Avis n° 18/2018 du 28 février 2018

Objet: Demande d'avis sur l'avant-projet de décret du Gouvernement wallon relatif aux organismes assureurs portant modification du Code wallon de l'Action sociale et de la Santé (CO-A-2018-003)

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après LVP), en particulier l'article 29 ;

Vu la demande d'avis de Mme Alda Greoli, ministre de l'Action sociale, de la Santé, de l'Egalité des chances, de la Fonction publique et de la Simplification administrative, reçue le 8 janvier 2018;

Vu le rapport de Monsieur Joël Livyns;

Émet, le 28 février 2018, l'avis suivant :

La Commission attire l'attention sur le fait qu'une nouvelle réglementation européenne relative à la protection des données à caractère personnel a été promulguée récemment : le Règlement 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 la Directive Police et Justice. Ces textes ont été publiés au journal officiel de l'Union européenne le 4 mai 2016[1].

Le Règlement, couramment appelé RGPD (Règlement général sur la protection des données), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et sera automatiquement d'application deux ans plus tard, soit le 25 mai 2018. La Directive Police et Justice doit être transposée dans la législation nationale au plus tard le 6 mai 2018.

Pour le Règlement, cela signifie qu'à partir du 24 mai 2016 et pendant le délai de deux ans de mise en application, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part une obligation négative, appelée "devoir d'abstention". Cette dernière obligation implique l'interdiction de promulguer une législation nationale qui compromettrait gravement le résultat visé par le Règlement. Des principes similaires s'appliquent également pour la Directive.

Il est dès lors recommandé d'anticiper éventuellement dès à présent ces textes. Et c'est en premier lieu au(x) demandeur(s) d'avis qu'il incombe d'en tenir compte dans ses (leurs) propositions ou projets. Dans le présent avis, la Commission a d'ores et déjà veillé, dans la mesure du possible et sous réserve d'éventuels points de vue complémentaires ultérieurs, au respect de l'obligation négative précitée.

I. OBJET DE LA DEMANDE

1. La Ministre de l'Action sociale, de la Santé, de l'Egalité des chances, de la Fonction publique et de la Simplification administrative, Mme Alda Greoli, a sollicité l'avis de la Commission concernant un avant-projet de décret relatif aux organismes assureurs portant modification du Code wallon de l'Action sociale et de la Santé (ci-après « l'avant-projet de décret »).

---

[1] 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)

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC

2. Faisant suite à l'accord institutionnel pour la 6ième réforme de l'Etat, conclu le 11 octobre 2011 et transcrit dans la loi spéciale du 6 janvier 2014 (MB 31 décembre 2014), l'avant-projet de décret vise à inscrire dans le Code wallon de l'action sociale et de la santé « *les fondements d'une assurance protection sociale wallonne, d'en formaliser l'ouverture des droits et le fonctionnement, d'y inscrire le rôle des organismes assureurs wallons dont les mutualités, et […] des caisses publiques […] à travers les prestations d'aide et de santé* » (exposé des motifs, p. 6).

3. L'avant-projet de décret procède à la reconnaissance des « organismes assureurs wallons » à savoir :

   - les sociétés mutualistes régionales wallonnes (sur la base de l'article 43bis de la loi du 6 août 1990 relative aux mutualités et unions nationales de mutualités), et ce, en tant qu'entités juridiques distinctes créées exclusivement pour la gestion des moyens liés à l'assurance protection sociale wallonne ; ces sociétés mutualistes sont constituées par le regroupement de mutualités dépendant d'une même union nationale ;
   - la Caisse auxiliaire d'assurance maladie-invalidité (CAAMI) ;
   - la Caisse HR Rail

   (article 3 10° de l'avant-projet de décret *juncto* Exposé des motifs, p. 7).

4. Ces organismes assureurs succèdent aux droits et obligations nés dans le chef des mutualités, unions nationales des mutualités, CAAMI et Caisse de soins de santé HR Rail (article 29 de l'avant-projet de décret *juncto* Exposé des motifs, p. 10).

II. EXAMEN DE LA DEMANDE

1. Application de la loi BCSS et avis du Comité sectoriel de la sécurité sociale

5. La Commission constate que les prestations des organismes assureurs régionaux impliquent différents échanges et/ou couplages de données à caractère personnel entre services publics. De tels échanges de données à caractère personnel entre services publics sont souvent soumis à une obligation d'autorisation préalable[1]. Le cas échéant, ce mécanisme d'autorisation devra

[1] Voir par exemple l'article 36bis de la LVP.

être respecté en pratique avant que ne soient rendus opérationnels les flux de données en question.

6. La Commission recommande en outre d'intégrer explicitement dans l'avant-projet de décret les principes d' « e-government »[2] qui sont reconnus dans la jurisprudence constante de la Commission, vu leur plus-value au niveau de la protection de la vie privée :

   a. la collecte unique de données (en tant qu'autorité, ne pas demander ce que l'on connaît déjà) ;
   b. l'utilisation de sources authentiques[3];
   c. la mise à disposition de sources authentiques via des intégrateurs de services[4].

7. De telles précisions ne sont toutefois pas nécessaires à la double condition que les organismes assureurs visés dans l'avant-projet de décret fassent bien partie du réseau de la Banque Carrefour de la Sécurité Sociale (BCSS), à titre d'institution de sécurité sociale au sens de l'article 2, 2° de la loi BCSS[5] (comme l'organisme assureur CAAMI), et/ou à titre d'institution participant au le réseau secondaire de la BCSS (comme c'est également le cas de la CAAMI)[6]. Ainsi, les mutuelles ont actuellement accès aux données de la BCSS via inscription dans ce réseau secondaire, plus précisément, via l'INAMI[7]. La Commission part du principe qu'il convient dès lors de veiller à ce que les mutuelles régionales soient bien inscrites dans ce réseau secondaire. En cas de doute pour l'un ou l'autre organisme assureur quant à sa participation à la BCSS, la Commission précise qu'il est toujours loisible au demandeur de prévoir explicitement l'adhésion de cet organisme à la BCSS via l'avant-projet de décret, ou, s'il y a lieu, prévoir une extension du réseau de la BCSS dans un arrêté royal fédéral, conformément à l'article 18 de la loi BCSS.

---

[2] Pour la rédaction, on peut s'inspirer de l'article 13 de la loi du 5 mai 2014 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier :
"Les services publics participants collectent, après qu'ils ont obtenu à cette fin les autorisations nécessaires, les données électroniques disponibles qui sont offertes par l'intégrateur de services fédéral auprès de ce dernier.
Les services publics participants ne recueillent plus les données dont ils disposent en exécution de l'alinéa 1er auprès de l'intéressé, ni auprès de son mandataire ou de son représentant légal. Les services publics participants qui disposent d'un accès direct auprès d'une source authentique réutilisent les données disponibles dans cette source et ne peuvent plus les demander à l'intéressé, ni à son mandataire ou à son représentant légal."

[3] Voir la recommandation de la Commission n° 09/2012 du 23 mai 2012 relative aux sources authentiques de données dans le secteur public.

[4] Voir la recommandation de la Commission n° 03/2009 du 1er juin 2009 concernant les intégrateurs dans le secteur public.

[5] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.

[6] Sur les réseaux primaires et secondaires de la BCSS, voir la description fournie sur le site de la BCSS à la page suivante : https://www.ksz-bcss.fgov.be/fr/a-propos-de-la-bcss/missions/structure-du-reseau.

[7] Ibid.

2. Adhésion des prestataires de soins à un intégrateur de service et compétence d'un Comité de surveillance

8. La Commission constate également qu'il convient d'encadrer de manière adéquate les flux et/ou couplages de données réalisés entre les organismes assureurs régionaux et les prestataires de soins, notamment du point de vue de la sécurisation des données et de la gestion des accès[8]. A cet égard, la Commission recommande de veiller à ce que les données échangées avec les prestataires de soins via un intégrateur de services adéquat et que les échanges de données concernés soient soumises au contrôle administratif d'un comité de surveillance indépendant.

3. Traitement de données de la santé

9. En ce qui concerne le traitement de données à caractère personnel relatives à la santé par les organismes assureurs régionaux, la Commission attire également l'attention sur le fait que dans la LVP, cette catégorie de données à caractère personnel est également soumise à un niveau de protection plus élevé. En principe, un traitement de données de ce type est même interdit (article 7, § 1 de la LVP), sauf dans les cas énumérés à l'article 7, § 2 de la LVP. L'une de ces exceptions concerne par exemple la situation où le traitement est rendu obligatoire en vertu d'une loi pour des motifs d'intérêt public importants. Une autre exception concerne le consentement écrit des personnes concernées.

10. La Commission recommande de faire un choix dans le projet (ou dans son Exposé des motifs) en ce qui concerne le fondement qui sera retenu pour justifier le traitement de données médicales dans le cadre des prestations fournies par les organismes assureurs wallons, et suggère d'opter ici pour la base prévue à l'article 7, § 2, c) de la LVP, à savoir, l'application de la sécurité sociale (équivalent, du point de vue de la base légale, à l'article 9.2.h du RGPD[9]).

11. En outre, de manière plus générale, la Commission recommande de prévoir explicitement une référence à l'application de la LVP dans l'avant-projet de décret. Le demandeur peut à cet égard s'inspirer librement de la législation relative à la protection sociale flamande et, par exemple, stipuler que les organismes assureurs wallons « *collectent et traitent les données à caractère personnel, et les échangent entre eux, y compris les données telles que visées aux*

[8] La Commission renvoie notamment à ses développements relatifs à la nécessité d'une gestion stricte des accès aux données de la santé, dans le cadre des obligations de sécurisation des données dans le chef des organismes assureurs (considérant 16).

[9] Article 9.2.h RGPD : « *le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3* ».

articles 6 et 7 de la loi du 8 décembre 1992, dans le souci de la protection de la vie privée des [usagers] ». (voir notamment l'article 41 du Décret du 24 juin 2016 relatif à la protection sociale flamande[10]).

12. La Commission se réfère par ailleurs aux autres conditions relatives au traitement de données médicales qui sont prévues dans la LVP ainsi qu'à l'article 25 de l'arrêté d'exécution du 13 février 2001, exposées ci-après :

a) les données doivent en principe être collectées auprès de la personne concernée elle-même (article 7 § 5 al.1);
b) le responsable du traitement doit tenir à jour une liste des catégories de personnes qui peuvent consulter les données. Ces personnes doivent être tenues au respect d'une obligation de confidentialité (article 25 1°, 2° et 3° de l'arrêté d'exécution);
c) les informations communiquées aux personnes concernées ou la déclaration à la Commission doivent mentionner des éléments supplémentaires, dont la base légale qui permet le traitement de données relatives à la santé dans de tels cas (article 25 4° de l'arrêté d'exécution);
d) le traitement doit en principe être réalisé sous la responsabilité d'un "professionnel des soins de santé" (article 7 § 4 LVP);
e) comme indiqué précédemment, pour certaines communications de données relatives à la santé, une autorisation préalable de la section Santé du Comité sectoriel de la Sécurité Sociale et de la Santé est requise (voir notamment l'article 15 de la loi BCSS).

13. La Commission précise toutefois qu'à partir du 25 mai 2018, certaines de ces obligations tomberont pour les données concernées, en vertu de l'article 9.3 du RGPD, à moins que l'Etat belge ne fasse usage de la faculté laissée par le RGPD d'insérer dans sa loi nationale des conditions supplémentaires en ce qui concerne le traitement de données de la santé (article 9.4 du RGPD).

---

[10] Article 41 du Décret du 24 juin 2016 relatif à la protection sociale flamande : « *Dans le présent article, on entend par :*
1° VAPH : la " Vlaams Agentschap voor Personen met een Handicap " (Agence flamande pour les Personnes handicapées), créée par l'article 3 du décret du 7 mai 2004 portant création de l'agence autonomisée interne dotée de la personnalité juridique " Vlaams Agentschap voor Personen met een Handicap " ;
2° porte d'entrée : la porte d'entrée, visée à l'article 2, § 1er, 51°, du décret du 12 juillet 2013 relatif à l'aide intégrale à la jeunesse ;
3° loi du 8 décembre 1992 : la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.
La VAPH, la porte d'entrée, l'agence et les caisses d'assurance soins enregistrent et traitent les données à caractère personnel et les échangent entre eux, y compris les données telles que visées aux articles 6 et 7 de la loi du 8 décembre 1992, dans le souci de la protection de la vie privée des usagers. L'enregistrement, le traitement et l'échange concernent les données à caractère personnel qui sont nécessaires pour l'octroi des interventions conformément au pilier de la protection sociale flamande. Les instances précitées demandent, en application de la réglementation relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les autorisations nécessaires pour l'accès à des données personnelles et pour leur utilisation, y compris des données mentionnées aux articles 6 et 7 de la loi du 8 décembre 1992, provenant de sources de données externes.
Les instances, visées à l'alinéa 2, transmettent au Gouvernement flamand toutes les données en vue de la politique flamande en matière d'aide sociale et de santé. Ces données sont anonymisées. Le Gouvernement flamand détermine quelles sont les données à fournir, ainsi que les modalités et la fréquence de la transmission de ces données. »

14. Ainsi, l'obligation de principe de récolter les données de la santé auprès des personnes concernées n'est pas imposée par le RGPD.

15. De même, à partir du 25 mai 2018, l'obligation de faire traiter les données relatives à la santé sous la responsabilité d'un professionnel ne s'appliquera pas si, comme c'est le cas dans le chef des organismes assureurs, "*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, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée*.[11]".

16. Enfin, l'obligation pour le responsable de traitement de tenir à jour une liste des catégories de personnes autorisées à consulter les données, n'est plus imposée par le RGPD. Néanmoins, sous l'empire du RGPD, vu la nature sensible des données (relatives à la santé) qui seront traitées dans le cadre de l'avant-projet, comme indiqué précédemment, la Commission souligne l'importance d'une gestion des utilisateurs et des accès stricte et appropriée[12], en vue d'un niveau de fiabilité élevé lors de l'identification et de l'authentification électroniques des utilisateurs, et ce, dans le cadre des obligations de sécurisation des données à charge des organismes assureurs et de leurs éventuels sous-traitants (article 32 RGPD).

17. Quant aux obligations d'autorisation préalables (condition e), que le RGPD permet aux Etats membres de les maintenir (article 36.5 RGPD[13]). Dans cette mesure, la Commission estime opportun que le demandeur y fasse référence dans l'avant-projet de décret, sur l'exemple du décret précité de l'autorité flamande[14]. La Commission renvoie à cet égard aux recommandations formulées sous le titre 1ier du présent avis (application de la loi BCSS et avis du Comité sectoriel de la sécurité sociale).

---

[11] Article 9(2)b du RGPD.

[12] Voir également la recommandation n° 01/2008 du 24 septembre 2008 relative à la gestion des accès et des utilisateurs dans le secteur public,

https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2008_0.pdf.

[13] Article 36.5 RGPD : « Nonobstant le paragraphe 1, le droit des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, y compris le traitement dans le cadre de la protection sociale et de la santé publique ».

[14] Article 41 du Décret du 24 juin 2016 relatif à la protection sociale flamande, voir note de bas de page n°12.

PAR CES MOTIFS,

Pour autant qu'il soit tenu compte des remarques formulées aux considérants 7, 8, 9, 10 à 16 et 17 impliquant :

- que les organismes assureurs visés dans l'avant-projet de décret fassent bien partie du réseau de la Banque Carrefour de la Sécurité Sociale (BCSS), et soient soumis pour leurs communications de données à l'obligation d'autorisation préalable du Comité sectoriel de la Sécurité Sociale, et ce, soit à titre d'institution de sécurité sociale au sens de l'article 2, 2° de la loi BCSS[15], soit à titre d'institution participant au le réseau secondaire de la BCSS (considérant 7);
- qu'un intégrateur de services adéquat soit désigné pour encadrer les communications de données entre organismes assureurs et prestataires, et que soit désigné un comité de surveillance chargé de contrôler la protection technique et administrative des flux de données (considérant 8);
- que la base légale de traitement des données par les organismes assureurs soit explicitée (considérant 11) ;
- que l'avant-projet de décret soit adapté afin de tenir compte des règles spécifiques de l'article 7 de la LVP (récolte des données de la santé auprès des personnes concernées) et de l'article 25 de l'arrêté royal du 13 février 2001 (désigner les catégories de personnes qui ont accès aux données de la santé et soumettre le traitement de ces données à la responsabilité d'un professionnel des soins de santé), tout en précisant dans l'exposé des motifs que ces obligations n'auront plus cours à dater de l'entrée en vigueur du RGPD (25 mai 2018), sauf si l'Etat belge réintroduit une telle obligation dans sa législation nationale sur pied de l'article 9.4 du RGPD (considérants 13 à 17);
- que l'avant-projet de décret se réfère à une stricte gestion des utilisateurs et des accès et à des mesures techniques et organisationnelles appropriées qui sont nécessaires à la protection des données à caractère personnel (considérant 17).

[15] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.

la Commission émet un avis **favorable** quant à l'avant-projet de décret relatif aux organismes assureurs portant modification du Code wallon de l'action sociale et de la santé.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere