Avis n° 04/2019 du 16 janvier 2019

Objet : Avis relatif à l'article 1er, 1° d'un projet d'arrêté royal *modifiant les articles 18, § 1er, A, et 19, § 1er de l'annexe à l'arrêté royal du 14 septembre 1984 établissant la nomenclature des prestations de santé en matière d'assurance obligatoire soins de santé et indemnités* (CO-A-2018-166)

L'Autorité de protection des données (ci-après "l'Autorité") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après "la LCA") ;

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* (ci-après "le RGPD") ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après "la LTD") ;

Vu la demande d'avis de Madame Maggie De Block, Ministre des Affaires sociales et de la Santé publique, reçue le 13/11/2018 ;

Vu le rapport de Monsieur Willem Debeuckelaere ;

Émet, le 16 janvier 2019, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. La Ministre des Affaires sociales et de la Santé publique (ci-après le demandeur) sollicite l'avis de l'Autorité concernant l'article 1er, 1° d'un projet d'arrêté royal *modifiant les articles 18, § 1er, A, et 19, § 1er de l'annexe à l'arrêté royal du 14 septembre 1984 établissant la nomenclature des prestations de santé en matière d'assurance obligatoire soins de santé et indemnités* (ci-après le projet d'arrêté royal).

Contexte et antécédents

2. L'article 9*ter* de la loi *relative à l'assurance obligatoire soins de santé et indemnités* coordonnée le 14 juillet 1994 (ci-après la loi du 14 juillet 1994), que le présent projet d'arrêté royal applique, prévoit que le Roi peut subordonner le remboursement de certaines prestations de santé à la condition de l'enregistrement de données déterminées relatives à ces prestations, et ce en vue d'une dispensation de soins plus rapide et plus efficiente, du contrôle de la qualité et du coût des soins dispensés ou de la recherche scientifique.

3. Dans son avis[1] concernant le projet d'article 9*ter* susmentionné, le prédécesseur en droit de l'Autorité (la Commission de la protection de la vie privée ou Commission) n'a pu que constater à l'époque qu'en l'absence d'informations concrètes concernant d'éventuels futurs projets d'enregistrement, elle ne pouvait pas se prononcer sur les principes majeurs en matière de protection des données à caractère personnel, notamment la finalité, la proportionnalité et la sécurité de l'information. La Commission a toutefois pris acte à l'époque que son avis préalable serait demandé concernant tout projet d'arrêté royal créant un projet d'enregistrement concret. Le présent projet d'arrêté royal crée un tel enregistrement, pour le remboursement des prestations d'irradiations stéréotaxiques qui y sont mentionnées.

4. En ce qui concerne l'enregistrement prescrit, le projet d'arrêté royal prévoit uniquement ce qui suit :
"Le remboursement des prestations 444636 - 444640, 444651 - 444662, 444673 - 444684, 444695 - 444706 dépend, en application de l'article 9ter de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, de l'enregistrement des irradiations stéréotaxiques exécutées.
Le Comité sectoriel de la Sécurité sociale et de la Santé, section Santé, autorise l'échange de données visé au premier alinéa, selon la prestation envisagée.

[1] Avis n° 28/2012 du 12 septembre 2012 *relatif aux articles 2 ; 24, 2° et 4°; 72 et 110 de l'avant-projet de loi portant dispositions diverses en matière de santé*.

La distinction faite entre les différentes modalités et les différents délais pour la conservation des données visées au premier alinéa, est, en fonction des finalités de ces données, également soumise à l'autorisation par le Comité sectoriel de la Sécurité sociale et de la Santé."

II. EXAMEN DE LA DEMANDE D'AVIS

5. À l'instar de ce que le prédécesseur en droit de l'Autorité a déjà fait remarquer dans un dossier similaire[2], l'Autorité répète - avant l'analyse du contenu - que le patient ne peut en aucun cas être la victime, au niveau de l'intervention de l'assurance ou plutôt de l'absence d'intervention, d'une négligence, dans le chef de l'hôpital/du médecin spécialiste, concernant la bonne exécution de l'enregistrement en ligne prescrit. En cas de négligence de ce dernier au niveau de l'enregistrement prescrit, il faudrait dès lors que ce soit l'hôpital/le médecin spécialiste qui supporte lui-même les répercussions financières d'un éventuel refus de l'intervention de l'assurance et non le patient[3].

6. L'Autorité constate ensuite que, comme cela a déjà été évoqué ci-dessus, le projet d'arrêté royal ne précise en fait rien quant au contenu de l'enregistrement dont dépend l'intervention de l'assurance pour les prestations mentionnées dans le projet d'arrêté royal. Une telle disposition réglementaire, où même les éléments les plus essentiels du traitement prescrit de données de santé sensibles font défaut, n'offre évidemment aucun point de repère pour les personnes concernées.

7. Une disposition sans la moindre précision de contenu de l'enregistrement envisagé ne permet d'ailleurs même pas à l'Autorité de procéder ne serait-ce qu'à un contrôle marginal au regard des garanties prescrites par le RGPD en matière de protection des données à caractère personnel, comme la licéité et la transparence, la finalité, la proportionnalité (minimisation des données), la limitation de conservation et la sécurité du traitement.

8. L'Autorité constate que le projet d'arrêté royal fait à proprement parler passer le contrôle au regard du RGPD entre les mains du *"Comité sectoriel de la Sécurité sociale et de la Santé, section Santé"*, qui, outre l'échange de données allant de pair avec l'enregistrement, devra également autoriser les modalités et les délais de conservation des données. Une délégation après une délégation légale n'est pas admissible. La doctrine et la jurisprudence constante du

---

[2] Voir aussi le point 9 de l'avis n° 17/2014 de la Commission du 26 février 2014 *relatif à un projet d'arrêté royal modifiant les articles 35 et 35bis de l'annexe de l'arrêté royal du 14 septembre 1984 établissant la nomenclature des prestations de santé en matière d'assurance obligatoire soins de santé et indemnités, en application de l'article 9ter de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994*.

[3] En la matière, l'Autorité renvoie également au plan d'actions e-Santé 2013-2018, en particulier le point d'action 18 : *"Inventaire et consolidation des registres"* (voir http://www.plan-egezondheid.be/fr/points-daction/onventaire-et-consolidation-des-registres/).

Conseil d'État sont claires en la matière : l'instance qui se voit confier une mission par le législateur doit l'exécuter elle-même et ne peut pas la déléguer sans y être autorisée explicitement par le législateur.

9. Ni l'article 8 de la CEDH, ni l'article 22 de la Constitution, ni le RGPD, en particulier l'article 6.3, ne permettent un tel "chèque en blanc" (voir ci-dessous le point 17). En effet, toute ingérence d'une autorité publique dans le droit au respect de la vie privée doit être prescrite dans une "disposition légale suffisamment précise" qui répond à un besoin social impérieux et qui est proportionnelle à la finalité poursuivie. Une telle disposition légale précise doit définir les éléments essentiels des traitements de données à caractère personnel allant de pair avec l'ingérence de l'autorité publique[4]. Dans ce cadre, il s'agit au moins :
   - des finalités déterminées, explicites et légitimes ;
   - des (catégories de) données à caractère personnel qui sont pertinentes et non excessives ;
   - du délai de conservation maximal des données à caractère personnel enregistrées ;
   - de la désignation du responsable du traitement.

   Cela n'empêche évidemment pas que, dans la mesure où les éléments les plus essentiels de l'enregistrement envisagé de données à caractère personnel relatives à la santé - au demeurant extrêmement sensibles - seraient définis dans le projet d'arrêté royal, d'autres détails, modalités d'exécution et mesures en matière de sécurité de l'information de l'enregistrement puissent être évalués par le biais d'une délibération du comité compétent en la matière.

10. L'Autorité constate aussi que le libellé concernant l' "autorisation" susmentionnée du "Comité sectoriel de la Sécurité sociale et de la Santé" ne tient pas compte de la nouvelle réglementation en la matière, en particulier : la loi du 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du RGPD* qui crée un comité de sécurité de l'information dont la chambre sécurité sociale et santé est notamment compétente pour rendre des "délibérations" pour la communication de données à caractère personnel relatives à la santé (voir l'article 39 de la loi susmentionnée du 5 septembre 2018).

11. L'Autorité recommande dès lors au demandeur d'aligner le libellé du projet d'arrêté royal sur ce plan sur le cadre juridique qui a été modifié en la matière.

[4] Voir DEGRAVE, E., "*L'e-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle*", Collection du CRIDS, Larcier, Bruxelles, 2014, p. 161 e.s. (voir e.a.: CEDH, arrêt *Rotaru c. Roumanie*, 4 mai 2000). Voir également quelques arrêts de la Cour constitutionnelle : l'arrêt n° 44/2015 du 23 avril 2015 (p. 63), l'arrêt n° 108/2017 du 5 octobre 2017 (p. 17) et l'arrêt n° 29/2018 du 15 mars 2018 (p. 26).

1. Finalités

12. Conformément à l'article 5.1.b) du RGPD, le traitement de données à caractère personnel n'est autorisé que pour des finalités déterminées, explicites et légitimes.

13. L'article 9*ter* de la loi du 14 juillet 1994, que le présent projet d'arrêté royal applique, dispose que l'enregistrement dont dépend l'intervention de l'assurance pour les irradiations stéréotaxiques qui y sont énumérées doit servir les finalités suivantes :
    - une dispensation de soins aux bénéficiaires plus rapide et plus efficiente ;
    - le contrôle de la qualité et du coût des soins dispensés **ou**
    - la recherche scientifique.

14. En l'absence d'autres précisions dans le projet d'arrêté royal, il n'apparaît pas d'emblée clairement lesquelles des finalités susmentionnées sont effectivement poursuivies dans le présent projet d'enregistrement. Le "ou" figurant à l'article 9*ter* susmentionné laisse en effet supposer que tous les projets d'enregistrement qui doivent être élaborés par arrêté royal ne viseront pas les mêmes finalités ou toutes les finalités susmentionnées. Une précision dans le projet d'arrêté royal s'impose.

15. En outre, l'Autorité estime que "la recherche scientifique", sans autre précision dans le projet d'arrêté royal, est tellement large et générale qu'elle ne répond pas non plus à la finalité déterminée et explicite requise en vertu de l'article 5.1.b) du RGPD.

2. Fondement juridique

16. Tout traitement de données à caractère personnel doit reposer sur un fondement juridique au sens de l'article 6 du RGPD, et dans la mesure où il s'agit également d'un traitement de données de santé sensibles, au sens de l'article 9, § 2 du RGPD. Vu le cadre réglementaire de l'enregistrement prescrit de données à caractère personnel à l'article 9*ter* de la loi du 14 juillet 1994 et dans le projet d'arrêté royal, le traitement semble pouvoir trouver un fondement juridique dans les articles 6.1.c) et 9.2.g) du RGPD.

17. Dans ce contexte, l'Autorité attire aussi l'attention sur l'article 6.3 du RGPD qui - lu conjointement avec l'article 8 de la CEDH et l'article 22 de la Constitution - prescrit que la réglementation qui encadre le traitement de données à caractère personnel doit en principe mentionner au moins les éléments essentiels suivants de ce traitement (voir également le point 9) :

- la finalité du traitement ;
- les types ou catégories de données à caractère personnel qui feront l'objet du traitement ;
- les personnes concernées ;
- les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ;
- les durées de conservation ;
- ainsi que la désignation du responsable du traitement.

Il ressort tant de ce qui précède que de ce qui suit encore que le projet d'arrêté royal ne mentionne nullement les éléments essentiels du traitement de données à caractère personnel envisagé. Des précisions supplémentaires et des compléments s'imposent (voir ci-après).

3. Proportionnalité du traitement

18. L'article 5.1.c) du RGPD prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités visées ("minimisation des données").

19. Comme déjà évoqué aux points 9 et 17, la détermination des types ou catégories de données à caractère personnel qui seront traitées par finalité est considérée comme un des éléments essentiels du traitement qui doivent en principe être définis dans la réglementation qui encadre le traitement de ces données à caractère personnel.

20. Le projet d'arrêté royal ne donne aucune indication des types ou catégories de données à caractère personnel qui doivent être enregistrées en vue d'une des différentes finalités.

21. L'absence soit des types ou catégories de données à caractère personnel à traiter, soit de la finalité visée ou les imprécisions à cet égard ne permettent pas à l'Autorité de réaliser ne fût-ce qu'un contrôle marginal du principe de minimisation des données, tel que prescrit par l'article 5.1.c) du RGPD. Le projet d'arrêté royal doit dès lors être complété et précisé sur ce point.

22. En ce qui concerne la finalité de recherche scientifique, l'Autorité rappelle d'emblée l'article 89, § 1er du RGPD : un traitement en vue de finalités de recherche ou statistiques doit être soumis à des garanties qui assurent le respect du principe de minimisation des données, comme la pseudonymisation. Chaque fois que de telles finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il *convient* de procéder de cette manière. Le traitement se fait donc de préférence à l'aide de données

anonymes[5]. S'il n'est pas possible d'atteindre la finalité de traitement visée à l'aide de données anonymes, des données à caractère personnel pseudonymisées[6] peuvent être utilisées. Si ces données ne permettent pas non plus d'atteindre la finalité visée, des données à caractère personnel non pseudonymisées peuvent aussi être utilisées, uniquement en dernière instance.

4. Délai de conservation des données

23. En vertu de l'article 5.1.e) du RGPD, les données à caractère personnel doivent 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 traitées.

24. Comme déjà mentionné aux points 9 et 17, la définition des durées de conservation des données à caractère personnel est également considérée comme un des éléments essentiels qu'il faut en principe fixer dans la réglementation qui encadre le traitement de données à caractère personnel.

25. L'Autorité constate que le projet d'arrêté royal ne prévoit pas le moindre délai de conservation des données à caractère personnel qui doivent être enregistrées.

26. À la lumière de l'article 6.3 du RGPD, l'Autorité recommande de remédier à cette lacune dans le projet d'arrêté royal et de quand même prévoir au moins des critères permettant de déterminer le(s) délai(s) de conservation des données à caractère personnel qui doivent être enregistrées en vue des différentes finalités.

5. Responsabilité

27. L'article 4.7) du RGPD dispose que pour les traitements dont les finalités et les moyens sont déterminés par la réglementation, le responsable du traitement est celui qui est désigné en tant que tel dans cette réglementation.

28. Le projet d'arrêté royal ne contient pas la moindre indication du responsable du traitement de l'enregistrement envisagé de données de santé. Il importe toutefois que toutes les personnes concernées (en l'occurrence certainement les patients) sachent parfaitement à qui s'adresser en vue d'exercer et de faire respecter les droits que leur confère le RGPD.

---

[5] Données anonymes : informations qui ne peuvent pas être reliées à une personne physique identifiée ou identifiable (article 4.1) du RGPD, *a contrario*).

[6] *"Pseudonymisation : 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."* (voir l'article 4.5) du RGPD).

29. Par souci d'exhaustivité – et sans préjudice de toutes les autres obligations imposées par le RGPD et par la LTD –, l'Autorité souligne l'obligation de tout responsable du traitement de vérifier s'il est nécessaire ou non de désigner un délégué à la protection des données (article 37 du RGPD)[7] et/ou de réaliser une analyse d'impact relative à la protection des données (article 35 du RGPD)[8] [9].

6. Mesures de sécurité

30. Les articles 5.1.f), 24.1 et 32 du RGPD mentionnent explicitement l'obligation pour le responsable du traitement de prendre les mesures techniques et organisationnelles appropriées qui sont requises pour protéger les données à caractère personnel. Ces mesures doivent assurer un niveau de sécurité approprié, compte tenu, d'une part, de l'état des connaissances en la matière et des coûts qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

31. L'article 32 du RGPD se réfère à cet égard à plusieurs exemples de mesures afin d'assurer, au besoin, un niveau de sécurité adapté au risque :
    - la pseudonymisation et le chiffrement des données à caractère personnel ;
    - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes de traitement ;

---

[7] Pour des directives en la matière, voir :

- Informations sur le site Internet de l'Autorité : https://www.autoriteprotectiondonnees.be/dossier-thematique-delegue-a-la-protection-des-donnees

- Recommandation de la Commission n° 04/2017 *relative à la désignation d'un délégué à la protection des données conformément au Règlement général sur la protection des données (RGPD), en particulier l'admissibilité du cumul de cette fonction avec d'autres fonctions dont celle de conseiller en sécurité* ;

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_04_2017.pdf)

- Lignes directrices du Groupe 29 (WP 243)

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/wp243rev01_fr.pdf).

[8] Pour des directives en la matière, voir :

- Informations sur le site Internet de l'Autorité : https://www.autoriteprotectiondonnees.be/analyse-dimpact-relative-a-la-protection-des-donnees

- Recommandation d'initiative de la Commission n° 01/2018 du 28 février 2018 *concernant l'analyse d'impact relative à la protection des données et la consultation préalable*.

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018_2018.pdf)

- Lignes directrices du Groupe 29 (WP 248)

(https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/wp248%20rev.01_fr.pdf).

[9] Une analyse d'impact relative à la protection des données peut d'ailleurs également être effectuée dès le stade de préparation de la réglementation. Voir à cet égard l'article 35.10 du RGPD et les points 90-91 de la recommandation de la Commission n° 01/2018.

- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

32. Pour l'exécution concrète de ces mesures, l'Autorité renvoie à la recommandation[10] visant à prévenir les fuites de données et aux mesures de référence[11] qu'il convient de respecter dans le cadre de tout traitement de données à caractère personnel.

33. Les catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD, dont des données de santé, requièrent des mesures de sécurité plus strictes. L'article 9 de la LPD indique quelles mesures de sécurité supplémentaires doivent être prévues :
    - désigner les catégories de personnes, ayant accès aux données à caractère personnel, avec une description précise de leur fonction par rapport au traitement des données visées ;
    - tenir la liste des catégories des personnes ainsi désignées à la disposition de l'Autorité ;
    - veiller à ce que ces personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

34. Le responsable du traitement doit veiller à ce que les mesures de sécurité susmentionnées soient respectées à tout moment.

III. CONCLUSION

35. L'Autorité estime qu'en l'absence de la moindre précision relative au contenu de l'enregistrement envisagé, le présent projet d'arrêté royal n'offre aucun point de repère aux personnes concernées. Le projet d'arrêté royal, dans sa forme actuelle, n'offre dès lors pas suffisamment de garanties en matière de protection des données à caractère personnel des

---

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

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

personnes concernées, en particulier en l'absence d'indication des éléments les plus essentiels du traitement/de l'enregistrement envisagé (tels que requis en vertu des articles 6.3 du RGPD, 8 de la CEDH et 22 de la Constitution). Les éléments suivants devraient au moins être repris dans le projet d'arrêté royal :

- préciser toutes les différentes finalités poursuivies par l'enregistrement de données de santé, en particulier la finalité de recherche (voir les points 14 et 15) ;
- indiquer les types ou catégories de données à caractère personnel à traiter pour les différentes finalités (voir les points 21 et 22) ;
- préciser la (les) durée(s) de conservation des données à caractère personnel pour les différentes finalités (voir le point 26) ;
- désigner le (les) responsable(s) du traitement en tant que tel(s) (voir le point 28) ;
- actualiser le libellé en matière d'autorisation/de délibération préalable en vertu de la loi du 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du* RGPD (voir le point 10).

PAR CES MOTIFS,

l'Autorité estime que les remarques mentionnées au point 35 doivent être mises en œuvre dans le présent projet d'arrêté royal *modifiant les articles 18, § 1er, A, et 19, § 1er de l'annexe à l'arrêté royal du 14 septembre 1984 établissant la nomenclature des prestations de santé en matière d'assurance obligatoire soins de santé et indemnités*.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere