Avis n° 65/2018 du 25 juillet 2018

Objet : demande d'avis relatif à l'avant-projet de loi portant modification de la loi du 25 février 2018 *portant création de Sciensano (1)* (CO-A-2018-047)

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 De Block, Ministre des Affaires sociales et de la Santé publique, reçue le 7 juin 2018 ;

Vu le rapport de Willem Debeuckelaere ;

Émet, le 25 juillet 2018, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE

1. Le 7 juin 2018, l'Autorité a reçu une demande d'avis de la Ministre des Affaires sociales et de la Santé publique (ci-après le demandeur) concernant l'avant-projet de loi *portant modification de la loi du 25 février 2018 portant création de Sciensano (1)*, ci-après l'avant-projet.

2. Sciensano a été créée par la loi susmentionnée du 25 février 2018. À cette occasion, deux établissements scientifiques fédéraux, à savoir l'Institut scientifique de santé publique (ISP) et le Centre d'étude et de recherches vétérinaires et agrochimiques (CERVA), ont été réunis en une nouvelle institution appelée "Sciensano". L'exercice conjoint des missions vise à assurer une réalisation plus efficace de ces missions.

3. L'avant-projet qui est soumis à l'avis de l'Autorité intègre le Centre fédéral d'expertise des soins de santé (KCE) et le Conseil Supérieur de la Santé, ainsi que leurs missions, dans Sciensano. Le demandeur profite de cette occasion pour insérer en même temps dans la loi du 25 février 2018 un chapitre relatif au traitement de données à caractère personnel.

4. En vertu de la loi du 25 février 2018, Sciensano est habilitée, dans le cadre de l'exécution de ses missions, à traiter des données à caractère personnel. Bien que l'Exposé des motifs de cette loi confirme que le traitement de données à caractère personnel doit être conforme à la législation et à la réglementation en matière de traitement de données à caractère personnel, le projet de loi relatif à la création de Sciensano n'a pas été soumis à l'avis du prédécesseur en droit de l'Autorité (la Commission de la protection de la vie privée)[1].

5. Afin de tenir compte de la remarque du Conseil d'État à cet égard, l'avant-projet est soumis à l'avis de l'Autorité. L'Autorité rappelle que le Règlement général sur la protection des données (RGPD) est d'application depuis le 25 mai 2018. En vertu de l'article 36.4 du RGPD, chaque proposition de mesure législative ou réglementaire qui se rapporte au traitement de données à caractère personnel *doit* être soumise à l'Autorité.

6. L'avis de l'Autorité concerne concrètement les articles 26 à 39 inclus de l'avant-projet qui insèrent les articles 39/1 à 39/12 inclus dans la loi du 25 février 2018.

[1] Il est fait référence à la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (LVP) et au 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)*).*

II. EXAMEN DE LA DEMANDE D'AVIS

A. Remarques préliminaires

7. L'Autorité constate que l'avant-projet renvoie de manière alternative tant à la loi vie privée, ci-après LVP[2], qu'au RGPD. L'Autorité prend acte du fait que le demandeur est conscient du fait que l'avant-projet devra encore être adapté au projet de loi *relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* et du projet de loi *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, approuvé par la Chambre le 19 juillet 2018 (DOC-54-3126/007).

8. L'article 26 de l'avant-projet traite de l'insertion d'un chapitre 8 dans la loi du 25 février 2018 intitulé "Traitements [NdT : il y a lieu de lire "Traitement"] de données à caractère personnel", tandis qu'à l'article 27, il est précisé que lorsque Sciensano traite des données à caractère personnel pour l'exécution de ses missions, elle doit respecter les dispositions du chapitre 8. L'Autorité n'a pas de remarque spécifique à ce sujet.

Définitions

9. L'Autorité constate que l'article 28 de l'avant-projet fait référence aux définitions du RGPD, "*sauf disposition contraire*". L'Autorité insiste pour qu'une terminologie uniforme et correcte soit utilisée. Ainsi, l'article 28 de l'avant-projet entend par "données à caractère personnel" les "*données telles que visées à l'article 4.1) du Règlement 2016/679*" alors que pour les "données pseudonymes", on reprend la définition complète du RGPD, sans faire référence à l'article 4.5) du RGPD. On pourrait en déduire, à tort, que cette définition diverge de celle du RGPD alors que ce n'est pas du tout le cas et d'ailleurs, cela n'est pas non plus autorisé. Une référence à l'article 4.5) du RGPD suffit donc. Quant aux termes "violation de données à caractère personnel", on entend, à juste titre, "*une violation telle que visée à l'article 4.12) du Règlement 2016/679*".

10. En ce qui concerne la définition de "données concernant la santé", on entend fautivement les "*données telles que visées à l'article 9.1) du Règlement 2016/679".* La référence correcte serait celle à la définition des données concernant la santé à l'article 4.15) du RGPD. En revanche, l'article 9.1 du

[2] Loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*.

RGPD énumère les catégories particulières de données à caractère personnel, dont font également partie, outre les données biométriques et génétiques, les données concernant la santé. L'Autorité recommande de remplacer la référence à l'article 9.1 du RGPD par "*données telles que visées à l'article 4.15) du Règlement 2016/679*".

11. À l'article 28, 4° de l'avant-projet, les données anonymes sont définies comme étant des "*données qui ne peuvent être mises en relation avec une personne physique identifiée ou identifiable*". Ces termes ne sont pas définis de manière normative dans le RGPD étant donné qu'il ne s'agit pas de données à caractère personnel. L'Autorité constate que la définition utilisée correspond toutefois à l'explication fournie dans le considérant 26 du RGPD concernant ces termes[3].

B. Finalité

12. L'article 4 de la loi du 25 février 2018 contient une énumération détaillée de missions générales qui peuvent être réalisées par Sciensano. Il s'agit notamment de rendre des avis fondés scientifiquement, d'effectuer de la recherche scientifique, de soutenir la recherche clinique en pratique, d'assurer le suivi des risques pour la santé et de l'état de santé de la population, de prester des services à des tiers dans le cadre de ses domaines d'expertise et de développer et d'élaborer des solutions pour le diagnostic, la prévention et le traitement des maladies et pour l'identification et la prévention d'autres risques pour la santé. En outre, Sciensano a également des missions relatives à la formation de doctorants et peut octroyer des bourses de doctorat.

13. L'article 29 de l'avant-projet précise que dans le cadre de l'exécution de ses missions, Sciensano ne peut pas porter atteinte aux dispositions de la LVP et du RGPD. Comme cela a déjà été observé au point 7, l'Exposé des motifs de l'avant-projet signale que cet article sera adapté à la législation en cours de préparation à la Chambre[4].

14. L'article 30 de l'avant-projet dispose que pour l'exécution de ses missions, Sciensano établit des rapports et des avis et met en œuvre des analyses et des études dans le cadre desquelles elle recueille, en son propre nom ou pour le compte d'un tiers, des données à caractère personnel auprès de la personne concernée ou reçoit les données à caractère personnel des institutions visées aux articles 31 et 32 de l'avant-projet.

15. Il ressort de l'Exposé des motifs de l'article 30 de l'avant-projet que le demandeur est conscient que l'article 4 de la loi du 25 février 2018 concerne des missions générales mais en raison de la nature

[3] "*(...) informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, [et les] données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable*".

[4] Exposé des motifs, p. 18.

diverse du traitement, il n'est pas possible d'expliquer a priori de manière exhaustive dans l'article 4 de cette loi toutes les fins et garanties[5].

16. Tout traitement de données à caractère personnel doit reposer sur un fondement juridique au sens de l'article 6 du RGPD. En outre, le traitement de catégories particulières de données à caractère personnel, dont "les données relatives à la santé", est en principe interdit en vertu de l'article 9.1. du RGPD. Cette interdiction ne s'applique toutefois pas si le responsable du traitement peut invoquer un des motifs de justification de l'article 9.2. du RGPD.

