au niveau de la plate-forme eHealth (le metahub), mais aussi pour les répertoires des références sectoriels locaux et régionaux (hubs) ;[3]
- de permettre la création du répertoire des références sans le consentement préalable du patient concerné et de subordonner uniquement la consultation/mise à disposition du registre des références à ce consentement, et ce tant pour permettre l'accès immédiat d'un prestataire de soins ou d'un établissement de soins[4] que pour fournir à tout moment au patient lui-même un relevé des endroits où les informations le concernant sont disponibles.[5]

5. L'avant-projet de loi vise ensuite à modifier la loi du 29 janvier 2014 *portant des dispositions relatives à la carte d'identité sociale et la carte ISI+* (ci-après "la loi carte ISI+") afin de permettre que la carte ISI+[6], qui est actuellement délivrée sur support physique, puisse également être délivrée sous format électronique.

6. Suite à la modification susmentionnée de la loi carte ISI+, il convient aussi d'adapter son arrêté d'exécution : l'arrêté royal du 26 février 2014 *exécutant la loi du 29 janvier 2014 portant des dispositions relatives à la carte d'identité sociale et la carte ISI+* (ci-après "l'arrêté carte ISI+") en fonction des nouvelles modalités (électroniques) relatives à la délivrance de la carte ISI+ à certaines catégories d'assurés sociaux. Cette adaptation est effectuée via le projet d'arrêté royal.

---

[3] "*Ce répertoire des références actuel se compose de deux couches. Une première couche (le metahub) se situe au niveau de la plate-forme eHealth et indique en principe que des informations sont disponibles dans un réseau local ou régional (un hub). Une deuxième couche se situe au niveau des différents hubs, qui tiennent à jour un répertoire des références dans lequel ils indiquent auprès de quel établissement de soins ou de quel autre réseau d'échange connecté au hub des données de santé sont disponibles concernant un patient. Le renvoi exprès à l'éventuelle collaboration avec des répertoires des références sectoriels offre une base légale pour l'enregistrement d'indications dans les deux couches (hub et metahub).*" (voir p. 2 de l'Exposé des motifs).

[4] "*En outre, il ne ressort pas suffisamment du texte actuel de la loi que l'indication dans le répertoire de référence des lieux où sont disponibles les informations sur le patient doit, sous réserve d'une opposition expresse du patient, être préparée à l'avance afin qu'elles puissent être immédiatement disponibles lorsque le patient le demande au professionnel de santé de consulter les données. L'absence d'indication préalable des références empêche alors un accès souvent nécessaire et immédiat aux informations pertinentes pour les professionnels de soins ou les institutions une fois que le patient a donné son consentement.*" (voir p. 2 de l'Exposé des motifs).

[5] "*Il ressort finalement insuffisamment du texte de loi actuel que le répertoire de référence peut également être utilisé pour permettre non seulement au professionnel de santé, mais également au patient lui-même de demander des informations aux endroits où des informations le concernant sont disponibles. Si la désignation du répertoire de référence des lieux où sont disponibles les informations sur le patient n'est reprise dans le répertoire de référence qu'après consentement du patient, ces informations ne seront pas immédiatement disponibles au moment où le patient souhaite consulter les données. Il convient donc de préciser que l'accord du patient porte sur la consultation des indications figurant dans le répertoire de référence et les documents référenciés par d'autres que le patient ou son représentant légal."* (voir p. 3 de l'Exposé des motifs).

[6] La carte ISI+ est délivrée depuis 2014 par les mutualités aux enfants âgés de moins de 12 ans et aux assurés sociaux qui ne peuvent ou ne doivent pas disposer de pièce d'identité électronique belge et vise l'identification de l'assuré social et la consultation d'informations en ce qui concerne son assurabilité sur le plan du remboursement des soins de santé. (voir p. 4 de l'Exposé des motifs)

II. EXAMEN DE LA DEMANDE

Remarques préalables

7. Chaque traitement de données à caractère personnel doit avoir une base juridique ou de licéité, comme le prévoit l'article 6, paragraphe 1 du RGPD. Les traitements de données qui sont instaurés par une mesure normative sont presque toujours basés sur l'article 6.1, point c) ou e) du RGPD[7].

8. En vertu de l'article 22 de la *Constitution*, de l'article 8 de la CEDH et de l'article 6, paragraphe 3 du RGPD, de tels traitements doivent être prévus par une réglementation claire et précise, dont l'application doit être prévisible pour les personnes concernées[8]. En d'autres termes, la réglementation qui encadre ou dont la mise en œuvre implique des traitements de données doit répondre aux exigences de prévisibilité et de précision, de telle sorte qu'à sa lecture, les personnes concernées peuvent entrevoir clairement les traitements qui seront faits de leurs données et les circonstances dans lesquelles ces traitements sont autorisés. En outre, selon l'article 22 de la *Constitution*, il est nécessaire que les "éléments essentiels" du traitement de données soient définis au moyen d'une norme légale formelle.

9. Conformément aux principes de légalité et de prévisibilité, la norme législative doit au moins définir les éléments essentiels suivants du traitement :

- la (les) finalité(s) précise(s) et concrète(s) ;
- l'identité du (des) responsable(s) du traitement (à moins que cela ne soit clair).

Lorsque les traitements de données envisagés représentent une ingérence importante dans les droits et libertés des personnes concernées, des éléments de traitement supplémentaires doivent être définis dans la norme législative.[9] Tel est - au moins partiellement - le cas dans le présent avant-projet de loi, vu que l'établissement du répertoire des références va manifestement de pair avec un traitement

[7] Article 6, paragraphe 1 du RGPD : "*Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :*
c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; (...)
e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; (...)".

[8] Voir également le considérant 41 du RGPD.

[9] Il sera généralement question d'ingérence importante dans les droits et libertés des personnes concernées lorsqu'un traitement de données présente une ou plusieurs des caractéristiques suivantes : le traitement consiste en un traitement (à grande échelle) de catégories particulières de données à caractère personnel (art. 9 et 10 du RGPD) relatives à des personnes vulnérables, impliquant le croisement ou le couplage de données à caractère personnel issues de différentes sources, à des fins de surveillance ou de contrôle, et pouvant, le cas échéant, mener à une décision ayant des conséquences négatives pour les personnes concernées. Des caractéristiques devant également être prises en compte sont entre autres : une communication des données à des tiers, une limitation des droits des personnes concernées et l'utilisation du numéro de Registre national.

