Avis n° 117/2018 du 7 novembre 2018

Objet : demande d'avis concernant un projet de base juridique pour la consultation de données de santé via une plateforme électronique (CO-A-2018-115)

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 ;

Vu la demande d'avis de Madame Maggie De Block, Ministre des Affaires sociales et de la Santé publique, reçue le 21/09/2018 ;

Vu le rapport de Monsieur Frank De Smet ;

Émet, le 7 novembre 2018, 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 un article X - qui doit être repris dans une loi portant des dispositions diverses en matière de santé - concernant un projet de base juridique pour la consultation de données de santé via une plateforme électronique (ci-après le projet).

Contexte

2. Le courrier accompagnant la demande d'avis et l'Exposé des motifs mentionnent que le projet ainsi soumis doit créer un cadre/une base juridique pour permettre au Roi de fixer les conditions et modalités selon lesquelles, après avoir obtenu à cet effet l'accord du patient, des données de santé peuvent être mises directement et sous forme électronique à disposition sur une plateforme sécurisée pour consultation par le patient concerné et/ou d'autres prestataires de soins traitants.

3. Le projet stipule ce qui suit : "*Le Roi peut fixer les conditions et modalités selon lesquelles un praticien d'une profession des soins de santé, après avoir obtenu à cet effet l'accord du patient, peut mettre directement et sous forme électronique à disposition sur une plateforme électronique sécurisée, les données de santé d'un patient que ce praticien a enregistrées, pour consultation par le patient concerné et/ou ses prestataires de soins traitants.*"

4. L'Exposé des motifs ajoute que le projet n'altère en rien le droit de consultation ni le droit d'obtenir une copie du dossier de patient et que c'est le praticien professionnel qui décide, avec l'accord du patient concerné, quelles données peuvent être partagées via la plateforme.

II. EXAMEN DE LA DEMANDE D'AVIS

5. Comme déjà indiqué ci-dessus, le projet doit permettre au Roi de fixer les conditions et modalités concernant la mise à disposition électronique et directe de données de santé sur une plateforme sécurisée pour le patient et ses prestataires de soins traitants.

6. Bien que l'Autorité soit favorable au principe de partage de données entre prestataires de soins traitants d'une part et à la consultation directe par un patient de ses données de santé d'autre part, elle estime néanmoins que la délégation susmentionnée au Roi n'est pas décrite de manière suffisamment précise, étant donné que les éléments essentiels du traitement de données de santé enregistrées sur 'une' plateforme sécurisée ne sont pas définis dans le projet.

En outre, l'intervention du Roi n'est pas obligatoire ; le projet prévoit en effet que "*Le Roi **peut** fixer les conditions et modalités (...)*". Une telle formulation large, peu précise et facultative ne constitue en aucun cas une indication pour les personnes concernées.

7. Ni l'article 8 de la CEDH, ni l'article 22 de la Constitution ne permettent un tel "chèque en blanc". 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[1]. 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.

8. Une telle disposition large et peu précise 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 Règlement général sur la protection des données (ci-après le RGPD)[2] 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.

1. Finalité

9. 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.

10. Le projet dispose que la finalité du traitement poursuivi est la suivante : 'mettre directement et sous forme électronique à disposition sur une plateforme sécurisée, les données de santé d'un patient qu'un praticien d'une profession des soins de santé a enregistrées, pour consultation par le patient concerné et/ou ses prestataires de soins traitants'.

---

[1] 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 : arrêt n° 44/2015 du 23 avril 2015 (p. 63), arrêt n° 108/2017 du 5 octobre 2017 (p. 17) et arrêt n° 29/2018 du 15 mars 2018 (p. 26).

[2] 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 ou RGPD).

11. L'Autorité constate que, bien que la finalité du traitement de données à caractère personnel poursuivi soit déterminée et explicite, beaucoup (voire tout) est laissé au bon vouloir du praticien de la profession des soins de santé qui a enregistré les données de santé en question : il 'peut' mettre à disposition les données pour consultation (voir le projet) et il décide également 'quelles données' peuvent être partagées via la plateforme (voir l'Exposé des motifs). Déjà sur ce point, cela manque d'indications pour les personnes concernées. Le but ne peut pas être de mettre à disposition, via la plateforme sécurisée, des données uniquement de manière sélective[3].

2. Fondement juridique

12. 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 il s'agit également d'un traitement de données de santé sensibles, au sens de l'article 9, § 2 du RGPD.

13. L'Autorité constate que le courrier accompagnant la demande d'avis et l'Exposé des motifs mentionnent explicitement que le projet entend créer un cadre/une base juridique pour mettre directement et sous forme électronique des données de santé à disposition du patient et/ou d'autres prestataires de soins traitants pour consultation.

14. Vu ce qui précède, l'accord du patient qui doit - selon le projet - être obtenu au préalable pour la mise à disposition pour consultation des données de santé enregistrées par un praticien d'une profession des soins de santé semble davantage devoir être considéré comme une "*mesure appropriée et spécifique (...) pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée*", dont il est question à l'article 9.2.g) du RGPD, que pouvoir être considéré comme un fondement juridique du traitement au sens des articles 6.1.a) et 9.2.a) du RGPD.

15. En vertu de la volonté susmentionnée - telle qu'elle ressort du courrier accompagnant la demande d'avis et de l'Exposé des motifs - de prévoir un cadre réglementaire pour le traitement de données poursuivi, celui-ci semble donc trouver un fondement juridique dans les articles 6.1.d) ou e)[4] et 9.2.g) du RGPD. Le projet lui-même ne précise rien en la matière. L'Autorité recommande dès lors que le fondement juridique au sens des articles 6.1 et 9.2 du RGPD soit précisé dans le projet.

---

[3] À l'exception bien sûr de "l'exception thérapeutique" dont il est question à l'article 7 de la loi du 22 août 2002 *relative aux droits du patient*.

[4] C'est évidemment le responsable du traitement lui-même qui est le mieux placé pour déterminer quel fondement juridique correspond au traitement de données à caractère personnel visé.

16. 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 :
    - 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.

    Tant de ce qui précède que de ce qui suit encore, il ressort que sur la plupart des points, le projet présente des manquements en ce qui concerne la mention des éléments essentiels du traitement de données à caractère personnel visé. Des précisions supplémentaires et des compléments s'imposent (voir ci-après).

3. Proportionnalité du traitement

17. 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").

18. Comme déjà évoqué aux points 7 et 16, 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.

19. Le projet ne parle toutefois que des "données de santé enregistrées par le praticien d'une profession des soins de santé". L'Exposé des motifs parle de "certaines données de santé comme notamment les résultats d'un examen sanguin" et du fait que c'est le praticien professionnel qui décide quelles données peuvent être mises à disposition via la plateforme et être partagées avec des prestataires de soins traitants.
    Aussi sur ce point, le projet et l'Exposé des motifs manquent de clarté et ne donnent aucune indication pour les personnes concernées.

20. 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 doit dès lors être complété et précisé en ce sens.

4. Durée de conservation des données

21. Selon 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.

22. Comme déjà mentionné aux points 7 et 16, 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.

23. L'Autorité constate que le projet ne prévoit pas de délai de conservation sur la plateforme[5] sécurisée des données à caractère personnel qui peuvent être mises à disposition du patient ou de ses prestataires de soins traitants pour consultation.

24. L'Autorité recommande dès lors de remédier à cette lacune dans le projet et de prévoir un délai de conservation spécifique ou au moins des critères qui permettent de déterminer le(s) délai(s) de conservation.

5. Responsabilité

25. 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.

[5] Dans la mesure où les données à caractère personnel sont effectivement conservées "sur" la plateforme sécurisée proprement dite et donc sous réserve des remarques formulées au point 33.

26. Le projet ne contient pas la moindre indication du responsable du traitement de la plateforme sécurisée[6] sur laquelle des données de santé seront mises à disposition pour consultation[7]. Il importe pourtant que les personnes concernées (les patients) sachent parfaitement à qui s'adresser en vue d'exercer et de faire valoir les droits qui leur sont accordés par le RGPD.

27. Par souci d'exhaustivité - et sans préjudice de toutes les autres obligations imposées par le RGPD et la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* -, l'Autorité souligne l'obligation de tout responsable du traitement de vérifier la nécessité ou non de désigner un délégué à la protection des données (article 37 du RGPD)[8] et/ou de réaliser une analyse d'impact relative à la protection des données (article 35 du RGPD)[9] [10].

6. Mesures de sécurité

28. 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

---

[6] Ni le projet, ni l'Exposé des motifs n'indiquent s'il s'agit d'une plateforme gouvernementale ou d'une plateforme privée, ni à quelles exigences de sécurité elle doit répondre.

[7] Le praticien d'une profession des soins de santé est-il le responsable du traitement pour les données qu'il a enregistrées ? Est-ce le fournisseur de la plateforme ? Si le praticien professionnel est le responsable du traitement, le fournisseur de la plateforme est-il alors le responsable du traitement pour les loggings par exemple ?

[8] 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).

[9] 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.pdf)

- Lignes directrices du Groupe 29 (WP 248)

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

[10] 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.

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.

29. 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 ;
    - 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.

30. Pour l'exécution concrète de ces mesures, l'Autorité renvoie à la recommandation[11] visant à prévenir les fuites de données et aux mesures de référence[12] qu'il convient de respecter dans le cadre de tout traitement de données à caractère personnel.

31. 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. La loi du 30 juillet 2018 susmentionnée en matière de protection des données[13] 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 au respect du caractère confidentiel des données visées.

---

[11] 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_2018.pdf).

[12] 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).

[13] Voir l'article 9 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.

32. Étant donné le fait que la plateforme sécurisée sera en principe accessible tant au responsable du traitement, qu'aux praticiens (traitants) d'une profession des soins de santé et aux patients, l'Autorité souligne spécialement l'importance d'une bonne gestion des utilisateurs et des accès[14]. L'Autorité rappelle en particulier les recommandations suivantes que son prédécesseur en droit a déjà formulées dans le cadre de l'organisation d'une bonne gestion des utilisateurs et des accès :
    - enregistrement minutieux de l'identité, des caractéristiques et des mandats ;
    - utilisation de l'eID pour l'identification et l'authentification de l'identité ;
    - contrôle des caractéristiques et des mandats à l'aide de sources authentiques validées ;
    - développement de cercles de confiance ;
    - enregistrement des autorisations dans une source authentique.

    Il n'est pas nécessaire que le responsable du traitement les mette toutes en œuvre lui-même. À cet effet, il peut par exemple recourir aux services de base de la plate-forme eHealth ou d'une plate-forme similaire. Ni le projet, ni l'Exposé des motifs n'expliquent d'ailleurs quel sera le rapport entre la plateforme sécurisée dont il est question et la plate-forme eHealth.

33. Étant donné que ni le projet, ni l'Exposé des motifs ne précisent comment la plateforme sécurisée dont il est question fonctionnera (surtout dans la mesure où la plateforme prévoirait éventuellement un enregistrement centralisé de données de santé), l'Autorité se permet d'attirer l'attention du demandeur sur ce qui suit :
    - le plan d'action e-santé[15], en particulier le point d'action 5 "*Partager les données via le système hubs & metahub pour les hôpitaux généraux et universitaires*", le point d'action 6 "*Partager afin de collaborer*", le point d'action 7 "*Établissements psychiatriques et autres et système hubs & metahub*" et le point d'action 10 "*Accès aux données par le patient (PHR)*", un alignement de la plateforme sécurisée dont il est question dans le projet avec le plan d'action e-santé semble recommandé ;
    - assurer une bonne qualité des données en évitant la création de fichiers dérivés et la duplication de données[16]. Le but ne peut pas être de conserver sur la plateforme dont il est question dans le projet des copies qui sont disponibles ailleurs (voir les hubs et le metahub ou les coffres-forts). Dans ce cas, la plateforme doit uniquement renvoyer vers les services en question qui accordent un accès aux données requises (enregistrées de manière décentralisée) ou utiliser ces services.

---

[14] Voir aussi la recommandation de la Commission 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).

[15] Voir http://www.plan-egezondheid.be/fr/.

[16] Voir le point 15 de la recommandation d'initiative de la Commission n° 09/2012 du 23 mai 2012 *relative aux sources authentiques de données dans le secteur public* (voir https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_09_2012_0.pdf).

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 raison de sa formulation large et peu précise, le présent projet est très vague et n'offre aucune indication pour les personnes concernées. Le projet n'offre pas suffisamment de garanties en matière de protection des données à caractère personnel des personnes concernées, en particulier en l'absence d'indication de la plupart des éléments essentiels pour le traitement envisagé (tels que requis en vertu des articles 6.3 du RGPD, 8 de la CEDH et 22 de la Constitution), plus précisément :
    - l'absence de précision de l'intervention du Roi, qui doit obligatoirement être prescrite (voir le point 6) ;
    - la réalisation de la finalité poursuivie du traitement de données dépend du bon vouloir du praticien de la profession des soins de santé qui a enregistré les données de santé en question (voir le point 11) ;
    - aucune mention du fondement juridique pour le traitement au sens des articles 6.1 et 9.2 du RGPD (voir le point 15) ;
    - aucune indication des types ou catégories de données à caractère personnel à traiter (voir les points 19 et 20) ;
    - l'absence de précision de la (des) période(s) de conservation des données à caractère personnel des patients concernés (voir le point 24) ;
    - aucune désignation du responsable du traitement en tant que tel (voir le point 26) ;
    - l'absence de précision des mesures (de sécurité) techniques et organisationnelles relatives à la plateforme visée, dont une bonne gestion des utilisateurs et des accès et un alignement avec le plan d'action e-santé (voir les points 32 et 33).

PAR CES MOTIFS,

l'Autorité émet

- un **avis favorable** quant au principe de partage de données entre prestataires de soins traitants d'une part, et une consultation directe par le patient de ses données de santé d'autre part, et

- un **avis défavorable** quant à l'élaboration de ce partage et de cette consultation par l'article X qui est soumis, portant un projet de base juridique pour la consultation de données de santé via une plateforme électronique.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere