



Avis n° 128/2018 du 7 novembre 2018

Objet: Demande d'avis de l'Autorité de protection des données sur l'avant-projet d'ordonnance sur les organismes assureurs bruxellois (CO-A-2018-114)

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

Vu la loi du 3 décembre 2017 *relative à la loi portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26;

Vu la demande d'avis de M. Guy Vanhengel et M. Didier Gosuin reçue le 20 septembre 2018;

Vu le rapport de Monsieur Debeuckelaere Willem;

Émet, le 7 novembre 2018 l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Les membres du Collège Réuni de la Commission communautaire commune (Cocom) compétents pour la politique de Santé (ci-après le demandeur), sollicitent l'avis de l'Autorité concernant un avant-projet d'ordonnance relative aux institutions d'assurance bruxelloises (ci-après l'avant-projet).
2. L'ordonnance vise essentiellement à permettre à une nouvelle institution « *Iriscare* » de reprendre les missions de l'INAMI dans les matières transférées à la Cocom suite à la sixième réforme de l'Etat. L'ordonnance combine ces nouvelles compétences avec les matières pour lesquelles la Cocom est compétente. Concrètement, il s'agit de prestations de soins individuelles, en ce compris les aides aux individus, en matière de soins de santé et d'aide aux personnes handicapées (Exposé des motifs, p. 2).
3. L'avant-projet est applicable à toute personne physique (ci-après l'« *assuré bruxellois* ») qui est assujettie à la Sécurité sociale belge et dont le domicile légal est situé sur le territoire bilingue de Bruxelles-capitale (articles 2.6° *juncto* 2.22° de l'avant-projet d'ordonnance¹)².
4. Afin de pouvoir bénéficier d'une intervention pour des prestations de soins, les assurés bruxellois doivent être affiliés à un organisme assureur (« *OA* ») bruxellois, c'est-à-dire, soit une société mutualiste régionale (« *SMR* ») bruxelloise, soit la Caisse auxiliaire bruxelloise (Exposé des motifs, p. 5).

II. EXAMEN DE LA DEMANDE D'AVIS

5. L'Autorité limite son examen de l'avant-projet aux trois dispositions qui concernent les traitements de données personnelles, à savoir les articles 11, 12 et 13.

¹ L'article 2.6° définit comme suit l'assuré bruxellois : « toute personne habitant sur le territoire de la Région bilingue de Bruxelles-capitale et à laquelle le régime de sécurité sociale de la Belgique est applicable [...] ». L'article 2 22° précise que « habiter » est avoir son domicile au sens de l'article 32 3° du Code judiciaire.

² Pour la définition du « domicile », l'ordonnance se réfère à l'article 32 3° du Code judiciaire, à savoir le lieu où la personne est inscrite à titre principal sur les registres de la population (Ibid.).

1. Rôle et responsabilité

6. L'article 12 prévoit que les OA bruxellois sont responsables du traitement des données concernées, et sont tenus de les traiter uniquement en vue de l'exécution de leurs missions. L'Autorité en prend note.

2. Légalité

7. Des données relatives à la santé seront traitées par les OA bruxellois, comme il ressort de l'énumération des prestations de soins aux individus pour lesquelles ils interviennent (article 3 du projet d'ordonnance).
8. L'article 6 du RGPD détermine limitativement les hypothèses dans lesquelles le traitement de données à caractère personnel est licite, et l'article 9 du RGPD détermine, tout aussi limitativement, les hypothèses dans lesquelles des catégories particulières de données à caractère personnel (dont les données concernant la santé) n'est pas interdit. Il s'agit notamment des cas où les traitements de données sont nécessaires à des fins de gestion des systèmes et des services de soins de santé ou de protection sociale sur base du droit de l'Union ou du droit d'un Etat membre (article 9.1.h du RGPD).
9. Les missions des OA bruxellois, telles que définies à l'article 10 de l'avant-projet, étant liées à la gestion des services de soins de santé ou de protection sociale, l'Autorité estime que le traitement des données concernées est légitimé par une base légale suffisante.
10. L'Autorité s'interroge toutefois sur la légalité du mécanisme de transfert de données prévu dans le projet d'arrêté sur base d'une convention à conclure entre les OA bruxellois et les destinataires de données concernés (article 13 de l'avant-projet d'ordonnance³). L'Autorité souligne que la conclusion d'une telle convention n'est envisageable que pour les matières non réglementées de manière prescriptive notamment, au niveau fédéral, et pour les circonstances dans lesquelles les communications de données effectuées par les OA bruxellois ne sont pas soumises à des autorisations préalables. De telles règles prescriptives et/ou obligations d'autorisation préalable existent dans les cas suivants :

³ Article 13§1 de l'avant-projet d'ordonnance : « *les OA bruxellois, les unions nationales de mutualités, les mutualités, la Caisse auxiliaire d'assurance maladie-invalidité et la Caisse de soins de santé de HR Rail échangent entre eux les données nécessaires dans le cadre de l'application de la présente ordonnance, conformément à une convention conclue à ce sujet* ».

- lorsque les données communiquées proviennent de certaines sources réglementées au niveau fédéral comme les données du Registre national (voir ci-dessous titre 4.2 « *Origine et qualité des données personnelles traitées à partir de sources authentiques* ») ;
- lorsque la communication des données concernées est subordonnée à une obligation d'autorisation préalable du Comité sécurité de l'information récemment institué par la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale (ci-après « loi BCSS »), telle que modifiée par la loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679.

11. A cet égard, l'Autorité note que les OA bruxellois « *font partie de la Banque-Carrefour de la sécurité sociale en tant qu'institutions de sécurité sociale au sens de l'article 2, alinéa 1^{er}, 2^o, b) de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale* » (article 11 § 3 de l'avant-projet d'ordonnance). A ce titre, les OA bruxellois sont soumis à la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale (ci-après « loi BCSS »), laquelle prévoit une obligation d'autorisation préalable de la chambre sécurité sociale de santé du comité de sécurité de l'information, sauf exemption par le Roi, et ce, pour toute « *communication de données sociales à caractère personnel par la Banque-Carrefour de la sécurité sociale ou une institution de la sécurité sociale à une autre institution de la sécurité sociale, ou à une instance autre qu'un service public fédéral, un service public de programmation ou un organisme fédéral d'intérêt public* » (article 15 de la loi BCSS).
12. Dès lors, l'Autorité recommande de préciser dans l'exposé des motifs du projet d'ordonnance, dans quelle mesure et dans quelles circonstances les OA bruxellois seront ou non soumis à une obligation d'autorisation préalable du Comité de sécurité de l'information. Dans tous les cas, l'Autorité souligne par ailleurs qu'une convention entre les parties concernées ne pourra en aucun cas déroger à une telle obligation d'autorisation préalable, le cas échéant (voir à cet égard les remarques de l'Autorité au sujet des destinataires de données sous le titre 6 « destinataires de données »).
13. L'Autorité recommande également de tenir compte des règles régissant l'accessibilité et la communication de données provenant de sources authentiques (voir les remarques faites à cet égard sous le titre 4.2 « *origine et qualité des données traitées à partir de sources authentiques* »).
14. L'Autorité remarque en outre qu'une mise à jour est nécessaire en ce qui concerne les références à la législation de protection des données personnelles incluses dans l'avant-

projet. En effet, l'article 12 de l'avant-projet prévoit que la collecte et le traitement de données dans le cadre de l'ordonnance s'effectueront dans le respect de la législation applicable en matière de données personnelles. A cet égard, l'Autorité recommande de mettre à jour la référence à la loi du 8 décembre 1992 relative à la protection de la vie privée, entretemps abrogée par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (article 280).

3. Finalité

15. Les finalités d'un traitement de données personnelles doivent être déterminées et explicites, en application de l'article 5.1.B du RGPD.
16. En l'occurrence, l'article 12 de l'avant-projet précise que les données à caractère personnel sont traitées uniquement en vue de l'exécution des missions des organismes assureurs bruxellois. Ces missions sont listées à l'article 10 de l'avant-projet. L'Autorité estime donc que les finalités du traitement des données concernées sont suffisamment explicites et déterminées, conformément aux exigences de l'article 22 de la Constitution belge tel qu'interprété par la Cour constitutionnelle⁴.

4. Proportionnalité

17. Les données personnelles traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, en application de l'article 5.1.d du RGPD.

4.1 Données personnelles traitées

18. Il est précisé à l'article 12 que « *les données traitées sont les données à caractère personnel nécessaires à l'application de la présente ordonnance et de ses arrêtés d'exécution* ».
19. Dans la mesure où les OA bruxellois font partie de la BCSS (article 11 § 3 de l'avant-projet), et interviennent dans le coût de prestations de soins aux individus (article 3 de l'avant-projet d'ordonnance), les données traitées comprennent sans aucun doute des « *données sociales à caractère personnel relatives à la santé* » telles que définies à l'article 9.a de la loi du 5

⁴ Dans le domaine eHealth notamment, voir Cour constitutionnelle, arrêt n° 29/2010 du 18 mars 2010, point B.16.3 : « *Compte tenu de l'objectif poursuivi par le législateur, la délégation au Roi est suffisamment précise pour répondre à la condition du respect du principe de la légalité, tel qu'il découle de l'article 22 de la Constitution. Elle ne porte pas sur une mission qui consisterait à déterminer les données auxquelles chaque institution aurait accès. C'est en effet la loi qui fixe les missions de la plate-forme eHealth.* »

septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679⁵.

20. A cet égard, l'Autorité recommande de préciser les catégories de données traitées, en vue de rencontrer les exigences de prévisibilité de l'article 22 de la Constitution, tel qu'interprété par la Cour constitutionnelle dans son arrêt n° 29/2010 relatif à la plateforme eHealth^{6,7}. La même remarque a déjà été formulée par la Commission de la protection de la vie privée (ci-après « la Commission vie privée ») au sujet d'un projet de décret flamand relatif à la régionalisation des organismes assureurs⁸. Dans son avis n° 45/2017 du 30 août 2017, la Commission vie privée recommandait en effet de préciser les catégories de données en question, soit dans le texte du décret, soit en les spécifiant par un arrêté⁹. L'avant-projet de décret sur la protection sociale flamande a ensuite été adapté pour prévoir que les catégories de données seront déterminées par décret après avis de la Commission pour la protection de la vie privée^{10,11}. Enfin, outre la perspective d'une meilleure prévisibilité de la loi, un renvoi explicite aux dispositions pertinentes qui permettent de déterminer de manière univoque les catégories de données pertinentes est également important afin de garantir la transparence à l'égard des personnes concernées (voir ci-après titre 7 « Transparence »).

4.2 Origine et qualité des données personnelles traitées à partir de sources authentiques

21. L'article 11 prévoit que les organismes assureurs (OA) bruxellois utilisent uniquement des données à caractère personnel provenant de sources authentiques. Ce n'est que lorsqu'une erreur ou une lacune est constatée lors de la consultation des sources authentiques que les

⁵ Article 9.a de la loi du 5 septembre 2018 instituant le comité de sécurité de l'information : « *données sociales à caractère personnel relatives à la santé : les données sociales à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».

⁶ Voir Cour constitutionnelle, arrêt n° 29/2010 du 18 mars 2010, point B.16.3 (reproduit en nbp 4).

⁷ Dans le domaine eHealth notamment, voir Cour constitutionnelle, arrêt n° 29/2010 du 18 mars 2010, point B.10.1 : « *Les droits que garantissent l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme ne sont pas absolus. Bien que l'article 22 de la Constitution reconnaisse à chacun le droit au respect de sa vie privée et familiale, cette disposition ajoute en effet immédiatement : « sauf dans les cas et conditions fixés par la loi ». Les dispositions précitées exigent que toute ingérence des autorités dans le droit au respect de la vie privée et familiale soit prévue par une disposition législative suffisamment précise et qu'elle soit nécessaire pour atteindre un objectif légitime, ce qui implique notamment qu'un lien raisonnable de proportionnalité doit exister entre les effets de la mesure pour la personne concernée et les intérêts de la société.* »

⁸ « *En ce qui concerne les articles 22, 37, 39, 50 et 65 du projet de décret, la Commission vie privée remarque dans son avis que l'actuelle description des catégories de données ne permet pas d'évaluer la proportionnalité du traitement de données. Pour ces articles, il est ajouté un article 49 prévoyant que le Gouvernement flamand spécifiera ces données, après avis de la Commission vie privée (notre traduction)* » (Parlement flamand, projet de décret relatif à la protection sociale flamande, DOC 1474 (2017-2018), p. 27).

⁹ Avis n° 45/2017 de la Commission vie privée du 30 août 2017 relatif à la protection sociale flamande, § 11.

¹⁰ Ibid.

¹¹ Dans son avis n° 63/2018 du 25 juillet 2018, l'Autorité a d'ailleurs formulé des remarques complémentaires à ce sujet, invitant le législateur flamand à plus de précisions quant à toutes les catégories de données concernées pour tous les piliers de soins concernés (Avis n° 63/2018 du 25 juillet 2018 de l'Autorité de protection des données sur l'avant-projet d'arrêté du Gouvernement flamand portant exécution du décret [...] relatif à la protection sociale flamande, § 10-14).

OA bruxellois peuvent s'adresser à la personne concernée pour obtenir les données complétées ou rectifiées.