à grande échelle de nombreuses données de santé sensibles.[10] Il s'agit des éléments de traitement (essentiels) complémentaires suivants :

- les (catégories de) données qui sont nécessaires à la réalisation de cette (ces) finalité(s) ;
- les catégories de personnes concernées dont les données seront traitées ;
- le délai maximal de conservation des données ;
- les (catégories de) destinataires auxquels les données seront communiquées et les circonstances dans lesquelles elles le seront, ainsi que les motifs y afférents ;
- le cas échéant et dans la mesure où cela est nécessaire, la limitation des obligations et/ou droits mentionné(e)s aux articles 5, 12 à 22 et 34 du RGPD.

10. L'article 22 de la *Constitution* interdit au législateur de renoncer à la possibilité de définir lui-même les ingérences qui peuvent venir restreindre le droit au respect de la vie privée[11]. Dans ce contexte, une délégation au pouvoir exécutif "*n'est pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur*[12]".

[10] Dans les formulaires de demande d'avis, le demandeur indique lui-même que les projets normatifs en question concernent des traitements de données ayant lieu à des fins de surveillance et de contrôle et que les données sont accessibles à des tiers.

L'Autorité constate ensuite que les projets normatifs prévoient l'utilisation du numéro de Registre national.

L'Autorité constate en outre que le répertoire des références, en particulier, constitue un traitement à grande échelle de données à caractère personnel pouvant - au moins les répertoires des références sectoriels - également inclure des catégories particulières de données à caractère personnel sensibles, à savoir des données de santé. Il ressort de l'Exposé des motifs (voir la note de bas de page 3) et des explications du demandeur (point 17 et note de bas de page 19) que le répertoire des références comporte 2 couches : une première couche (le metahub) au niveau de la plate-forme eHealth, où il est en principe indiqué que des informations sont disponibles dans un réseau local ou régional (un hub), et une deuxième couche au niveau des différents hubs, qui tiennent à jour un répertoire des références dans lequel ils indiquent auprès de quel établissement de soins ou de quel autre réseau d'échange connecté au hub des données de santé sont disponibles concernant un patient. Des références à des établissements (spécialisés, psychiatriques, ...) révèlent souvent des informations sur la (nature de la) pathologie.

[11] Avis n° 63.202/2 du 26 avril 2018 du Conseil d'État émis concernant un avant-projet de loi *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du 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, Doc. Parl.,* Chambre, 54-3185/001, p. 121-122.

Voir dans le même sens les avis suivants du Conseil d'État :

- l'Avis n° 26.198/2 rendu le 2 février 1998 sur un avant-projet de loi qui a conduit à la loi du 11 décembre 1998 *transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, *Doc. Parl.* Chambre, 1997-98, n° 49-1566/1, p. 189 ;
- l'Avis n° 33.487/1/3 des 18 et 20 juin 2002 relatif à un avant-projet de loi qui a conduit à la loi du 22 août 2002 *portant des mesures en matière de soins de santé*, *Doc. Parl.* Chambre 2002-03, n° 2125/2, p. 539 ;
- l'Avis 37.765/1/2/3/4 rendu le 4 novembre 2004 sur un avant-projet de loi-programme qui a donné lieu à la loi-programme du 27 décembre 2004, *Doc. Parl.* Chambre 2004-05, n° 1437/2.

[12] Voir également Cour constitutionnelle, Arrêt n° 29/2010 du 18 mars 2010, point B.16.1 ; Arrêt n° 39/2013 du 14 mars 2013, point B.8.1 ; Arrêt n° 44/2015 du 23 avril 2015, point B.36.2 ; Arrêt n° 107/2015 du 16 juillet 2015, point B.7 ; Arrêt n° 108/2017 du 5 octobre 2017, point B.6.4 ; Arrêt n° 29/2018 du 15 mars 2018, point B.13.1 ; Arrêt n° 86/2018 du 5 juillet 2018, point B.7.2 ; Avis du Conseil d'État n° 63.202/2 du 26 avril 2018, point 2.2.

11. La confusion relative à la portée de plusieurs notions et concepts néanmoins fondamentaux - utilisés tout au long de l'avant-projet de loi[13] et de son Exposé des motifs[14] - nuit à la lisibilité et à la prévisibilité de l'avant-projet de loi, telles que requises par le RGPD et l'article 22 de la *Constitution* pour toute réglementation qui régit le traitement de données à caractère personnel ; la lecture de l'avant-projet de loi en soi ne permet effectivement pas, en ce qui concerne le "répertoire des références eHealth", ni dans le chef de l'Autorité, ni dans celui des personnes concernées, de saisir clairement et de comprendre quels traitements de quelles données auront lieu, et dans quelles circonstances ces traitements sont autorisés.

12. Cela complique également la mission d'avis de l'Autorité, indépendamment de la constatation que dans sa forme actuelle, l'avant-projet de loi, du moins en ce qui concerne "le répertoire des références eHealth", ne répond pas aux exigences des principes de légalité et de prévisibilité, tels que définis ci-avant (aux points 8 et 9). L'Autorité insiste pour qu'un avant-projet de loi éventuelement retravaillé - suite aux remarques formulées dans le présent avis -, en tout cas en ce qui concerne la partie 'répertoire des références eHealth', lui soit à nouveau soumis pour avis.

A. *LE RÉPERTOIRE DES RÉFÉRENCES EHEALTH (article 2 de l'avant-projet de loi)*

13. Conformément à l'article 2 de l'avant-projet de loi, à l'article 5, 4°, b), de la loi eHealth, en ce qui concerne les services de base que doit développer, gérer et mettre à disposition la plate-forme eHealth, le passage relatif au "répertoire des références" est modifié comme suit :
ANCIENNE VERSION *: "un répertoire des références indiquant, avec l'accord des patients concernés, auprès de quels acteurs des soins de santé sont conservés quels types de données pour quels patients ; l'implémentation du répertoire des références ne pourra être réalisée qu'après délibération de la chambre sécurité sociale et santé du comité de sécurité de l'information*"
NOUVELLE VERSION : "*en collaboration éventuelle avec des répertoires des références sectoriels, gérés par les acteurs des soins de santé, un répertoire des références indiquant auprès de quels acteurs des soins de santé sont conservés quels types de données pour quels patients ; l'implémentation du répertoire des références ne pourra être réalisée qu'après délibération de la chambre sécurité sociale et santé du Comité de sécurité de l'information ; la consultation du répertoire des références par des personnes autres que la personne concernée ou ses représentants légaux n'est possible que dans la mesure où la personne concernée a donné son consentement à cet effet".*

[13] On peut, entre autres, se référer aux notions non définies : répertoires des références sectoriels et acteurs des soins de santé.

[14] On peut, entre autres, se référer aux notions suivantes : metahub, hubs ou réseaux (d'échange) locaux et régionaux et relation thérapeutique.

(soulignement par l'Autorité)

14. Sous réserve d'une argumentation contraire avancée par le demandeur et sur la base des documents et réponses dont elle dispose, l'Autorité estime devoir parvenir aux conclusions suivantes en ce qui concerne la licéité des traitements de données allant de pair avec le répertoire des références:

- l'article 5, 4°, b) de la loi eHealth revu suite à l'avant-projet de loi constitue - en application des articles 6.1, c) et 9.2, g) du RGPD - la base de licéité pour l'enregistrement de données à caractère personnel dans le répertoire des références ;[15]
- pour la mise à disposition et le traitement des données à caractère personnel ainsi enregistrées dans le répertoire des références et pour l'échange, via la plate-forme eHealth, des données à caractère personnel (y compris des données de santé) auxquelles renvoie le répertoire des références, une (autre) base de licéité doit être trouvée dans les articles 6 et 9 du RGPD, en vertu de laquelle (le choix de) la mise à disposition d'informations relatives aux patients à partir du répertoire des références et via celui-ci doit en tout état de cause faire l'objet du consentement préalable éclairé du patient concerné.

15. Vu que la base de licéité pour l'enregistrement de données à caractère personnel dans le répertoire des références doit être trouvée dans la loi eHealth qui doit être modifiée par l'avant-projet de loi, celle-ci doit respecter les principes de légalité et de prévisibilité expliqués ci-avant.[16]

16. L'Autorité rappelle que la réglementation qui encadre un traitement de données à caractère personnel doit être formulée avec précision afin qu'à sa lecture, les personnes concernées puissent entrevoir clairement les traitements qui seront effectués avec leurs données et dans quelles circonstances.

17. Des notions et des concepts vagues ou indéfinis - pourtant cruciaux - nuisent à la lisibilité et à la prévisibilité. L'Autorité a interrogé le demandeur entre autres concernant :

- <u>les répertoires des références sectoriels ou hubs</u>, que le demandeur explique comme suit :

"Dans le répertoire des références géré par la plate-forme eHealth ne sont conservées que des références soit aux réseaux hospitaliers, soit aux coffres-forts de santé où sont disponibles des

[15] Le demandeur lui-même confirme également à cet égard : "*Le répertoire des références*(…) *trouve sa base juridique à l'article 5, 4°, b), de la* (loi eHealth)*"* et "*Le présent avant-projet offre en effet une base juridique pour le répertoire des références de la plate-forme eHealth et tous les répertoires des références sectoriels*. " [Ndt : les passages cités du demandeur sont des traductions libres effectuées par le service de traduction du Secrétariat Général de l'Autorité, en l'absence de traduction officielle]

[16] L'Autorité laisse au Conseil d'État le soin de se prononcer sur la possibilité pour le législateur fédéral de créer une base légale pour les traitements de données allant de pair avec les 'répertoires des références sectoriels' et sur la nécessité éventuelle d'élaborer un accord de coopération en la matière au sens de l'article 92*bis* de la loi spéciale *de réformes institutionnelles* du 8 août 1980.

données de santé relatives à une personne, sans que des données à caractère personnel relatives à la santé soient conservées. (…)

Un réseau hospitalier est un groupe d'hôpitaux et de laboratoires cliniques qui sont interconnectés dans un réseau pour un échange sécurisé de données. Chaque réseau hospitalier est géré par un hôpital ou une organisation de prestataires de soins de santé. Le gestionnaire est appelé 'hub'. Tous les hôpitaux et laboratoires cliniques belges sont rattachés à un réseau hospitalier. Le hub de chaque réseau hospitalier met à disposition un répertoire des références dans lequel les hôpitaux et les laboratoires cliniques affiliés peuvent indiquer pour quelles personnes des documents électroniques sont disponibles dans leur dossier électronique de patient. (…)

Il existe 4 réseaux hospitaliers : le Réseau Santé Bruxellois, géré par Abrumet (Bruxelles)[17]; la Collaboratief Zorgplatform, gérée par l'UZ Gent (une partie de la Flandre) ; le Réseau Santé Wallon, géré par le CHU Charleroi (Wallonie) ; le Vlaams Ziekenhuisnetwerk, géré par l'UZ Leuven (une partie de la Flandre).

Un coffre-fort de santé est un lieu de stockage sécurisé pour les données de santé provenant de prestataires de soins de santé ou d'autres organisations qui ne possèdent pas eux-mêmes de lieu de stockage sécurisé où les données en question sont disponibles 24 heures sur 24, 7 jours sur 7. (...)

Il y a 3 coffres-forts de santé : BruSafe+ pour les personnes résidant à Bruxelles ; Intermed pour les personnes résidant en Wallonie et Vitalink[18] pour les personnes résidant en Flandre." [Ndt : les extraits du dossier sont des traductions libres effectuées par le Secrétariat général de l'Autorité, en l'absence de traduction officielle][19]

- acteur des soins de santé, que le demandeur définit comme suit :

"*Il s'agit de tout acteur des soins de santé visé à l'article 4 de la* (loi eHealth) *(professionnels des soins de santé, professionnels de soins ou organisations de santé ou de soins).*"

---

[17] L'Autorité rappelle son récent avis n° 83/2023 du 27 avril 2023 *concernant un avant-projet d'ordonnance modifiant l'ordonnance du 4 avril 2019 portant sur la plate-forme d'échange électronique des données de santé*.

[18] L'Autorité rappelle son récent avis n° 88/2023 du 17 mai 2023 *concernant un projet d'arrêté du Gouvernement flamand portant exécution du décret du 8 juillet 2022 portant création de la plate-forme Vitalink*. [Ndt : uniquement disponible en néerlandais]

[19] Le demandeur précise également : "*La plate-forme eHealth assure l'échange sécurisé de données entre les acteurs des soins et est appelée dans ce contexte 'metahub'. À cette fin, la plate-forme eHealth met à disposition un répertoire des références dans lequel*

- *les hubs peuvent indiquer les personnes concernant lesquelles des références sont disponibles dans leur propre répertoire des références*
- *les coffres-forts de santé peuvent indiquer les personnes concernant lesquelles ils conservent des données de santé.*

(...) L'organisation par niveau des répertoires des références via le 'système hub et metahub' évite que le répertoire des références géré par la plate-forme eHealth ne reprenne des références directes à des lieux de stockage à partir desquels des données à caractère personnel relatives à la santé pourraient être indirectement déduites, par exemple une référence à un hôpital qui ne traite que des patients présentant une pathologie déterminée. L'hôpital de Melsbroek, par exemple, ne traite que des patients atteints de sclérose en plaques, l'hôpital de Kortenberg, par exemple, uniquement des patients psychiatriques. Les deux hôpitaux font partie du réseau hospitalier flamand. Le répertoire des références géré par la plate-forme eHealth permet uniquement de déduire que des données de santé concernant une personne sont disponibles dans le réseau hospitalier flamand, mais pas dans quel hôpital. La pathologie ne peut donc pas être déduite du répertoire des références géré par la plate-forme eHealth."

L'Autorité estime donc pouvoir en conclure que de telles informations sur la pathologie (à savoir des données de santé) peuvent bel et bien être déduites des répertoires des références sectoriels/hubs.

L'Autorité observe toutefois que cet article 4 ne prévoit pas de définition d' "acteur des soins de santé". L'article 3 de la loi eHealth, qui consiste en une énumération des définitions applicables pour cette loi, ne définit pas non plus 'acteur des soins de santé'.[20] Une définition et une délimitation claires s'imposent.

- les 'types de données', que le demandeur décrit comme suit :

"Tant dans le répertoire des références de la plate-forme eHealth (par ex. SumEHR, statut vaccinal, ...) que dans les répertoires des références sectoriels, il peut être référé à des 'types de données disponibles' (par ex. résultat de laboratoire, lettre de sortie de l'hôpital, ...). Il ne sert en effet à rien de formuler des requêtes électroniques à des lieux où aucune donnée pertinente n'est disponible."

L'Autorité constate que cette explication mentionne quelques exemples. Une liste plus exhaustive des 'catégories de types de données' visées s'impose.

- 'des personnes autres' qui peuvent consulter le répertoire des références, que le demandeur explique comme suit :

"Les mandataires[21] du patient et les titulaires d'un mandat de soins[22] du patient."

Il n'est toujours pas clair de savoir comment ce groupe de 'personnes autres' peut être défini. En effet, dans ses explications complémentaires, le demandeur se réfère uniquement aux "*mandataires*" et aux "*titulaires d'un mandat de soins*", tandis que dans l'Exposé des motifs (p. 3)[23], il est question dans ce contexte d' "*un professionnel de santé en relation thérapeutique ou d'autres personnes désignées par la personne concernée* ". Outre la définition des diverses 'autres personnes' dans l'avant-projet de loi, un alignement avec la notion de 'relation thérapeutique' telle que définie à l'article 37 de la loi du 22 avril 2019*relative à la qualité de la pratique des soins de santé* (ci-après la "loi qualité")[24] semble également nécessaire. (voir ci-après le point 44 du présent avis).

---

[20] On ne sait pas non plus clairement, parmi les organismes définis à l'article 3 de la loi eHealth (prestataires de soins, établissements de soins, institutions de sécurité sociale, organismes assureurs, etc.) lesquels il convient de considérer comme 'acteur des soins de santé'.

[21] Le demandeur précise : "*Un mandataire est une personne avec laquelle une autre personne conclut un contrat de mandat en vue d'accomplir certains actes (juridiques) en son nom et pour son compte.*"

[22] Le demandeur précise : "*Un mandat de soins de santé est un contrat de mandat spécifique qui est généralement émis par acte notarié. Une relation thérapeutique est une relation/un contrat qu'une personne établit/conclut avec un prestataire de soins ou un établissement de soins pour obtenir des soins.*"

[23] L'Exposé des motifs (p. 3) précise en la matière : "*La consultation du répertoire de référence par un professionnel de santé en relation thérapeutique ou d'autres personnes désignées par la personne concernée reste soumise à l'enregistrement du consentement au partage de données préalable de la personne concernée sur la plateforme eHealth.*"

[24] Conformément à l'article 37 de cette loi qualité du 22 avril 2019, une 'relation thérapeutique' est définie en ces termes : "*toute relation entre un patient et un professionnel des soins de santé dans le cadre de laquelle des soins de santé sont dispensés*", "soins de santé " étant définis comme : "*les services dispensés par un praticien professionnel en vue de promouvoir, de déterminer, de conserver, de restaurer ou d'améliorer l'état de santé d'un patient, de modifier son apparence corporelle à des fins principalement esthétiques ou de l'accompagner en fin de vie*".

L'article 38 de la loi qualité précise également : "*Le professionnel des soins de santé qui entretient une relation thérapeutique avec le patient, a uniquement accès aux données à caractère personnel relatives à la santé de ce patient dans le respect des conditions suivantes :*

1° la finalité de l'accès consiste à dispenser des soins de santé ;

2° l'accès est nécessaire à la continuité et à la qualité des soins de santé dispensés ;

18. Cette interprétation et sa portée (qui est d'ailleurs largement insuffisante) ne peuvent absolument pas être déduites du texte de l'avant-projet de loi (qui n'est même pas complété par le biais de l'Exposé des motifs) par le patient concerné lui-même. Il est impératif de définir et de délimiter davantage ces notions dans l'avant-projet de loi.

19. Vu que cette interprétation touche aux éléments essentiels du traitement (visés aux points 8 et 9 concernant les principes de légalité et de prévisibilité), elle ne peut pas non plus être laissée à une éventuelle délibération de la chambre sécurité sociale et santé du comité de sécurité de l'information.[25] Les délibérations et les notes du comité de sécurité de l'information ne correspondent pas à une 'réglementation' dans laquelle, conformément au principe de légalité, des traitements de données doivent être encadrés, comme le confirme également la Cour constitutionnelle.[26]

1. Finalités des traitements

20. En vertu de l'article 5.1.b) du RGPD, le traitement de données à caractère personnel n'est autorisé que pour des finalités déterminées, explicites et légitimes.

21. La lecture conjointe de l'article 4 et de l'article 5, 4°, b) à modifier de la loi eHealth fait apparaître ce qui suit : "*[afin] d'optimaliser la qualité et la continuité des prestations de soins de santé et la sécurité du patient, de promouvoir la simplification des formalités administratives pour tous les acteurs des soins de santé et de soutenir la politique en matière de santé*", la plate-forme eHealth a pour but d'organiser "*des prestations de services et des échanges d'informations électroniques mutuels entre tous les acteurs des soins de santé*" et est chargée à cette fin de "*concevoir, gérer, développer et*(…) *mettre [...] à [...] disposition* (…)*des services de base*" tels qu' "*un répertoire des références indiquant, avec l'accord des patients concernés, auprès de quels acteurs des soins de santé sont*

3° l'accès se limite aux données utiles et pertinentes dans le cadre de la prestation de soins de santé."

[25] L'article 5, 4°, b) de la loi eHealth prescrit entre autres : "*l'implémentation du répertoire des références ne pourra être réalisée qu'après délibération de la chambre sécurité sociale et santé du comité de sécurité de l'information*".

[26] L'Autorité renvoie à l'arrêt n° 110/2022 de la Cour constitutionnelle du 22 septembre 2022 (en particulier les points B.35 à B.40) dont les points de vue en la matière sont résumés comme suit dans le communiqué de presse de la Cour constitutionnelle :

"La Cour rappelle que l'article 22 de la Constitution réserve au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée et familiale. Une habilitation à un autre pouvoir est cependant admissible, pour autant qu'elle soit définie de manière suffisamment précise et que le législateur ait lui-même fixé les éléments essentiels.

La Cour relève que le Comité de sécurité de l'information est un organe qui est indépendant de l'Autorité de protection des données et qui a été créé par une loi du 5 septembre 2018. La Cour constate que les ***décisions du Comité de sécurité de l'information*** *sont contraignantes, qu'elles font l'objet d'un faible contrôle de la part de l'Autorité de protection des données et d'un contrôle juridictionnel mais qu'elles* ***ne sont pas soumises au contrôle parlementaire****. Les personnes concernées sont donc privées de la garantie d'un contrôle par le Parlement, sans que cela soit imposé par le droit européen. Par ailleurs,* ***l'habilitation critiquée porte sur des éléments essentiels****, puisque les législateurs n'ont pas identifié les destinataires de la communication des données concernées. La Cour en conclut que* ***l'habilitation critiquée est inconstitutionnelle****."*

conservés quels types de données pour quels patients", et ce "*en collaboration éventuelle avec les répertoires des références sectoriels*".

22. Bien qu'il ressorte de ce qui précède que le répertoire des références doive permettre/faciliter un échange électronique d'informations entre acteurs des soins de santé, l'absence d'une définition claire de certaines notions et certains concepts cruciaux ne permet pas d'évaluer la portée exacte du fonctionnement du répertoire des références (voir ci-avant : 'acteur des soins de santé' et 'répertoires des références sectoriels'). L'avant-projet de loi doit être complété par une définition et une délimitation précises de ces notions afin qu'il puisse être question d'une finalité déterminée et explicite, comme le requiert l'article 5.1.b) du RGPD.
Il est préférable d'exclure clairement toute (ré)utilisation à des fins purement commerciales (directement ou indirectement).

2. Catégories de données à caractère personnel et personnes concernées

23. L'article 5.1.c) du RGPD prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités visées (minimisation des données).

24. Conformément à l'article 5, 4°, b) à modifier de la loi eHealth, le répertoire des références indiquera "*auprès de quels acteurs des soins de santé sont conservés quels types de données pour quels patients*" .

25. L'article 3 de la loi eHealth définit le 'patient' comme étant : "*la personne physique à qui des soins de santé sont dispensés, à sa demande ou non*".

26. Interrogé par l'Autorité, le demandeur indique que le patient sera identifié dans le répertoire des références uniquement au moyen de son '*numéro d'identification de la sécurité sociale*'. Bien que l'article 8 de la loi eHealth dispose que "*Lors de la communication de données à caractère personnel non codées à ou par la plate-forme eHealth,* (…)*seuls les numéros d'identification visés à l'article 8 de la loi relative à la Banque Carrefour de la sécurité sociale* sont *utilisés*", l'Autorité recommande, en vue de la transparence et de la prévisibilité, d'indiquer explicitement dans l'avant-projet de loi que ces numéros d'identification seront enregistrés dans le répertoire des références.

27. Comme déjà indiqué ci-avant, il n'est pas clair de savoir ce qu'il convient d'entendre exactement par 'acteur des soins de santé', ce qui rend impossible toute estimation de la portée exacte

de l'article 5, 4°, b), de la loi eHealth, tant en ce qui concerne les données de patients que les données à caractère personnel d'un 'acteur des soins de santé' qui pourraient être enregistrées.

28. L'Autorité a également interrogé le demandeur en ce qui concerne les 'types de données' à enregistrer dans le répertoire des références. Comme déjà indiqué ci-avant, l'explication du demandeur ne mentionne que quelques exemples (par ex. SumEHR ou le statut vaccinal au niveau de la plate-forme eHealth et le résultat de laboratoire ou une lettre de sortie de l'hôpital au niveau des répertoires des références sectoriels). Une liste plus exhaustive des 'catégories de types de données' visées s'impose, tant pour le répertoire des références auprès de la plate-forme eHealth que pour les répertoires des références sectoriels.

3. Durée de conservation des données à caractère personnel

29. En vertu de l'article 5.1.e) du RGPD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

30. Ni l'avant-projet de loi, ni la loi eHealth ne déterminent le délai de conservation maximal des données à caractère personnel qui seront enregistrées dans le répertoire des références.

31. Interrogé à ce sujet par l'Autorité, le demandeur déclare ce qui suit : "*Les références sont conservées tant que des références sont disponibles dans les hubs ou que des données sont disponibles dans les coffres-forts de santé.*" Dans la mesure où il n'y a pas d'indication sur la conservation des données à caractère personnel dans les différents répertoires des références sectoriels[27], cette explication du demandeur n'apporte pas grand-chose.

32. Bien que conformément à l'Exposé des motifs et aux explications complémentaires obtenues du demandeur, l'avant-projet de loi devrait créer une base légale tant pour le répertoire des références au niveau de la plate-forme eHealth que pour les répertoires des références sectoriels, il ne prévoit

[27] Uniquement pour Vitalink, l'article 9 du décret flamand du 8 juillet 2022 *portant création de la plate-forme Vitalink* prévoit le délai de conservation suivant :

"§ 1er. Les données à caractère personnel traitées visées à l'article 6, alinéa 2, 1° à 5°, sont conservées pendant une durée maximale de six mois après le décès de l'usager des soins.

Les données à caractère personnel visées à l'article 6, alinéa 2, 6°, sont conservées pendant une durée maximale de cinq ans après leur dernier traitement.

§ 2. Le Gouvernement flamand peut fixer, pour des données spécifiques, une durée de conservation plus courte que celle visée au paragraphe 1er."

pas de délai de conservation ni de critères permettant de le déterminer[28]. Il convient de remédier à cette lacune.[29]

4. Responsables du traitement

33. L'article 4.7) du RGPD dispose que pour les traitements dont les finalités et les moyens sont déterminés par la réglementation, le responsable du traitement est celui qui est désigné en tant que tel dans cette réglementation.

34. Bien que cela ne soit pas précisé explicitement, le libellé de l'article 4 et de l'article 5, 4°, b) à modifier de la loi eHealth permet de déduire que la plate-forme eHealth peut être considérée comme le responsable du traitement pour les traitements de données allant de pair avec le répertoire des références, du moins pour le répertoire des références instauré à son niveau (en tant que metahub).[30]

35. Bien que conformément à l'Exposé des motifs et aux explications complémentaires obtenues du demandeur, l'avant-projet de loi devrait créer une base légale tant pour le répertoire des références au niveau de la plate-forme eHealth (metahub) que pour les répertoires des références sectoriels (hubs), il n'est pas d'emblée évident de savoir qui doit être considéré comme le(s) responsable(s) respectif(s) (conjoints ?) du traitement de ces répertoires des références sectoriels[31]. Il convient de

---

[28] Un délai de conservation maximal de 6 mois après le décès du patient concerné pourrait être envisagé, à moins que des circonstances spécifiques (par ex., une enquête judiciaire) n'exigent absolument un délai plus long.

[29] L'Autorité laisse au Conseil d'État le soin de se prononcer sur la possibilité pour le législateur fédéral de créer une base légale pour les traitements de données allant de pair avec les 'répertoires des références sectoriels' et sur la nécessité éventuelle d'élaborer un accord de coopération en la matière au sens de l'article 92*bis* de la loi spéciale *de réformes institutionnelles* du 8 août 1980.

[30] Interrogé à ce sujet, le demandeur confirme effectivement ce qui suit en la matière : "*En effet, en ce qui concerne le répertoire des références qu'elle tient en tant que metahub.*"

[31] Dans ses explications complémentaires, le demandeur indique certes que le Réseau Santé Bruxellois est géré par Abrumet, la Collaboratief Zorgplatform par l'UZ Gent, le Réseau Santé Wallon par le CHU Charleroi et le Vlaams Ziekenhuisnetwerk par l'UZ Leuven, mais il n'est absolument pas clair de savoir si ces instances devraient donc être considérées comme les responsables respectifs des traitements des données allant de pair avec les répertoires des références sectoriels qui doivent être créés en la matière.

L'Autorité constate que l'article 8 du décret flamand du 8 juillet 2022 *portant création de la plate-forme Vitalink* dispose entre autres dans ce contexte : "*L'agence (= l'agence des Soins et de la Santé, créée par l'arrêté du Gouvernement flamand du 7 mai 2004 portant création de l'agence autonomisée interne Soins et Santé) est le responsable du traitement des données à caractère personnel dans le cadre de la gestion de Vitalink." L'agence et le receveur des données à caractère personnel agissent en tant que responsables conjoints du traitement pour les échanges de données visées aux articles 5 et 7 du présent décret*(…). *Le présent article n'exclut pas que l'agence agisse en tant que sous-traitant pour certains traitements de données à Vitalink, où elle traite les données exclusivement pour le compte d'un responsable du traitement dans le cadre d'un projet spécifique.* (…)*"*

L'Autorité renvoie à l'avis n° 83/2023, (points 31 e.s.) du 17 mai 2023 *concernant un projet d'arrêté du Gouvernement flamand portant exécution du décret du 8 juillet 2022 portant création de la plate-forme Vitalink*. [Ndt : uniquement disponible en néerlandais]

L'Autorité constate également que l'article 7 de l'ordonnance du 4 avril 2019 *portant sur la plate-forme d'échange électronique des données de santé* prévoit entre autres dans ce contexte : "*§ 1er. Les acteurs de santé sont responsables du traitement des données à caractère personnel nécessaires à l'accomplissement des finalités de la plate-forme, telles que les données de santé, définies à l'article 2, 2°, et les données d'identification du patient qui sont échangées électroniquement ou hébergées au sein du "coffre-fort", au sens de l'article 4, 7° du* (RGPD). *§ 2. La plate-forme est considérée, au sens de l'article 4, 8° du* (RGPD), *comme sous-traitant des acteurs de santé.*(…)*"*

L'Autorité renvoie à l'avis n° 83/2023, (points 7 e.s.) du 27 avril 2023 *concernant un avant-projet d'ordonnance modifiant l'ordonnance du 4 avril 2019 portant sur la plate-forme d'échange électronique des données de santé*.

remédier également à cette lacune.[32]

36. La désignation du (des) responsable(s) du traitement dans la réglementation doit correspondre au rôle que cet (ces) acteur(s) joue(nt) dans la pratique et au contrôle qu'il(s) a (ont) sur les moyens essentiels mis en œuvre pour le traitement. En juger différemment serait non seulement contraire à la lettre du texte du RGPD mais pourrait aussi compromettre la finalité du RGPD qui consiste à garantir un niveau de protection cohérent et élevé pour les personnes physiques.

37. Par souci d'exhaustivité, l'Autorité rappelle également que l'article 26 du RGPD s'applique aux responsables conjoints du traitement. Pour les conséquences pratiques en la matière, l'Autorité renvoie au point 2 de la deuxième partie des lignes directrices 07/2020 *concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*, adoptées par le Comité européen de la protection des données le 7 juillet 2021..[33]

38. L'Autorité fait également remarquer à cet égard que 'définir de manière transparente les responsabilités respectives' ne peut se limiter à l'exercice par les personnes concernées des droits qui leur sont conférés par le RGPD, mais doit couvrir toutes les obligations propres à un responsable du traitement.

39. Dans le cas de responsables conjoints du traitement, l'Autorité recommande dans tous les cas qu'un point de contact unique[34] soit mis à la disposition des personnes concernées, ce qui doit permettre aux responsables conjoints du traitement de faciliter effectivement l'exercice des droits qui sont conférés aux personnes concernées par le RGPD.[35]

L'Autorité constate également que l'article 418/8 du *Code wallon de l'action sociale et de la santé* stipule, entre autres, dans ce contexte : "*Les hôpitaux et les professionnels de la santé sont responsables du traitement des données de santé qui sont échangées électroniquement et centralisées au sein du "coffre-fort" de santé.*(…) *La plate-forme peut agir comme sous-traitant en ce qui concerne l'échange électronique des données de santé et la centralisation de ces données au sein du "coffre-fort" de santé.*(…)*"*

L'Autorité renvoie à son avis n° 53/2014 (points 30 e.s.) du 3 septembre 2014 *concernant un projet d'arrêté du Gouvernement wallon présentant le projet de décret insérant certaines dispositions dans le Code wallon de l'Action sociale et de la Santé, relatives à la création d'une plate-forme d'échange électronique de données de santé* .