17. Bien qu'en vertu de l'article 6.3 du RGPD, ainsi que de l'article 8 de la CEDH et de l'article 22 de la Constitution[6], la réglementation qui encadre le traitement de données à caractère personnel devrait en principe au moins mentionner plusieurs éléments essentiels de ce traitement[7], l'Autorité estime que dans des cas exceptionnels, la réglementation peut aussi prévoir qu'un certain nombre de ces éléments essentiels doivent être précisés ultérieurement dans le cadre d'une délibération qui sera émise par le comité compétent en la matière. L'Autorité prend acte du fait que le demandeur préfère cette dernière option. Ce point sera à nouveau abordé dans le présent avis ultérieurement.

18. L'Autorité attire toutefois l'attention sur le fait que le fonctionnement du Comité sectoriel de la Sécurité Sociale et de la Santé est actuellement géré par des mesures transitoires[8]. Comme cela est précisé ci-dessus, l'Autorité prend acte du fait que lors de la finalisation de l'avant-projet, le demandeur devra veiller à la cohérence du texte de la réglementation en vigueur à ce moment-là concernant le successeur en droit du Comité sectoriel de la Sécurité Sociale et de la Santé (voir plus loin).

19. À la lumière de cette remarque, l'Autorité estime que la finalité des traitements est conforme à l'article 5.1.b) du RGPD, vu que les données à caractère personnel ne sont collectées et traitées que pour des finalités déterminées, explicites et légitimes et que les traitements sont basés sur un fondement légal conformément à l'article 6.1.c) du RGPD.

---

[5] Ibid.

[6] Voir DEGRAVE, E., *"L'e-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle",* Collection du CRIDS, Larcier, 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).

[7] On peut faire référence ici aux types ou catégories de données à caractère personnel à traiter, aux personnes concernées, aux entités auxquelles les données à caractère personnel peuvent être communiquées et aux finalités pour lesquelles elles peuvent l'être, à la limitation des finalités, aux durées de conservation et à la désignation du (des) responsable(s) du traitement.

[8] Voir l'article 114, § 3 et 4 de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, ainsi que les p. 4 et 5 de l'Exposé des motifs de la loi du 25 mai 2018 qui a remplacé cet article 114 dans la loi de décembre 2017 (DOD 54 3104/001 (http://www.dekamer.be/FLWB/PDF/54/3104/54K3104001.pdf)).

C. Commentaire des articles de l'avant-projet

Article 30

20. Comme observé au point 14, un article 39/2 est inséré dans la loi du 25 février 2018 qui établit au § 1 que les objectifs et garanties relatifs au traitement des données à caractère personnel sont déterminés par analyse ou étude, après avis du délégué à la protection des données (ci-après DPO, *Data Protection Officer*) et, si le traitement concerne des données relatives à la santé, par le professionnel de la santé désigné.

21. Bien que le RGPD ne prévoie pas une compétence d'avis du professionnel de la santé, l'Autorité comprend que l'avis du professionnel de la santé puisse être nécessaire et utile pour des missions déterminées. L'Autorité fait toutefois remarquer que cette compétence d'avis du professionnel de la santé n'ôte rien à la condition que des données relatives à la santé soient traitées sous la responsabilité du professionnel de la santé (voir l'article 9.3 du RGPD). Il est recommandé que cette compétence d'avis ne soit pas exercée par le même professionnel de la santé que celui sous la responsabilité duquel les données à caractère personnel sont traitées. Il faut également veiller à ce que cette compétence d'avis ne porte pas préjudice à la mission du DPO (voir le point 44).

22. Selon l'article 30, Sciensano traite les données à caractère personnel "*en son propre nom ou pour le compte d'un autre responsable de traitement*". Il en résulte au moins implicitement que Sciensano se positionne en tant que responsable du traitement au sens de l'article 4.7) du RGPD. L'Autorité est favorable à ce que Sciensano soit désignée explicitement dans la disposition légale en tant que responsable du traitement pour ses missions. On observe que Sciensano peut également être responsable du traitement pour les activités de traitement qu'elle exécute pour le compte d'autres institutions. En outre, elle peut aussi intervenir en tant que sous-traitant. Dans ce cas, Sciensano traite *de facto* des données à caractère personnel pour le compte du responsable du traitement (une autre institution), auquel cas un contrat de sous-traitance doit être conclu[9]. Dans un souci de sécurité juridique et de prévisibilité, il est recommandé d'illustrer ces scénarios dans l'Exposé des motifs.

23. Selon l'article 30, Sciensano peut effectuer aussi bien des traitements initiaux que des traitements ultérieurs. Il ressort du point précédent qu'elle peut le faire aussi bien pour ses propres missions que pour le compte d'une autre institution.

[9] Voir les articles 4.8) et 28 du RGPD.

24. L'Autorité constate que l'article 30 de l'avant-projet n'autorise le traitement ultérieur que dans la mesure où celui-ci est compatible avec les missions générales de l'article 4 de la loi du 25 février 2018. Concrètement, cela signifie qu'il faut au préalable recueillir l'avis du DPO. En ce qui concerne les traitements ultérieurs réalisés avec des données à caractère personnel qui lui sont fournies par les institutions visées aux articles 31 et 32, l'article 34 de l'avant-projet prévoit un système d'autorisations (voir les points 35 et 36).

Article 31

25. Dans le cadre de l'exécution de ses missions, "*Sciensano analyse les données relatives aux hôpitaux visées à l'article 156 de la loi du 29 avril 1996 portant des dispositions sociales* (ci-après la loi du 29 avril 1996) *suivant les modalités prévues par cet article*".

26. Ceci est lié à la *Loi-programme (I)* du 24 décembre 2002 (ci-après la loi du 24 décembre 2002) qui a créé le KCE et qui le charge de l'analyse des données relatives aux hôpitaux qui sont collectées et couplées par la cellule technique. Ce fractionnement des activités de traitement entre le KCE et la cellule technique s'est produit à la suite de l'avis n° 33/2002 du 22 août 2002 du prédécesseur en droit de l'Autorité[10].

27. En vertu de l'article 31 de l'avant-projet, Sciensano reprendra et continuera d'assurer les compétences du KCE, qui est abrogé. Sciensano recevra les données selon les mêmes modalités que celles définies à l'article 156 de la loi du 29 avril 1996. Dans l'Exposé des motifs de l'avant-projet, il est expliqué que l'article 31 "*reprend en partie*[11] *l'article 265 de la Loi-programme (I)*" L'Autorité constate que l'article 265 de la loi du 24 décembre 2002 mentionne uniquement que le KCE analyse les données relatives aux hôpitaux, telles que visées à l'article 156 de la loi du 29 avril 1996.

28. L'Autorité estime qu'il ne suffit pas de renvoyer aux modalités de l'article 156 de la loi susmentionnée. Cet article décrit un système très complexe de modalités, d'échange de données et de types de données (données anonymes, données à caractère personnel) qui rend l'article 31 de l'avant-projet opaque et en fait une source de confusion, notamment parce que l'article 156 de la loi du 29 avril 1996 doit être lu à la lumière des différentes modifications législatives qui ont été apportées. Ainsi, l'article 156 de la loi susmentionnée concernait initialement les traitements réalisés par la cellule technique pour les hôpitaux. Cette cellule assurait la collecte, le couplage, la validation, l'anonymisation et l'analyse de données à caractère personnel. Avec la création du KCE en 2002, l'analyse de données a été confiée au KCE. Entre-temps, la plate-forme eHealth, chargée de recueillir, agréger, coder ou

[10] Exposé des motifs de la loi du 24 décembre 2002, p. 138.

[11] Soulignement propre.

anonymiser et mettre à disposition des données, a été créée[12]. Comme cela est évoqué ci-après, cette plate-forme se voit également confier un rôle dans l'avant-projet. En outre, dans l'article 156 de la loi du 29 avril 1996, la communication de données à caractère personnel est liée à une autorisation du comité sectoriel compétent, alors que cette exigence est également mentionnée dans l'avant-projet. Par ailleurs, l'article 156 de la loi susmentionnée mentionne des données qui ne comportent pas d'identification et des données anonymes. L'Autorité se demande quelle "partie" de l'article 156 de la loi susmentionnée, telle qu'indiquée dans l'Exposé des motifs, est visée précisément[13].

29. L'Autorité estime dès lors que les modalités concernant l'analyse de données relatives aux hôpitaux que Sciensano doit effectuer selon les modalités de l'article 156 de la loi du 29 avril 1996 doivent être explicitement définies à l'article 31 de l'avant-projet, de manière à ce que le justiciable sache clairement quelles modalités Sciensano doit précisément respecter.

Article 32

30. L'article 32 de l'avant-projet traite des données que Sciensano peut traiter. Il s'agit de données qui doivent obligatoirement être fournies à Sciensano par les institutions citées nommément dans le même article en vue de l'exécution de ses missions. À cet effet, les articles 285, 288 et 296 correspondants de la loi du 24 décembre 2002 relatifs à la transmission des données par les institutions au KCE sont abrogés.

31. La plate-forme eHealth intervient comme organisation intermédiaire, conformément à la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions* lorsque les données sont couplées à d'autres données. La communication des données est régie à l'article 34 de l'avant-projet (voir le point 34). L'Autorité n'a pas de remarque spécifique à cet égard, à l'exception de ce qui a été observé aux points 27 à 29 inclus concernant la confusion et l'opacité relatives aux modalités en matière d'échange de données à l'article 31 de l'avant-projet.

Article 33

32. Si Sciensano traite, pour ses missions, d'autres données que celles visées aux articles 30 et 31 de l'avant-projet, elle traitera "*de préférence des données pseudonymes*" et donc pas non plus des données codées. Selon l'Exposé des motifs, il s'agit d'un "*contenu similaire à l'article 266 de la loi-programme (I) du 24 décembre 2002*". L'Autorité constate que Sciensano, contrairement au KCE,

[12] Article 5, 8° de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions*.

[13] Ce n'est pas parce que dans les dispositions transitoires de l'avant-projet, le nom du KCE est remplacé par "Sciensano" que les modalités transférées se traduisent immédiatement dans l'avant-projet.

a le choix d'utiliser ou non des données pseudonymes. Dans l'article 266 correspondant de la loi du 24 décembre 2002, le KCE "*est compétent pour réaliser des analyses sur la base de données codées*".

33. Cette plus large marge de manoeuvre de Sciensano n'est pas justifiée. L'incorporation d'un organe ne constitue pas en soi une raison pour l'agrandir. L'Autorité renvoie à l'article 89.1 du RGPD qui exige qu'avant d'utiliser des données pseudonymes, on examine si les données ne peuvent pas être traitées sans que la personne concernée puisse être identifiée (données anonymes). Cette condition est directement liée au principe de minimisation des données (article 5.1.c) du RGPD). L'Autorité constate toutefois que rien n'indique que les initiateurs de l'avant-projet ont réalisé cet exercice. L'Autorité estime donc que l'article 33 doit être adapté, par analogie avec l'article 89.1 du RGPD. L'Exposé des motifs doit au moins justifier pour quelles raisons cette flexibilité est nécessaire dans le chef de Sciensano. Quoi qu'il en soit, il faut documenter pour chaque cas les raisons pour lesquelles des données codées ne peuvent pas être utilisées.

Article 34

34. Toute communication de données à caractère personnel par ou à Sciensano est liée à une autorisation. L'Autorité renvoie à nouveau aux remarques formulées aux points 27 à 29 inclus du présent avis concernant la clarté de l'article 31 de l'avant-projet. N'y a-t-il pas un conflit avec le troisième paragraphe de l'article 156 de la loi du 29 avril 1996 qui déroge à l'exigence d'une autorisation du comité sectoriel compétent ?

35. L'article 34 de l'avant-projet exige une autorisation de principe du Comité sectoriel de la Sécurité Sociale et de la Santé, sauf lorsqu'un autre comité sectoriel est compétent, lorsque la communication est autorisée conformément à une disposition légale ou réglementaire ou est exemptée d'une autorisation de principe ou si la communication est exemptée par le Roi par un arrêté établi après consultation du Conseil des ministres et après avis de la Commission de la protection de la vie privée.

36. L'Autorité renvoie à la remarque formulée au point 18 concernant le fonctionnement du Comité sectoriel de la Sécurité Sociale et de la Santé qui est actuellement géré par des mesures transitoires et qui sera remplacé dans un avenir proche par le Comité de sécurité de l'information. En vertu du projet de loi *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en oeuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, approuvé par la Chambre le 19 juillet 2018 (DOC-54-3126/007), le Comité sectoriel de la Sécurité Sociale et de la Santé est en effet transformé en une chambre sécurité sociale et santé du nouveau Comité de sécurité de

l'information. L'échange de données sociales à caractère personnel ou de données de santé par la Banque carrefour de la Sécurité Sociale ou par une institution de la sécurité sociale sera soumis dans certains cas à une délibération préalable de la chambre sécurité sociale et santé du Comité de sécurité de l'information. L'Autorité recommande au demandeur de suivre de près l'évolution de ce projet de loi de manière à pouvoir adapter l'article 34 de l'avant-projet.

Articles 35 à 38 inclus

37. L'article 35 de l'avant-projet ajoute un chapitre 9 relatif à la sécurité et à la confidentialité dans la loi du 25 février 2018 portant création de Sciensano. L'article 36 de l'avant-projet concerne la désignation d'un DPO. L'article 37 de l'avant-projet concerne la désignation d'un professionnel de la santé sous la surveillance et la responsabilité duquel les données sont traitées. L'article 38 de l'avant-projet impose une obligation de confidentialité aux personnes qui traitent des données (à caractère personnel).

38. L'article 36 de l'avant-projet définit les tâches du DPO. Bien qu'une certaine flexibilité soit laissée au responsable du traitement (et au sous-traitant) concernant l'organisation des tâches du DPO, les tâches imposées doivent être conformes au minimum des missions mentionnées à l'article 39 du RGPD.

39. Selon l'article 36 de l'avant-projet, le DPO a une tâche de conseil, de documentation, d'encouragement et de contrôle. L'article renvoie (encore) à cet égard à la LVP et au RGPD. La LVP sera abrogée dès que le projet de loi cité ci-dessus *relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* aura été approuvé par le Parlement et sera d'application. L'Autorité constate que le renvoi à ces tâches générales s'inspire encore partiellement des tâches d'un conseiller en sécurité en vertu de l'application de la LVP (voir la recommandation n° 04/2017 du prédécesseur en droit de l'Autorité du 24 mai 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*).

40. Dans ce cadre, il convient de faire remarquer que l'article 39.1.b) du RGPD dispose que le DPO doit contrôler le respect du RGPD. Le considérant 97 du RGPD précise le contrôle en ce sens que le DPO aide le responsable du traitement (ou le sous-traitant) à vérifier le contrôle, au niveau interne, du RGPD. Il importe donc de souligner que la responsabilité de la mission de contrôle est entre les mains du responsable du traitement et pas entre celles du DPO. Concrètement, le DPO devra veiller à ce que Sciensano exerce un contrôle sur le traitement de données à caractère personnel dans le cadre de ses missions. Sciensano a l'obligation d'associer le DPO à ce contrôle (article 38 du RGPD).

41. L'élaboration et l'actualisation permanente du niveau de sécurité pour les données à caractère personnel ne peuvent pas non plus relever de la responsabilité du DPO. Par contre, le DPO a bel et bien une mission d'information et de conseil en la matière. Ce sera également le cas si Sciensano effectue un traitement de données à caractère personnel qui est préalablement soumis à une analyse d'impact relative à la protection des données (par exemple, dans le cas d'un traitement à grande échelle de données relatives à la santé)[14].

42. Selon l'article 36 de l'avant-projet, le DPO exerce sa mission "*de conseiller et d'encourager*"[15] sous "*le contrôle fonctionnel direct*" du directeur général qui est responsable de la gestion journalière. L'Autorité souligne que le DPO ne peut recevoir aucune instruction pour l'exercice de ses missions (article 38.3 du RGPD). En ce sens, la formulation de l'article 36 de l'avant-projet est équivoque sur ce point.

43. L'article 36 de l'avant-projet confère au Roi une délégation pour déterminer des règles supplémentaires concernant les missions du DPO. L'Autorité estime que dans ce cadre, son avis est requis, étant donné que les missions du DPO concernent le traitement de données à caractère personnel, ce qui implique la consultation obligatoire de l'Autorité (article 36.4 du RGPD). À titre de suggestion, l'Autorité recommande d'ajouter l'élément de phrase suivant après "(...) *exerce ses missions*" : "*, après avis de l'Autorité de protection des données*".

44. L'article 37 de l'avant-projet prévoit la désignation d'un professionnel de la santé. L'Autorité constate que les tâches du professionnel de la santé chevauchent partiellement celles du DPO. Ainsi, le professionnel de la santé a la mission de formuler des objectifs de sécurité, d'informer le directeur général lorsque la sécurité des données à caractère personnel est compromise ("*des situations dangereuses concernant des données à caractère personnel concernant la santé*") et s'assurer que la politique de sécurité est mise en oeuvre. Bien que l'Autorité comprenne la plus-value d'une collaboration étroite entre le DPO et le professionnel de la santé, ce chevauchement de tâches doit être évité.

45. L'article 38 de l'avant-projet établit une obligation de confidentialité dans le chef des personnes qui traitent des données. L'Autorité n'a pas de remarque spécifique à cet égard.

---

[14] Voir l'article 35.3.b) du RGPD.

[15] Les termes "*de contrôler*" semblent à nouveau faire défaut ici.

46. L'article 39 de l'avant-projet reprend l'article 286 de la loi du 24 décembre 2002 qui dispose que toutes les institutions ou autorités avec lesquelles Sciensano échange des données à caractère personnel doivent désigner un DPO. Par souci d'exhaustivité, l'Autorité fait remarquer que l'article 37.1 du RGPD donne une énumération non limitative d'activités de traitement pour lesquelles la désignation d'un DPO est obligatoire. Pour les institutions publiques, la désignation d'un DPO est obligatoire. Dans la mesure où Sciensano collabore aussi avec des entités qui ne sont pas des institutions publiques, l'obligation évoquée à l'article 39 de l'avant-projet n'est pas, selon l'Autorité, contraire à l'article 37 du RGPD. Au contraire, il s'agit du traitement de données à caractère personnel qui touchent (l'essentiel de) la vie privée, de sorte que la désignation du DPO renforce la conformité du traitement de données avec le RGPD, et la sécurité de l'information en particulier.

D. Droits de la personne concernée

47. Pour l'exécution de ses missions, à savoir des avis, des études, des rapports et des analyses, outre des données anonymes, Sciensano traite aussi des données à caractère personnel, pseudonymisées ou non, qui relèvent de (l'essentiel de) la vie privée. L'Exposé des motifs de l'avant-projet précise que Sciensano vise à définir clairement les garanties dans le cadre desquelles le traitement de données à caractère personnel peut avoir lieu[16].

48. L'autorité estime que Sciensano doit prévoir un système par lequel la personne concernée, si elle constate lors de la consultation de ses données chez Sciensano que cette dernière est en faute, est dirigée vers la source authentique d'où proviennent les données afin que la personne concernée puisse y exercer son droit de rectification.

PAR CES MOTIFS,
L'Autorité de protection des données

émet un avis **favorable**, à condition qu'il soit tenu compte des remarques formulées aux points susmentionnés, à savoir :

- l'utilisation d'une terminologie exacte et uniforme (9-11) ;
- la compatibilité de la compétence d'avis du professionnel de la santé et de sa responsabilité lors du traitement de données relatives à la santé (21) ;
- la désignation de Sciensano en tant que responsable du traitement (22) ;
- l'avis du DPO lors d'un traitement ultérieur de données à caractère personnel (24) ;

[16] Exposé des motifs, p. 16-17.

- définir explicitement dans l'avant-projet les modalités relatives à la nature des données à caractère personnel et à l'échange de données (27-29) ;
- encadrer plus concrètement le traitement de données pseudonymes (33) ;
- accorder une attention à l'application des tâches du DPO conforme au RGPD (40-43) ;
- la délégation au Roi après avis de l'Autorité (43) ;
- éviter des tâches qui se chevauchent entre le DPO et le professionnel de la santé (44) ;
- accorder une attention aux droits de la personne concernée (48).

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere