CHAMBRE DES SALARIES
LUXEMBOURG

Procedure consultative

Projet No 13/2020-1 **20 février 2020**

Données de santé en matière d'assurance et de réassurance

Texte du projet

Projet de loi relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances

Informations techniques :

No du projet :	13/2020
Remise de l'avis :	meilleurs délais
Ministère compétent :	Ministère des Finances
Commission :	Commission « Affaires sociales, sécurité et santé au travail et environnement »

18 rue Auguste Lumière L-1950 Luxembourg
B.P. 1263 L-1012 Luxembourg
T. +352 27 494 200 F. +352 27 494 250
csl@csl.lu www.csl.lu

PROJET DE LOI DU [--]

relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances

*

I. EXPOSE DES MOTIFS

L'article 7, paragraphe 3 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (« loi de 2002 ») prévoyait que le traitement de données relatives à la santé nécessaire aux fins de la gestion de services de santé peut être mis en œuvre notamment par les compagnies d'assurance lorsque le responsable du traitement est soumis au secret professionnel.

L'introduction du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« RGPD ») et plus précisément de son article 9, paragraphe 1 a affecté le régime légal du traitement de données concernant la santé par les compagnies d'assurance et de réassurance, étant donné que le RGPD interdit par principe et sauf les exceptions prévues au paragraphe 2 du même article le traitement de données concernant la santé.

En vue d'opérationnaliser le RGPD, la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du RGPD (« loi de 2018 ») a remplacé la loi de 2002 sans inclure de formule similaire à celle qui se trouvait dans la loi de 2002 pour légitimer explicitement le traitement de données concernant la santé par les compagnies d'assurance.

Par conséquent, les compagnies d'assurances se trouvent dans une situation d'insécurité juridique quant au traitement de données concernant la santé alors que pourtant il est indispensable pour les compagnies d'assurance de traiter des données concernant la santé dans le cadre notamment des contrats d'assurance maladie, d'assurance-vie ou d'assurance-accident.

Les seules dispositions sur lesquelles les compagnies d'assurance peuvent se baser pour le traitement de données concernant la santé en l'état actuel du droit positif sont celles de l'article 9, paragraphe 2 du RGPD.

Ainsi, l'article 9, paragraphe 2, lettre b) du RGPD autorise le traitement de données concernant la santé lorsque *le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale.*

La Commission nationale pour la protection des données (« CNPD ») a analysé la doctrine étrangère en la matière et a constaté *que les entreprises d'assurance ne font pas partie d'un système de protection sociale nationale lorsque la loi ne le prévoit pas. En effet, les lois*

françaises et allemandes, par exemple, prévoient expressément que les contrats complémentaires de nature privée d'assurance-maladie sont assimilés à l'assurance-maladie obligatoire et font donc partie du système national de protection sociale. Toujours est-il que les autres types d'assurances (...) ne peuvent pas être considérés comme faisant partie du système de protection sociale. Au Luxembourg, les compagnies d'assurance ne font pas partie d'un tel système de protection sociale nationale, puisque la loi ne le prévoit pas, ce qui, pour les assureurs luxembourgeois, amplifie l'insécurité juridique en matière de traitement de données concernant la santé.

En vertu de l'article 9, paragraphe 2, lettre f) du RGPD, les traitements de données concernant la santé par les compagnies d'assurance qui sont nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle peuvent être considérés comme licites. Cependant, cette disposition est trop restrictive et ne peut pas servir de base générale pour les traitements de données concernant la santé par les compagnies d'assurance.

La demande du consentement explicite pour chaque traitement de données à caractère personnel en dehors des cas visés aux paragraphes précédents, en application de l'article 9, paragraphe 2, lettre a) du RGPD, ne constitue guère une solution appropriée. Ainsi, la CNPD estime que, de façon générale, un contrat d'assurance doit être considéré comme un contrat d'adhésion et par conséquent le consentement ne pourra pas être donné librement. Le consentement ne peut donc pas être considéré comme approprié pour légitimer le traitement de données concernant la santé.

Pour lever l'insécurité juridique dans laquelle les compagnies d'assurance se trouvent, il reste ainsi comme seul remède une intervention du législateur sur la base de l'article 9, paragraphe 2, lettre g) et paragraphe 4 du RGPD en invoquant des motifs d'intérêt public important.

Ce raisonnement est soutenu par la CNPD qui a précisément estimé qu'il est nécessaire de prévoir *une disposition nationale, conformément à l'article 9, paragraphe 4 du RGPD pour légitimer le traitement de données de santé en matière d'assurances*[1].

Les assurances participent à un intérêt public important, *dans la mesure où l'assurance apporte à l'assuré la certitude qu'il sera indemnisé si c'est sur lui ou sur ses biens que le risque qui menace chacun de nous, individuellement aussi bien que collectivement se réalise.* Dans ce sens, le Comité Directeur pour les Droits de l'homme du Conseil de l'Europe (« CDDH ») a précisé qu'il faut garder à l'esprit *l'importance prise par les contrats d'assurance privés de personnes couvrant un risque lié à la santé, à l'intégrité physique, à l'âge ou au décès d'une personne* et il est convaincu de l'importance sociale que revêt dans chaque pays la couverture appropriée de ces risques, *tout en reconnaissant l'intérêt légitime de l'assureur à l'évaluation du niveau de risque présenté par l'assuré*. En effet, il faut être *conscient du rôle que l'assurance privée volontaire peut jouer pour compléter (et parfois même suppléer) la couverture de ces risques par la sécurité sociale ou d'autres assurances publiques ou obligatoires*. Les services proposés par les compagnies d'assurance sont vitaux pour la collectivité qui compte sur les assurances pour se protéger dans la vie quotidienne financièrement mais aussi au-delà. Les produits d'assurance ont une incidence sur la qualité des services sociaux et leur accessibilité à tous, notamment les services sociaux et les soins de santé. Il parait indispensable de veiller à

[1] Deuxième avis complémentaire de la CNPD du 8 juin 2018 relatif au projet de loi 7184 p. 5

ce que tout individu puisse avoir accès à des systèmes d'assurance pour se protéger et pour préserver ses moyens de subsistance.

Le traitement de données concernant la santé par les compagnies d'assurance pour effectuer le service de leurs prestations participe ainsi de manière substantielle à l'intérêt public et la mise en place d'une disposition en droit national autorisant un tel traitement sur cette base est nécessaire.

Le projet de loi a pour objectif d'introduire dans la loi modifiée du 7 décembre 2015 sur le secteur des assurances une disposition nationale pour légitimer explicitement le traitement de données de santé en matière d'assurances en invoquant, conformément à l'article 9, paragraphe 4 du RGPD, des motifs d'intérêt public important.

II. TEXTE DU PROJET DE LOI

Article unique

Dans la partie 2, titre II, sous-titre II de la loi modifiée du 7 *décembre 2015 sur le secteur des assurances*, il est inséré après l'article 181 un nouveau chapitre 2*bis* qui prend la teneur suivante :

« ***Chapitre 2bis – Traitement de données concernant la santé***

Art. 181*bis* - Traitement de données concernant la santé

Conformément à l'article 9, paragraphe 2, lettre g) du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, le traitement de données concernant la santé, à l'exception de données génétiques, est licite lorsqu'il est nécessaire à l'exécution de mesures précontractuelles en matière d'assurance ou de réassurance ou à l'exécution d'un contrat d'assurance ou de réassurance sous réserve :

1. du respect des dispositions en matière de secret professionnel énoncées à l'article 300 et

2. de la mise en œuvre des mesures appropriées compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes concernées, telles que :

   a) la désignation d'un délégué à la protection des données ;
   b) la réalisation d'analyses d'impact conformément à l'article 35 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif

à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

c) l'anonymisation ou la pseudonymisation des données concernant la santé ou d'autres mesures de séparation fonctionnelle pour certaines opérations de traitement de données concernant la santé ;
d) le chiffrement des données concernant la santé en transit, ainsi qu'une gestion des clés conformes à l'état de l'art ;
e) la mise en place de restrictions d'accès aux données concernant la santé ;
f) la mise en place de fichiers de journalisation qui permettent d'établir le motif, la date et l'heure de la consultation et l'identification de la personne qui a collecté, modifié ou supprimé les données concernant la santé ;
g) la sensibilisation du personnel à la protection des données concernant la santé et au secret professionnel ;
h) l'évaluation régulière de l'efficacité des mesures techniques et organisationnelles mises en place à travers un audit indépendant ;
i) l'adoption de codes de conduite sectoriels tels que prévus à l'article 40 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;
j) la mise en place d'une politique interne prévoyant notamment comment sont respectés les principes prévus à l'article 5 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Chaque responsable de traitement, et le cas échéant sous-traitant, doit documenter et justifier en interne l'exclusion, le cas échéant, d'une ou plusieurs des mesures énumérées au point 2. »

III. COMMENTAIRE DES ARTICLES

I. Observation générale

Pour les raisons exposées à l'exposé des motifs, il est nécessaire d'adopter une disposition légale au niveau national sur la base de l'article 9, paragraphe 2, lettre g) du RGPD et de l'article 9, paragraphe 4 du RGPD afin de permettre le traitement de données concernant la santé en matière d'assurance et de réassurance.

En effet, les autres bases envisageables aux termes de l'article 9, paragraphe 2 du RGPD s'avèrent problématiques en ce qui concerne le traitement des données concernant la santé par les compagnies d'assurances parce que le contexte spécifique y visé n'est pas donné en l'occurrence.

Ainsi, une solution aurait pu consister pour les compagnies d'assurance de demander le consentement explicite pour chaque traitement de données à charactère personnel en application de l'article 9, paragraphe 2, lettre a) du RGPD.

Dans ce contexte, l'article 4, paragraphe 11 du RGPD prévoit que le consentement de la personne concernée fait référence à toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement. De plus, l'article 7, paragraphe 4 du RGPD précise qu'*au « moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat ».*

Il convient de noter que l'article 9, paragraphe 2, lettre a) du RGPD précise que le consentement doit être « explicite ». Les Lignes directrices sur le consentement au sens du règlement 2016/679 précisent que « *le terme explicite se rapporte à la façon dont le consentement est exprimé par la personne concernée*[2] ». Ainsi, depuis l'introduction du RGPD, il est spécifiquement prévu que le consentement doit être donné librement et qu'il doit être spécifique, informé, non ambigu, clair et sans déséquilibre de pouvoirs.

Dans les travaux préparatoires du RGPD, il a été précisé que « *the provision on the processing of sensitive data for specified health-related purposes has been implemented by most Member States; in some with corresponding provisions, in others with either more stringent or less stringent conditions. For example, in Cyprus and Denmark this exception is restricted to health professionals only, whereas in the Czech Republic and in Slovakia the exception is extended also to health insurance. In the other Member States, which do not recognise such extension to insurance, processing for the purpose of health insurance contracts is normally based on the exception of explicit consent; this leads, for example, to the use of blanket declarations by insurance companies, which might be doubtful both as regards "informed" and "free" consent*[3] ».

Le Groupe de travail « Article 29 »[4] précise par ailleurs que l'adjectif « libre » implique un choix et un contrôle réel pour les personnes concernées. « *En règle générale, le RGPD dispose que si la personne concernée n'est pas véritablement en mesure d'exercer un choix, se sent contrainte de consentir ou subira des conséquences négatives importantes si elle ne donne pas son consentement, le consentement n'est pas valable. » « Le consentement ne sera par conséquent pas considéré comme étant donné librement si la personne concernée n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice. La notion de déséquilibre entre le responsable du traitement et la personne concernée est également prise en compte par le RGPD.*[5] »

Il faut noter aussi que les auteurs du projet de loi n°4735 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel (Directive 95/46/CE)[6] avaient déjà à

---

[2] Groupe de travail « Article 29 » - Lignes directrices sur le consentement au sens du règlement 2016/679 p. 21

[3] Commission Staff Working Paper Impact Assessment /* SEC/2012/0072 final */ p. 29

[4] Le Groupe de travail « Article 29 » est le groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018 (avant l'entrée en vigueur du RGPD).

[5] Groupe de travail « Article 29 » - Lignes directrices sur le consentement au sens du règlement 2016/679 p. 6

[6] devenu la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel abrogée par Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes

l'époque souligné que le consentement doit être libre et « *qu'en présence d'une situation dans laquelle le responsable du traitement se trouve en position de force face à la personne concernée, comme par exemple lorsque la personne concernée souhaite obtenir un prêt bancaire ou souscrire une assurance-vie, il peut « s'avérer fort probable que le consentement de la personne concernée n'est pas forcément libre »*[7] ».

S'y ajoute qu'un des droits fondamentaux de la personne concernée, notamment en application de l'article 7 du RGPD, est de pouvoir à tout moment retirer son consentement. Néanmoins, il est fondamental pour l'exécution des divers contrats d'assurance que les compagnies d'assurance puissent réellement traiter les données concernant la santé sans qu'elles ne se heurtent par la suite à un refus sous forme de retrait de consentement. Ainsi, si la personne concernée devait retirer son consentement, l'assureur « perdrait » la justification qui légitimerait le traitement des données concernant la santé. L'assureur se retrouverait alors dans l'impossibilité de traiter les données concernant la santé, le consentement étant en effet une cause de légitimation par nature fragile pour pouvoir à tout moment être retiré.

Si à cet égard le Conseil d'Etat, dans son avis du 30 mars 2018, a remarqué que *se pose encore la question du consentement des personnes concernées dans le cadre de la conclusion d'un contrat d'adhésion*, la CNPD a pu estimer[8] que, pour elle, le consentement explicite des personnes concernées ne permet pas de légitimer le traitement de données dites « sensibles », alors qu'il pourrait ne pas être considéré comme libre au sens du RGPD pour certains types d'assurance tels que par exemple l'assurance-vie ou l'assurance solde restant dû. La CNPD explique encore que, de façon générale, un contrat d'assurance est considéré comme un contrat d'adhésion et par conséquent le consentement n'est en principe pas considéré comme approprié pour légitimer le traitement de données concernant la santé sur base de l'argument selon lequel le consentement ne pourra pas être donné librement dans un tel cas. C'est ainsi que la CNPD estime qu'aucune des conditions de légitimité de l'article 9 paragraphe 2 du RGPD n'est susceptible de légitimer le traitement de données concernant la santé par les compagnies d'assurance et qu'il s'avère nécessaire qu'une disposition nationale, conformément à l'article 9 paragraphe 4 du RGPD, soit adoptée pour légitimer le traitement de données concernant la santé en matière d'assurance et de réassurance.
C'est pour ces raisons que déjà lors des travaux parlementaires du projet de loi n°4735 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel (Directive 95/46/CE)[9], « *la commission a décidé d'inclure les „entreprises d'assurance, les sociétés gérant les fonds de pension et la Caisse médico-chirurgicale mutualiste" dans les prévisions de l'article 7, paragraphe (1), sous peine de leur interdire toute activité*[10] ».

---

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).

[7] J-2001-O-1658 4735/13 Projet de loi relatif à la protection des personnes à l'égard du traitement des données à caractère personnel Rapport de la Commission des Media et des Communications (10.7.2002) p. 5

[8] Deuxième avis complémentaire de la CNPD du 8 juin 2018 relatif au projet de loi 7184 p. 5

[9] devenu la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel abrogée par Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[10] J-2001-O-1658 4735/13 Projet de loi relatif à la protection des personnes à l'égard du traitement des données à caractère personnel Rapport de la Commission des Media et des Communications (10.7.2002) p. 15

En raison de ce qui précède, le consentement ne peut donc pas davantage être considéré comme une base habilitante fiable et solide pour le traitement de données concernant la santé par les compagnies d'assurance.