[32] L'Autorité laisse au Conseil d'État le soin de se prononcer sur la possibilité pour le législateur fédéral de créer une base légale pour les traitements de données allant de pair avec les 'répertoires des références sectoriels' et sur la nécessité éventuelle d'élaborer un accord de coopération en la matière au sens de l'article 92*bis* de la loi spéciale *de réformes institutionnelles* du 8 août 1980.

[33] Il faudra ainsi notamment définir de manière transparente qui des différentes entités est responsable pour répondre aux personnes concernées qui exercent les droits qui leur sont conférés dans le cadre du RGPD (cela ne porte en effet pas préjudice au fait que conformément à l'article 26.3 du RGPD, les personnes concernées peuvent exercer leurs droits dans le cadre du RGPD vis-à-vis de chacun des responsables conjoints du traitement). (https://edpb.europa.eu/system/files/2022-02/edpb_guidelines_202007_dataprotection_by_design_and_by_default_v09_fr.pdf)

[34] La création d'un point de contact unique implique évidemment l'instauration des procédures nécessaires qui font également fonctionner efficacement cette centralisation.

[35] Voir également à cet égard des avis antérieurs de l'Autorité : l'avis n° 138/2020 du 18 décembre 2020, l'avis n° 16/2021 du 10 février 2021, l'avis n° 122/2021 du 8 juillet 2021 et l'avis n° 20/2022 du 16 février 2022, l'avis n° 08/2023 van 20 janvier 2023 ; l'avis n° 40/2023 du 9 février 2023 et l'avis n° 88/2023.

5. Destinataires tiers des données à caractère personnel

40. En vertu des principes de légalité et de prévisibilité (voir les points 8 et 9 du présent avis), la réglementation qui instaure un traitement de données à caractère personnel doit également définir, le cas échéant, les (catégories de) destinataires de ces données, ainsi que les circonstances dans lesquelles les données sont communiquées et les motifs y afférents.

41. L'article 5, 4°, b) à modifier de la loi eHealth dispose que "*la consultation du répertoire des références par des personnes autres que la personne concernée ou ses représentants légaux n'est possible que dans la mesure où la personne concernée a donné son consentement à cet effet*". (soulignement par l'Autorité)

42. L'Exposé des motifs (p. 3) précise à cet égard : "*La consultation du répertoire de référence par un professionnel de santé en relation thérapeutique ou d'autres personnes désignées par la personne concernée reste soumise à l'enregistrement du consentement au partage de données préalable de la personne concernée sur la plate-forme eHealth.*"

43. Comme déjà indiqué plus haut, l'Autorité a interrogé le demandeur sur la portée des termes 'des personnes autres' dans l'article 5, 4°, b) précité à modifier et donc sur les destinataires tiers des données à caractère personnel du répertoire des références. D'après les explications du demandeur, il s'agit ici des personnes suivantes : "*Les mandataires[36] du patient et les titulaires d'un mandat de soins[37] du patient.*"

44. Il n'est toujours pas clair de savoir comment ce groupe de 'personnes autres' peut être défini. Bien que, conformément aux articles 4 et 5, 4°, b) de la loi eHealth, le répertoire des références doive permettre/faciliter un échange électronique d'informations entre acteurs des soins de santé, l'Autorité ne peut se défaire de l'impression que le groupe de 'personnes autres' non défini et non délimité pourrait donc également être issu d'un milieu extérieur au 'contexte des soins', ce qui ne semble pas d'emblée conforme à l'intention de la loi eHealth.[38] L'Autorité se demande dès lors si la définition

---

[36] Le demandeur précise : "*Un mandataire est une personne avec laquelle une autre personne conclut un contrat de mandat en vue d'accomplir certains actes (juridiques) en son nom et pour son compte.*"

[37] Le demandeur précise : "*Un mandat de soins de santé est un contrat de mandat spécifique qui est généralement émis par acte notarié. Une relation thérapeutique est une relation/un contrat qu'une personne établit/conclut avec un prestataire de soins ou un établissement de soins pour obtenir des soins.*"

[38] Dans la mesure où le numéro de Registre national est enregistré dans le répertoire des références, l'Autorité rappelle toutefois que l'utilisation de ce numéro est strictement régie par l'article 8 de la loi du 8 août 1983 *organisant un registre national des personnes physique.* L'utilisation du numéro de Registre national et l'accès aux informations du Registre national ne sont pas permis sans autorisation préalable soit du Ministre de l'Intérieur, soit par ou en vertu d'une loi, d'un décret ou d'une ordonnance, étant entendu que seul(e)s les autorités, les organismes et les personnes énuméré(e)s à l'article 5, § 1er de la loi Registre national peuvent en principe prétendre à une telle autorisation.

En prévoyant dans l'avant-projet de loi, le cas échéant, un accès au répertoire des références en dehors du cadre des soins de santé, le régime d'autorisation susmentionné peut être contourné, étant donné que cela peut permettre l'utilisation du numéro de Registre national pour des personnes et des organismes qui, en vertu de la loi Registre national, ne sont pas habilité(e)s à

d' 'autres personnes' ne peut pas se limiter au professionnel de santé ayant une relation thérapeutique avec le patient, par analogie avec la manière dont les articles 36 e.s. de la loi qualité régissent l'accès aux données de santé. Une définition plus précise de ces destinataires tiers s'impose quoi qu'il en soit, en soulignant que ceux-ci doivent disposer d'une (autre) base de licéité issue des articles 6 et 9 du RGPD pour le traitement de données à caractère personnel (dont des données de santé) auxquelles renvoie le répertoire des références, et que (le choix de) la mise à disposition d'informations relatives aux patients à partir du répertoire des références et via celui-ci doit en tout état de cause faire l'objet du consentement préalable éclairé du patient concerné.

45. L'échange/la mise à disposition de données, enregistrées par un prestataire de soins déterminé, à l'égard d'autres prestataires de soins en vue de dispenser des soins est de toute façon soumis(e) aux principes relatifs à l'accès à des données de santé, conformément aux articles 36 e.s. de la loi qualité.[39]

B. LA CARTE ISI+ (articles 3, 4 et 5[40] de l'avant-projet de loi et du projet d'arrêté royal)

46. Conformément aux articles 3 et 4 de l'avant-projet de loi, les articles 2 et 3 de la loi carte ISI+ sont complétés comme suit:
Article 2: "*Une carte ISI+ est délivrée sur support physique et/ou sous format électronique :*(…).*"*
Article 3 : "*Tout assuré social visé à l'article 2 est tenu de présenter sa carte ISI+, quel que soit son mode de délivrance, chaque fois qu'il* (…)*.*"

47. Suite à la modification susmentionnée de la loi carte ISI+, son arrêté d'exécution est également modifié dans le même sens, en fonction des nouvelles modalités relatives à la délivrance de la carte ISI+ à certaines catégories d'assurés sociaux, plus précisément :

- en vertu de l'article 1er, 2° du projet d'arrêté royal, l'arrêté carte ISI+ sera notamment complété par un nouveau § 2, libellé comme suit : *"§ 2. Les données visées au § 1er peuvent, selon le mode de délivrance de la carte ISI+, notamment être consultées à l'aide de codes-barres unidimensionnels, de codes-barres bidimensionnels et/ou d'un fichier électronique dont*

le faire (les prestataires de soins de santé sont autorisés à utiliser le numéro de Registre national en vertu de l'article 8/1 de la loi eHealth). L'organisation d'un tel accès abusif doit être évitée en toutes circonstances.

[39] L'Autorité a déjà demandé par le passé que ces principes/cette autorisation soient clarifiés et développés par arrêté royal, comme le prévoient les articles 36 et 37 de la loi du 22 avril 2019 précitée (voir : Note sur le traitement de données provenant de dossiers de patients : https://www.autoriteprotectiondonnees.be/professionnel/themes/donnees-sensibles).

[40] L'article 5 de l'avant-projet de loi se limite au remplacement, dans l'article 12 de la loi ISI+, de la référence à la loi entre-temps abrogée du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* par la référence au RGPD.

les spécifications techniques garantissant notamment l'authenticité et la sécurisation des données susvisées sont déterminées par la Banque-carrefour de la sécurité sociale."

- l'arrêté carte ISI+ est également complété, en vertu de l'article 2 du projet d'arrêté royal, par un nouvel article 3/1 qui dispose ce qui suit : "*La carte ISI+ peut être demandée par :*

  1° le titulaire, pour l'enfant mineur qui est inscrit à sa charge en vertu de l'article 123, 3, de l'arrêté royal du 3 juillet 1996 portant exécution de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994 ;

  2° les personnes qui exercent l'autorité parentale ou, à défaut, le représentant légal en vertu de la loi ou d'une décision judiciaire, pour l'enfant mineur qui peut bénéficier de prestations sociales dans le cadre de l'assurance obligatoire soins de santé et indemnités ;

  3° la personne majeure visée à l'article 2, 1°, de la loi du 29 janvier 2014 portant des dispositions relatives à la carte d'identité sociale et la carte ISI+.

  Les organismes assureurs sont responsables du traitement des demandes et de la délivrance des cartes ISI+."

48. Dans la mesure où, suite aux modifications réglementaires envisagées, la carte ISI+ pourra également être délivrée sous format électronique, l'Autorité rappelle :

- l'article 32 du RGPD relatif à la *Sécurité du traitement*[41] , ainsi que
- l'article 25 du RGPD relatif à la *Protection des données dès la conception et protection des données par défaut*[42].

---

[41] L'article 32 du RGPD dispose entre autres ce qui suit :

"1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

c) 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 ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il doit être tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite."

[42] L'article 25 du RGPD dispose notamment que :

"1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement

49. L'Autorité souligne également que des mesures de sécurité techniques doivent être mises en œuvre dans le format/fichier électronique afin de fournir une protection au moins équivalente à celle qui existe actuellement pour le support physique.

50. Le nouvel article 3/1, premier alinéa, qui doit être inséré dans l'arrêté carte ISI+ et qui énumère les personnes qui peuvent demander une carte ISI+ n'appelle pas de remarque particulière d'emblée.

51. L'Autorité prend également acte de la désignation explicite, dans le nouvel article 3/1, deuxième alinéa, qui sera inséré dans l'arrêté carte ISI+, des organismes assureurs en tant que responsables du traitement des demandes et de la délivrance des cartes ISI+. Bien que cette désignation soit conforme aux missions confiées aux organismes assureurs[43] par l'article 3 de la loi du 6 août 1990 *relative aux mutualités et aux unions nationales de mutualités*, l'Autorité recommande, conformément au principe de légalité (voir les points 8 et 9 du présent avis), de reprendre la désignation de ces responsables du traitement plutôt dans la loi carte ISI+ que dans son arrêté d'exécution.

PAR CES MOTIFS,
l'Autorité,

estime que l'avant-projet de loi présente des manquements en tant qu'encadrement légal du répertoire des références eHealth et des traitements de données y afférents car il ne satisfait pas aux principes de légalité et de prévisibilité applicables en la matière ;

estime qu'au minimum, les modifications suivantes s'imposent dans l'avant-projet de loi :

- définir et délimiter précisément plusieurs notions et concepts cruciaux (voir les points 11, 17, 18, 22) ;
- exclure explicitement toute utilisation du répertoire des références à des fins commerciales (voir le point 22) ;

sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée."

[43] Conformément à l'article 3, premier alinéa, a) de cette loi du 6 août 1990, ces organismes assureurs/ces mutualités sont chargé(e)s d'instaurer un service ayant entre autres pour objectif : "*la participation à l'exécution de (l'assurance obligatoire soins de santé et indemnités, réglée par la loi coordonnée du 14 juillet 1994, précitée), pour autant qu'elles aient reçu dans ce but une autorisation de l'union nationale".*

- préciser les personnes concernées dont des données sont traitées dans le cadre du répertoire des références (voir le point 27) ;
- dresser une liste plus exhaustive des catégories de types de données qui seront reprises dans le répertoire des références (voir les points 26 à 28) ;
- mentionner le délai de conservation maximal des données à caractère personnel enregistrées dans le répertoire des références ou au moins les critères sur la base desquels ce délai peut être déterminé (voir le point 32) ;
- préciser les responsables (conjoints ?) du traitement respectifs pour les traitements de données allant de pair avec le répertoire des références (voir les points 35 e.s.) ;
- délimiter et préciser les destinataires tiers de données à caractère personnel provenant du répertoire des références (voir les points 44 et 45) ;
- désigner les responsables du traitement pour le traitement des demandes et la délivrance des cartes ISI+ (au lieu de les désigner dans le projet d'arrêté royal) (voir le point 51) ;

souligne l'importance des éléments suivants :

- une application rigoureuse des principes de légalité et de prévisibilité (voir les points 8, 9, 15 et 16) ;
- un avis préalable supplémentaire de l'Autorité concernant un avant-projet de loi éventuellement retravaillé - suite aux remarques formulées dans le présent avis -, en tout cas en ce qui concerne la partie 'répertoire des références eHealth' (voir le point 12) ;

- une sécurité adaptée du traitement de données (également dès la conception et par défaut) (voir les points 48 et 49).

Pour le Centre de Connaissances,
(sé) Cédrine Morlière, Directrice