Avis n° 66/2018 du 25 juillet 2018

Objet : projet d'arrêté royal modifiant l'arrêté royal du 12 août 1993 *relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale* et l'arrêté royal du 20 septembre 2012 *organisant la sécurité de l'information au sein de la plate-forme eHealth et fixant les missions et les compétences du médecin sous la surveillance et la responsabilité duquel s'effectue le traitement de données à caractère personnel relatives à la santé par la plate-forme e-Health* (CO-A-2018-051)

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 M. De Block, Ministre des Affaires sociales et de la Santé publique, reçue le 20 juin 2018 ;

Vu le rapport de Monsieur J. Baret ;

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

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. La Ministre des Affaires sociales et de la Santé publique (ci-après "le demandeur") a sollicité le 20 juin 2018 l'avis de l'Autorité sur un projet d'arrêté royal modifiant l'arrêté royal du 12 août 1993 *relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale* et l'arrêté royal du 20 septembre 2012 *organisant la sécurité de l'information au sein de la plate-forme eHealth et fixant les missions et les compétences du médecin sous la surveillance et la responsabilité duquel s'effectue le traitement de données à caractère personnel relatives à la santé par la plate-forme e-Health* (ci-après "le Projet").

2. Il est indiqué dans le courrier accompagnant la demande d'avis que le Projet a pour but d'adapter des dispositions réglementaires existantes conformément à la nouvelle terminologie introduite en vertu du RGPD.

3. Le Projet doit aussi être lu conjointement avec le projet de loi[1] instituant le comité de sécurité de l'information introduit au Parlement le 20 juin 2018 qui a été approuvé par la Chambre des Représentants le 19 juillet 2018. Les articles 24 et 48 de ce projet de loi visent à apporter des adaptations respectivement à l'article 25 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* et à l'article 10 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*. Ces adaptations envisagées impliqueraient en résumé que des délégués à la protection des données seront désignés par les instances visées et que ces nouvelles dispositions constitueront d'emblée une base juridique pour les modifications proposées dans le Projet.

II. EXAMEN DE LA DEMANDE D'AVIS

4. L'Autorité constate que les modifications visées par le Projet n'appellent aucune remarque à la lumière du RGPD. Ces dispositions visent en effet à mettre la terminologie des arrêtés royaux précités du 12 août 1993 et du 20 septembre 2012 en conformité avec le RGPD.

5. L'Autorité observe dans le même temps que les deux arrêtés royaux cités doivent être lus et appliqués conformément au RGPD et que chaque délégué à la protection des données qui est désigné dans ce contexte doit aussi satisfaire dans la pratique à toutes les conditions du RGPD[2]. Le demandeur a par exemple choisi de confier le rôle de délégué à la protection des données à la même personne que celle qui émet également des avis en matière de sécurité de l'information. À cet égard, l'Autorité rappelle la position adoptée par la Commission de la protection de la vie privée (ci-après la CPVP) au point 31 de sa recommandation n° 04/2017 :

"Par le passé, la CPVP a développé une jurisprudence en application de laquelle elle opère une distinction nette entre les fonctions de conseiller en sécurité et de préposé à la protection des données tout en ne s'opposant pas à ce qu'une seule personne cumule les deux fonctions pour autant que la loi lui garantisse l'indépendance indispensable à l'accomplissement de cette double tâche (...) Cette jurisprudence ne peut être utilisée aujourd'hui pour conclure que dans tous les cas, le conseiller en sécurité en fonction à l'heure actuelle peut de façon automatique être le délégué à la protection des données de demain.

Comme déjà mentionné, c'est désormais à l'aune de la fonction telle que décrite par le RGPD que cet aspect doit être examiné."

6. Dans le présent avis, l'Autorité ne peut donc pas se prononcer sur la conformité avec le RGPD de toutes les désignations de délégués à la protection des données qui interviendront sur la base des deux arrêtés royaux précités qui seront modifiés suite au Projet. Comme déjà indiqué par la CPVP, elle ne peut emprunter cette voie pour diverses raisons :

"a. Aux termes du RGPD, l'autorité de protection des données n'a pas reçu la compétence de valider le choix de son délégué à la protection des données par le responsable de traitement ou le sous-traitant. À cet égard, la notification à l'autorité de protection des données des coordonnées du délégué à la protection des données prévue à l'article 37.7 n'est en aucune façon à considérer comme une forme de demande d'accord ou de validation de la DPA sur cette désignation. Une telle approche serait contraire à l'accountability.

b. Une nécessaire flexibilité doit être laissée aux responsables de traitement et sous-traitants dans la manière dont ils souhaitent organiser les tâches et rôles de chacun en leur sein. Un modèle organisationnel unique ne doit pas être imposé.

---

[1] Il s'agit 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* (DOC 54 3185/001 http://www.lachambre.be/FLWB/PDF/54/3185/54K3185001.pdf) Voir à cet égard l'avis de la Commission de la protection de la vie privée n° 34/2018 du 11 avril 2018, en particulier les points 14 à 20 inclus.

[2] 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 CPVP n° 04/2017

(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)

c. La CPVP doit conserver toute son indépendance dans la perspective de contrôles qu'elle serait amenée à opérer, par exemple à la suite de plaintes à l'encontre du responsable de traitement ou du sous-traitant ou d'initiative. Ces responsables de traitement ou sous-traitants ont-ils désigné un délégué à la protection des données dès lors qu'ils y sont tenus ? Ce délégué est-il effectivement indépendant ? Présente-il les qualifications requises ? Dispose-t-il de suffisamment de temps pour exercer effectivement ses missions ?[3]

7. L'Autorité souligne en outre qu'il incombe au demandeur de veiller à ce que l'intégralité du texte des deux arrêtés royaux précités soient mis en conformité avec le RGPD. Afin d'assister le demandeur dans cet exercice en cours et ne voulant pas voir intégrer explicitement à cet égard l'ensemble des obligations du RGPD dans le texte des deux arrêtés royaux précités[4], l'Autorité attire d'initiative[5] l'attention sur les points suivants :

- Dans l'arrêté royal du 12 août 1993
  - il convient, par souci de clarté, d'également faire référence à l'article 4, troisième alinéa - qui traite des critères sur la base desquels le comité de sécurité de l'information désignera les délégués à la protection des données - aux critères repris aux articles 37-38 du RGPD ;
  - il convient à chaque fois qu'il est fait référence à la "sécurité (de l'information)" (comme par ex. aux articles 3, 6, 7 et 8), d'également faire référence explicitement à l'aspect "protection des données à caractère personnel" ;
  - les articles 3 et 4[6] pourraient être regroupés, par exemple sous la dénomination "service chargé de la sécurité de l'information et de la

[3] Point 25 de la recommandation de la CPVP n° 04/2017.

[4] Le RGPD est en effet directement applicable et prévaut sur les deux arrêtés royaux cités. D'un point de vue logistique, il convient aussi d'éviter les répétitions du RGPD dans le droit national. Les deux arrêtés royaux cités doivent donc de toute façon toujours être lus conjointement avec le RGPD et en cas de contradiction entre des dispositions nationales et le RGPD, ce dernier prévaut. Cela n'empêche pas que les deux arrêtés royaux doivent être harmonisés le plus possible avec les prescriptions du RGPD, d'où les recommandations supplémentaires de l'Autorité au point 7 du présent avis.

[5] Strictement parlant, le demandeur n'a en effet sollicité l'avis de l'Autorité que sur le Projet et pas sur les dispositions ne faisant pas partie du Projet, comme certaines dispositions des deux arrêtés royaux cités.

[6] *"Article 3. Le service chargé de la sécurité de l'information a une mission d'avis, de stimulation, de documentation et de contrôle.*

Le service chargé de la sécurité de l'information conseille le responsable de la gestion journalière de son institution, à la demande de celui-ci ou de sa propre initiative, au sujet de tous les aspects de la sécurité de l'information. Sauf si les risques ne sont pas suffisamment importants, les avis s'expriment par écrit et sont motivés. Dans le délai requis par les circonstances, mais avec un maximum de trois mois, le responsable de la gestion journalière décide de suivre ou non les avis et informe le service chargé de la sécurité de la décision adoptée. Si la décision déroge à un avis exprimé par écrit, elle doit être communiquée de façon écrite et motivée.

Le service chargé de la sécurité de l'information promeut également le respect des règles de sécurité imposées par une disposition légale ou réglementaire ou en vertu d'une telle disposition, ainsi que l'adoption par les personnes employées dans l'institution concernée d'un comportement favorisant la sécurité.

Le service chargé de la sécurité de l'information rassemble la documentation utile à ce sujet.

protection des données". La subdivision entre les deux articles - l'article 4 traite en effet du délégué à la protection des données tandis que l'article 3 traite du service qui se trouve sous sa direction - semblera en effet artificelle/inutilement complexe, en particulier après l'intégration des modifications visées par le Projet ;

- l'article 5 doit être adapté. Actuellement, cet article est en effet libellé comme suit : *"Le service chargé de la sécurité de l'information est placé sous l'autorité fonctionnelle directe du responsable de la gestion journalière de l'institution."* L'Autorité propose de remplacer les mots *" l'autorité fonctionnelle directe "* par tout simplement le mot "*l'autorité de*", afin d'éviter que le projet donnerait l'impression que le délégué recevrait des instructions en ce qui concerne l'exercice de ses missions, ce qui serait contraire à l'article 38.3 du RGPD. Dans le considérant 97 du RGPD, il est ajouté à cela que les délégués à la protection des données *"qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance* "[7].

- Dans l'arrêté royal du 20 septembre 2012
  - à chaque fois qu'il est fait référence à la notion de "(service de) sécurité (de l'information)" (comme par ex. aux articles 2, 3 et 4 de l'arrêté royal du 20 septembre 2012), il convient d'également faire référence explicitement à l'aspect "protection des données à caractère personnel" ;
  - les termes "conseiller en sécurité de l'information" doivent systématiquement être remplacés par les termes "délégué à la protection des données" (voir par

---

Le service chargé de la sécurité de l'information veille au respect, dans l'institution, des règles de sécurité imposées par une disposition légale ou réglementaire ou en vertu d'une telle disposition. Toutes les infractions constatées sont communiquées par écrit et exclusivement au responsable de la gestion journalière, accompagnées des avis nécessaires en vue d'éviter de telles infractions à l'avenir.

Article 4. Le service chargé de la sécurité de l'information est placé sous la direction du conseiller en sécurité. Le conseiller en sécurité peut se faire assister par un ou plusieurs adjoints.

Le conseiller en sécurité et ses adjoints éventuels dans les institutions gérant un réseau secondaire et dans les institutions n'appartenant pas à un réseau secondaire ne sont désignés qu'après avis du Comité de surveillance.

Avant d'émettre son avis, le Comité de surveillance vérifie notamment si les intéressés disposent d'une connaissance suffisante et du temps nécessaire pour pouvoir mener cette mission à bien et s'ils n'exercent pas d'activités qui pourraient être incompatibles avec cette mission. Après leur désignation, l'identité du conseiller en sécurité et de ses adjoints éventuels est communiquée sans délai au Comité de surveillance.

Après leur désignation, l'identité du conseiller en sécurité et de ses adjoints éventuels dans les autres institutions que celles visées à l'alinéa 2 est communiquée à l'institution gérant le réseau secondaire concerné, qui la communique à son tour sans délai au Comité de surveillance.

Les conseillers en sécurité et leurs adjoints éventuels ne peuvent être relevés de cette fonction en raison des opinions qu'ils émettent ou des actes qu'ils accomplissent dans le cadre de l'exercice correct de leur fonction."

[7] Le Groupe 29 a donné l'explication suivante dans son avis WP 243 : *"(...) Cela signifie que, dans l'exercice de leurs missions au titre de l'article 39, les [délégués à la protection des données] ne doivent pas recevoir d'instructions sur la façon de traiter une affaire, par exemple, quel résultat devrait être obtenu, comment enquêter sur une plainte ou s'il y a lieu de consulter l'autorité de contrôle. En outre, ils ne peuvent être tenus d'adopter un certain point de vue sur une question liée à la législation en matière de protection des données, par exemple, une interprétation particulière du droit. (...)"*

ex. les articles 7 et 8 de l'arrêté royal du 20 septembre 2012 qui - contrairement à l'article 3 du même arrêté royal - ne sont pas modifiés en vertu de l'article 11 du Projet);

- o les termes "données à caractère personnel relatives à la santé" doivent être systématiquement remplacés par la notion du RGPD "données concernant la santé"[8];
- o par souci de clarté, il pourrait être précisé à l'article 9, premier alinéa, que les propositions du professionnel des soins de santé sont communiquées non seulement au responsable de la gestion journalière mais aussi au délégué à la protection des données (mais ceci découle en fait également de l'article 38.1. du RGPD) ;
- o la communication interne de violations de données à caractère personnel prévue à l'article 9, dernier alinéa, doit être mise en conformité avec les articles 33 et 34 du RGPD afin que, le cas échéant, le responsable du traitement puisse également communiquer de telles violations à l'Autorité et à la personne concernée dans les délais fixés par le RGPD. Actuellement, l'article 9, dernier alinéa de l'arrêté royal du 20 septembre 2012 ne prévoit en effet pas de délais;
- o par souci de clarté, il pourrait être précisé à l'article 10 que le professionnel des soins de santé ne désignera les personnes qui prendront part au traitement de données concernant la santé qu'après avis du délégué à la protection des données (mais ceci découle en fait également de l'article 38.1. du RGPD).

PAR CES MOTIFS,

L'Autorité émet un **avis favorable** concernant le Projet, et ce à la condition expresse que

- chaque délégué à la protection des données qui, dans ce contexte, est désigné dans la pratique réponde également à toutes les conditions du RGPD (points 5 et 6) ;

[8] Article 4, 15) du RGPD.

- le demandeur apporte des adaptations supplémentaires aux arrêtés royaux susmentionnés du 12 août 1993 et du 20 septembre 2012 afin de les mettre en conformité avec le RGPD (point 7).

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere