

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

Délibération n° 489/2018 du 7 décembre 2018

Conformément à l'article 57 paragraphe (1) lettre (c) du règlement européen 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 (ci-après désigné « le RGPD »), chaque autorité de contrôle a pour mission de conseiller « conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ». L'article 7 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit précisément que la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») exerce les missions dont elle est investie en vertu de l'article 57 du RGPD.

Par courrier du 12 octobre 2018, Madame la Ministre de la Santé a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire (ci-après « le projet de règlement grand-ducal »).

Il ressort du commentaire des articles que ce projet de règlement grand-ducal vise à répondre aux exigences formulées à l'article 2, paragraphe (2), à l'article 3 paragraphe (1), à l'article 5 paragraphe (2), à l'article 7 paragraphe (3), ainsi qu'à l'article 10 paragraphe (2), alinéa 2 et paragraphe (3) de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique (ci-après : « la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies »).

Le projet de règlement grand-ducal sous avis a plus précisément comme objet de dresser une liste des maladies à déclaration obligatoire et des maladies présentant une menace grave pour la santé publique, ainsi que le délai endéans duquel la déclaration doit être faite au directeur de la Santé ou à son délégué (ci-après désigné sous « l'autorité sanitaire ») par les médecins, les médecins-dentistes et les responsables des laboratoires d'analyses médicales (article 1^{er} du projet de règlement grand-ducal pris sur base de l'article 2, paragraphe (2), de l'article 3



Avis de la Commission nationale pour la protection des données

à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

paragraphe (1) et de l'article 5 paragraphe (2) de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies).

L'article 2 du projet de règlement grand-ducal sous avis vise d'un côté à fixer une liste des maladies pour lesquelles la souche isolée ou le matériel biologique est à transférer par le laboratoire d'analyses médicales après établissement du diagnostic au laboratoire national de référence, sans demande spécifique par l'autorité sanitaire, ainsi que les délais y afférents, tel que prévu par l'article 7 paragraphe (3) de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies. D'autre côté, l'article en cause détermine les souches bactériennes, virales ou parasitaires pour lesquelles un laboratoire national de référence peut être désigné (tel que prévu par l'article 10 paragraphe (3) de la loi en cause). Finalement, l'article 10 paragraphe (2), alinéa 2 de ladite loi quant à lui laisse le soin au règlement grand-ducal sous avis de prévoir un modèle d'un cahier de charge visant à réaliser l'appel à candidatures par le ministre ayant la Santé dans ses attributions pour désigner un laboratoire national de référence.

Les articles 3 et 4 de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies indiquent quelles données à caractère personnel les déclarations de telles maladies par les médecins, médecins-dentistes et les laboratoires d'analyses médicales à destination de l'autorité sanitaire doivent comporter.

Pour rappel, la Commission nationale a rendu, le 10 mai 2017¹, un avis relatif au projet de loi n°7160 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique (ci-après « le projet de loi »)², devenu la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies. Dans ledit avis, la CNPD s'était souciée notamment du recours à des données nominatives sans mise en place de mesures d'anonymisation irréversible des données, du manque de précisions quant aux mesures de sécurité et à la durée de conservation des données à caractère personnel, ainsi qu'à l'obligation de respecter le droit à l'information des personnes concernées. Au vu de la teneur actuelle de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies, la Commission nationale constate qu'elle n'a malheureusement pas été suivie par le législateur dans la majorité de ses recommandations.

Dès lors, la Commission nationale saisit l'occasion de réitérer certaines observations ayant trait au respect de la vie privée et la protection des données à caractère personnel dans le cadre du projet de règlement grand-ducal sous avis qui concernent aussi la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies. Par ailleurs, comme son avis précité du 10 mai 2017 a été émis sur base de l'ancienne loi du 2 août 2002 relative à la protection des personnes

¹ Délibération n°401/2017 du 10 mai 2017.

² Nouvel intitulé entier du 8 mai 2018: « *Projet de loi sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique et modifiant : 1. la loi modifiée du 29 avril 1983 concernant l'exercice des professions de médecin, de médecin-dentiste et de médecin-vétérinaire ; 2. la loi modifiée du 16 juillet 1984 relative aux laboratoires d'analyses médicales ; 3. la loi modifiée du 16 janvier 1990 relative aux dispositifs médicaux ; 4. la loi modifiée du 8 juin 1999 relative au Collège médical ; 5. la loi du jj/mm/aaaa sur les conditions d'hygiène et de salubrité relatives à la pratique des techniques de tatouage par effraction cutanée, du perçage, du branding, cutting, ainsi que du bronzage UV* ».



Avis de la Commission nationale pour la protection des données

à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

à l'égard du traitement des données à caractère personnel,³ elle tient à ajouter certaines observations se basant spécifiquement sur le RGPD.

1. Quant à la base de légitimité de la création d'un système centralisé des maladies infectieuses

D'après l'exposé des motifs du projet de loi n°7160, ledit projet permet « *d'améliorer le système de surveillance des maladies infectieuses au Grand-Duché de Luxembourg et de regrouper les données portant sur les maladies infectieuses dans un système centralisé.* » L'exposé continue en ce sens qu'afin d'éviter des doubles notifications et de permettre l'investigation d'épidémies ou d'alertes, « *les déclarations doivent être nominatives, mais la confidentialité et la sécurité du traitement des données personnelles doivent être strictement garanties par l'ensemble des acteurs impliqués.* » En effet et comme susmentionné, la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies, qui est issue du projet de loi n°7160, contient dans ses articles 3 et 4 une liste de données à caractère personnel que les déclarations de maladies par les médecins, médecins-dentistes et les laboratoires d'analyses médicales à destination de l'autorité sanitaire doivent comporter « au moins ». Il s'agit plus particulièrement du nom, prénom, adresse, date de naissance, sexe, diagnostic médical du patient, ainsi que pour les déclarations effectuées par les médecins et médecins-dentistes de la date des premiers symptômes et du diagnostic, du pays où la maladie a été contractée et, le cas échéant, de la source d'infection. Les déclarations des laboratoires d'analyses médicales contiennent par ailleurs la date et l'origine du prélèvement des analyses du patient.

Il convient de noter dans ce contexte que 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'Etat 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 Ladite loi a été abrogée par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.



Avis de la Commission nationale pour la protection des données

à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

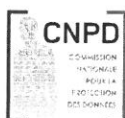
En effet, outre l'hypothèse d'un consentement explicite de la personne (article 9 paragraphe (2) lettre a) du RGPD), plusieurs situations peuvent légitimer un traitement portant sur des catégories particulières de données à caractère personnel, en particulier des données de santé. C'est notamment le 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).

La Commission nationale estime que les traitements de données mis en œuvre dans le cadre de la création du système centralisé des maladies infectieuses (ci-après : « le système centralisé ») relèvent des motifs d'intérêt public dans le domaine de la santé publique visés à l'article 9 paragraphe (2) lettre i) 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.* »



Avis de la Commission nationale pour la protection des données

à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

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 ». 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 ». « Le degré de précision requis de la "loi" à cet égard dépendra du sujet en question. »

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. »

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 (...). »



Avis de la Commission nationale pour la protection des données

à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

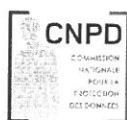
La CNPD ne peut dès lors que saluer que l'Etat luxembourgeois ait pris la décision de respecter les exigences développées ci-avant en légiférant en la matière. Si on se réfère donc à l'article 9 paragraphe (2) lettre i) du RGPD comme condition de licéité, il y a lieu de vérifier si le droit luxembourgeois prévoit des « *mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée* » telles qu'exigées par le RGPD. Or, comme la CNPD n'a pas été suivie dans le contexte de son avis du 10 mai 2017 émis dans le cadre du projet de loi n°7160 susmentionné, elle tient à souligner encore une fois dans cet avis-ci quelles dispositions devraient figurer dans un texte légal (loi ou règlement grand-ducal), donc a priori dans le projet de règlement grand-ducal sous avis.

2. Quant aux données à caractère personnel destinées à figurer dans le système centralisé

A titre préliminaire, la Commission nationale tient à relever qu'elle a constaté que ni la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies, ni le projet de règlement grand-ducal sous avis ne prennent position quant à l'identité du responsable du traitement des données contenues dans le système centralisé, qui est défini à l'article 4 point 7) du RGPD comme la « *personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.* » Or, comme déjà mentionné dans son avis du 10 mai 2017, la CNPD considère qu'il ressort implicitement des textes légaux susmentionnés que l'autorité sanitaire est à considérer comme responsable du traitement, sous condition que les médecins, médecins dentistes et les laboratoires d'analyses médicales ont pour unique charge d'alimenter indirectement le système centralisé par leurs déclarations, mais qu'ils n'ont pas d'accès direct aux données contenues dans ledit système. En ce qui concerne le traitement de données prévu à l'article 2 du projet de règlement grand-ducal sous examen (transfert de souche ou matériel biologique par le laboratoire d'analyses médicales au laboratoire national de référence), la Commission nationale se demande si le laboratoire national de référence agira en tant que sous-traitant⁴ de l'autorité sanitaire ou si, par contre, ledit laboratoire assumera le rôle du responsable pour le traitement spécifique des échantillons biologiques ?

Par ailleurs, il convient de noter que l'article 2 du projet de loi n°7160 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique avait initialement prévu d'indiquer dans les déclarations pour certaines maladies visées par un astérisque dans la version initiale du projet de règlement grand-ducal sous avis uniquement les initiales du patient. Le règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire, qui sera abrogé par le règlement grand-ducal qui va résulter de ce projet, contenait déjà dans son article 2 une disposition similaire qui avait la teneur suivante : « *Les maladies signalées par un astérisque (*) sont déclarées de façon*

⁴ Voir l'article 4 point 8) du RGPD pour la définition du sous-traitant « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.* »



Avis de la Commission nationale pour la protection des données

à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

anonyme par les lettres initiales du prénom, du nom patronymique et du sexe, suivies par l'année de naissance. »

Or, par des amendements adoptés en date du 7 mars 2018 par la Commission de la Santé, de l'Egalité des Chances et des Sports, cette disposition a été supprimée *« afin d'éviter toute forme de stigmatisation. Ainsi, la déclaration se fait avec des données nominatives, permettant à l'autorité sanitaire d'écarter tous les doublons. »*⁵ La CNPD ne peut pas suivre ce raisonnement. En effet, la pseudonymisation est une garantie appropriée en termes de protection des données et de la vie privée. Le fait de signaler les maladies de manière nominative, au contraire, a pour effet de stigmatiser les personnes atteintes de telle ou telle maladie. Déjà dans son avis du 10 mai 2017, la CNPD se demandait si le recours aux données nominatives des patients pour écarter les doublons est véritablement proportionné et nécessaire compte tenu des autres données dont dispose déjà l'autorité sanitaire. La Commission nationale tient donc à réitérer qu'en *« l'absence de justification de la collecte systématique des nom, prénom et adresse des patients dans le cas des maladies non marquées d'un astérisque dans le projet de règlement grand-ducal et compte tenu du risque important que représente l'association de ces données d'identification à des données sensibles concernant la santé des personnes, la CNPD estime nécessaire que la collecte des données d'identification des patients se limite à leurs initiales, ce qui harmoniserait par ailleurs le régime de collecte de l'ensemble des cas de maladies à déclaration obligatoire. Elle considère par ailleurs, s'agissant des maladies non marquées d'un astérisque dans le projet de règlement grand-ducal, que la transmission systématique de l'adresse du patient n'est pas pertinente. »*

Les articles 3 et 4 de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies contiennent néanmoins une liste des données nominatives que la déclaration obligatoire de certaines maladies par les médecins, médecins-dentistes et les laboratoires d'analyses médicales à destination de l'autorité sanitaire doit comporter « au moins ». Il en ressort que ladite liste n'est pas à considérer comme exhaustive et que d'autres données que celles y prévues pourraient figurer dans la déclaration. La Commission nationale se demande si dès lors les différents acteurs (médecins, médecins-dentistes et laboratoires d'analyses médicales) pourraient décider, à leur gré, de compléter leurs déclarations par d'autres données à caractère personnel. Elle tient à souligner dans ce contexte l'importance du principe de minimisation des données prévu à l'article 5 paragraphe (1) lettre c) du RGPD exigeant 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 »*, qui ne semble pas être respecté en l'espèce par la loi précitée.

Finalement, la Commission nationale considère qu'en vertu de l'article 32 du RGPD, il revient à l'autorité sanitaire de garantir un niveau de sécurité particulièrement élevé dont notamment en ce

⁵ Voir les amendements adoptés en date du 7 mars 2018 par la Commission de la Santé, de l'Egalité des Chances et des Sports dans le cadre du projet de loi n°7160 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique.



Avis de la Commission nationale pour la protection des données

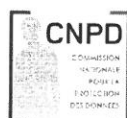
à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

qui concerne la confidentialité des données des personnes concernées. Comme soulevé dans son avis du 10 mai 2017 et en l'absence de précisions concernant les mesures techniques et organisationnelles mises en place dans les textes légaux en cause, la Commission nationale n'est toujours pas en mesure d'apprécier si le dispositif envisagé satisfait aux exigences de sécurité des données traitées. Elle est d'avis qu'au vu de l'extrême sensibilité des données collectées, des mesures d'anonymisation irréversible des données, passé un certain délai, devraient être mis en place afin de garantir une meilleure protection des personnes à l'égard de leurs données à caractère personnel. La CNPD avait constaté dans son avis précité qu'elle « *pourrait comprendre la nécessité de pseudonymiser les données, dans un premier temps, afin de pouvoir ré-identifier un patient en cas de besoin particulier lié à la surveillance et au suivi des maladies à déclaration obligatoire.* » La pseudonymisation des données est en effet une des mesures de sécurité énumérées à l'article 32 lettre a) du RGPD.

La CNPD estime primordial de prévoir en la matière une obligation de pseudonymiser, puis d'anonymiser les données, à l'instar de la procédure de gestion des données prévue par le code de la santé publique français qui est beaucoup plus protectrice de la vie privée des personnes concernées que celle actuellement prévue par les textes légaux luxembourgeois. En effet, le système prévu en France est tel que les notifications de maladies graves contiennent un numéro d'anonymat établi par codage informatique irréversible à partir des trois premières lettres des nom, prénom, date de naissance et sexe de la personne et c'est le déclarant lui-même ou le médecin de l'agence régionale de santé désigné par le directeur général de l'agence qui établit la correspondance entre le numéro d'anonymat et les éléments d'identité de la personne. Ces derniers doivent assurer la conservation de ladite liste de correspondance, aux fins de validation et d'exercice du droit d'accès, dans des conditions garantissant la confidentialité des informations.⁶

En vertu de l'article R3113-2, paragraphe (2) du code français de la santé publique, des arrêtés du ministre chargé de la santé doivent fixer pour chaque maladie, entre autres et en fonction des nécessités de constatations et de suivi, « *la période, d'une durée maximale de cinq ans à compter de la date de notification, pendant laquelle est conservée la correspondance, mentionnée à l'article R. 3113-3, entre le numéro d'anonymat et les éléments d'identité de la personne. A l'issue de cette même période, le médecin de l'Agence nationale de santé publique supprime de la fiche les coordonnées du prescripteur et, le cas échéant, celles du responsable du service de biologie ou du laboratoire.* »

⁶ Article R3113-2, Paragraphe (1) point 2° et R3113-3, alinéa 2 du Code français de la santé publique.



Avis de la Commission nationale pour la protection des données

à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

3. Quant au traitement de données génétiques

Contrairement au texte légal européen précédant, la directive 95/46 du 24 octobre 1995,⁷ le RGPD contient une définition des « données génétiques ». En effet, son article 4 point 13) prévoit que les données génétiques sont des « *données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.* »

L'article 2 du projet de règlement grand-ducal sous examen renvoie à l'annexe B qui établit une liste des pathogènes dont la souche ou le matériel biologique est à transférer par le laboratoire d'analyses médicales au laboratoire national de référence après l'établissement du diagnostic du patient sans demande spécifique par l'autorité sanitaire. Même si ledit article ne précise pas si l'envoi de ces échantillons biologiques devra être accompagné par d'autres données à caractère personnel du patient en cause, comme son nom, prénom et son adresse, la Commission nationale suppose que ceci est bel est bien le cas. Les différents laboratoires opèrent donc un traitement de données génétiques ; données particulièrement intimes et potentiellement discriminantes nécessitant une protection accrue. Comme mentionné sous le « *point 2. Quant aux données à caractère personnel destinées à figurer dans le système centralisé* », la Commission nationale recommande aux auteurs du projet de règlement grand-ducal de préciser dans ce contexte le rôle du laboratoire national de référence, c'est-à-dire d'indiquer si ce dernier agit en tant que sous-traitant de l'autorité sanitaire, en tant que responsable du traitement, ou si la notion de « responsabilité conjointe » introduite par l'article 26 du RGPD est à prendre en compte.

La CNPD tient à souligner que des données à caractère personnel peuvent uniquement être collectées pour des « *finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* » (article 5 paragraphe (1) lettre b) du RGPD). Elle se demande notamment qu'elles sont exactement les finalités poursuivies par le traitement susmentionné des données génétiques. Est-ce que l'objectif de ce transfert de données au laboratoire national de référence vise à garantir une meilleure prise en charge du patient en cause en analysant ses échantillons pour trouver le suivi médical le mieux adapté à sa maladie? Ou est-ce que ledit laboratoire utilise les données à des fins de recherche scientifique ultérieure ? Dans ce dernier cas, nous tenons à souligner que les articles 63 à 65 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données contiennent des conditions spécifiques à respecter

⁷ Directive 95/46/CE du Parlement européen et du Conseil, 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.



Avis de la Commission nationale pour la protection des données

à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

par un responsable du traitement en cas de traitement de données personnelles à des fins de recherche scientifique.

Enfin, la Commission nationale s'interroge si les laboratoires nationaux de référence vont recourir à un tiers de confiance qui assurera la pseudonymisation des données à caractère personnel, donc des échantillons biologiques y stockées. En effet, le recours à un organisme tiers de confiance, distinct de l'organisme traitant les données et qui serait seul en mesure d'établir le lien entre des personnes et des données les concernant, est considéré comme une garantie supplémentaire de respect de la vie privée des personnes et de protection de leurs données personnelles.

4. Quant aux droits des personnes concernées et à la durée de conservation des données

Le chapitre III du RGPD accorde certains droits aux personnes concernées par un traitement de données à caractère personnel, tandis que son article 23 prévoit la possibilité pour l'Union européenne ou pour les États membres de limiter par la voie de mesures législatives la portée des obligations et desdits droits pour garantir par exemple des objectifs importants d'intérêt public général dans les domaines de la santé publique et de la sécurité sociale. Le paragraphe (2) de l'article 23 du RGPD contient une liste minimale de dispositions qu'une telle mesure législative limitative doit contenir, comme par exemple les finalités du traitement et les catégories de données concernées. Or, sur base de notre lecture du texte, le législateur luxembourgeois n'a pas prévu de limiter les droits des personnes concernées en la matière règlementée par la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et par le projet de règlement grand-ducal sous avis, et de ce fait, les personnes concernées par les traitements de données à caractère personnel y prévus disposent intégralement de tous les droits prévus aux articles 12 à 22 du RGPD.

Lesdites personnes ont notamment le droit de recevoir certaines informations du responsable du traitement, soit au moment où les données en question sont directement obtenues auprès de la personne, soit au cas où les données ne sont pas collectées auprès de la personne concernée, au plus tard lorsque les données sont communiquées pour la première fois à un autre destinataire. Ainsi, au moment où l'autorité sanitaire obtient en sa qualité de responsable du traitement des déclarations des médecins, médecins-dentistes et des laboratoires d'analyses médicales qui contiennent des données à caractère personnel des patients en cause, ladite autorité est obligée d'informer les patients, entre autres, sur les finalités du traitement, les catégories de données traitées ou encore sur la source d'où proviennent les données en cause. La CNPD avait par ailleurs ajouté dans son avis du 10 mai 2017, qu'en sus de l'obligation d'information imposée à l'autorité sanitaire, « *le médecin ou le laboratoire qui signale une maladie à déclaration obligatoire devra en informer les personnes concernées, et ce au moment de l'annonce du diagnostic ou au moment qu'il jugera, en conscience, le plus opportun.* »



Avis de la Commission nationale pour la protection des données

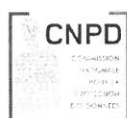
à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

Par ailleurs, la CNPD tient à souligner que l'article 5, paragraphe (1), lettre (e) du RGPD impose au responsable du traitement de veiller à ce que les données qu'il traite ne soient pas conservées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées. Or, ni la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies, ni le projet de règlement grand-ducal sous avis ne contiennent une disposition spécifique quant à la durée de conservation d'un côté des données à caractère personnel contenues dans le système centralisé et d'autre côté des échantillons biologiques stockés au laboratoire national de référence. Dans son avis du 10 mai 2017, elle a déjà soulevé la nécessité de prévoir les dispositions concernant la durée de conservation des données dans un texte légal. Ainsi, elle estime absolument nécessaire de préciser la durée de conservation des données dans ce projet de règlement grand-ducal. La Commission nationale tient à renvoyer dans ce contexte à ses considérations sous le « *point 2. Quant aux données à caractère personnel destinées à figurer dans le système centralisé* » concernant le système mis en place en France.

5. Quant à l'accessibilité au système centralisé et à la mise en place de mesures de sécurité appropriées

La Commission nationale tient à rappeler tout d'abord 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 sécurité et notamment de la confidentialité des données à caractère personnel constitue un enjeu majeur en cas de traitement de données sensibles (données de santé / données génétiques) dans la mesure où la divulgation de ces données pourrait causer un préjudice grave aux patients. Ces risques peuvent augmenter avec le recours accru à certaines nouvelles technologies par les professionnels de santé qui pourraient par exemple utiliser des dispositifs mobiles (tablettes) pour accéder aux dossiers de leurs patients, ainsi que pour envoyer des déclarations à l'autorité sanitaire. Elle tient à insister sur la nécessité de prévoir des mesures de sécurité à l'état de l'art et conformément à l'article 32 du RGPD, afin de protéger l'identité des patients, tout en permettant une surveillance et un suivi efficace en cas de maladies infectieuses déclarées. Comme soulevé sous le point « *2. Quant aux données à caractère personnel destinées à figurer dans le système centralisé* », elle insiste que des mesures de pseudonymisation avec une anonymisation subséquente irréversible soient mises en place.

La Commission nationale recommande dans ce contexte le recours à un tiers de confiance, distinct de l'organisme traitant les données et qui serait seul en mesure d'établir le lien entre des personnes et les données les concernant, qui assurera la pseudonymisation des données à caractère personnel. Le recours à un tiers de confiance est considéré comme une garantie supplémentaire de respect de la vie privée des personnes et de protection de leurs données personnelles. La CNPD est ainsi d'avis qu'une obligation de mettre en place des mesures de sécurité appropriées comme susmentionnées est absolument nécessaire en la matière, d'autant



Avis de la Commission nationale pour la protection des données

à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

plus que le risque en cas d'attaque informatique extérieure est particulièrement élevé si des données de santé nominatives sont enregistrées dans un système centralisé.

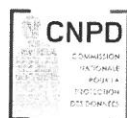
Elle a constaté par ailleurs que l'article 5 de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies laisse la possibilité aux différents acteurs d'envoyer les déclarations en cause, entre autres, par télécopie. Néanmoins, la Commission nationale est d'avis que le télécopie ne constitue pas a priori un moyen de communication sécurisé au regard de l'état de l'art pour transmettre des données nominatives hautement sensibles. Comme les télécopies se trouvent souvent au secrétariat d'une institution, ceci peut conduire à divulguer à des destinataires non habilités des informations couvertes par le secret médical et à porter ainsi gravement atteinte à l'intimité de la vie privée des personnes. Ainsi, la Commission nationale estime, sur base de recommandations émises par son homologue français, la Commission Nationale de l'Informatique et des Libertés (CNIL),⁸ que l'autorité sanitaire doit mettre en place des mesures de sécurité adéquates, comme par exemple vérifier que le télécopie est situé dans un local physiquement contrôlé et accessible uniquement au personnel médical et paramédical et que l'impression d'un message est subordonnée à l'introduction d'un code d'accès personnel. Il convient de noter dans ce contexte que la législation française autorise la transmission des notifications de maladies graves uniquement par voie postale sous pli confidentiel portant la mention " secret médical " ou par télétransmission après chiffrement des données.⁹

Par ailleurs, la CNPD recommande aux auteurs du projet de règlement grand-ducal de préciser qui aura au sein de l'autorité sanitaire accès aux données figurant dans le système centralisé, ainsi que les modalités d'accès aux données y contenues. En effet, il est important que seules les personnes qui en ont besoin dans l'exercice de leur fonction et de leurs tâches professionnelles soient habilitées à y avoir accès. Dans ce même contexte, la CNPD se demande où seront stockées les données contenues dans le système centralisé. Est-ce que lesdites données restent sur les serveurs du Ministère de la Santé ou est-ce qu'elles seront stockées dans des serveurs d'un sous-traitant qui est, le cas échéant, établi en dehors de l'Union européenne ? Elle se pose la même question dans le contexte des échantillons biologiques. Est-ce que ceux-ci sont conservés au laboratoire national de référence ou est-ce qu'un transfert vers une infrastructure de bio-banque est prévu ?

Finalement, la CNPD estime nécessaire de prévoir explicitement un système de journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus. Ainsi, à l'instar d'autres lois ou règlements grand-ducaux, il conviendrait de rajouter une disposition qui pourrait avoir la teneur suivante: « *L'accès au système centralisé doit être conçu et implémenté de sorte que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de*

⁸ CNIL, "Données de santé, messagerie électronique et fax », 1^{er} décembre 2015, disponible sous : <https://www.cnil.fr/fr/donnees-de-sante-messagerie-electronique-et-fax>.

⁹ Article R3113-3, alinéa 1^{er} du code français de la santé publique.



Avis de la Commission nationale pour la protection des données

à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle ».

Ainsi décidé à Esch-sur-Alzette en date du 7 décembre 2018.

La Commission nationale pour la protection des données



Tine A. Larsen
Présidente



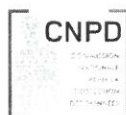
Thierry Lallemand
Commissaire



Christophe Buschmann
Commissaire



Josiane Pauly
Membre suppléant



Avis de la Commission nationale pour la protection des données

à l'égard du projet de règlement grand-ducal portant exécution de la loi du 1^{er} août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

