N° 7511[9]

CHAMBRE DES DEPUTES

PROJET DE LOI

portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances en vue d'insérer un chapitre 2ter relatif au traitement de données concernant la santé

* * *

RAPPORT DE LA COMMISSION DES FINANCES

(14.1.2025)

La Commission se compose de : Mme Diane ADEHM, Président, M. Marc SPAUTZ, Rapporteur ; MM. Guy ARENDT, Maurice BAUER, André BAULER, Mmes Taina BOFFERDING, Corinne CAHEN, MM. Sven CLEMENT, Franz FAYOT, Patrick GOLDSCHMIDT, Claude HAAGEN, Fred KEUP, Laurent MOSAR, Mme Sam TANSON et M. Michel WOLTER, Membres

*

1. ANTECEDENTS

Le projet de loi n°7511 a été déposé par le Ministre des Finances le 23 décembre 2019.

Lors de la réunion de la Commission des Finances et du Budget (COFIBU) du 24 janvier 2020, Monsieur André Bauler a été désigné rapporteur du projet de loi sous rubrique. Le projet de loi a été présenté à la COFIBU au cours de la même réunion.

La Commission nationale pour la protection des données a émis son avis le 27 janvier 2020.

L'avis de la Chambre de commerce date du 3 février 2020.

Le Conseil d'État a émis son avis le 28 avril 2020.

La Chambre des salariés a émis un avis le 28 mai 2020.

Des amendements gouvernementaux ont été déposés le 4 juin 2024.

La Commission nationale pour la protection des données a émis son avis complémentaire le 28 juin 2024.

L'avis complémentaire de la Chambre de commerce porte la date du 1er juillet 2024.

Le projet de loi amendé a été présenté aux membres de la Commission des Finances (COFI) le 22 novembre 2024 et M. Marc Spautz a été nommé nouveau rapporteur au cours de la même réunion.

L'avis complémentaire du Conseil d'État date du 20 décembre 2024.

La COFI a examiné l'avis complémentaire du Conseil d'État au cours de la réunion du 7 janvier 2025.

Le projet de rapport a été adopté au cours de la réunion du 14 janvier 2025.

*

2. OBJET DU PROJET DE LOI

2.1 Objet du projet de loi

Le projet de loi sous examen a pour objet de modifier la loi modifiée du 7 décembre 2015 sur le secteur des assurances en vue d'y insérer un nouveau chapitre 2bis ayant spécifiquement trait au traitement de données concernant la santé afin de combler un vide juridique qui existe depuis l'abrogation de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données.

Il est prévu d'introduire 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.

*

Au cours des discussions portant sur le présent projet de loi au sein de la Commission des Finances, le « droit à l'oubli » a été évoqué à maintes reprises.

Les membres de la Commission des Finances s'accordent sur le fait qu'il s'agit d'un sujet sensible et important et ont pu constater que le ministre des Finances partage ce point de vue.

Ils encouragent le Gouvernement à examiner des pistes de renforcement de ce droit à l'oubli, y compris à travers une éventuelle extension de ce droit à d'autres maladies.

2.2 Historique

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 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.

Si, en principe, le traitement de telles données est interdit, le paragraphe 2 de l'article 9 du règlement (UE) 2016/679 précité, autorise des dérogations à l'interdiction de traiter des catégories particulières de données à caractère personnel sous certaines conditions.

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. Toutefois, elle n'a pas repris une disposition équivalente à celle qui se trouvait dans la loi de 2002 qui légitimait explicitement le traitement des données de santé par les compagnies d'assurance.

Par conséquent, les compagnies d'assurances se trouvent actuellement 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.

Plusieurs solutions aux termes du paragraphe 2 de l'article 9 du règlement (UE) 2016/679 précité ont été analysés (p.ex. demande de consentement explicite) mais elles n'auraient pas apporté une réponse satisfaisante pour lever cette insécurité juridique au niveau du traitement de données concernant la santé par les compagnies d'assurance.

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. En effet cette disposition précise qu'il est possible de déroger à l'interdiction de traitement si « *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 ».

Ce raisonnement est d'ailleurs soutenu par la Commission nationale pour la protection des données 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*.

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.

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 cette 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.

*

3. LES AVIS

3.1 Avis de la Chambre de commerce

La Chambre de commerce note que le projet de loi sous avis a pour objet d'introduire dans la loi modifiée du 7 décembre 2015 sur le secteur des assurances une disposition spécifique afin de légitimer explicitement le traitement des données de santé en matière d'assurance et de réassurance, après l'entrée en vigueur du règlement général sur la protection des données et de la loi du 1er août 2018 ayant mis en œuvre le règlement précité.

La Chambre de commerce accueille très favorablement le projet de loi qui permet d'apporter au secteur des assurances une base de légitimité explicite en matière de traitement de données de santé.

Elle se félicite qu'il soit ainsi mis un terme à une insécurité juridique qui pèse actuellement sur les compagnies d'assurance.

Dans son avis complémentaire, la Chambre de commerce approuve les amendements gouvernementaux qui visent principalement à redresser une opposition formelle du Conseil d'Etat.

3.2 Avis de la Commission nationale pour la protection des données

Dans son avis du 27 janvier 2020, la Commission nationale pour la protection des données (CNPD) salue le texte du projet de loi. Elle estime que le point 2 de l'article 181bis de la loi modifiée du 7 décembre 2015 sur le secteur des assurances énumère de manière suffisante des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée qui sont à respecter en cas de traitement de données de santé 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, à l'instar d'autres législations européennes comme par exemple celle de l'Irlande, du Royaume-Uni ou des Pays-Bas.

La CNPD tient également à souligner que le projet de loi sous examen n'a pas d'incidence sur l'application des règles du RGPD, c'est-à-dire que toutes les dispositions prévues au RGPD restent applicables aux sociétés d'assurance et de réassurance qui traitent des données de santé conformément à l'article unique du projet de loi. Notamment, les principes relatifs au traitement des données à caractère personnel énumérés à l'article 5 du RGPD et toutes les obligations générales incombant au responsable du traitement et prévues au chapitre IV du RGPD sont à respecter.

Dans son avis complémentaire du 28 juin 2025, la CNPD approuve les amendements gouvernementaux du 4 juin 2024.

3.3 Avis de la Chambre des salariés

La Chambre des salariés (CSL) ne peut approuver le présent projet de loi ni en ce qui concerne sa finalité ni en ce qui concerne le texte proprement dit.

Selon la Chambre professionnelle, l'intérêt soi-disant « public » poursuivi par les compagnies d'assurance met en danger le système de protection sociale de l'Etat fondé sur l'équité, la répartition des risques, la solidarité intergénérationnelle et porte atteinte à la cohésion sociale.

La CSL est d'avis que les conditions pour avoir recours à l'article 9, paragraphe 2, lettre g) du RGPD qui dispose que l'interdiction du traitement de données concernant la santé ne s'applique pas lorsque « *le traitement est nécessaire pour des motifs d'intérêt public important, sur base du droit de l'Union ou droit d'un Etat 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* » ne sont pas remplies. Selon la CSL, les compagnies d'assurance à travers le traitement de données concernant la santé ne poursuivent pas exclusivement un intérêt public qui est uniquement réservé aux assurés qui ont les moyens financiers pour conclure de telles assurances, mais ont surtout comme objectif d'engranger des bénéfices.

Même à supposer que les assurances agissent partiellement dans un intérêt public, la CSL estime que la proportionnalité d'une telle mesure consistant à demander de telles données sensibles aussi bien dans le cadre de mesures précontractuelles que dans le cadre de l'exécution d'un contrat d'assurance n'est pas donnée parce que 1) les compagnies d'assurance peuvent faire dépendre la validité des contrats de la transmission récurrente de telles données par les assurés, 2) la sécurité de telles données n'est pas garantie et 3) l'exploitation de telles données conduit indéniablement vers une individualisation de la protection sociale au détriment du système obligatoire de protection sociale.

Pour la CSL, il est également inacceptable que les compagnies d'assurance puissent renoncer en interne à une des mesures de protection prévues sous le point 2) de l'article 181 sans avoir à rendre compte à personne – ni à l'assuré ni aux autorités publiques. Pour la CSL, cet article n'est rien d'autre qu'une farce et permet aux compagnies d'assurance qui sont à la fois juge et partie du traitement des données des assurés de disposer comme bon leur semble.

En raison de ces remarques, la CSL marque son désaccord avec le projet de loi sous rubrique.

3.4 Avis du Conseil d'Etat

Le Conseil d'État souligne dans son avis du 28 avril 2020 que les données concernant la santé relèvent des catégories particulières de données à caractère personnel visées à l'article 9 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.

La Haute Corporation note que si, en principe, le traitement de telles données est interdit, le paragraphe 2 de l'article 9 du règlement (UE) 2016/679, précité, autorise des dérogations à l'interdiction de traiter des catégories particulières de données à caractère personnel sous certaines conditions. Ainsi, l'article 9, paragraphe 2, lettre g), du règlement (UE) 2016/679 précise qu'il est possible de déroger à l'interdiction de traitement si « *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* ».

Selon le Conseil d'État, une telle dérogation requiert l'intervention du législateur qui devra prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

Dans son avis du 28 avril 2020, le Conseil d'État s'est opposé formellement à la disposition qui accordait au responsable du traitement la possibilité de déroger à tout ou partie des mesures destinées à assurer la protection des droits fondamentaux et des intérêts de la personne concernée par un traitement de données, ceci au motif qu'une telle dérogation risquait de dénaturer l'obligation de protection

des droits et libertés des personnes concernées, étant donné que le projet de loi lui-même constitue déjà une dérogation à l'interdiction du traitement des données de santé.

Au vu des amendements gouvernementaux du 4 juin 2024, des explications données par les auteurs des amendements et à la lecture de l'avis complémentaire de la Commission nationale pour la protection des données le Conseil d'État, dans son avis complémentaire du 10 décembre 2024, a levé son opposition formelle émise à l'égard du texte initial de la disposition en question.

*

4. COMMENTAIRE DES ARTICLES

Observation générale accompagnant le dépôt du projet de loi

Pour les raisons exposées à l'exposé des motifs du document parlementaire 7511, 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*[1] ». 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*[2] ».

Le Groupe de travail « Article 29 »[3] 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*

---

1 Groupe de travail « Article 29 » – Lignes directrices sur le consentement au sens du règlement 2016/679 p. 21

2 Commission Staff Working Paper Impact Assessment /* SEC/2012/0072 final */ p. 29

3 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).

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.*[4] »

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)[5] avaient déjà à 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* »[6] ».

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[7] 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)[8], « *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*[9] ».

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.

---

4 Groupe de travail « Article 29 » – Lignes directrices sur le consentement au sens du règlement 2016/679 p. 6

5 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).

6 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

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

8 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).

9 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

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)* ».[10]

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* ».[11] 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*[12] ». Dans ce sens, le Comité Directeur pour les Droits de l'homme du Conseil de l'Europe (« CDDH »)[13] 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 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 n'était 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.[14] 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.

---

10 Commission Staff Working Paper Impact Assessment /* SEC/2012/0072 final */ p. 29 (nous soulignons)

11 Nicolas Jacob – Les Assurances (édition Dalloz de 1974) n°2

12 Nicolas Jacob – Les Assurances (édition Dalloz de 1974) n°24

13 CDDH(2016)R85 Addendum III p. 3 et 4

14 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

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,

(c) an occupational pension, a retirement annuity contract or any other pension arrangement, or

(d) the mortgaging of property.[15] »

Le Royaume-Uni avec le Data Protection Act 2018, les Pays-Bas avec la *Uitvoeringswet Algemene Verordening Gegevensbescherming*[16] 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*[17] ».

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*[18] ».

---

15 Irish Data Protection Act 2018 section 50

16 Loi de mise en œuvre RGPD

17 https://hansard.parliament.uk/Lords/2018-01-17/debates/264211B9-3233-4BC2-8E26-145C859FBA42/DataProtectionBill(HL)#contribution-F787F69D-EBCB-4A02-9FD8-33B8527BD55B

18 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

Article unique initial

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).

Avis du Conseil d'Etat à l'égard de l'article unique initial :

L'article unique initial propose de donner une base légale aux traitements de données concernant la santé opérés par les compagnies d'assurance et de réassurance conformément à l'article 9, paragraphe 2, lettre g), du règlement (UE) 2016/679 en insérant un nouvel article 181*bis* dans la loi modifiée du 7 décembre 2015 sur le secteur des assurances.

Le Conseil d'État note, à l'instar de la CNPD, que le point 2 de l'article 181*bis* en projet sous avis prévoit une série de mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et

des intérêts de la personne concernée visant à satisfaire à l'exigence énoncée à l'article 9, paragraphe 2, lettre g), du règlement (UE) 2016/679.

Si les mesures prévues par la disposition sous avis, à titre de garanties pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée, trouvent l'accord du Conseil d'État, le texte proposé appelle toutefois deux remarques.

Le Conseil d'État constate tout d'abord que l'article 181*bis* ne mentionne pas de « motif d'intérêt public important » tel que visé à l'article 9, paragraphe 2, lettre g), du règlement (UE) 2016/679.

Le Conseil d'État relève, à cet égard, que l'article 9, paragraphe 2, lettre g), du règlement (UE) 2016/679 ne précise pas les motifs d'intérêt public qui sont susceptibles d'être invoqués afin de justifier la dérogation à l'interdiction de traitement des catégories particulières de données. L'approche retenue par le législateur européen diffère, sur ce point, de celle retenue à l'article 23 du même règlement, qui énumère les finalités visées en ce qui concerne les mesures législatives visant à limiter certains droits et obligations prévus par le règlement (UE) 2016/679. La loi belge se réfère aux « motifs d'intérêt public important » sans en préciser la portée[19]. La loi française se réfère, quant à elle, aux « […] traitements comportant des données concernant la santé justifiés par l'intérêt public et conformes aux dispositions du chapitre IX de la présente loi »[20]. Le Conseil d'État pourrait concevoir un dispositif qui, outre d'invoquer l'article 9, paragraphe 2, lettre g), du règlement (UE) 2016/679, se référerait aux motifs d'intérêt public importants, poursuivis par une législation sur le secteur des assurances. D'après l'exposé des motifs, « [l]es 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 ».

La phrase liminaire du nouvel article 181*bis* pourrait se lire comme suit :

> « 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), et au regard des motifs

---

19 Article 8 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard de traitements de données à caractère personnel :

« § 1er. En exécution de l'article 9.2.g) du Règlement, les traitements ci-après sont considérés comme traitements nécessaires pour des motifs d'intérêt public important :

1° le traitement effectué par des associations dotées de la personnalité juridique ou par des fondations qui ont pour objet statutaire principal la défense et la promotion des droits de l'homme et des libertés fondamentales, en vue de la réalisation de cet objet, à condition que ce traitement soit autorisé par le Roi, par arrêté délibéré en Conseil des ministres, après avis de l'autorité de contrôle compétente. Le Roi peut prévoir des modalités de ce traitement;

2° le traitement géré par la fondation d'utilité publique „Fondation pour Enfants Disparus et Sexuellement Exploités" pour la réception, la transmission à l'autorité judiciaire et le suivi de données concernant des personnes qui sont suspectées, dans un dossier déterminé de disparition ou d'exploitation sexuelle, d'avoir commis un crime ou un délit;

3° le traitement de données à caractère personnel concernant la vie sexuelle, effectué par une association dotée de la personnalité juridique ou par une fondation, qui a pour objet statutaire principal l'évaluation, la guidance et le traitement des personnes dont le comportement sexuel peut être qualifié d'infraction, et qui est agréée et subventionné par l'autorité compétente en vue de la réalisation de cet objet. Ces traitements, qui doivent être destinés à l'évaluation, la guidance et le traitement des personnes visées dans le présent paragraphe et qui ne peuvent porter que sur des données à caractère personnel qui, pour autant qu'elles soient relatives à la vie sexuelle, concernent les personnes visées dans le présent paragraphe, sont soumis à une autorisation spéciale individuelle accordée par le Roi, dans un arrêté royal délibéré en Conseil des ministres, après avis de l'autorité de contrôle compétente.

L'arrêté visé à l'alinéa 1er, 3°, précise la durée de validité de l'autorisation, les modalités du traitement des données, les modalités de contrôle de l'association ou de la fondation par l'autorité compétente et la façon dont cette autorité informe l'autorité de contrôle compétente sur le traitement de données à caractère personnel effectué dans le cadre de l'autorisation accordée.

Sauf dispositions légales particulières, le traitement de données génétiques et biométriques aux fins d'identifier une personne physique de manière unique par ces associations et fondations est interdit.

§ 2. Le responsable du traitement et, le cas échéant, le sous-traitant établissent une liste des catégories de personnes, ayant accès aux données à caractère personnel avec une description de leur fonction par rapport au traitement des données visées. Cette liste est tenue à la disposition de l'autorité de contrôle compétente.

Le responsable du traitement et, le cas échéant, le sous-traitant veillent à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

§ 3. La fondation visée au paragraphe 1er, alinéa 1er, 2°, ne peut tenir un fichier de personnes suspectes d'avoir commis un crime ou un délit ou de personnes condamnées. Elle désigne également un délégué à la protection des données. »

20 Article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

d'intérêt public importants, inhérents aux contrats d'assurance et de réassurance réglés par la présente loi pour lesquels la santé de l'assuré constitue un élément déterminant, 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 : »

Le dernier alinéa du nouvel article 181*bis* prévoit le droit pour le responsable du traitement d'exclure une ou plusieurs des mesures énumérées au point 2. Cette exclusion devra, par ailleurs, être documentée et justifiée « en interne ».

Le Conseil d'État a des réserves sérieuses par rapport à ce dispositif.

Il rappelle que l'article 9, paragraphe 2, lettre g), du règlement (UE) 2016/679 constitue déjà une dérogation à l'interdiction de traitement des données concernant la santé si « le traitement est nécessaire pour des motifs d'intérêt public important ». Dans le souci de sauvegarder les droits des personnes visées, les garanties prévues au point 2 du nouvel article 181*bis* sont destinées à encadrer cette dérogation. La possibilité de déroger à tout ou partie des mesures prévues aux lettres a) à j) risque d'avoir pour effet de dénaturer l'obligation imposée au point 2.

La loi belge précitée du 30 juillet 2018 énumère également des mesures supplémentaires à mettre en place par le responsable du traitement souhaitant traiter des données relatives à la santé, sans toutefois prévoir la possibilité pour le responsable du traitement d'y déroger[21].

Il est vrai que l'alinéa en question est inspiré de l'article 65 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, concernant le traitement de catégories particulières de données à caractère personnel mis en œuvre à des fins de recherche scientifique ou historique[22]. Il y a toutefois lieu de souligner que « [l]e responsable de traitement doit documenter et justifier pour chaque projet à des fins de recherche scientifique ou historique ou à des fins statistiques l'exclusion, le cas échéant, d'une ou plusieurs des mesures énumérées à cet article ». L'article 65 précité se base sur l'article 9, paragraphe 2, point j), du même règlement (UE) 2016/679 qui prévoit une dérogation à l'interdiction de traitement si « le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit

---

21 L'article 8, paragraphe 2, de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard de traitements de données à caractère personnel prévoit, en effet, que le responsable de traitement ou son sous-traitant devra ainsi établir une liste des personnes ayant accès à ces données avec une description précise de leur fonction, tenir cette liste à disposition de l'Autorité de protection des données et veiller à ce que ces personnes soient tenues à une obligation de confidentialité.

22 **Art. 65.** Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable d'un traitement mis en œuvre à des fins de recherche scientifique ou historique, ou à des fins statistiques, doit mettre en œuvre les mesures appropriées additionnelles suivantes :

1° la désignation d'un délégué à la protection des données ;

2° la réalisation d'une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel ;

3° l'anonymisation, la pseudonymisation au sens de l'article 4, paragraphe 5, du règlement (UE) 2016/679 ou d'autres mesures de séparation fonctionnelle garantissant que les données collectées à des fins de recherche scientifique ou historique, ou à des fins statistiques, ne puissent être utilisées pour prendre des décisions ou des actions à l'égard des personnes concernées ;

4° le recours à un tiers de confiance fonctionnellement indépendant du responsable du traitement pour l'anonymisation ou la pseudonymisation des données ;

5° le chiffrement des données à caractère personnel en transit et au repos, ainsi qu'une gestion des clés conformes à l'état de l'art ;

6° l'utilisation de technologies renforçant la protection de la vie privée des personnes concernées ;

7° la mise en place de restrictions de l'accès aux données à caractère personnel au sein du responsable du traitement ;

8° des 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 à caractère personnel ;

9° la sensibilisation du personnel participant au traitement des données à caractère personnel et au secret professionnel ;

10° l'évaluation régulière de l'efficacité des mesures techniques et organisationnelles mises en place à travers un audit indépendant ;

11° l'établissement au préalable d'un plan de gestion des données ;

12° l'adoption de codes de conduite sectoriels tels que prévus à l'article 40 du règlement (UE) 2016/679 approuvés par la Commission européenne en vertu de l'article 40, paragraphe 9, du règlement (UE) 2016/679.

Le responsable de traitement doit documenter et justifier pour chaque projet à des fins de recherche scientifique ou historique ou à des fins statistiques l'exclusion, le cas échéant, d'une ou plusieurs des mesures énumérées à cet article.

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 ».

Le dispositif de l'article 65, précité, porte dès lors sur un autre type de traitement et est soumis à un cadre particulier. Un traitement de données concernant la santé à des fins de recherche scientifique ou historique, ou à des fins statistiques est moins « sensible » qu'un traitement opéré dans le secteur des assurances.

En outre, le Conseil d'État a du mal à saisir la portée de l'obligation de documenter et de justifier les dérogations aux mesures prévues au point 2 de l'article 181*bis* « en interne ». Une telle documentation ou justification « en interne » ne saurait conférer les garanties appropriées en matière de transparence aux personnes dont les données sont collectées.

Il résulte de l'ensemble des considérations qui précèdent que le dernier alinéa, n'est pas compatible avec l'article 9, paragraphe 2, lettre g), du règlement (UE) 2016/679. Par conséquent, le Conseil d'État doit émettre une **opposition formelle**.

Le Conseil d'État souligne, par ailleurs, au même titre que la CNPD, que les compagnies d'assurance et de réassurance demeurent soumises à l'ensemble des dispositions prévues par le règlement (UE) 2016/679, ce qui implique notamment que les personnes dont les données à caractère personnel font l'objet d'un traitement peuvent de manière générale se prévaloir des droits prévus aux articles 13 à 22 du règlement (UE) 2016/679.

Observations d'ordre légistique

Intitulé

L'intitulé ne doit pas induire en erreur sur le contenu du dispositif. Pour fixer l'attention des personnes qui s'intéressent aux textes en cours d'élaboration et des lecteurs du journal officiel, il peut s'avérer utile d'indiquer dans l'intitulé d'un acte exclusivement modificatif la portée des modifications qu'il est envisagé d'apporter à un dispositif comportant un nombre important d'articles En recourant à ces techniques, l'on évitera cependant de donner à l'acte modificatif un intitulé qui pourrait faire croire qu'il revêt un caractère autonome. Par conséquent, le Conseil d'État demande aux auteurs de reformuler l'intitulé de la manière qui suit :

> « Projet de loi portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances en vue d'insérer un chapitre 2*bis* relatif au traitement de données concernant la santé ».

Amendements gouvernementaux du 4 juin 2024

Les amendements gouvernementaux ont pour objectif d'apporter des ajustements ciblés au projet de loi n° 7511, suite à l'avis du Conseil d'Etat.

Les amendements gouvernementaux visent principalement à donner suite à l'opposition formelle du Conseil d'Etat relative au droit d'une entreprise d'assurance ou de réassurance de déroger à une ou plusieurs des mesures spécifiques, destinées à préserver les droits fondamentaux et les intérêts d'une personne concernée par un traitement de données médicales, énumérées sous le point 2 du nouvel article 181-3 (précédemment 181*bis*) qu'il est proposé d'introduire dans la loi modifiée du 7 décembre 2015 sur le secteur des assurances. En effet, le Conseil d'Etat estime qu'un tel dispositif de dérogation dénaturerait *in fine* l'utilité des mesures de sauvegarde des droits fondamentaux de la personne concernée.

Dès lors, il est proposé de modifier le texte du projet de loi en ce sens que l'entreprise d'assurance ou de réassurance ne puisse plus déroger à l'intégralité des mesures listées sous le point 2 du nouvel article 181-3. Une différence sera ainsi faite entre les mesures auxquelles l'entreprise d'assurance ou de réassurance ne pourra en aucun cas déroger et celles auxquelles il pourra être dérogé dans le cadre d'une approche basée sur la proportionnalité. Toute dérogation à cette deuxième catégorie de mesures devra être documentée en interne. Par ailleurs, afin de compléter le dispositif déjà mis en place dans le projet de loi initial, les amendements gouvernementaux introduisent désormais l'obligation de tenir cette documentation à la disposition de la Commission nationale pour la protection des données.

*

Texte et commentaire des amendements gouvernementaux

Amendement 1 concernant l'intitulé

L'intitulé de la loi en projet prend la teneur suivante :

« Projet de loi portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances en vue d'insérer un chapitre 2*ter* relatif au traitement de données concernant la santé ».

Motivation de l'amendement

Le présent amendement donne suite à la remarque d'ordre légistique formulée par le Conseil d'Etat, moyennant un ajustement ciblé visant à refléter le fait que le chapitre nouvellement introduit sera désormais un chapitre 2*ter* et non 2*bis*, suite à l'introduction d'un chapitre 2*bis* par la loi du 30 mars 2022 relative aux comptes inactifs, aux coffres-forts inactifs et aux contrats d'assurance en déshérence.

Amendement 2 concernant l'article unique initial (nouvel article 1er)

L'article unique du projet de loi devient l'article 1er et est modifié comme suit :

1° Dans la phrase introductive, les mots « l'article 181 » sont remplacés par les mots « l'article 181-2 » et les mots « nouveau chapitre 2*bis* » sont remplacés par les mots « chapitre 2*ter* nouveau » ;

2° Dans l'intitulé du chapitre nouvellement introduit, les mots « Chapitre 2*bis* » sont remplacés par les mots « Chapitre 2*ter* » et les mots « Art. 181*bis* » sont remplacés par les mots « Art. 181-3 » ;

3° À l'endroit du nouvel article 181-3, alinéa 1er, la phrase liminaire prend la teneur suivante :

« Conformément à l'article 9, paragraphe 2, lettre g), du règlement (UE) 2016/679, et au regard des motifs d'intérêt public importants, inhérents aux contrats d'assurance et de réassurance pour lesquels la santé de la personne concernée constitue un élément déterminant, 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 : » ;

4° À l'endroit du nouvel article 181-3, alinéa 1er, point 2, le mot « suivantes » est inséré entre les mots « mesures appropriées » et les mots « compte tenu de », et les mots « , telles que » sont supprimés ;

5° À l'endroit du nouvel article 181-3, alinéa 1er, point 2, lettres b), i) et j), les mots « 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 » sont remplacés par les mots « règlement (UE) 2016/679 » ;

6° À l'endroit de l'article 181-3, alinéa 2, les mots « au point 2 » sont remplacés par les mots « à l'alinéa 1er, point 2, lettres a), b), c), h) et i) » ;

7° À l'endroit de l'article 181-3, alinéa 2, sont ajoutées une deuxième et une troisième phrase, libellées comme suit :

« Cette documentation est tenue à la disposition de la Commission nationale pour la protection des données. En aucun cas il ne peut être dérogé aux mesures énumérées à l'alinéa 1er, point 2, lettres d), e), f), g) et j). ».

Motivation de l'amendement

Dans un souci de cohérence de la numérotation des différents articles de la loi modifiée du 7 décembre 2015 sur le secteur des assurances, les points 1° et 2° de l'amendement visent à ajuster la numérotation du nouveau chapitre concernant le traitement de données de santé en matière d'assurance et de l'article 181*bis*, suite à l'introduction d'un chapitre 2*bis* par la loi du 30 mars 2022 relative aux comptes inactifs, aux coffres-forts inactifs et aux contrats d'assurance en déshérence comprenant un article 181-1, ainsi que l'introduction d'un article 181-2 par la loi du 29 mars 2024 portant transposition de la directive (UE) 2021/2118 du Parlement européen et du Conseil du 24 novembre 2021 modifiant la directive 2009/103/CE concernant l'assurance de la responsabilité civile résultant de la circulation de véhicules automoteurs et le contrôle de l'obligation d'assurer cette responsabilité.

Le point 3° de l'amendement reprend en grande partie la proposition de texte du Conseil d'Etat formulée dans son avis du 28 avril 2020 en invoquant le motif d'intérêt public important poursuivi par

une législation sur le secteur des assurances, moyennant quelques ajustements. En effet, une précision est apportée à la proposition de texte du Conseil d'Etat, afin de faire référence à la « personne concernée » au lieu de « l'assuré », étant donné qu'il ne s'agit pas seulement des motifs d'intérêt public importants inhérents aux contrats d'assurance et de réassurance pour lesquels la santé de l'assuré lui-même constitue un élément déterminant. Il est nécessaire de viser les motifs d'intérêt public importants, inhérents aux contrats d'assurance ou de réassurance pour lesquels la santé de toute « personne concernée », telles que les personnes lésées ou les bénéficiaires, constitue un élément déterminant. Ainsi, à titre d'exemple, lors d'un accident routier, la personne lésée peut être une tierce personne, qui doit être remboursée par l'assureur de la personne responsable. Afin que l'assureur puisse traiter le dossier du sinistre, il doit être en mesure de pouvoir traiter les données médicales de la personne concernée par le sinistre.

Les points 4°, 6° et 7° de l'amendement visent à donner suite à l'opposition formelle du Conseil d'Etat, qui estime que « *La possibilité de déroger à tout ou partie des mesures prévues aux lettres a) à j) risque d'avoir pour effet de dénaturer l'obligation imposée au point 2* ».

En effet, le fait que la liste des mesures à mettre en place soit précédée à l'article 181-3, alinéa 1er, point 2, par les mots « telles que » pourrait être interprété comme signifiant que cette liste a un caractère exemplaire et que les entreprises d'assurance peuvent simplement choisir sans justification quelles mesures elles veulent mettre en place. Pourtant, il s'agit d'une liste de mesures énumérant des garanties additionnelles à prévoir par une entreprise d'assurance, en sus des garanties juridiques et mesures techniques ou organisationnelles habituellement nécessaires conformément à l'état d'art, comme exigées par l'article 9, paragraphe 2, lettre g), du règlement (UE) 2016/679 (ci-après « RGPD »).

Le point 6° de l'amendement s'inscrit dans la continuité du point 4° et de la sauvegarde des droits fondamentaux et intérêts des personnes concernées par un traitement de données médicales dans le cadre de l'assurance. En introduisant les mots « aux lettres a), b), c), h) et i) » à l'alinéa 2 de l'article 181-3, l'amendement identifie clairement les mesures qui pourraient faire l'objet d'une dérogation par l'entreprise d'assurance, et le point 7° met en évidence les mesures pour lesquelles aucune dérogation n'est possible. Dès lors, le principe de base, ancré dans le projet de loi, est celui de la mise en place obligatoire, sans possibilité de dérogation par l'entreprise d'assurance, des mesures listées sous les lettres d), e), f), g) et j). Ces mesures sont considérées comme essentielles pour maintenir les droits fondamentaux et les intérêts de la personne concernée en matière de traitement de données médicales.

En effet, la mesure sous la lettre d) qui préconise « le chiffrement des données concernant la santé en transit, ainsi qu'une gestion des clés conformes à l'état de l'art » ne pourra pas faire l'objet d'une dérogation étant donné que les données de santé sont particulièrement à risque au moment du transit des données. Le chiffrement garantira en plus que le traitement des données médicales ne pourra se faire que par les personnes habilitées et destinataires de ces données.

La mesure figurant à la lettre e), qui oblige l'entreprise d'assurance à mettre en place des restrictions d'accès aux données concernant la santé, permet d'assurer que seuls certains employés de l'entreprise d'assurance, notamment ceux en charge de la gestion des sinistres, aient accès aux données médicales. Il sera ainsi évité qu'une personne n'ayant pas un motif légitime lié à l'exécution d'un contrat d'assurance ne puisse avoir accès à des données sensibles.

La mise en place de fichiers de journalisation sous la lettre f) rajoute un niveau supplémentaire de contrôle à la mesure énoncée sous la lettre e) et constitue un moyen pour contrôler que l'accès aux données médicales était nécessaire et légitime.

La sensibilisation du personnel à la protection des données sous la lettre g) reflète une pratique déjà bien établie dans le secteur des assurances pour l'ensemble des données nominatives et permet de maintenir les niveaux les plus élevés en matière de protection des données au sein des compagnies d'assurance.

Finalement, « *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* » devra être respectée à tout moment à des fins de transparence envers la personne concernée.

Il s'ensuit que les mesures auxquelles les entreprises d'assurance peuvent déroger sont restreintes aux lettres a), b), c), h) et i), et ce conformément aux conditions décrites à l'alinéa 2, en application d'une approche basée sur la proportionnalité.

En effet, il est proportionné qu'une entreprise d'assurance puisse déroger à la lettre a), en application du RGPD qui contient une disposition d'ouverture à l'article 37, paragraphe 4, concernant l'obligation de désigner un délégué à la protection des données (ci-après, « DPO »).

La lettre a) propose la désignation d'un DPO comme mesure d'atténuation des risques liés au traitement des données médicales. Néanmoins, en cas de raisons dûment justifiées, une entreprise d'assurance pourra, le cas échéant, décider de ne pas appliquer cette mesure. De telles raisons pourraient être, par exemple, le fait qu'une entreprise d'assurance ne traite que de manière occasionnelle des données de santé (par exemple, une entreprise d'assurance spécialisée principalement dans la couverture de dommages matériels, des risques liés à la perte d'exploitation, dans l'assurance crédit-caution ou encore dans l'assurance responsabilité civile maritime).

La lettre b) prévoit la réalisation d'analyses d'impact relatives à la protection des données (ci-après, « AIPD ») prévues à l'article 35 du RGPD. Il convient de noter qu'en plus des cas prévus au paragraphe 3 de l'article 35 précité, la CNPD a adopté conformément au paragraphe 4 dudit article une liste de types d'opérations de traitement pour lesquelles une AIPD est requise[23]. Ainsi, en vertu d'une approche basée sur le risque, le responsable du traitement doit apprécier la probabilité et le degré de risque encouru pour les droits et libertés des individus lorsqu'il entame un traitement. Ainsi, il serait disproportionné de contraindre une entreprise d'assurance à réaliser une AIPD si elle estime ne pas tomber sous une des hypothèses où une AIPD serait obligatoire en vertu de l'article 35 du RGPD ou de la liste nationale adoptée par la CNPD.

L'anonymisation des données proposée par la lettre c) ne pourra se concrétiser en pratique que si la durée de conservation des données à caractère personnel s'est écoulée. En effet, une fois que l'objectif poursuivi par un traitement est atteint, les données à caractère personnel doivent être supprimées, ou faire l'objet d'un processus d'anonymisation des données, afin de rendre impossible la « ré-identification » des personnes. Ces données, n'étant plus des données à caractère personnel, peuvent ainsi être conservées librement et servir à la production de statistiques.

De plus, la lettre c) propose la pseudonymisation des données. La pseudonymisation est définie à l'article 4, point 5), du RGPD comme « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ». Dans la mesure où les entreprises d'assurance ont besoin de données de santé nominatives liées à des personnes concernées directement identifiables afin de pouvoir exécuter un contrat d'assurance, il pourrait s'avérer disproportionné de pseudonymiser toutes les données à caractère personnel concernant les personnes concernées durant la validité du contrat.

La mesure prévue à la lettre h) propose une évaluation régulière de l'efficacité des mesures techniques et organisationnelles à travers un audit indépendant. Alors qu'un audit interne ou externe est reconnu en tant qu'instrument de contrôle, celui-ci peut représenter un exercice intensif en ressources et disproportionnellement complexe à réaliser dans le cas où l'entreprise d'assurance est amenée de par ses activités principales à ne traiter qu'occasionnellement des données de santé.

Enfin, la mesure énoncée au point 2, lettre i), prévoit l'adoption de codes de conduite sectoriels tels que prévus à l'article 40 du RGPD. Cet article encourage l'élaboration de codes de conduite volontaires destinés à contribuer à la bonne application du RGPD. Un tel code de conduite sectoriel ne peut pas être élaboré par un responsable du traitement, mais doit être mis en place par une organisation représentative d'un secteur d'activité. La volonté du secteur entier des assurances est alors nécessaire, afin que les entreprises d'assurance puissent respecter cette exigence.

Enfin, il convient de noter que si une entreprise d'assurance ou de réassurance fait usage de la faculté de déroger aux lettres a), b), c), h) ou i), elle devra, conformément à l'alinéa 2 de l'article 181-3, documenter et justifier en interne cette exclusion, et devra, conformément au point 7° du présent amendement, tenir la documentation nécessaire relative à cette exclusion à la disposition de la CNPD.

Le point 5° vise, ensemble avec l'amendement 3, à assurer la cohérence rédactionnelle du dispositif de la loi modifiée du 7 décembre 2015 sur le secteur des assurances, en introduisant l'intitulé de citation

---

23 Délibération N° 34/2019 du 6 mars 2019 de la Commission nationale pour la protection des données 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.

du règlement RGPD dans l'annexe III de ladite loi, et en employant la formule abrégée dans le dispositif de l'article 181-3.

Le point 7° de l'amendement vise, afin de tenir compte de la remarque du Conseil d'Etat, à introduire une disposition supplémentaire qui vise à apporter « *les garanties appropriées en matière de transparence aux personnes dont les données sont collectées* ».

En effet, il ne ressortait précédemment pas clairement de l'alinéa 2 de l'article 181-3 comment les entreprises d'assurance seraient amenées à documenter et justifier en interne de manière transparente envers la personne concernée, l'exclusion d'une ou de plusieurs des mesures susmentionnées.

Etant donné que le projet de loi n'a pas d'incidence sur l'application des règles du RGPD, les principes relatifs au traitement des données à caractère personnel énumérés à l'article 5 du RGPD et toutes les obligations générales incombant au responsable du traitement et prévues au chapitre IV du RGPD doivent être respectées. Ainsi, les personnes concernées disposent de tous les droits prévus aux articles 13 à 22 du RGPD dans les conditions y énumérées et doivent plus particulièrement être informées par les entreprises d'assurance conformément aux articles 12 à 14 du RGPD. Ainsi, toutes les informations y prévues doivent leur être fournies selon les modalités et conditions y énumérées. En ce qui concerne spécifiquement « *la base juridique du traitement* » (article 13.1.c) et 14.1.c) du RGPD), il convient de se référer conjointement à l'article 9.2.g) du RGPD, ainsi qu'au futur article 181-3 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances, pour le traitement de données de santé en matière d'assurances.

Même si les personnes concernées sont informées conformément aux dispositions existantes du RGPD, il convient d'apporter des précisions supplémentaires en ce qui concerne les informations qui doivent être tenues à la disposition de la CNPD. Ainsi, à travers le point 7° de l'amendement, il est précisé que les entreprises d'assurance doivent tenir à disposition de la CNPD toute documentation justifiant les raisons qui ont mené à la dérogation à une ou plusieurs des mesures énoncées aux lettres a), b), c), h) et i).

Amendement 3 introduisant un nouvel article 2

Il est inséré un nouvel article 2, libellé comme suit :

« Art. 2. L'annexe III, rubrique « Règlements », de la même loi, est complétée par l'alinéa suivant :

« « Règlement (UE) 2016/679 » : 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) ». ».

Motivation de l'amendement

Vu l'introduction à l'article 181-3 de la LSA de références au règlement (UE) 2016/679, il y a lieu de citer l'intitulé complet de ce règlement à l'annexe III de la LSA, en application de l'article 32, paragraphe 2, de ladite loi.

Prise de position du gouvernement par rapport à l'avis du Conseil d'Etat du 28 avril 2020

Quant aux considérations générales et aux remarques du Conseil d'Etat relatives à l'article unique, il est renvoyé à l'**amendement 2** et à la motivation dudit amendement.

Concernant certaines observations d'ordre légistique, il est renvoyé aux **amendements 1 et 3**.

Les autres observations d'ordre légistique ont été prises en compte telles que reflétées dans le texte coordonné du projet de loi.

Avis complémentaire du Conseil d'Etat (20/12/24):

Amendement 1

Sans observation.

Amendement 2

Les points 1°, 2° et 5° n'appellent pas d'observation.

Le point 3° modifie la phrase liminaire de l'article 181-3 nouveau. En reprenant en grande partie la proposition de texte formulée par le Conseil d'État dans son avis du 28 avril 2020 qui se réfère aux motifs d'intérêt public pouvant être invoqués par les compagnies d'assurance et de réassurance pour justifier la dérogation à l'interdiction de traitement des données de santé.

Les points 4°, 6° et 7°, entendent répondre à l'opposition formelle que le Conseil d'État avait formulée, dans son avis précité du 28 avril 2020, au sujet de l'article 181*bis* initial, et plus particulièrement en ce qui concerne l'alinéa 2. Dans sa version initiale, l'alinéa 2 permettait au responsable du traitement d'exclure une ou plusieurs des mesures destinées à assurer la protection des droits fondamentaux et des intérêts de la personne concernée par un traitement de données. Les mesures énoncées sont:

a) la désignation d'un délégué à la protection des données ;

b) la réalisation d'analyses d'impact ;

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 ;

j) la mise en place d'une politique interne indiquant notamment comment sont respectés les principes prévus à l'article 5 du règlement général sur la protection des données.

Dans son avis du 28 avril 2020, le Conseil d'État s'était opposé formellement à la disposition qui accordait au responsable du traitement la possibilité de déroger à tout ou partie de ces mesures, ceci au motif qu'une telle dérogation risquait de dénaturer l'obligation de protection des droits et libertés des personnes concernées, étant donné que le projet de loi lui-même constitue déjà une dérogation à l'interdiction du traitement des données de santé.

L'amendement proposé entend exclure la possibilité pour le responsable du traitement de déroger à l'intégralité des mesures énumérées ci-dessus, en interdisant toute dérogation aux mesures visées au point 2, lettres d), e), f), g), et j). Les autres mesures peuvent faire l'objet d'une dérogation dans le cadre d'une approche fondée sur la proportionnalité. Cette dérogation doit être documentée et la documentation doit être tenue à disposition de la Commission nationale pour la protection des données.

Au vu des amendements, des explications données par les auteurs et à la lecture de l'avis complémentaire de la Commission nationale pour la protection des données, le Conseil d'État se voit en mesure de lever son opposition formelle sur ce point.

Amendement 3

Sans observation.

Observation d'ordre légistique

Amendement 2

Au point 7°, à l'article 181-3, alinéa 2, troisième phrase, le Conseil d'État signale qu'il convient d'insérer une virgule à la suite des termes « En aucun cas ».

*

La Commission des Finances insère la virgule à l'endroit indiqué par le Conseil d'État.

*

5. TEXTE PROPOSE PAR LA COMMISSION PARLEMENTAIRE

Compte tenu de ce qui précède, la Commission des Finances recommande à la Chambre des Députés d'adopter le projet de loi n°7511 dans la teneur qui suit :

*

PROJET DE LOI

portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances en vue d'insérer un chapitre 2ter relatif au traitement de données concernant la santé

Art. 1er. À 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 181-2, un chapitre 2*ter* nouveau intitulé « Traitement de données concernant la santé », libellé comme suit :

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

Art. 181-3 – Traitement de données concernant la santé

Conformément à l'article 9, paragraphe 2, lettre g), du règlement (UE) 2016/679, et au regard des motifs d'intérêt public importants, inhérents aux contrats d'assurance et de réassurance pour lesquels la santé de la personne concernée constitue un élément déterminant, 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 ;
2. de la mise en œuvre des mesures appropriées suivantes 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:
   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 ;
   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 ;
   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.

Chaque responsable de traitement et, le cas échéant, chaque sous-traitant, doit documenter et justifier en interne l'exclusion, le cas échéant, d'une ou plusieurs des mesures énumérées à l'alinéa 1er, point 2, lettres a), b), c), h) et i). Cette documentation est tenue à la disposition de la

Commission nationale pour la protection des données. En aucun cas, il ne peut être dérogé aux mesures énumérées à l'alinéa 1er, point 2, lettres d), e), f), g) et j). »

Art. 2. L'annexe III, rubrique « Règlements », de la même loi, est complétée par l'alinéa suivant :

« « Règlement (UE) 2016/679 » : 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) ».

Luxembourg, le 14 janvier 2025

Le Président,
Diane ADEHM

Le Rapporteur,
Marc SPAUTZ

Impression: CTIE – Division Imprimés et Fournitures de bureau