Ainsi, il reste comme seul remède une intervention du législateur sur la base de l'article 9, paragraphe 2, lettre g) et paragraphe 4 du RGPD en invoquant des motifs d'intérêt public important.

Au regard de l'article 9, paragraphe 2, lettre g) du RGPD, il faut noter qu'il n'existe aucune disposition législative ou réglementaire définissant la notion d'intérêt public. Dans les travaux préparatoires du RGPD, il a été noté que « *the possibility for Member States to add further exemptions for reasons of substantial public interest has led to a broad range of exceptions allowing for the processing of sensitive data for different purposes. These purposes are mostly related to public security (e.g. in Germany, Spain, UK), social security and welfare (e.g. Austria, Czech Republic, Ireland, Latvia, Spain), research and statistics (e.g. Austria, Belgium, Denmark, France, Germany, Malta, Netherlands, Poland, Spain, Sweden), journalistic and artistic purposes (e.g. Belgium, Spain, UK), the administration of justice (e.g. Ireland, UK), the functioning of government (Ireland), protection of public health and fiscal control (Spain) and obligations under international law (Netherlands). Some national laws refer to regulations made for reasons of "substantial public interest" (Ireland) or, for certain categories of data, to the "general interest" (Spain)* ».[11]

Comme détaillé à l'exposé des motifs, les assurances participent à un intérêt public important, voire même une utilité publique puisque « *le risque menace chacun de nous, individuellement aussi bien que collectivement* ».[12] Ainsi, « *l'assurance apporte à l'assuré la certitude qu'il sera indemnisé si c'est sur lui ou sur ses biens que le risque se réalise*[13] ». Dans ce sens, le Comité Directeur pour les Droits de l'homme du Conseil de l'Europe (« CDDH »)[14] a précisé qu'il faut garder à l'esprit « *l'importance prise par les contrats d'assurance privés de personnes couvrant un risque lié à la santé, à l'intégrité physique, à l'âge ou au décès d'une personne* » et il est convaincu de l'importance sociale que revêt dans chaque pays la couverture appropriée de ces risques, « *tout en reconnaissant l'intérêt légitime de l'assureur à l'évaluation du niveau de risque présenté par l'assuré* ». En effet, le CCDH est « *conscient du rôle que l'assurance privée volontaire peut jouer pour compléter (et parfois même suppléer) la couverture de ces risques par la sécurité sociale ou d'autres assurances publiques ou obligatoires* ». Par conséquent, les services proposés par les compagnies d'assurance sont vitaux pour la collectivité qui compte sur les assurances pour se protéger dans la vie quotidienne financièrement mais aussi au-delà. Les produits d'assurance ont une incidence sur la qualité des services sociaux et leur accessibilité à tous, notamment les services sociaux et les soins de santé. Il parait indispensable de veiller à ce que tout individu puisse avoir accès à des systèmes d'assurance pour se protéger et pour préserver ses moyens de subsistance.

Selon l'article 54 de la loi française n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *la garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux constitue une finalité d'intérêt public*. Les

---

[11] Commission Staff Working Paper Impact Assessment /* SEC/2012/0072 final */ p. 29 (nous soulignons)
[12] Nicolas Jacob – Les Assurances (édition Dalloz de 1974) n°2
[13] Nicolas Jacob – Les Assurances (édition Dalloz de 1974) n°24
[14] CDDH(2016)R85 Addendum III p. 3 et 4

services proposés par les compagnies d'assurance pour lesquels elles doivent traiter des données concernant la santé entrent pleinement dans cette définition puisqu'ils garantissent aux assurés le remboursement de frais et charges par exemple de soins de santé dont ceux-ci ne pourraient pas profiter si un tel système ne serait pas mis en place, faute de ne pas pouvoir les payer. Il en va de même de l'assurance-accident et de l'assurance-vie.

Bien que la majorité des traitements nécessaires à l'exécution d'une mission d'intérêt public soient effectués pour le compte de l'Etat par les ministères, les administrations, les services publics ou d'autres établissements publics, un tel traitement effectué par une personne privée ne constitue pas un obstacle à l'application de l'article 9, paragraphe 2, lettre g) du RGPD.[15] Le même raisonnement peut être appliqué aux motifs d'intérêt public important exigés pour le traitement de données concernant la santé conformément à l'article 9, paragraphe 2, lettre g) du RGPD qui peuvent ainsi être exécutés aussi bien par des établissements publics que par des établissements de droit privé.

A relever aussi que le Considérant (50) du RGPD précise que lorsque « *le traitement est fondé sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir, en particulier, d'importants objectifs d'intérêt public général, le responsable du traitement devrait être autorisé à effectuer un traitement ultérieur des données à caractère personnel indépendamment de la compatibilité des finalités*. Le Considérant (52) ajoute que *des dérogations à l'interdiction de traiter des catégories particulières de données à caractère personnel devraient également être autorisées lorsque le droit de l'Union ou le droit d'un État membre le prévoit, et sous réserve de garanties appropriées, de manière à protéger les données à caractère personnel et d'autres droits fondamentaux, lorsque l'intérêt public le commande. (…) Ces dérogations sont possibles à des fins de santé, en ce compris la santé publique et la gestion des services de soins de santé, en particulier pour assurer la qualité et l'efficience des procédures de règlement des demandes de prestations et de services dans le régime d'assurance-maladie, ou à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques* ».

Ainsi l'Irlande, dans son Data Protection Act 2018 prévoit par exemple une dérogation au bénéfice des compagnies d'assurance pour le traitement de données concernant la santé :

> *« Subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of data concerning health shall be lawful where the processing is necessary and proportionate for the purposes of the following:*
>
> *(a) a policy of insurance or life assurance,*
> *(b) a policy of health insurance or health-related insurance,*

[15] voir dans ce sens : J-2000-O-0752 Projet de loi n°4735/00 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel. 1) Arrêté Grand-Ducal de dépôt (6.12.2000) 2) Texte du projet de loi 3) Commentaire des articles 4) 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 5) Exposé des motifs p. 31

(c) an occupational pension, a retirement annuity contract or any other pension arrangement, or
(d) the mortgaging of property.[16]»

Le Royaume-Uni avec le Data Protection Act 2018, les Pays-Bas avec la *Uitvoeringswet Algemene Verordening Gegevensbescherming*[17] ainsi que la Finlande avec son Data protection Act ont adopté des dispositions spécifiques sur base de l'article 9, paragraphe 2, lettre g) du RGPD légitimant le traitement de données concernant la santé par les compagnies d'assurance.

Au Royaume-Uni, Lord Ashton, lors de la troisième lecture du projet de loi, a plus spécifiquement reconnu l'importance fondamentale des produits d'assurance en soulignant que « *we consider that ensuring the availability of insurance at a reasonable cost to members of the public through risk-based pricing, the ability to detect and investigate fraudulent claims and the efficient administration and payment of insurance claims are matters of substantial public interest. Nevertheless, as this processing condition for insurance purposes is drawn more widely than those previously included in the Bill, we consider it reasonable to ask data controllers to consider whether, in respect of a particular processing activity they propose to undertake, it is necessary for a purpose that is in the substantial public interest*[18] ».

D'autres Etats membres ont donc dans le contexte du RGPD adopté des lois nationales portant sur le traitement de données concernant la santé en matière d'assurance et de réassurance (sans imposer aux assureurs de devoir passer par le consentement explicite, par définition précaire).

Le traitement de données concernant la santé par les compagnies d'assurance pour effectuer le service de leurs prestations participe ainsi de manière substantielle à l'intérêt public et la mise en place d'une disposition en droit national autorisant un tel traitement sur cette base est nécessaire. En effet, il existe des situations dans lesquelles il est nécessaire et légitime de traiter des données à caractère personnel dites « sensibles », « *tel que dans les domaines du travail, de la circulation routière, des assurances, de la statistique et de la recherche, comme dans ceux de la justice et de la police, domaines dans lesquels il n'est pas toujours possible, ni par ailleurs opportun, de requérir le consentement de la personne concernée, voire de toutes les personnes concernées par le traitement*[19] ».

II. Article unique

---

[16] Irish Data Protection Act 2018 section 50
[17] Loi de mise en œuvre RGPD
[18] https://hansard.parliament.uk/Lords/2018-01-17/debates/264211B9-3233-4BC2-8E26-145C859FBA42/DataProtectionBill(HL)#contribution-F787F69D-EBCB-4A02-9FD8-33B8527BD55B (nous soulignons).
[19] J-2000-O-0752 Projet de loi n°4735/00 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel. 1) Arrêté Grand-Ducal de dépôt (6.12.2000) 2) Texte du projet de loi 3) Commentaire des articles 4) 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 5) Exposé des motifs p. 32

Conformément à l'article 9, paragraphe 2, lettre g) du RGPD, le traitement des données concernant la santé en matière d'assurance et de réassurance doit être *nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un Etat membre.*

Une telle base du droit luxembourgeois est créée par le présent article qui, en application de l'article 9, paragraphe 2, lettre g) du RGPD, *doit être proportionnée 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.*

Afin de s'assurer que l'article soit « proportionné à l'objectif poursuivi », il précise que le traitement doit être nécessaire à l'exécution de mesures précontractuelles en matière d'assurance ou de réassurance ou à l'exécution d'un contrat d'assurance ou de réassurance. L'objectif poursuivi par l'article unique est de permettre le traitement de données concernant la santé en matière d'assurance et de réassurance afin notamment de ne pas entraver la bonne exécution de contrats d'assurance et surtout de ne pas retarder les remboursements attendus par les assurés.

Pour s'assurer que l'article respecte « l'essence du droit à la protection des données », il est veillé à ce qu'il respecte les principes du RGPD notamment en excluant les données génétiques dont le traitement serait incompatible avec les finalités. L'article est ainsi aussi en conformité avec l'article 66 de la loi de 2018 qui interdit expressément le traitement de données génétiques aux fins de l'exercice des droits propres au responsable du traitement en matière d'assurance.

Pour faire en sorte que l'article prévoit des « mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée », il précise que le traitement de données concernant la santé est licite sous réserve du respect des dispositions en matière de secret professionnel énoncées à l'article 300 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances et de la mise en œuvre des mesures appropriées telles que énoncées à l'article unique compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes concernées.

Les mesures énoncées sont la désignation d'un délégué à la protection des données ; la réalisation d'analyses d'impact conformément à l'article 35 du RGPD (en tenant compte notamment de la délibération 34/2019 du 6 mars 2019 de la CNPD portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise) ; l'anonymisation ou la pseudonymisation des données ou d'autres mesures de séparation fonctionnelle pour certaines opérations de traitement de données ; le chiffrement des données en transit, ainsi qu'une gestion des clés conformes à l'état de l'art ; la mise en place de restrictions d'accès aux données ; la mise en place de fichiers de journalisation qui permettent d'établir le motif, la date et l'heure de la consultation et l'identification de la personne qui a collecté, modifié ou supprimé les données ; la sensibilisation du personnel à la protection des données et au secret professionnel ; l'évaluation régulière de l'efficacité des mesures techniques et organisationnelles mises en place à travers un audit indépendant (interne ou externe) ; l'adoption de codes de conduite sectoriels tels que prévus à l'article 40 du RGPD et la mise en place d'une politique interne prévoyant notamment comment sont respectés les principes prévus à l'article 5 du RGPD.

Chaque responsable de traitement, et le cas échéant sous-traitant, doit documenter et justifier en interne l'exclusion, le cas échéant, d'une ou de plusieurs des mesures énumérées au point 2 de l'article.

Le respect des dispositions s'impose aussi bien aux responsables de traitement (au sens du RGPD), qu'à leurs éventuels sous-traitants (au sens du RGPD).