Avis n° 45/2017 du 30 août 2017

Objet : Avis concernant un avant-projet de décret relatif à la protection sociale flamande (CO-A-2017-043)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

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 "la LVP"), en particulier l'article 29 ;

Vu le 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, ci-après le RGPD) ;

Vu la demande d'avis de Monsieur J. Vandeurzen, Ministre flamand du Bien-être, de la Santé publique et de la Famille, reçue le 27 juin 2016 ;

Vu le rapport de Monsieur J. Baret ;

Émet, le 30 août 2017, l'avis suivant :

Remarque générale préalable

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 général 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 est automatiquement applicable 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 que depuis le 24 mai 2016, pendant le délai d'exécution de deux ans, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part aussi 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) de l'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.

---

[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.)

I. OBJET DE LA DEMANDE D'AVIS

1. Le Ministre flamand du Bien-être, de la Santé publique et de la Famille (ci-après le demandeur), sollicite l'avis de la Commission concernant un avant-projet de décret relatif à la protection sociale flamande (ci-après l'avant-projet de décret).

Contexte

2. Dans le cadre de la sixième réforme de l'État, plusieurs compétences supplémentaires en matière de soins de santé et de protection sociale ont été transférées aux entités fédérées. En ce qui concerne la Communauté flamande, cette matière est régie parmi d'autres par le décret du 24 juin 2016 *relatif à la protection sociale flamande*.[1] L'actuel avant-projet de décret vise à remplacer le décret existant relatif à la protection sociale flamande.

3. L'avant-projet de décret étendrait les piliers existants de la protection sociale flamande par plusieurs nouveaux piliers. La protection sociale flamande comprendrait notamment les piliers suivants :
    1) le budget de soins pour les personnes lourdement dépendantes ;
    2) le budget de soins pour les personnes âgées nécessitant des soins ;
    3) le budget d'assistance de base ;
    4) les soins résidentiels pour personnes âgées ;
    5) les soins de santé mentale, incluant la revalidation qui est principalement axée sur les aspects psychosociaux ;
    6) la revalidation qui est principalement axée sur le rétablissement de fonctions physiques ;
    7) les soins à domicile ;
    8) les soins transmuraux ;
    9) les aides à la mobilité.[2]

4. Le Gouvernement flamand opte pour le regroupement des diverses interventions et des divers systèmes de soins liés aux revenus au sein d'une seule protection sociale flamande. Il adopte à cet effet une vision de "financement qui suit la personne", où l'indication d'une personne détermine quel genre de soins et de soutien sont possibles (ainsi que leur intensité et leur financement).[3] En rassemblant les différentes interventions dans un seul et même système de protection sociale, le Gouvernement flamand vise la simplification administrative. Cette simplification devrait

[1] Décret du 24 juin 2016 *relatif à la protection sociale flamande*, M.B., 6 septembre 2016. Ce décret n'a pas été préalablement soumis à l'avis de la Commission de la protection de la vie privée.

[2] Article 4 de l'avant-projet de décret.

[3] L'indication (à savoir l'évaluation des besoins en termes de soins) se ferait à cet égard via la méthode BelRAI, une échelle standardisée pour mesurer les besoins en termes de soins (article 60, § 2 de l'avant-projet de décret).

déboucher à terme notamment sur la prévention de doubles classifications et l'attribution automatique de droits.[4] En outre, les personnes concernées n'auraient qu'un seul point de contact pour toutes les interventions, à savoir la caisse d'assurance soins (en tant que "guichet unique ").[5] L'affiliation à une caisse d'assurance soins est obligatoire pour les personnes résidant dans la région linguistique néerlandophone à partir d'un délai déterminé par le Gouvernement flamand.[6] L'affiliation est libre pour les personnes qui résident dans la Région bilingue de Bruxelles-Capitale.[7]

5. Étant donné que l'avant-projet de décret annonce le 1er janvier 2019 comme date générale d'entrée en vigueur, la Commission estime utile d'évaluer l'avant-projet non seulement à la lumière de la LVP mais aussi du Règlement général sur la protection des données (RGPD).

II. EXAMEN DE LA DEMANDE D'AVIS

1. Finalités et licéité du traitement

6. Conformément à l'article 4, § 1, 2° de la LVP et à l'article 5(1)a du RGPD, les données à caractère personnel ne peuvent être collectées que pour des finalités déterminées, explicites et légitimes.

7. L'avant-projet de décret avance différentes finalités donnant lieu au traitement de données à caractère personnel, dont :
   a. l'attribution de budgets de soins "qui suivent la personne" et de tickets de soins sur la base d'une indication préalable (article 55 et 60 de l'avant-projet de décret);
   b. la numérisation et l'intégration de différentes interventions en vue d'un accès plus rationalisé aux droits aux interventions et aux soins (article 6, 5° de l'avant-projet de décret);
   c. la création d'un instrument de classification unique pour les personnes ayant besoin de soins (article 6, 7° de l'avant-projet de décret;
   d. un accès à un guichet unique pour toutes les questions relatives à des dossiers et aux droits concernant les interventions dans le cadre de la protection sociale flamande (article 6, 8° de l'avant-projet de décret);
   e. l'attribution automatique d'interventions de la protection sociale flamande (article 8 de l'avant-projet de décret);
   f. le contrôle de l'exactitude des indications et l'évaluation des aides requises par le prestataire d'aides à la mobilité et leur fourniture (article 34 de l'avant-projet de décret);

[4] Exposé des motifs de l'avant-projet de décret relatif à la protection sociale, p. 8-9.

[5] Id. Voir également l'article 6, 8° de l'avant-projet de décret.

[6] Article 42 de l'avant-projet de décret.

[7] Id.

g. le recouvrement d'interventions payées indûment (article 73 de l'avant-projet de décret);
h. le calcul des dépenses de l'Agence de la Protection sociale flamande (article 15, § 3 de l'avant-projet de décret);
i. l'analyse de données afin de documenter la politique flamande en matière de bien-être et de santé (article 49, § 5 de l'avant-projet de décret).

8. La Commission constate que les finalités précitées de la collecte de données sont déterminées, explicites et légitimes. Le projet de décret indique à cet égard que le traitement de données à caractère personnel dans le cadre de de la protection sociale flamande se fonde sur l'article 6, premier alinéa, 1) c) du RGPD. En ce qui concerne les données relatives à la santé, on renvoie à l'article 9, deuxième alinéa, h) du RGPD (voir ci-après le point 16). En vertu de la législation actuelle, le traitement pourrait se fonder sur l'article 5, c) de la LVP et l'article 7, § 2, c) ou j) de la LVP.

9. L'avant-projet de décret prévoit également une communication de données à l'Agence Intermutualiste en vue d'une analyse, sans toutefois préciser une quelconque finalité pour cette communication ou analyse (article 50, § 6). Vu la mission légale de l'Agence Intermutualiste, la Commission présume que le transfert et l'analyse auront pour but de documenter l'élaboration ultérieure de la politique.[8] Par souci de clarté, il est souhaitable que la finalité de la communication soit mentionnée explicitement dans le décret. Cela augmenterait également la transparence à l'égard du citoyen.

2. Proportionnalité du traitement

10. Conformément à l'article 4, § 1, 3° de la LVP, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement. L'article 5(1)c du RGPD dispose en outre que les données à caractère personnel doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ("minimisation des données").

11. L'avant-projet de décret prévoit plusieurs nouveaux flux de données (échanges de données à caractère personnel) par rapport au décret qu'il est censé abroger. À cet égard, l'avant-projet de décret ne détermine en outre pas clairement quelles catégories de données seraient échangées pour quelles finalités. L'article 50 de l'avant-projet de décret dispose que les caisses d'assurance soins, mutuelles et compagnies d'assurance échangeront les données "*nécessaires dans le cadre*

[8] Voir l'article 278 de la Loi-programme I du 24 décembre 2002, M.B. du 31 décembre 2002 qui prévoit la création de l'Agence intermutualiste.

de l'application des dispositions du présent décret, conformément à un contrat conclu à ce sujet".[9] Par ailleurs, l'article 50 comporte une énumération non limitative des catégories de données échangées entre les caisses d'assurance soins, les mutuelles et les compagnies d'assurance, à savoir :

1) la situation en matière d'assurance des utilisateurs dans le cadre de l'assurance obligatoire soins de santé et indemnités ;
2) les informations nécessaires à l'exécution de la réglementation européenne et internationale ;
3) les informations nécessaires à la prévention du double financement des frais de soins.[10]

Enfin, l'article 50 prévoit également un accès aux données pour les médecins-conseil, les services sociaux et les centres publics d'aide sociale, dans la mesure où cet accès pourrait être utile à l'exercice de leurs tâches respectives.[11] L'avant-projet de décret ne prévoit pas que le Gouvernement flamand précisera davantage les catégories de données ou que l'échange ou l'accès aux données seront soumis ultérieurement à une quelconque autorisation.

12. La Commission estime que la description actuelle des catégories de données ne permet pas d'évaluer la proportionnalité du traitement de données car cette description (1) n'est pas limitative ; (2) ne permet pas de déterminer de manière univoque quelles catégories de données seront concernées par le traitement de données à caractère personnel pour une finalité déterminée. En outre, la Commission estime que la description des catégories de données pertinentes doit être correctement encadrée par voie légale et non par simple voie contractuelle. La Commission insiste dès lors pour que soit
    - les catégories de données à caractère personnel soient décrites par finalité dans l'avant-projet même[12] ; soit

---

[9] Tous les passages cités de l'avant-projet sont des traductions libres effectuées par le Secrétariat de la Commission vie privée, en l'absence de traduction officielle.

[10] D'après les explications complémentaires du demandeur, il apparaît que le but de ces flux de données consiste notamment à éviter les doubles indemnisations et à pouvoir exécuter le règlement de subrogation.

[11] La Commission fait également remarquer que l'actuel avant-projet de décret, contrairement à l'article 41, 3° du décret du 24 juin 2016 *relatif à la protection sociale flamande* ne prévoit pas expressément que le VAPH, la porte d'accès, l'agence et les caisses d'assurance soins "échangeront" des données à caractère personnel entre elles. Dans la mesure où cet échange de données aura encore lieu en vertu de l'avant-projet de décret, cet échange doit également être mentionné explicitement et être encadré légalement. L'Exposé des motifs laisse entendre que tous les autres acteurs mentionnés à l'article 49, § 3 de l'avant-projet de décret échangeront potentiellement des données entre eux ("*les acteurs qui traitent/échangent des données [...] sont les suivants [...]*) (Exposé des motifs, p. 60). Bien que l'échange de données puisse être considéré comme un "traitement" de données, la Commission insiste pour que l'avant-projet de décret soit adapté pour indiquer expressément à quel moment il sera question d'un échange de données (au lieu d'un simple enregistrement de données) par les acteurs concernés.

[12] L'article 51 de l'avant-projet de décret prévoit toutefois une description spécifique des données qui peuvent être consultées pour une finalité déterminée, à savoir en ce qui concerne l'admission d'une personne dans un établissement de soins ou en vue de l'octroi d'une aide à la mobilité. L'article 51 de l'avant-projet de décret est énoncé comme suit *"En vue d'admettre un utilisateur dans un établissement de soins, ou d'octroyer une aide à la mobilité, l'établissement de soins concerné ou le fournisseur concerné d'une aide à la mobilité ont accès aux données suivantes :* 1° la caisse d'assurance soins à laquelle l'utilisateur concerné est affilié ; *2° la situation en matière d'assurance de l'utilisateur concerné, y compris les éventuels arriérés de ce dernier dans le cadre du paiement des cotisations*". Ces données sont, d'après la Commission, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

- l'avant-projet dispose que le Gouvernement flamand précisera les catégories de données (par finalité) après avis de la Commission ; soit
- l'avant-projet renvoie toujours expressément à la base légale ou décrétale existante permettant de déterminer de manière univoque les catégories de données concernées (par finalité) [13] ; soit
- l'avant-projet dispose que les échanges de données restent soumis à l'avenir à l'obligation d'obtenir une autorisation préalable.

13. Une recommandation similaire s'impose en ce qui concerne le renvoi aux traitements de données existants et nouveaux visés à l'article 22, deuxième alinéa (données dont disposent les caisses d'assurance soins), à l'article 37, premier alinéa (données dont dispose la Commission des caisses d'assurance soins), à l'article 39, dernier alinéa (données dont dispose la Commission d'experts) et à l'article 62 (données dont dispose l'Agence de la Protection sociale flamande).

14. La Commission fait remarquer que sauf disposition contraire expresse, les échanges de données visés en vertu de la législation existante sont soumis à l'obligation d'une autorisation préalable de la Vlaamse Toezichtcommissie ou des Comités sectoriels institués au sein de la Commission. Il ressort de contacts avec le demandeur que l'intention est de maintenir une telle méthode. La Commission recommande de reprendre cela dans la réglementation afin que via cette procédure, une évaluation de la proportionnalité puisse éventuellement avoir lieu.

15. Elle fait également remarquer que l'article 23 de l'avant-projet de décret dispose que la caisse d'assurance soins peut collecter de sa propre initiative tous les renseignements manquants afin de pouvoir évaluer les droits de personnes concernées. À cet effet, elle peut procéder ou faire procéder à des enquêtes supplémentaires et réclamer des renseignements auprès de la personne concernée (ou son représentant) "*si elle ne peut pas obtenir les renseignements manquants d'une autre manière*". L'avant-projet prévoit à cet égard une compétence d'enquête définie très largement et utilise la collecte indirecte comme point de départ. Ici aussi, un encadrement légal clair s'impose, en ce qui concerne tant les données à collecter que la provenance de ces données. Une remarque similaire vaut également pour l'article 34 de l'avant-projet de décret, qui prévoit une compétence de contrôle pour ladite Commission des caisses d'assurance soins.

[13] Un renvoi explicite aux dispositions pertinentes qui permettent de déterminer de manière univoque les catégories de données pertinentes est également important afin de garantir la transparence à l'égard des personnes concernées (voir ci-après le point 31).

3. Traitement de données sensibles

16. Différentes finalités reprises dans l'avant-projet de décret supposent le traitement de données relatives à la santé (voir ci-avant, point n°7). Conformément à l'article 7, § 2 de la LVP, le traitement de données relatives à la santé est autorisé lorsque le traitement est nécessaire à la réalisation d'une finalité fixée par ou en vertu de la loi, en vue de l'application de la sécurité sociale ainsi que lorsque le traitement est nécessaire aux fins de la gestion de services de santé agissant dans l'intérêt de la personne concernée et que les données sont traitées sous la surveillance d'un professionnel des soins de santé.

17. Conformément à l'article 9, deuxième alinéa, h) du RGPD, les données relatives à la santé peuvent être traitées aux fins "*... 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*". Conformément à l'article 9, troisième alinéa du RGPD, les données relatives à la santé ne peuvent toutefois faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), que *"si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents."*

18. L'avant-projet de décret prévoit à l'article 37, § 2 un secret professionnel pour les membres de la Commission des caisses d'assurance soins, mais ne prévoit pas un tel secret professionnel pour les autres entités qui ont accès aux données des personnes qui font appel ou souhaitent faire appel à la protection sociale flamande (comme par exemple la Commission d'experts mentionnée à l'article 39). La Commission insiste pour que l'avant-projet de décret indique clairement quelles entités ont ou non accès aux données relatives à la santé et précise à cet égard que ces données sont traitées soit sous la responsabilité d'une personne tenue au secret professionnel soit sous la responsabilité d'une personne qui est tenue à une obligation de secret (pour autant qu'un tel secret professionnel ou qu'une telle obligation de secret ne soit pas encore explicitement ancrée légalement).

19. L'avant-projet de décret prévoit que l'Agence de la Protection sociale flamande puisse infliger dans certains cas une amende administrative (article 47, § 1, quatrième alinéa de l'avant-projet de décret). La Commission fait remarquer que le traitement de données à caractère personnel en matière de sanctions administratives est actuellement soumis à des conditions supplémentaires,

en vertu de l'article 8, § 2 de la LVP. En vertu du RGPD, les sanctions administratives ne sont par contre plus considérées comme une "catégorie particulière" de données à caractère personnel.

20. Enfin, la Commission fait encore remarquer que le traitement à grande échelle de catégories particulières de données, dont les données relatives à la santé, doit en principe faire l'objet d'une analyse d'impact relative à la protection des données (AIPD) si le traitement commence après le 25 mai 2018 ou s'il est question d'un changement au niveau du risque engendré par les traitements ou si les données sont utilisées pour une nouvelle finalité (article 35 du RGPD).[14] Vu la date générale d'entrée en vigueur fixée au 1er janvier 2019, la réalisation d'une AIPD sera nécessaire.

4. Durée de conservation des données

21. En vertu de l'article 4, § 1, 5° de la LVP, les données à caractère personnel peuvent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. L'article 5(1)e du RGPD prévoit une limitation analogue de la conservation.

22. La Commission constate que l'avant-projet de décret ne prévoit aucun délai de conservation. La Commission insiste pour que cette lacune soit comblée ou du moins qu'il soit prévu que le Gouvernement, lors de la précision des données à caractère personnel qui seront concrètement traitées, établisse également le délai concret pendant lequel ces données seront conservées au maximum, et ce après avis de la Commission.

5. Responsabilité

23. L'article 1, § 4, deuxième alinéa de la LVP dispose que pour les traitements dont les finalités et les moyens sont déterminés par ou en vertu de la loi, le responsable du traitement est celui qui est désigné en la matière dans le document réglementaire. L'article 4(7) du RGPD dispose que "*lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État*

[14] Voir à cet égard le Groupe de travail de protection des données Article 29, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", WP 248, 4 avril 2017, p. 11-12 et p. 18-19 et Commission de la protection de la vie privée, "Projet de recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable soumis à la consultation publique (CO-AR-2016-004) p. 18-19.

membre".

24. La Commission prend acte du fait que l'article 49, § 4 de l'avant-projet de décret indique explicitement dans quelles circonstances quelles entités interviennent en qualité de responsables du traitement. Par souci d'exhaustivité et de clarté, il est recommandé de compléter cette formulation comme suit : '*les responsables du traitement au sens de l'article 4(7) du Règlement général sur la protection des données'.*[15] Par ailleurs, la Commission observe que la désignation des responsables du traitement à l'article 49, § 4 de l'avant-projet de décret semble incomplète. L'article 67 de l'avant-projet de décret prévoit ainsi par exemple la création d'une banque de données des indications appliquées, mais ne précise pas sous la responsabilité de qui cette banque de données est tenue.

25. L'article 28 de l'avant-projet prévoit le développement d'une "plateforme numérique Protection sociale flamande". D'après l'Exposé des motifs, les flux de données entre les différents acteurs de l'assurance soins flamande se feraient via cette plateforme numérique. La plateforme proprement dite serait développée sous la responsabilité de l'Agence de la Protection sociale flamande en concertation avec les caisses d'assurance soins.

26. La Commission fait remarquer l'Agence de la Protection sociale flamande (auparavant : le Fonds de soins flamand) a été intégrée au réseau de la sécurité sociale le 27 janvier 2004 par le Comité de gestion de la BCSS, après avis favorable du Comité sectoriel de la Sécurité Sociale (avis n° 04/03 du 6 janvier 2004).[16] La Commission fait également remarquer que certains échanges de données envisagés relèvent du champ d'application du décret du 25 avril 2014 *relatif à l'organisation du réseau pour le partage de données entre acteurs des soins*, dans lequel d'une part la plateforme e-health et d'autre part la Banque Carrefour de la Sécurité Sociale sont désignées comme intégrateurs de services[17]. La Commission recommande au demandeur de préciser davantage la répartition des rôles et des tâches entre la plateforme numérique "Protection sociale flamande" et les intégrateurs de services précités.

---

[15] La Commission fait également remarquer que l'Exposé des motifs utilise apparemment erronément la notion de "sous-traitant". Celui-ci dispose en effet que "*Les acteurs qui traitent/échangent des données, et qui doivent donc être considérés comme "sous-traitants", sont les suivants [...]*". (Exposé des motifs, page 60). La qualité de "sous-traitant" au sens de l'article 1, § 5 de la LVP et de l'article 4(8) du RGPD ne découle toutefois pas de la simple circonstance qu'une certaine entité traite des données à caractère personnel (des responsables du traitement peuvent en effet également traiter des données à caractère personnel). Le passage cité de l'Exposé des motifs est en outre contredit par les termes de l'article 49, § 4 de l'avant-projet de décret (qui désigne plusieurs des acteurs cités comme "responsables du traitement").

[16] Cette décision a été prise en application de l'arrêté royal du 16 janvier 2002 *relatif à l'extension du réseau de la sécurité sociale à certains services publics et institutions publiques des Communautés et des Régions, en application de l'article 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.*

[17] *M.B.* 20 août 2014 (article 72).

6. Mesures de sécurité

27. L'article 16 de la LVP oblige le responsable du traitement à "*prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel*" et précise que "*Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels*". Pour une interprétation concrète de cette disposition[18], la Commission renvoie à la recommandation qu'elle a émise visant à prévenir les fuites de données et aux mesures de référence[19] qui devraient être respectées dans le cadre de tout traitement de données à caractère personnel.

28. L'article 32 du RGPD prévoit une obligation de sécurité similaire à celle de l'article 16 de la LVP et se réfère en outre aux mesures suivantes pour assurer, au besoin, un niveau de sécurité adapté au risque :
    a. la pseudonymisation et le chiffrement des données à caractère personnel;
    b. des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes,
    c. des moyens permettant de rétablir la disponibilité des données personnelles et l'accès à celles-ci dans des délais appropriés en cas d'incident,
    d. une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

29. Vu le caractère sensible des données qui seront échangées dans le cadre de l'avant-projet de décret, la Commission souligne l'importance d'une gestion des utilisateurs et des accès correcte.[20] Dans la mesure où la plateforme numérique Protection sociale flamande mentionnée à l'article 28 de l'avant-projet interviendrait en quelque sorte comme un intégrateur de services, il est souhaitable que ce rôle soit décrit de manière plus précise et soit bien encadré légalement.[21]

---

[18] Recommandation d'initiative n° 01/2013 du 21 janvier 2013 *relative aux mesures de sécurité à respecter afin de prévenir les fuites de données*https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2013.pdf.

[19] Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel, Version 1.0, https://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel_0.pdf.

[20] 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.

[21] Voir également la recommandation d'initiative n° 03/2009 du 1er juillet 2009 concernant les intégrateurs dans le secteur public,
https://wwwhttps://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_03_2009_1.pdf
("*En tout cas, on espère que les instances chargées d'une intégration de services ou de données à caractère personnel dans le secteur public disposent toujours d'une réglementation légale explicite en la matière qui réponde aux dispositions de la présente recommandation*").).

7. Droits de la personne concernée

30. La Commission constate que l'avant-projet de décret ne comporte aucune disposition expresse ni aucun renvoi quant aux droits de la personne concernée. Elle souhaite attirer l'attention sur deux droits qui peuvent être d'une importance particulière dans le cadre de l'avant-projet de décret et pour lesquels le demandeur doit éventuellement prévoir des garanties légales supplémentaires.

31. L'article 9 de la LVP et les articles 12-14 du RGPD définissent les informations qui doivent être fournies à la personne concernée et font une distinction selon que les données à caractère personnel ont été obtenues ou non auprès de la personne concernée (collecte directe ou indirecte). L'article 14.5(c) du RGPD est particulièrement important pour l'avant-projet de décret car il prévoit une possibilité de dérogation lorsque les données à caractère personnel n'ont pas été obtenues auprès de la personne concernée si "*l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis* ", mais uniquement si "*[ce droit] prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée"*. La Commission invite dès lors le demandeur à vérifier la manière dont la transparence des traitements de données envisagés sera assurée et à prendre au besoin des mesures supplémentaires appropriées pour protéger les intérêts légitimes de la personne concernée.[22] Outre un cadre légal clair qui expose les informations à fournir qui sont citées à l'article 14, la Commission recommande que le projet prévoie que les caisses d'assurance soins (qui interviendront en tant que guichet unique) soient rendues responsables de la transmission d'informations dans leurs communications et leurs interactions individuelles avec les personnes concernées, informations qui incluent les coordonnées du délégué à la protection des données à qui elles peuvent s'adresser pour de plus amples informations.

32. L'article 8 de l'avant-projet de décret prévoit que les interventions de la protection sociale flamande "*sont automatiques octroyées, sauf impossibilité. Dans ce dernier cas, le Gouvernement flamand peut déterminer que les interventions soient octroyées sur demande*". L'Exposé des motifs précise que l'octroi automatique des droits signifie que, dans la mesure du possible, la personne concernée recevra le montant des interventions auxquelles elle a droit sans tracasseries administratives une

---

[22] Voir également à cet égard Cour de Justice, Affaire C-201/14 (*Smaranda Bara e.a. contre Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF)*), 1er octobre 2015, points 40-41 ("*40. Or, outre la circonstance, relevée par la juridiction de renvoi, selon laquelle les données relatives aux revenus ne font pas partie des données personnelles nécessaires à l'établissement de la qualité d'assuré, il y a lieu de souligner que l'article 315 de la loi n° 95/2006 ne fait qu'envisager, en son principe, la transmission de ces dernières données personnelles détenues par des autorités, des institutions publiques et d'autres institutions. Il ressort également de la décision de renvoi que la définition des informations transmissibles ainsi que les modalités de mise en œuvre de la transmission de ces informations ont été élaborées au moyen non pas d'une mesure législative, mais du protocole de 2007 conclu entre l'ANAF et la CNAS, lequel n'aurait pas fait l'objet d'une publication officielle. 41. Dans de telles circonstances, il ne saurait être considéré que les conditions posées à l'article 13 de la directive 95/46 pour qu'un État membre puisse déroger aux droits et aux obligations qui découlent de l'article 10 de cette directive sont réunies."*)

fois que l'indication a eu lieu.[23] La Commission souhaite ici attirer l'attention sur l'article 12*bis* de la LVP et sur l'article 22 du RGPD qui prévoient une interdiction de principe des "prises de décision automatisées".[24] Cette interdiction ne s'applique pas si la décision est autorisée "*par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis"*, mais de nouveau uniquement si cette disposition prévoit également des "*mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée*". La Commission invite dès lors le demandeur à prévoir des mesures appropriées supplémentaires afin de protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée.[25]

8. Réutilisation de données à caractère personnel à des fins stratégiques

33. Les §§ 5 et 6 de l'article 49 de l'avant-projet de décret prévoient la réutilisation de données anonymisées en vue de l'élaboration ultérieure de la politique. L'avant-projet indique à cet égard que le Gouvernement flamand déterminera quelles données seront fournies, ainsi que les modalités et la périodicité de la transmission. La Commission recommande d'indiquer que cet arrêté sera soumis à l'avis préalable de la Commission. Elle recommande également dans le cadre de la préparation de cet arrêté de tenir compte du Chapitre II de l'arrêté royal du 13 février 2001 ("Traitements ultérieurs à des fins historiques, statistiques ou scientifiques") et en particulier d'identifier quelle(s) entité(s) se chargera (chargeront) d'anonymiser les données en tant que tiers de confiance (Trusted Third Party ou TTP)[26], ainsi que du règlement repris à l'article 5 et à l'article 15 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* [27]*.*

III. CONCLUSION

34. Vu ce qui précède, la Commission estime que l'avant-projet de décret peut offrir suffisamment de garanties quant à la protection des données à caractère personnel des personnes concernées, à condition d'intégrer les remarques suivantes :

---

[23] Exposé des motifs, page 36.

[24] La "prise de décision automatisée" doit en l'occurrence être comprise comme "*une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire*" (article 22 RGPD).

[25] Voir également le considérant (71) du RGPD.

[26] Voir également la recommandation n° 02/2010 du 31 mars 2010 *concernant le rôle de protection de la vie privée des Trusted Third Parties (TTP ou tiers de confiance) lors de l'échange de données*, publiée à l'adresse suivante https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_02_2010_0.pdf.

[27] Le cadre des notions de ces instruments doit toutefois être mis en conformité avec les notions utilisées par le RGPD. Le RGPD ne parle ainsi pas de "données à caractère personnel codées" mais de "données à caractère personnel qui ont fait l'objet d'une pseudonymisation". Pour plus d'informations, voir la Note relative aux données anonymes, codées et on codées dans le cadre d'enquêtes statistiques et scientifiques, https://www.privacycommission.be/sites/privacycommission/files/documents/Note%20concernant%20les%20donn%C3%A9es%20anonymes%20cod%C3%A9es%20et%20non%20cod%C3%A9es%206.2%20%28002%29.pdf.

- précision de la finalité de la communication de données à l'Agence intermutualiste en vue d'analyse (voir le point 9) ;
- précision des catégories de données concernées, soit dans le texte du décret, soit en prévoyant que les catégories de données soient davantage spécifiées dans un arrêté, soit en renvoyant expressément à la base légale ou décrétale spécifique existante à l'aide de laquelle les catégories données concernées peuvent être déterminées de manière univoque. Si à l'avenir, les échanges de données restent soumis à l'obligation d'obtenir une autorisation préalable, la Commission recommande de le reprendre dans la réglementation (voir les points 12 et 13) ;
- précision de la compétence d'enquête des caisses d'assurance soins et de la Commission des caisses d'assurance soins, plus précisément en ce qui concerne les données à collecter ainsi que la provenance de ces données (voir le point 15) ;
- précision des entités qui ont accès ou non aux données relatives à la santé en mentionnant que ces données sont traitées sous la responsabilité d'une personne qui est tenue soit au secret professionnel, soit à une obligation de secret (voir le point 18) ;
- précision du délai de conservation des données à caractère personnel traitées ou prévoir au moins que le Gouvernement déterminera le délai maximal concret pendant lequel ces données seront conservées, et ce après avis de la Commission (voir le point 22) ;
- précision de garanties supplémentaires afin d'assurer un niveau de protection adéquat (voir les points 19 et 28) ;
- désignation des responsables du traitement au sens de l'article 1, § 4 de la LVP et de l'article 4(7) du RGPD (voir le point 24) ;
- clarification de la répartition des rôles et tâches entre la plateforme numérique Protection sociale flamande, la plateforme eHealth et la Banque Carrefour de la Sécurité Sociale (voir les points 26 et 29) ;
- référence aux droits de la personne concernée et précision des garanties supplémentaires en matière de transparence et en cas de prise de décision automatisées (voir le point 31) ;
- précision du fait que l'arrêté du Gouvernement flamand relatif à la réutilisation envisagée de données à caractère personnel à des fins stratégiques sera préalablement soumis à l'avis de la Commission, avec prise en compte des conditions reprises au Chapitre II de l'arrêté royal du 13 février 2001 et indication de la ou des entités qui se chargeront de l'anonymisation des données en tant que tiers de confiance (voir les points 33 et 32).

PAR CES MOTIFS,

la Commission émet un avis favorable quant à l'avant-projet de décret relatif à la protection sociale flamande, et ce à la condition expresse que les remarques précitées y soient intégrées.

L'Administrateur ff., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere