Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé

Délibération n° 242/2018 du 5 avril 2018

Conformément à l'article 32 paragraphe (3) lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée « la loi modifiée du 2 août 2002 » ou « la loi »), la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

Par courrier en date du 28 septembre 2017, Monsieur le Ministre de la Sécurité Sociale a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé (ci-après « le projet de règlement grand-ducal » ou « le projet »).

Ce projet pose le cadre règlementaire applicable au dossier de soins partagé (ci-après « le DSP »). Il est pris en application de l'article 60*quater* du Code de la sécurité sociale, introduit par la loi du 17 décembre 2010 portant réforme du système de soins de santé[1].

Le projet de règlement grand-ducal détaille les modalités et conditions de mise en place du DSP. Il fixe ainsi les grands principes applicables à la création du DSP (article 2), à son activation et son accès par le titulaire dudit dossier (article 3), à sa fermeture et suppression (article 4), à l'accès au DSP par les professionnels de santé (article 5), aux droits d'accès, d'écriture et d'opposition du titulaire (article 6), aux titulaires mineurs non émancipés et titulaires majeurs protégés par la loi (article 7), aux droits d'accès et d'écriture des professionnels de santé (article 8), à la traçabilité des accès et des actions (article 9), au délai de versement des données au DSP (article 10), à la sécurité de la plateforme électronique nationale (article 11), aux modalités techniques de versements des données au DSP et interopérabilité (article 12) et à la coopération et échanges transfrontaliers (article 13).

Pour rappel, la Commission nationale a rendu, le 24 novembre 2010[2], un avis relatif au projet de loi portant réforme du système de soins de santé dans lequel elle a formulé ses observations concernant la mise en œuvre du DSP.

La CNPD relève que le règlement n° 2016/679 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 ») sera applicable dans tous les Etats membres de l'Union européenne à partir du 25 mai 2018.

[1] Loi du 17 décembre 2010 portant réforme du système de soins de santé (Mémorial A-2010-242 du 27 décembre 2010, p. 4041, doc. parl. 6196).
[2] Délibération n°345/2010 du 24 novembre 2010 portant avis de la CNPD sur le projet de loi portant réforme du système de soins de santé et modifiant 1. le Code de la Sécurité sociale, 2. la loi modifiée du 28 août 1998 sur les établissements hospitaliers, doc. parl. 6196/04.

Ainsi, elle considère qu'il y a plus aucun intérêt à analyser le projet de règlement grand-ducal à la lumière de la loi modifiée du 2 août 2002 qui est la législation actuellement en vigueur, mais uniquement sur base des dispositions du RGPD.

La Commission nationale entend limiter ses observations aux dispositions du projet de règlement grand-ducal ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel. Elle se propose de suivre l'ordre de rédaction du projet de règlement grand-ducal pour exprimer ses recommandations.

I. Remarques préliminaires

a. Base de légitimité de la création du DSP

L'article 60*quater* du Code de la sécurité sociale, ainsi que les dispositions du règlement grand-ducal sous examen prévoient qu'un DSP sera activé d'office pour tout patient dès son affiliation à l'assurance maladie luxembourgeoise et qu'il n'a pas signalé son opposition (système de l' « opt-out »), à l'inverse de la solution du législateur français qui a opté de baser la création d'un dossier électronique pour les bénéficiaires de l'assurance maladie sur leur consentement préalable[3] (système de l' « opt-in »),.

Il n'appartient pas à la CNPD de commenter le choix politique fait par le législateur en 2010, en optant pour un système d'opt-out. Il convient cependant d'analyser si un système d'opt-out introduit à l'époque sous la directive 95/46[4] et la loi modifiée du 2 août 2002 est toujours compatible avec les dispositions du RGPD qui sera applicable à partir du 25 mai 2018.

Contrairement à la position de la Chambre des salariés exprimée dans son avis du 14 novembre 2017, ainsi que celle de l'Association des Médecins et Médecins-Dentistes (AMMD), de la COPAS et du Syndicat des Pharmaciens Luxembourgeois, exposée dans une lettre adressée au Président de la Commission européenne, Monsieur Jean-Claude Juncker, en date du 4 janvier 2018, la CNPD ne voit *a priori* pas d'incompatibilité de principe avec le RGPD, et ce pour les raisons qui suivent.

Tout d'abord, l'article 6 paragraphe (3) du RGPD, lu ensemble avec son paragraphe (1) lettres (c) et (e), prévoit une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect d'une obligation légale ou 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. Dans ces deux cas de figure, le fondement et les finalités des traitements de données doivent spécifiquement être prévus soit par le droit de l'Union européenne, soit par le droit de l'État membre auquel le responsable du traitement est soumis.

En qui concerne spécifiquement le traitement de catégories particulières de données à caractère personnel, le considérant (54) du RGPD reconnaît des hypothèses dans lesquels le traitement de catégories particulières de données à caractère personnel (données dites « sensibles ») *« peut être nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique, sans le consentement de la personne concernée. Un tel traitement devrait faire l'objet de mesures appropriées et spécifiques de façon à protéger les droits et libertés des personnes physiques ».*

[3] Articles L.1111-8 et L.1111-14 et suivants du Code de la santé publique.
[4] La directive 95/46/CE du 24 octobre 1995, 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 sera abrogée en date du 25 mai 2018 par le RGPD.

En effet, outre l'hypothèse d'un consentement explicite de la personne (article 9 paragraphe (2) lettre a) du RGPD), plusieurs situations peuvent légitimer un traitement portant sur des catégories particulières de données à caractère personnel, en particulier des données de santé. C'est notamment le cas lorsque « *le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel* » (article 9 paragraphe (2) lettre i) du RGPD), ou encore lorsque « *le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un 'État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* » (article 9 paragraphe (2) lettre g) du RGPD).

La Commission nationale estime que les traitements de données mis en œuvre au moyen d'un DSP activé d'office, avec possibilité pour le titulaire de s'y opposer, pourraient relever des motifs d'intérêt public important, et plus spécifiquement des motifs d'intérêt public dans le domaine de la santé publique visés à l'article 9 paragraphe (2) lettres i) et g) du RGPD susmentionné du RGPD, à condition que le droit national le prévoit et que cette législation prévoit de telles « *mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée* ».

L'article 6 paragraphe (3) du RGPD précise encore que la *« base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du règlement, entre autres: les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX ».*

Le considérant (45) du RGPD précise qu'il devrait « *[…] appartenir au droit de l'Union ou au droit d'un État membre de déterminer la finalité du traitement. Par ailleurs, ce droit pourrait préciser les conditions générales du présent règlement régissant la licéité du traitement des données à caractère personnel, établir les spécifications visant à déterminer le responsable du traitement, le type de données à caractère personnel faisant l'objet du traitement, les personnes concernées, les entités auxquelles les données à caractère personnel peuvent être communiquées, les limitations de la finalité, la durée de conservation et d'autres mesures visant à garantir un traitement licite et loyal. […]* »

Le considérant (41) énonce encore que *« cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne (ci-après dénommée « Cour de justice ») et de la Cour européenne des droits de l'homme. »*

Ainsi, la Commission nationale se doit de souligner l'importance fondamentale du principe de licéité d'un traitement de données à caractère personnel qui doit être lu à la lumière de l'article 8 paragraphe (2) de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée, ainsi que de l'article 52 paragraphes (1) et (2) de la Charte des droits

fondamentaux de l'Union européenne. En substance, ces deux articles, ensemble avec la jurisprudence constante de la Cour européenne des droits de l'Homme, retiennent qu'un traitement de données effectué par une autorité publique peut constituer une ingérence dans le droit au respect de la vie privée ou limiter l'exercice du droit à la protection des données. Cette ingérence ou limitation peut être justifiée à condition qu'elle:

- soit prévue par une loi accessible aux personnes concernées et prévisible quant à ses répercussions, c'est-à-dire formulée avec une précision suffisante ;
- soit nécessaire dans une société démocratique, sous réserve du principe de proportionnalité ;
- respecte le contenu essentiel du droit à la protection des données ;
- réponde effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui.

En ce qui concerne la première condition, selon la jurisprudence de la Cour européenne des droits de l'Homme, une ingérence au droit au respect de la vie privée n'est *« prévue par la loi »*, au sens de l'article 8 paragraphe (2) de la Convention, que si elle repose sur un article du droit national qui présente certaines caractéristiques. La loi doit être *« accessible aux personnes concernées et prévisible quant à ses répercussions »*[5]. Une règle est prévisible *« si elle est formulée avec une précision suffisante pour permettre à toute personne – bénéficiant éventuellement d'une assistance appropriée – d'adapter son comportement »*[6]. *« Le degré de précision requis de la "loi" à cet égard dépendra du sujet en question. »*[7]

Au niveau national, la Commission nationale tient à rappeler à cet égard l'exigence de la Cour constitutionnelle selon laquelle « *dans les matières réservées par la Constitution à la loi, l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc.* »[8]

Le Conseil d'Etat rappelle lui aussi régulièrement dans ses avis que *« (…) l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi.*

La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication (…). »[9]

---

[5] CouEDH, Amann c. Suisse [GC], n° 27798/95, 16 février 2000, para. 50 ; voir également CouEDH, Kopp c. Suisse, n° 23224/94, 25 mars 1998, para. 55 et CouEDH, Iordachi et autres c. Moldavie, n° 25198/02, 10 février 2009, para. 50.

[6] CouEDH, Amann c. Suisse [GC], n° 27798/95, 16 février 2000, para. 56 ; voir également CouEDH, Malone c. Royaume-Uni, n° 8691/79, 26 avril 1985, para. 66 ; CouEDH, Silver et autres c. Royaume-Uni, n° 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, para. 88.

[7] CouEDH, The Sunday Times c. Royaume-Uni, n° 6538/74, 26 avril 1979, para. 49 ; voir également CouEHD, Silver et autres c. Royaume-Uni, n° 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, para. 88.

[8] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015

[9] Voir par exemple : Conseil d'Etat, Avis n° 6975/5 du 7 juin 2016 relatif au projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures.

Si on se réfère donc à l'article 9 paragraphe (2) lettres i) et g) du RGPD comme base légale, il y a lieu de vérifier si le droit luxembourgeois prévoit des « *mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée* » telles qu'exigées par le RGPD. A cet égard, la CNPD avait déjà fait remarquer dans son avis n° 345/2010 précité que « *l'introduction d'un système généralisé de dossiers électroniques partagés répond au critère posé à l'article 8 paragraphe 4 de la directive 95/46/CE*[10] *dès lors que le projet de loi [n°6196 portant réforme du système de soins de santé] apporte les garanties appropriées suffisantes en matière de protection de la vie privée et des données personnelles* ».

Or, suite à l'adoption du projet de loi n°6196 susmentionné, l'article 60*quater* du Code de la sécurité sociale renvoie à un règlement grand-ducal afin de préciser les garanties prévues dans le cadre du DSP. A cet égard, il conviendra de veiller à une application rigoureuse des principes d'encadrement normatif susmentionnés s'agissant de la distinction entre ce qui doit relever, par essence, de la loi au sens stricte et ce qui peut faire l'objet d'un encadrement normatif par un texte réglementaire. La CNPD considère ainsi qu'au moins les dispositions concernant la durée de conservation des données au DSP, figurant actuellement aux articles 4 paragraphes (2) à (5) et 10 paragraphe (5) du projet, les dispositions réglementant les droits des titulaires mineurs non émancipés et titulaires majeurs protégés par la loi (actuel article 7 du projet), ainsi que la limitation du droit d'accès telle que prévue par l'article 9 paragraphe (2) et la limitation du droit à l'effacement (article 6)du projet devraient être prévues dans la loi au sens stricte du terme et plus précisément par l'article 60*quater* du Code de la sécurité sociale, et non pas dans un acte réglementaire. Elle reviendra sur ces différents points plus loin dans le présent avis.

b. La question de la responsabilité du traitement

L'article 60*ter* (4) du Code de la sécurité sociale prévoit que l'Agence nationale des informations partagées dans le domaine de la santé (ci-après désignée « l'Agence eSanté ») a la qualité de responsable du traitement des données à caractère personnel au sens de la loi modifiée du 2 août 2002.

En ce qui concerne précisément les questions de responsabilité, le groupe de travail « article 29 » a précisé que « *tout système de DME [dossiers médicaux électroniques] doit également garantir que le risque d'atteintes à la vie privée dû au stockage de données médicales et à la fourniture de ces données soit adéquatement contrebalancé par la responsabilité pour le préjudice causé, par exemple par l'utilisation incorrecte ou non autorisée de données des DME.* » Il a recommandé aux Etats membres désirant instaurer un système de DSP de « *mener minutieusement au préalable des études approfondies de droit civil et médical réalisées par des experts et des évaluations d'impact pour clarifier les nouvelles questions de responsabilité susceptibles de se poser dans ce contexte, notamment en ce qui concerne l'exactitude et l'exhaustivité des données inscrites dans le DME, la définition du degré de connaissance qu'un professionnel de santé traitant un patient doit avoir du DME de celui-ci ou les conséquences prévues par le droit de la responsabilité si l'accès est indisponible pour des raisons techniques, etc.* » [11]

---

[10] Son article 8 paragraphe 4 dispose que « *sous réserve de garanties appropriées, les États membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle.* »

[11] Document de travail (WP 131) sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007, p. 23.

Or, la CNPD considère que la responsabilité unique de l'Agence eSanté concernant les traitements des données à caractère personnel contenues dans le DSP ne correspond pas à la réalité tel que le système est envisagé. En effet, déjà dans son avis relatif au projet de loi n°6196 portant réforme du système de soins de santé, la CNPD a estimé qu'il résulte de l'économie générale dudit projet de loi que la responsabilité est exercée de manière conjointe.

Ainsi, tout professionnel de santé qui consulte un DSP est tenu de traiter les données de manière loyale et licite et dans le respect des finalités légales du traitement tel que prévu par l'article 5 paragraphe (1) lettres a) et b) du RGPD.

Ensuite, le professionnel de santé qui inscrit des informations dans un DSP est tenu de vérifier l'exactitude de ses informations et il doit s'astreindre à intégrer uniquement les données « *utiles et pertinentes*[12] ». L'article 5, paragraphe (1), lettres (c) et (d) du RGPD précise que les données à caractère personnel doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) (et) exactes et, si nécessaire, tenues à jour [...]* ».

Pour sa part, le médecin référent se voit attribuer un rôle plus important dans le fonctionnement du DSP. Ses missions sont plus nombreuses que celles qui incombent aux différents intervenants isolés. L'article 19bis du Code de la sécurité sociale précise que le médecin référent a notamment pour mission de « *3) suivre régulièrement le contenu du dossier de soins partagé de l'assuré* [...] ». L'article 8 paragraphe (2) alinéa 2 du projet de règlement grand-ducal prévoit d'ailleurs que le médecin référent est présumé intervenir dans la prise en charge du titulaire pendant la durée de relation patient médecin référent et de ce fait, il peut d'office accéder au DSP de ses patients et y verser des données.

Le groupe de travail « Article 29 » suggère par ailleurs qu'une seule personne soit responsable envers les patients de l'usage correct des demandes d'accès : « *Les systèmes de DME sont toutefois des systèmes de mise en commun d'informations qui comptent de nombreux responsables du traitement des données. Dans ces conditions, une seule institution spéciale doit être responsable envers les personnes concernées du traitement correct des demandes d'accès. Vu la complexité prévisible d'un DME pleinement opérationnel et la nécessité de faire en sorte que les patients aient confiance dans le système, il semble essentiel que les patients dont les données sont traitées dans un DME sachent comment contacter un partenaire responsable avec lequel ils peuvent discuter des éventuelles lacunes du système. Des dispositions spéciales à cet effet devront être incluses dans tout règlement sur les systèmes de DME.* »[13]

Enfin, l'Agence eSanté a une responsabilité particulière en matière de sécurité du système en étant chargée notamment d'une mission technique et administrative pour mettre en place l'architecture technique et organisationnelle du dossier de soins partagé.

La Commission nationale note par ailleurs que les différents intervenants doivent en tout état de cause, chacun pour ce qui le concerne, assumer les obligations prévues à l'article 32 du RGPD en matière de sécurité du traitement.

La notion de « responsabilité conjointe » introduite par le RGPD est à prendre en compte dans ce contexte, la Commission nationale étant d'avis qu'il ressort de l'économie générale de la loi du 17 décembre 2010 portant réforme du système de soins de santé que l'Agence eSanté d'un côté, et les professionnels de santé d'autre côté, participent conjointement à la réalisation

[12] Article 60*quater* paragraphe (2) du Code de la Sécurité sociale.
[13] Pages 23 et 24 du document de travail WP 131.

des finalités et des moyens du traitement tels que définis par le législateur. L'article 26 paragraphe (1) du RGPD exige que « *les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis.* »

Or, dans la mesure où le texte prévoit par exemple à l'article 6 paragraphe (5) que la rectification des données inexactes ou incomplètes dans un DSP peut être sollicitée par un titulaire auprès du professionnel de santé auteur de la donnée et non pas auprès de l'Agence eSanté, les droits des personnes concernées ne s'exercent pas exclusivement auprès du responsable du traitement, c'est-à-dire auprès de l'Agence e-Santé. La Commission nationale renvoie dans ce contexte à ses commentaires sous le point « *VI. Droits d'accès, d'écriture et d'opposition du titulaire* ».

Sur base des considérations ci-dessus, la CNPD est d'avis que l'article 60*ter* (4) du Code de la sécurité sociale devrait être modifié afin de prévoir les responsabilités des différents acteurs.

c. La question des sanctions

Dans son avis relatif au projet de loi n°6196 portant réforme du système de soins de santé, la CNPD avait critiqué le manque de précision quant à la responsabilité des différents intervenants du DSP et quant aux éventuelles sanctions :

« En définitive, la Commission nationale constate que les différentes obligations qui incombent au responsable du traitement sont, dans le projet de loi, éclatées entre différents intervenants au dossier de soins partagé. Or, en cas de non-respect des différentes obligations légales, le texte sous examen ne règle pas la question de la responsabilité. Notons que la loi du 2 août 2002 prévoit des sanctions pénales à l'égard du responsable du traitement. »[14]

En France, des sanctions pénales sont prévues en cas de manquement aux dispositions du Code de la santé publique concernant l'accès au dossier médical partagé.[15]

En ce qui concerne précisément les sanctions pénales, l'article 84 paragraphe (1) du RGPD prévoit que « *Les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives.* » Le considérant (149) y afférent énonce à ce titre que « *Les États membres devraient pouvoir déterminer le régime des sanctions pénales applicables en cas de violation du présent règlement, y compris de violation des dispositions nationales adoptées en application et dans les limites du présent règlement. Ces sanctions pénales peuvent aussi permettre la saisie des profits réalisés en violation du présent règlement. Toutefois, l'application de sanctions pénales en cas de violation de ces dispositions nationales et l'application de sanctions administratives ne devrait pas entraîner la violation du principe ne bis in idem tel qu'il a été interprété par la Cour de justice* »

[14] Délibération 345/2010 du 24 novembre 2010, p.5.
[15] Article L1111-18, alinéa 4 du Code de la santé publique.

Ainsi, la CNPD profite de l'occasion pour réitérer sa recommandation émise dans le cadre de son avis relatif au projet de loi n° 7184 portant création de la CNPD et la mise en œuvre du RGPD qu'afin « *de ne pas laisser impunis des agissements illicites perpétrés par des personnes physiques, que ce soit dans le cadre de traitements de données visées par le présent projet de loi ou du projet de loi 7168, la Commission nationale estime indispensable que le projet de loi érige en infraction pénale :*

- *le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite ou par des manœuvres trompeuses,*
- *le fait de vendre les données à caractère personnel obtenues par les moyens précités et*
- *le fait, par une personne qui a recueillie, à l'occasion de l'enregistrement, du classement, de la transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir (c'est-à-dire un détournement de finalité). »*

Ainsi, la CNPD estime qu'à l'instar du Code de la santé publique français la législation luxembourgeoise devrait prévoir des sanctions pénales en cas d'abus d'accès au DSP.

II. La création du dossier de soins partagé

A titre liminaire, la CNPD voudrait remarquer qu'en fournissant une définition du terme « patient », le commentaire relatif à l'article 1ier point 4 ne concorde pas avec la définition prévue audit point 4 concernant le terme « titulaire ». Ainsi, les auteurs du projet devraient analyser la pertinence de l'ajout de la définition du terme « patient » dans l'article 1ier du projet.

La Commission nationale s'interroge par ailleurs sur les catégories de données contenues dans le DSP lors de sa création / activation.

Selon l'article 1ier point 3° lettre b) de la loi du 13 décembre 2017 modifiant certaines dispositions du Code de la sécurité sociale, le paragraphe 2 de l'article 60*ter* du Code de la sécurité sociale est complété, entre autres, par les alinéas suivants :

« *L'annuaire référentiel d'identification des patients comprend les données d'identification, les caractéristiques personnelles et la situation de famille du patient ainsi que les noms, prénoms, adresses et numéros d'identification des représentants légaux des mineurs d'âge non émancipés et des personnes majeures protégées par la loi.*

[…]

L'annuaire référentiel d'identification des prestataires de soins comprend les données d'identification et les données en relation avec la profession et l'emploi du prestataire. »

Néanmoins, la Commission nationale se pose la question si les données issues de ces annuaires seront aussi intégrées dans les DSP ? Dans l'affirmative, les catégories de données inclues dans lesdits annuaires devraient être ajoutées à celles déjà prévues à l'annexe 1 du projet de règlement grand-ducal sous le numéro (2).

L'article 2 paragraphe (1) du projet prévoit ensuite que l'assuré est informé par le Centre commun de la sécurité sociale de la création d'un DSP par l'Agence eSanté, sans précisant à quel moment cette information aura lieu et sur quoi elle porte. La CNPD s'interroge à quel titre le Centre commun de la sécurité sociale intervient dans la mesure où l'obligation d'information incombe au responsable du traitement, c'est-à-dire à l'Agence eSanté. N'y a-t-il pas une incohérence entre le paragraphe (1) et le paragraphe (3) de l'article 2 ?

En vertu de l'article 2 paragraphe (2) du projet de règlement grand-ducal, le patient non affilié bénéficiant de soins de santé par un prestataire de soins établi au Luxembourg, peut demander l'ouverture d'un DSP moyennant un formulaire de demande à adresser à l'Agence eSanté. Le commentaire des articles précise à cet égard que ledit formulaire doit être accompagné des « *pièces justificatives nécessaires* ». La CNPD considère que cette catégorie de données manque de clarté et de précision et elle estime nécessaire de décrire de manière plus précise et concise ces *« pièces justificatives nécessaires »* dans le corps du texte. En effet, s'agissant d'une collecte de données et au regard du principe de proportionnalité et de nécessité (principe de minimisation des données prévu à l'article 5 paragraphe (1) lettre c) du RGPD), la CNPD n'est pas en mesure d'apprécier si ce principe est respecté.

L'article 2 paragraphe (3) du projet quant à lui oblige l'Agence eSanté à fournir certaines informations aux titulaires dès la création du DSP. Or, la liste des informations à communiquer aux personnes concernées a été allongée par rapport à la loi modifiée du 2 août 2002, respectivement à la directive européenne 95/46 du 24 octobre 1995, en vertu des articles 13 et 14 du RGPD (applicables à partir du 25 mai 2018), dépendant du fait si les données ont été collectées directement auprès de la personne concernée ou non.

Ainsi, il est important de préciser qu'à côté des informations prévues à l'article 2 paragraphe (3) du projet, l'Agence doit prendre en considération les listes d'informations obligatoires prévues aux articles 13 et 14 du RGPD. Elle doit par exemple informer les titulaires sur les finalités précises du DSP, les coordonnées du délégué à la protection des données, sur les destinataires ou les catégories de destinataires des données à caractère personnel, sur la durée de conservation des données à caractère personnel, ainsi que sur le droit d'introduire une réclamation auprès de la CNPD. De même, il parait utile d'informer les titulaires sur le contenu précis du DSP lors de son activation.

Finalement, l'exposé des motifs précise que « *le dossier de soins partagé ne se substitue pas au dossier individuel du patient que tout prestataire de soins doit obligatoirement tenir.* » La Commission nationale estime que cette précision devrait figurer dans le texte même du règlement grand-ducal en projet. Dans le cas où il serait tenu compte de cette suggestion de la CNPD, cette précision pourrait figurer dans un paragraphe (4) nouveau de l'article 2 du projet.

III. L'activation du dossier de soins partagé et accès par le titulaire

L'article 3 paragraphe (1) du projet précise que pour accéder à son DPS, le titulaire est obligé d'activer au préalable un compte sur la plateforme et de se connecter par après à l'application moyennant les identifiants de connexion lui envoyés par l'Agence eSanté selon l'article 2 paragraphe (3) lettre c) du projet. Or, le commentaire des articles indique que *« le titulaire doit lui-même activer son compte sur la plateforme pour recevoir ses identifiants de connexion »*. Néanmoins, lors de l'activation de son compte sur la plateforme, le titulaire devrait en principe déjà disposer de ses identifiants de connexion ?

De même, il ne ressort pas clairement du texte ce que les auteurs du projet entendent par « plateforme ». Ce n'est que si on lit la définition de la notion « Application dossier de soins partagé » (article 1ier, point 2 du projet) qu'on comprend qu'il s'agit de la plateforme électronique nationale d'échange et de partage de données de santé visée à l'article 60*ter* du Code de la sécurité sociale. Pour des raisons de compréhension, la CNPD suggère de préciser dans l'article 3 du projet que le DSP est accessible aux professionnels de santé, ainsi qu'à son titulaire, par voie électronique depuis un site internet.

Par ailleurs, en lisant l'article 3 paragraphe (3) du projet, on a l'impression qu'à défaut d'activation dans les 30 jours suivant l'envoi des informations visées à son article 2 paragraphe (3), le DSP peut exclusivement être consulté et alimenté par les professionnels de santé, et non plus par son titulaire. Le commentaire des articles précise toutefois que le titulaire peut, même après l'écoulement de ce délai, accéder à son DSP en procédant à son activation et à la configuration de son compte sur la plateforme.

Le commentaire des articles énonce dans ce même contexte qu'afin « *d'éviter la création de dossiers de soins partagés non utilisables par les professionnels de santé faute de création active d'un compte par les titulaires, il est prévu d'instaurer une période dite « blanche » au-delà de laquelle, à défaut d'activation du compte par son titulaire, le dossier devient* ***automatiquement fonctionnel pour les professionnels de santé.*** »

Or, même sans activation de compte par un titulaire sur la plateforme, la CNPD a pu comprendre qu'en vertu de l'article 8 paragraphe (2) du projet, un professionnel de santé peut uniquement accéder ou alimenter un DSP d'un titulaire dans le cadre d'une prise en charge documentée, à l'exception du médecin référent qui peut y accéder à tout moment. Ou est-ce que le fait que le DSP « *devient automatiquement fonctionnel pour les professionnels de santé* » implique que ces derniers pourront en dehors du cadre d'une prise en charge, suivant la matrice des accès d'habilitation par défaut, consulter et alimenter le DSP d'une personne qui pour une raison ou une autre n'aura pas pu prendre connaissance de la création de son DSP ?

La CNPD est ainsi d'avis que les auteurs du projet devraient au moins prévoir que le titulaire qui n'aura pas encore activé son DSP recevra une deuxième information lors du premier accès à son DSP par un professionnel de santé. Elle renvoie dans ce contexte également à ses observations formulées au point « *VIII. Droits d'accès et d'écriture des professionnels de santé* ».

IV. Fermeture et suppression du dossier de soins partagé

L'article 4 du projet accorde la possibilité au titulaire de fermer son DSP à tout moment, soit via l'application DSP, soit par demande à adresser à l'Agence eSanté.

La CNPD renvoie à ses commentaires sous le point « *I. Remarques préliminaires* » en ce qui concerne l'intégration des dispositions concernant la durée de conservation des données au DSP dans une loi, c'est-à-dire dans l'article 60*quater* du Code de la sécurité sociale et non pas dans un acte réglementaire.

A l'instar de l'article L.1111-18 du Code de la santé publique français, les données du DSP sont supprimées dix ans après sa fermeture par le titulaire. Pendant ce laps de temps et selon le commentaire des articles, les données versées au DSP deviennent inaccessibles au titulaire, ainsi qu'aux professionnels de santé. « *Toutefois, en vue de permettre ultérieurement non seulement au titulaire d'exercer son droit d'accès à ses données à travers l'Agence et la*

traçabilité des actions passées mais également afin de lui donner la possibilité de rouvrir son dossier sans perte préjudiciable pour sa bonne prise en charge au regard de la finalité du dossier de soins partagé, il est prévu de conserver les données pendant une durée de dix ans à partir de la fermeture. »[16]

La CNPD considère néanmoins qu'une durée d'archivage intermédiaire des données de dix ans apparaît comme excédant celle nécessaire au regard des finalités d'exercice du droit d'accès et d'une éventuelle réouverture du DSP. En effet, le DSP n'a pas vocation à se substituer aux dossiers des patients tenus par les médecins, établissements hospitaliers et autres professionnels de santé.

Par ailleurs, si on se réfère à l'avis des praticiens, c'est-à-dire aux professionnels de santé et en particulier à l'avis de l'Association des médecins et médecins-dentistes (ci-après : « l'AMMD »), cette durée de conservation ne correspondrait pas à la réalité des moyens et de l'utilité de la profession, alors qu'ils estiment qu'un professionnel de santé ne serait pas en mesure de consulter les données sur une période de dix ans. L'AMMD insiste sur le fait que la finalité de partage et d'échange de données ne soit pas détournée en une finalité de stockage ou d'archivage des données de santé contenues dans le DSP. Suivant l'adage « trop d'information tue l'information », elle est d'avis qu'un « *temps de conservation de 5 ans ou au-delà ne fera que saturer le DSP de documents inutiles voire obsolètes rendant ainsi laborieuse la consultation du DSP par les médecins et les autres prestataires de santé.* »[17]

Sur base des considérations ci-dessus, la CNPD estime qu'une durée de conservation des données de cinq ans suite à une fermeture d'un DSP respecte le principe de la limitation de conservation prévu par l'article 5 paragraphe (1) lettre e) du RGPD, selon lequel des données à caractère personnel doivent uniquement être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.* »

La CNPD renvoie aussi à ses observations sous le point X *« Délai de versement des données au dossier de soins partagé »* concernant l'appréciation de la durée de conservation des données dans le DSP en dehors du contexte d'une fermeture par le titulaire.

Par ailleurs, le paragraphe (3) de l'article 4 du projet énonce que les « *données du DSP sont supprimées* » dix ans après la fermeture du DSP à défaut de réouverture endéans ce délai. La CNPD estime néanmoins que non seulement les données doivent être supprimées du DSP, mais que le DSP en lui-même doit être supprimé intégralement.

La CNPD partage également la position de la CNIL exprimée dans son avis relatif au projet de décret en Conseil d'Etat autorisant la création d'un traitement de données à caractère personnel dénommé «dossier médical partagé»[18] en ce sens qu'elle recommande qu'en cas de clôture d'un DMP « *son titulaire soit informé que les données qu'il contient ne seront plus accessibles. Une telle information apparaît d'autant plus pertinente quand le DMP contient des données particulières telles que les directives anticipées du titulaire. Dans cette hypothèse, le titulaire pourrait, par exemple, être invité à recourir à l'un des autres modes de dépôt prévus pour les directives anticipées* ». Dans le cadre de ce projet, cette recommandation est aussi

[16] Commentaire de l'article 4 du projet de règlement grand-ducal.
[17] Avis de l'AMMD du 11 juillet 2017 au sujet du DSP et la durée de conservation des documents qui y sont attachés.
[18] Délibération no 2016-258 du 21 juillet 2016 de Commission nationale de l'informatique et des libertés portant avis sur un projet de décret en Conseil d'Etat autorisant la création d'un traitement de données à caractère personnel dénommé «dossier médical partagé» (demande d'avis no 16017107).

valable en ce qui concerne les volontés du titulaire en matière de don d'organes au sens de l'article 6 paragraphe (2) lettre b) du projet.

Finalement, la CNPD estime nécessaire de clarifier dans le projet quelles sont les modalités d'exercice des droits d'accès spécifiques au DSP d'une personne décédée et si, le cas échéant, ces accès s'exerceront conformément à l'article 19 de la loi du 24 juillet 2014 relative aux droits et obligations du patient.

V. Accès au dossier de soins partagé par les professionnels de santé

L'article 5 du projet règlemente l'accès au DSP par les professionnels de santé. Il ressort de son paragraphe (1) qu'afin d'accéder au DSP de ses patients, le professionnel de santé doit au préalable créer un compte sur la plateforme. Ce compte ne sera créé par l'Agence eSanté que sur demande explicite, soit d'un professionnel de santé individuel, soit d'une collectivité de santé. Un professionnel de santé a donc la possibilité de ne pas faire de telle demande et de refuser d'utiliser le DSP ? La CNPD constate donc qu'il y aura un système « d'opt-out » pour les patients, tandis que pour les professionnels de santé un système « d'opt-in » s'appliquera.

Notons encore que les auteurs du projet ne définissent pas la notion de « collectivité de santé ». Le commentaire de l'article 9 du projet se contente d'expliquer qu'il s'agit par exemple des établissements hospitaliers, laboratoires, des centres d'aide et de soins, etc.

VI. Droits d'accès, d'écriture et d'opposition du titulaire

L'article 6 du projet encadre les droits d'accès, d'écriture et d'opposition du titulaire. Pour ce qui est plus particulièrement du paragraphe (3), la CNPD a l'impression que la lettre b) se trouve en contradiction avec la lettre d) dans la mesure où d'abord le droit est accordé au titulaire de rendre inaccessible certaines données spécifiques aux professionnels de santé, « *à l'exception de son médecin référent et des professionnels d'un service d'urgence d'un établissement hospitalier* », alors qu'il lui est aussi accordé possibilité de refuser « *aux professionnels de santé d'un service d'urgence d'un établissement hospitalier l'accès aux données de niveau « restreint » ou en leur refusant l'accès à son dossier de soins partagé* ». Cette dernière hypothèse apparaît en elle-même contradictoire par rapport à son commentaire des articles qui énonce que « *le masquage peut être appliqué envers tout professionnel de santé (niveau privé) ou simplement envers certains d'entre eux (niveau restreint), à condition, dans ce dernier cas, qu'il ne s'agisse pas du médecin référent ou, sauf masquage étendu, d'un professionnel de santé d'un service d'urgence d'un établissement hospitalier.* »

Le groupe de travail européen « article 29 » a précisé dans ce contexte que même si un système de DSP n'a pas uniquement le consentement pour base juridique, « *la détermination par le patient lui-même de quand et comment ses données sont utilisées devrait constituer une garantie majeure* ».[19] L'autodétermination informationnelle du patient joue donc un rôle central au niveau de trois stades successifs : lors de la création du DSP, lors de l'inscription des données dans le DSP, ainsi que lors de la consultation du DSP par les professionnels de santé.

Par ailleurs, il ressort implicitement de l'article 6 du projet que le titulaire peut, soit s'opposer directement au préalable lors de sa prise en charge au versement de données dans son DSP, soit rendre inaccessible par le masquage une donnée spécifique aux professionnels de santé.

[19] Document de travail (WP 131) sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007, p. 15

A contrario, le titulaire ne dispose pas du droit de demander a posteriori la suppression d'une donnée de son DSP qu'il juge particulièrement sensible. Est-ce que le contrôle du titulaire sur ses données de santé ne devrait-il pas inclure cette possibilité de pouvoir supprimer (et non seulement masquer) un document de santé, d'autant plus que le médecin traitant aura toujours accès à ce document qui se trouvera dans son dossier patient ?

En ce qui concerne une limitation des droits des personnes concernées, comme notamment le droit à l'effacement (« droit à l'oubli »), l'article 23 paragraphe (1) du RGPD dispose que le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter, entre autres, la portée du droit à l'effacement prévu par l'article 16 du RGPD. Une telle limitation doit respecter l'essence des libertés et droits fondamentaux et elle doit constituer une mesure nécessaire et proportionnée dans une société démocratique pour garantir un des dix motifs y prévus. Une mesure législative limitative doit d'ailleurs contenir certaines dispositions spécifiques énumérées à l'article 23 paragraphe (2) du RGDP.

Ainsi, comme l'article 6 du projet sous examen limite implicitement le droit à l'effacement des titulaires d'un DSP, cette limitation doit être prévue par une loi au sens stricte du terme et respecter les exigences susmentionnées prévues à l'article 23 du RGPD.

Pour ce qui est précisément de la faculté pour le titulaire de rendre inaccessible « *certaines données spécifiques aux professionnels de santé [...]* », la CNPD estime que cette possibilité ne correspond pas à la réalité du système tel qu'il est conçu et elle se demande notamment comment concrètement l'Agence eSanté en tant que responsable du traitement entend faire droit à de telles requêtes. En effet, le DSP ne contient que peu de données individuelles ou structurées, mais se compose en réalité et surtout de documents scannés, chaque document contenant une multitude d'informations ou données de santé relatives à un patient.

LA CNPD est dès lors à se demander comment il pourra être garanti qu'un titulaire puisse rendre inaccessible « certaines données spécifiques » (par exemple des données relatives à une interruption volontaire de grossesse) contenues dans plusieurs documents médicaux scannés. A moins de rendre inaccessible l'intégralité de documents, elle est d'avis qu'il ne sera pratiquement pas possible de « masquer » ou d'isoler certaines données spécifiques dans l'ensemble des documents contenant ces données spécifiques.

Il y a donc lieu de constater que le texte du règlement grand-ducal en projet ne reflète pas la réalité, de sorte que les dispositions en question, pourtant fondamentales en termes de protection des données et de la vie privée, risquent de ne pas pouvoir être appliquées en pratique.

Le paragraphe (5) de l'article 6 prévoit finalement que la rectification des données inexactes ou incomplètes dans son DSP peut être sollicitée par le titulaire auprès du professionnel de santé auteur de la donnée. Or, l'article 16 du RGPD dispose que la « *personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes.* » En application du RGPD et du Code de la Sécurité sociale, la demande de rectification des données devrait être adressée par le titulaire à l'Agence eSanté en sa qualité de responsable du traitement.

A ce titre il est encore renvoyé aux observations faites au point « *l.c* » du présent avis relatif à la question du responsable du traitement du DSP, respectivement d'une responsabilité conjointe de l'Agence eSanté et des professionnels de santé.

VII. Titulaires mineurs non émancipés et titulaires majeurs protégés par la loi

L'article 7 du projet réglemente les droits des titulaires mineurs non émancipés et titulaires majeurs protégés par la loi. A titre préliminaire, quant à la forme la CNPD tient à souligner que l'article 7 déroge aux dispositions du Code civil. En effet, alors que l'article 7 paragraphe (1) alinéa 2 du projet accorde un droit de consultation au DSP au mineur âgé de 16 ans et plus (ou âgé de moins de 16 ans en cas de demande de son ou ses représentants légaux), l'article 488 du Code civil prévoit que la majorité est fixée à dix-huit ans accomplis et que ce n'est qu'à cet âge qu'une personne est capable de tous les actes de la vie civile. En ce qui concerne les majeurs protégés par la loi, des procédures spécifiques sont prévues aux articles 491 à 515 du Code Civil.

Or, en vertu du principe de la hiérarchie des normes, un acte réglementaire ne peut déroger à une loi. La CNPD estime dès lors nécessaire de prévoir les dispositions en question dans une loi.

Ceci dit, la Commission nationale voudrait formuler les observations suivantes quant au fond. Le considérant (58) du RGPD précise que les enfants méritent une protection spécifique et ainsi *« toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre. »*

Selon l'article 12 paragraphe (1) du RGPD, le responsable du traitement doit prendre des mesures appropriées pour fournir toute information ou procéder à toute communication au titre des articles 13 à 22 et 34 du RGPD et ceci d'une *« façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. »*

L'article 7, paragraphe (2) du projet sous examen prévoit que les informations prévues à l'article 2 paragraphe (3) du projet sont, en sus d'être adressées aux représentants légaux du titulaire mineur non émancipé, également transmises au mineur âgé de 16 ans ou plus et, en cas de demande de son ou ses représentants légaux, au mineur âgé de moins de 16 ans. Ainsi, la CNPD se demande s'il ne faudrait pas prévoir des feuillets d'information spécifique désignés aux mineurs en cause conformément au RGPD.

Par ailleurs, l'article 7 paragraphe (1) alinéa 3 du projet accorde la possibilité au titulaire mineur non émancipé de s'opposer au versement des données liées à une interruption volontaire de grossesse à son DSP. Or, la CNPD se demande pourquoi les auteurs ont choisi de limiter le projet à ce cas spécifique ? Elle suggère d'utiliser la formulation plus large du commentaire des articles prévoyant que ledit mineur peut « *dans les cas légalement prévus* » demander au professionnel de santé de ne pas introduire une donnée à son DSP afin de la garder confidentielle envers son ou ses représentants légaux.

Finalement, afin de respecter l'autodétermination informationnelle des mineurs devenus majeurs, la CNPD demande que la désactivation des identifiants de connexion personnels des représentants légaux au DSP du mineur devenu majeur s'opère de manière automatique.

VIII. Droits d'accès et d'écriture des professionnels de santé

Les droits d'accès et d'écriture des professionnels de santé sont prévus par l'article 8 du projet. Son paragraphe (1) renvoie à la matrice d'accès figurant à l'annexe 1 du projet en ce qui concerne les « *les droits d'accès et d'écriture maximaux par catégorie de données des professionnels de santé intervenant dans la prise en charge du titulaire* ».

En vertu de l'article 25 paragraphe (2) du RGPD, le responsable du traitement doit mettre « *en oeuvre 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 sont traitées* » (principe du « Privacy by Default »). Ledit article précise qu'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.* » Une matrice des accès par défaut, comme celle prévue à l'annexe 1 du projet sous examen, doit par principe être considérée comme étant contraire audit principe du « Privacy by Design ».

L'alinéa 2 du paragraphe (1) de l'article 8 du projet de règlement grand-ducal précise que ledit classement, ainsi que « *d'éventuelles restrictions d'accès et d'écriture à certains types de données à l'intérieur d'une même catégorie de données se font conformément aux procédures déterminées par l'Agence.* » Or, la Commission nationale est d'avis que le texte du règlement grand-ducal doit préciser quelles sont ces procédures.

Le paragraphe (2) de l'article 8 du projet prévoit des modalités spécifiques pour le « *classement d'un type de donnée au sein d'une catégorie de données* ». En se référant à ses commentaires sous le point « *VI. Droits d'accès, d'écriture et d'opposition du titulaire* » et en tenant compte du fait que figurent au sein du DSP surtout des documents scannés qui ne présentent aucune granularité, la CNPD rappelle que le texte du projet ne correspond pas à la réalité de la configuration des systèmes mis en place. Elle se demande notamment comment l'Agence eSanté en tant que responsable du traitement va maîtriser la situation dans laquelle plusieurs catégories de données se retrouvent dans un même document scanné et qu'un professionnel de santé n'a droit d'accéder uniquement à une catégorie, mais non pas à l'autre ?

Selon l'article 8 paragraphe (2) du projet, uniquement les professionnels de santé intervenant dans la prise en charge du titulaire peuvent y accéder selon la matrice des accès par défaut annexée au projet sous examen. Le but du DSP est précisément de regrouper à des fins de partage des données de santé d'un patient nécessaires pour lui assurer un meilleur suivi par les professionnels de santé qui s'occupent de lui. Il ressort ainsi implicitement de cet article que les données de santé contenues dans le DSP ne peuvent pas être utilisées pour d'autre fins, en excluant ainsi l'accès au DSP par « *des praticiens de la médecine qui agissent en tant qu'experts pour le compte de tiers: par exemple pour des compagnies d'assurance privées, dans des litiges, pour l'octroi de l'aide à la retraite, pour les employeurs de la personne concernée, etc.* » [20]

Déjà dans son avis n° 345/2010 précité, la CNPD avait estimé, dans le souci du respect des finalités pour lesquelles le DSP est institué, que la liste des destinataires ne devrait pas être élargie à l'avenir à d'autres catégories de personnes. Elle avait renvoyé dans ce contexte à l'article L1111-18 du Code français de la santé publique qui dispose ce qui suit : « *l'accès au dossier médical partagé est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. L'accès à ce dossier ne peut également être exigé ni préalablement à la conclusion d'un contrat, ni à aucun moment ou à aucune occasion de son application.* »

[20] Document de travail (WP 131) sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007, p. 18.

Ainsi, la CNPD rappelle qu'il est primordial d'inclure une telle disposition dans une loi, sinon dans le texte du projet de règlement grand-ducal sous avis.

Le paragraphe (2) de l'article 8 du projet, en limitant l'accès au DSP aux seuls professionnels de santé intervenant dans la prise en charge du titulaire, parait par ailleurs en contradiction avec l'article 10 paragraphe (1) du projet, en ce sens qu'il autorise tout professionnel de santé, sans distinction s'il intervient dans la prise en charge du titulaire ou non à verser toute donnée qu'il détient et qu'il estime utile et pertinente au DSP *« dans un délai raisonnable après la prise de connaissance de cette donnée ou après son premier accès au dossier de soins partagé si cette donnée est antérieure à son activation. »* La CNPD renvoie à ce titre à ses commentaires sous le point « *X. Délais de versement des données au dossier de soins partagé* ».

L'article 8 paragraphe (4) du projet permet au prestataire de santé d'inclure une information dans un DSP qui sera temporairement inaccessible au titulaire jusqu'à ce qu'une consultation médicale avec ce dernier aura lieu. Comme cette possibilité se trouve en contradiction avec la philosophie générale du DSP où le contrôle réside auprès du titulaire, la CNPD est d'avis que cette faculté devrait être strictement encadrée et limitée au cas strictement nécessaires et proportionnels.

Dans son avis précité, la Commission consultative statutaire « aspects éthiques et déontologiques en relation avec la protection et l'accessibilité des données » a estimé que la possibilité d'un masquage ciblé de documents devrait être offerte aux professionnels de santé désireux de procéder à une consultation d'annonce de leur contenu, sous condition « *de prévoir en tant que garde-fous [...] la levée automatique du masquage après l'écoulement d'un délai raisonnable (par exemple de six semaines).* »

C'est précisément ce que le législateur français a prévu, alors que l'article R1111-42 du Code de la santé publique prévoit que *« dans un délai de deux semaines suivant le versement d'une information inaccessible, et en l'absence de la consultation d'annonce, le patient est informé par tout moyen y compris dématérialisé d'une mise à jour de son dossier médical partagé, l'invitant à consulter un professionnel de santé, notamment son médecin traitant, pour en prendre connaissance. Si la consultation d'annonce n'a pas eu lieu un mois après le versement de l'information dans le dossier médical partagé du patient, elle devient automatiquement accessible. »* Ainsi, la CNPD estime nécessaire que les auteurs précisent une telle durée limitée de masquage dans le projet de règlement grand-ducal.

Par ailleurs, il ressort de l'article 8 paragraphes (2) et (3) du projet, ainsi que du commentaire des articles, que contrairement aux professionnels de santé exerçant dans un cabinet médical privé, ceux qui interviennent dans une collectivité de santé ou dans un service d'urgence n'ont pas besoin de recevoir au préalable, lors de l'acte ou de la consultation, l'identifiant de connexion du titulaire, mais peuvent directement y accéder. Bien sûr, le commentaire des articles précise qu'un « *titulaire a toujours le droit de s'opposer à l'accès soit au moment de son admission soit moyennant configuration dans son DSP* ». Cette différence de traitement est justifiable en ce qui concerne les services d'urgence, le titulaire n'étant souvent pas en état de fournir ses identifiants. Or, qu'en est-il de la différence de traitement entre les professionnels de santé exerçant dans un cabinet médical privé et ceux qui interviennent dans une collectivité de santé ? Comment « la prise en charge », qui n'est d'ailleurs pas définie, est-elle constatée ou documentée par une « collectivité de santé » (qui n'est pas non plus définie par le texte en projet), étant donné que le patient ne donne pas son identifiant de connexion à la collectivité de santé pour manifester son accord à l'accès de son DSP ? Autrement dit, comment le patient peut-il savoir qu'une collectivité de santé (par exemple un laboratoire, un centre d'aide et de soins, etc.) va accéder à son DSP et qu'il a la possibilité de refuser l'accès

à son DSP, s'il n'en a pas conscience ou s'il n'en est pas informé ? Le texte du projet reste muet à ce sujet, alors qu'il ne prévoit aucune obligation pour une collectivité de santé d'informer le patient en ce sens au moment de la prise en charge.

La CNPD doit dès lors insister que le règlement grand-ducal prévoit une disposition qui oblige une collectivité de santé d'informer le patient qu'elle entend accéder à son DSP et qu'il a la possibilité de refuser l'accès ; la collectivité de santé devra être en mesure de démontrer que cette information au patient a bien eu lieu. La CNPD rappelle dans ce contexte sa recommandation déjà formulée en 2010 que le recours à une « carte de santé » de type « carte vitale française » ou « elektronische Gesundheitskarte » allemande faciliterait ce procédé, de même qu'elle faciliterait l'utilisation d'autres procédés / fonctionnalités dans le cadre du système du DSP (tel que par exemple le recours à un identifiant de connexion peu pratique ou convivial).

La CNPD s'interroge en outre si un patient ne s'oppose pas lors de son admission dans un établissement hospitalier à l'accès à son DSP, est-ce que par défaut tous ceux qui travaillent dans cet établissement auront accès à son DSP ?

A ce titre, le commentaire des articles y répond en précisant qu'en *« cas de séjour dans un établissement, seuls les professionnels de santé intervenant dans la prise en charge du titulaire peuvent accéder à son dossier de soins partagé* ***et non l'ensemble des membres du personnel de cet établissement***. » La CNPD estime cependant que cette précision doit figurer au texte du projet sous avis.

Le commentaire des articles précise dans ce contexte qu'il « *appartient aux collectivités de santé de mettre en place les mesures adéquates en vue d'assurer le respect de cette matrice.* » Pour vérifier la conformité de ces mesures, , ainsi que pour permettre aux titulaires des DSP d'avoir un droit de regard sur qui a accédé leur DSP, la CNPD estime nécessaire que le texte prévoit l'obligation pour les collectivités de santé de mettre en place des systèmes de traçage des accès qui sont nominatifs et individuels. Ainsi, elle recommande aux auteurs d'ajouter à la fin du paragraphe (1) de l'article 9 du projet les mots suivants : « *indépendamment du fait si cette personne est un professionnel de santé individuel ou fait partie d'une collectivité de santé* ».

Enfin, la Commission nationale se demande comment l'« accord » du titulaire qui permet à l'introducteur d'une donnée de limiter son accès en vertu de l'article 8 paragraphe (5) du projet se manifestera concrètement. Est-ce qu'il s'agit d'un consentement écrit du titulaire, acté dans le DSP, ou d'un simple consentement oral ? L'article 7 du RGPD prévoit dans ce contexte que si un traitement repose sur le consentement de la personne concernée, le responsable du traitement doit être en *« mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant. »* En application de cette disposition et sauf modification ultérieure du texte concernant une éventuelle responsabilité conjointe comme préconisée par la CNPD, l'Agence eSanté devrait être en mesure de prouver que le titulaire a consenti à ce que l'introducteur d'une donnée peut limiter son accès tel que prévu audit article 8, paragraphe (5) du projet.

IX. Traçabilité des accès et des actions

L'article 9 du projet ne précise pas pendant combien de temps les données de journalisation seront conservées à partir de leur enregistrement. Ce n'est qu'en lisant le commentaire des articles qu'on comprend que la durée de conservation des traces est la même que celle des

données du DSP. Or, la CNPD estime nécessaire de préciser la durée de conservation des données de journalisation dans le corps du texte du projet sous examen.

Le paragraphe (2) de l'article en cause prévoit que le titulaire, ses représentants légaux et le médecin référent peuvent consulter l'ensemble des traces des accès et des actions relatives aux données du DSP, hormis celles concernant les données qui leur ont été rendues inaccessibles conformément aux dispositions du présent règlement. En ce qui concerne une limitation des droits des personnes concernées, comme notamment le droit d'accès, l'article 23 paragraphe (1) du RGPD dispose que le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter, entre autres, la portée du droit d'accès prévu par l'article 15 du RGPD. Une telle limitation doit respecter l'essence des libertés et droits fondamentaux et elle doit constituer une mesure nécessaire et proportionnée dans une société démocratique pour garantir un des dix motifs y prévus. Une mesure législative limitative doit d'ailleurs contenir certaines dispositions spécifiques énumérées à l'article 23 paragraphe (2) du RGDP.

Ainsi, comme l'article 9 paragraphe (2) du projet sous examen limite le droit d'accès des titulaires, représentants légaux et médecins référents, cette limitation doit être prévue par une loi au sens stricte du terme et respecter les exigences susmentionnées prévues à l'article 23 du RGPD.

X. Délai de versement des données au dossier de soins partagé

L'article 10 paragraphe (3) prévoit que certaines données utiles et pertinentes doivent être versées au DSP au plus tard « *quinze jours après la fin de la prise en charge par le professionnel de santé qui en est l'auteur [...]* » La Commission nationale estime qu'il serait utile de définir la notion de « prise en charge », respectivement « fin de la prise en charge ».

Ensuite, conformément à l'article 8 paragraphe (2) du projet, le professionnel de santé, hormis le médecin référent, ne saura en principe plus accéder au DSP d'un de ses patients au-delà du délai de 15 jours après la prise en charge du titulaire. Or, l'article 10 paragraphe (1) du projet est en contradiction avec l'article 8 paragraphe (2) du projet alors qu'il prévoit que le *« professionnel de santé détenteur d'une donnée qu'il estime utile et pertinente au sens de l'article 60quater, paragraphe 2 du Code de la sécurité sociale, verse celle-ci au dossier de soins partagé dans un délai raisonnable après la prise de connaissance de cette donnée ou après son premier accès au dossier de soins partagé si cette donnée est antérieure à son activation. »*

Est-ce que le professionnel de santé pourra donc accéder au DSP en dehors d'une prise en charge du titulaire, alors qu'en principe il n'aura pas accès d'office au DSP sans l'identifiant de connexion du titulaire ? Pourquoi ne précise-t-on pas qu'après l'écoulement d'un délai de 15 jours suivant son premier accès au DSP, le professionnel de santé devra y verser les données qu'il juge utiles et pertinentes et qui sont antérieures à l'activation du DSP ?

En ce qui concerne la conservation des données au DSP, en dehors de l'hypothèse d'une fermeture active par son titulaire, l'article 10 paragraphe (5) du projet prévoit une durée de conservation de dix ans à compter du versement des données dans le DSP, *« à l'exception des informations relatives à l'expression personnelle du titulaire qui sont conservées jusqu'à ce que le titulaire les modifie ou supprime et de certaines données médicales jugées utiles et pertinentes à vie par le médecin qui sont conservées jusqu'à la fermeture du dossier de soins partagé. »*

Au regard du RGPD, il est nécessaire et primordial de définir une durée de conservation des données au sein du DSP, qui soit proportionnée au regard de la finalité du DSP. Partant, il est nécessaire de définir des critères objectifs permettant de justifier une durée de conservation adéquate, étant entendu que le DSP ne se substitue pas au dossier médical tenu par les professionnels de santé « *pendant dix ans au moins à partir de la date de la fin de la prise en charge.* » [21]

L'exposé des motifs du projet précise d'ailleurs que le DSP « *n'a pas vocation à être exhaustif mais exclusivement à regrouper parmi les catégories de données mentionnées à l'article 60quater paragraphe 2 celles qui sont utiles et pertinentes pour la continuité et la coordination des soins du patient.* »

Si le critère retenu est donc celui de la continuité et de la coordination des soins, la durée de cette coordination est nécessairement variable selon la nature de la pathologie et la prise en charge envisagée par les professionnels de santé. Toutefois, suivant le commentaire des articles, les auteurs du projet ont décidé de fixer, sauf exceptions susmentionnées, une durée de conservation unique pour toutes les catégories de données *« étant donné la diversité de données susceptibles d'être versées au dossier et la variabilité dans le temps de leur caractère utile et pertinent respectif dans le parcours de soins […]. »* Les auteurs ajoutent que *« compte tenu de la finalité d'échange et de partage de données importantes pour une meilleure qualité et sécurité dans le parcours des soins, cette durée est fixée de manière à garantir que tous les patients, y inclus ceux qui consultent moins régulièrement, puissent disposer d'un minimum de données importantes dans leur dossier. »*

Or, comme mentionné sous le point « *IV. Fermeture et suppression du dossier de soins partagé* », les professionnels de santé et en particulier les médecins, représentés par l'AMMD, considèrent par contre qu'une durée de conservation de dix ans ne correspond pas à la réalité des moyens et de l'utilité de la profession, alors qu'ils estiment qu'un professionnel de santé ne serait pas en mesure de consulter les données sur une telle période. Suivant l'adage « trop d'information tue l'information », elle est d'avis qu'un « *temps de conservation de 5 ans ou au-delà ne fera que saturer le DSP de documents inutiles voire obsolètes rendant ainsi laborieuse la consultation du DSP par les médecins et les autres prestataires de santé.* »[22]

Le Collège médical émet des réserves similaires : il est d'avis qu'il faudrait : « *élaborer une stratégie d'hiérarchisation de la pertinence des données et leur révision régulière, en vue de supprimer ou de transférer en arrière-plan les données non pertinentes* » et que « *la conservation d'anciennes données confirmées ou infirmées par de nouvelles données concernant le même objet n'a aucun intérêt* ».[23] Selon le Collège médical, ces données devraient pouvoir être supprimées pour ne pas encombrer inutilement le DSP.

Les principes de minimisation des données et de la limitation de la conservation, exigent que seules des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités spécifiques soient traitées et conservées pendant une durée n'excédant pas celle nécessaire au regard desdites finalités (article 5 paragraphe (1) lettres c) et e) du RGPD). Considérant que le DSP a comme finalité principale le partage et l'échange de données utiles et pertinentes entre professionnels de santé pour une meilleure qualité de soins, que le DSP n'a pas comme vocation d'être exhaustif, qu'il ne se substitue pas aux dossiers tenus par les

[21] Selon l'article 15 paragraphe (4) de la loi du 24 juillet 2014 relative aux droits et obligations du patient.
[22] Avis de l'AMMD du 11 juillet 2017 au sujet du DSP et la durée de conservation des documents qui y sont attachés.
[23] Avis du Collège médical du 29 novembre 2017 sur le projet de règlement grand-ducal sous examen.

professionnels de santé ou les établissements hospitaliers et qu'il n'a certainement pas comme finalité de stockage ou d'archivage, la CNPD estime qu'une durée de conservation de cinq ans à compter du versement des données dans le DSP est suffisante et appropriée au regard des finalités réellement et légalement poursuivies.

Comme déjà indiqué sous le point « *IV. Fermeture et suppression du dossier de soins partagé* », la CNPD estime nécessaire d'intégrer les dispositions concernant la durée de conservation des données au sein du DSP dans une loi, c'est-à-dire dans l'article 60*quater* du Code de la sécurité sociale, et non pas dans un acte réglementaire.

Enfin, le paragraphe (5) de l'article 10 prévoit que certaines données médicales jugées utiles et pertinentes à vie par le médecin sont conservées jusqu'à la fermeture du DSP. Le commentaire des articles énumère à titre d'exemple *« des données relatives à des allergies ou maladies chroniques pouvant avoir des conséquences graves ou à des antécédents chirurgicaux importants comme par exemple des transplantations d'organes. »*

La Commission nationale ne remet pas en cause l'utilité de conserver de telles données de santé fondamentales « à vie » dans le DSP. Néanmoins, elle se demande si chaque professionnel de santé qui a accès au DSP d'un titulaire peut inscrire de telles données dans le DSP et si, le cas échéant, le titulaire du DSP sera au moins alerté lors d'une telle inscription ?

XI. Sécurité de la plateforme électronique nationale

La Commission nationale rappelle qu'en vertu de l'article 32 du RGPD, le responsable du traitement doit mettre en œuvre les mesures appropriées afin de garantir un niveau de sécurité adapté au risque.

Elle est par ailleurs d'avis que la protection de la confidentialité et de la sécurité des données à caractère personnel constitue un enjeu majeur en cas de traitement de données sensibles (données de santé) dans la mesure où la divulgation de ces données pourrait causer un préjudice grave aux patients. Ces risques augmentent avec le recours accru aux nouvelles technologies par les professionnels de santé qui pourraient utiliser des dispositifs mobiles (tablettes) pour accéder à leur compte et aux DSP de leurs patients.

Selon l'article 11 paragraphe (1) du projet, l'Agence eSanté s'engage à mettre en œuvre un système de management de la sécurité de l'information certifié conforme à la Norme internationale ISO/IEC 27001. Néanmoins, la CNPD suggère de préciser dans le texte du projet de règlement grand-ducal le périmètre minimum sur lequel ladite certification ISO devra se porter. Le périmètre devra porter sur l'intégralité des systèmes, processus et éléments organisationnels impliqués directement ou indirectement sur la plateforme et reflétant bien, le cas échéant, la situation de la responsabilité conjointe.

L'article 11 paragraphe (1) lettre e) du projet envisage la « *mise en place d'audits de sécurité annuels* ». L'article 32 paragraphe (1) du RGPD contient dans ce contexte une liste non exhaustive de mesures techniques et organisationnelles que le responsable du traitement et le sous-traitant doivent mettre en œuvre afin de garantir un niveau de sécurité adapté au risque. Une de ces mesures est précisément la mise en place 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* » (article 32 paragraphe (1) lettre d) du RGPD). Si les auteurs du projet de règlement grand-ducal sous avis entendent viser cette disposition du RGPD, ils devraient en préciser les détails dans le corps du texte. Entre autres,

la CNPD estime nécessaire de définir si ces audits seront effectués par des auditeurs indépendants ou par des auditeurs externes à l'Agence eSanté. De même, le projet reste muet sur le périmètre spécifique de ces audits, alors qu'une approche régulièrement adoptée en la matière se manifeste par un plan d'audit tri-annuel validé par le conseil d'administration pour qu'au bout de 3 ans, toutes les procédures ont été auditées.

Le paragraphe (2) dudit article oblige les prestataires et éditeurs d'un programme informatique connecté à la plateforme nationale à mettre en œuvre des mesures de sécurité appropriées au regard de son type, de sa taille, de ses processus ou de ses activités. Or, la CNPD est d'avis que la taille du prestataire ou éditeur n'est pas à considérer comme un critère pertinent dans ce contexte. En effet, l'article 32 paragraphe (1) du RGPD précise que les mesures techniques et organisationnelles à mettre en place doivent être adaptées à « *l'état des connaissances, des coûts de mise en oeuvre 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 risque peut par exemple être particulièrement élevé si un prestataire a accès à un grand nombre de DSP.

Par ailleurs, même si des précisions quant à la notion d'un « prestataire » se retrouvent dans le commentaire des articles *(« Vu la diversité des prestataires susceptibles de se connecter à la plateforme ou d'utiliser l'une de ses applications, à savoir un établissement hospitalier, une pharmacie, un laboratoire d'analyses médicales et de biologie clinique, une association de médecins ou un cabinet individuel et, pour les données mentionnées à l'article 60quater, paragraphe 2 du Code de la sécurité sociale, un réseau d'aides et de soins, un centre semi-stationnaire, un établissement d'aides et de soins, un établissement à séjour intermittent [...] »)*, la CNPD recommande aux auteurs d'ajouter une définition dudit terme à l'article 1ier du projet.

En ce qui concerne particulièrement les éditeurs d'un programme informatique connecté à la plateforme nationale, on pourrait interpréter l'article 11 (2) du projet de telle manière que ces derniers pourraient se connecter directement à la plateforme. Or, la CNPD tient à souligner qu'il n'est pas acceptable que des acteurs IT aient eux-mêmes un accès direct au DSP, ceci n'étant absolument pas la pratique en la matière.

Enfin, la Commission nationale se demande à quelles intervalles l'Agence eSanté entend mettre en œuvre les mesures de sensibilisation du personnel telles que prévues à l'article 11 paragraphe (2) lettre e) du projet.

XII. Modalités techniques de versement des données au dossier de soins partagé et interopérabilité

Selon l'article 12 paragraphe (2) alinéa 4 lettre a) du projet, les tests mentionnés au paragraphe 2, alinéa 3 lettre a) dudit article seront effectués non pas par l'Agence eSanté, mais par un organisme ou une société experte en interopérabilité des systèmes de santé. La CNPD se pose surtout la question qui devra assumer les frais concernant les travaux de cet expert, et surtout qui désignera cet expert et sur base de quels critères les compétences de ce dernier seront vérifiées ?

Le paragraphe (2) de l'article 12 du projet continue en ce sens qu'une attestation de conformité sera délivrée par l'Agence eSanté sur base du résultat des tests réalisés par l'expert susmentionné. Or, sur quels critères l'Agence eSanté va-t-elle baser sa décision et comment va-t-elle se décider concrètement ? Est-ce que des représentants ne faisant pas partie de l'Agence eSanté seront impliqués pour garantir l'indépendance de la décision? La CNPD recommande ainsi aux auteurs d'indiquer dans le projet que l'Agence eSanté doit mettre en place un règlement d'ordre intérieur fixant les procédures de délivrance, de blocage et de retrait des attestations afin de garantir une équité de traitement des attestations pour tous les acteurs.

Enfin, dans l'article 12 paragraphe (2) alinéa 6 du projet il est indiqué que l'attestation des résultats des tests reste valable tant qu'aucune modification ne l'affecterait. Or cette approche ne correspond pas au bonnes pratiques en la matière, car même sans changement dans les systèmes, des nouvelles vulnérabilités dans des applications existantes pourraient tout à fait être découvertes et par la suite potentiellement exploitées. Ainsi la CNPD estime qu'une « procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement » telle que préconisée dans l'article 32 (1) (d) du RGPD devrait être mise en place – et ceci indépendamment si des modifications ont eues lieu.

XIII. Coopération et échanges transfrontalier

La CNPD constate que le transfert de données de santé par l'Agence eSanté au point de contact « santé en ligne » d'un autre Etat est subordonné au consentement préalable du titulaire. En prenant en considération que ce transfert comportera certainement des catégories particulières de données à caractère personnel, dont notamment des données de santé, la CNPD tient à relever qu'en vertu de l'article 9 paragraphe (1) lettre a) du RGPD, ce consentement par la personne concernée doit être « explicite ».

Enfin, il est important de mentionner qu'en sus des informations prévues à l'article 13 paragraphe (1) du RGPD, l'Agence doit informer les patients sur l'existence du droit de retirer leur consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci (article 13 paragraphe (2) lettre c) du RGPD).

Ainsi décidé à Esch-sur-Alzette en date du 5 avril 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	Christophe Buschmann Membre effectif