22. L'article 11 de l'avant-projet précise que la source authentique qui doit être consultée en priorité par les OA bruxellois est le Registre national des personnes physiques. Ainsi par exemple, pour déterminer la résidence principale, les organismes assureurs feront appel à la source authentique du Registre national des personnes physiques¹². L'utilisation d'une autre source authentique n'est autorisée que lorsque les données nécessaires ne peuvent être obtenues auprès du Registre national des personnes physiques (article 11 § 2 de l'avant-projet).
23. L'avant-projet précise également que les OA bruxellois font partie de la Banque-carrefour de la sécurité sociale ou « BCSS » (article 11 § 3). L'Autorité comprend donc que les sources authentiques auxquelles la BCSS donne accès¹³, sont susceptibles d'être consultées par les OA Bruxellois.
24. En ce qui concerne la qualité des données obtenues à partir de sources authentiques telles que le RN ou à partir de la BCSS, l'avant-projet introduit des dispositions que l'Autorité recommande de supprimer ou amender.
25. En ce qui concerne la mise à jour des données obtenues du RN et de la BCSS, l'avant-projet introduit une obligation non pertinente à charge des OA bruxellois. L'avant-projet prévoit en effet que les données issues du RN feront foi jusqu'à preuve du contraire (article 11 § 2 al. 3 de l'avant-projet). Ce principe est redondant par rapport à l'article 4 § 3 de la loi du 8 août 1983 sur le Registre national (ci-après « *loi RN* »). L'Autorité recommande donc de supprimer cette mention dans le projet d'ordonnance.
26. L'avant-projet prévoit également une procédure de rectification des données obtenues à partir de sources authentiques. L'avant-projet introduit deux mécanismes, l'un spécifique au RN, l'autre valable pour toutes les sources authentiques, avec une précision concernant la BCSS. D'une part, en effet, les OA Bruxellois sont chargés de communiquer au RN toute information contraire dont ils estiment avoir obtenu la preuve (article 11 § 2 al. 4). D'autre part, tant pour le RN que pour la BCSS et toute autre source authentique visée, l'avant-projet impose aux OA Bruxellois de prévoir une procédure pour intégrer les données complétées et corrigées dans la source authentique (article 11 § 4 de l'avant-projet). Plus précisément,

¹³ Voir <https://www.ksz-bcss.fgov.be/fr/services-et-support/services/ssh>.

pour ce qui est de la BCSS, l'avant-projet impose aux OA d'enregistrer les données mises à jour dans le répertoire des personnes visé à l'article 6 de la loi du 15 janvier 1990 relative à la BCSS.

27. A cet égard, l'Autorité remarque de manière générale qu'il incombe au législateur bruxellois de vérifier que la législation applicable à chaque source authentique concernée permet bien la mise en œuvre des mécanismes d'information et rectification prévus à l'article 11 de l'avant-projet.

28. Ainsi par exemple, en ce qui concerne le Registre national, l'Autorité souligne qu'une instance régionale n'a de son avis pas compétence pour réglementer les procédures d'information à fournir au RN ou les procédures de rectification du RN qui ressortent des compétences fédérales. A ce jour, à la connaissance de l'Autorité, aucune disposition des lois applicables au RN ne permet au législateur bruxellois et/ou aux OA de mettre en place les mécanismes susmentionnés envisagés à l'article 11 § 2 et 3 de l'avant-projet, comme explicité ci-dessous.

- En ce qui concerne la BCSS, la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une BCSS (ci-après « *loi BCSS* ») permet à cette institution de s'entendre avec d'autres intégrateurs de services pour déterminer « *qui réalise quelle authentification de l'identité, quels vérifications et contrôles à l'aide de quels moyens et qui en assume la responsabilité* » (article 3ter de la loi BCSS). Ceci n'emporte pas la possibilité de s'entendre dans tous les cas avec des sources authentiques telles que le registre RN. La loi BCSS prévoit une synchronisation des données des registres BCSS avec les données RN dans le sens où le registre BCSS est mis à jour au moyen des données du RN lesquelles sont « *mises à jour de façon systématique dans le RN* »¹⁴. Il faut constater que, selon la compréhension de l'Autorité, la procédure de mise à jour inverse, à savoir des registres BCSS vers le RN n'est pas prévue dans la loi BCSS.
- La procédure d'enregistrement des données dans les registres de la BCSS semble certes permettre une certaine souplesse visant à permettre une mise à jour des données au moyen de pièces justificatives, après concertation avec le RN. Il est ainsi prévu que le Comité de gestion de la BCSS peut déterminer, « *après concertation avec le Registre national* », « *les pièces justificatives sur base desquelles les données*

¹⁴ Article 4 § 2 al. 2 de la loi BCSS : « *Entre les registres Banque-Carrefour et le Registre national, une synchronisation régulière est opérée, de telle manière qu'il ne soit pas gardé dans les registres Banque-Carrefour des données relatives aux personnes physiques qui sont inscrites dans le Registre national et dont toutes les données d'identification nécessaires sont mises à jour de façon systématique dans le Registre national, à l'exception des éventuelles données historiques relatives à la période pendant laquelle ces personnes étaient inscrites dans les registres Banque-Carrefour.* »

d'identification peuvent être reprises et modifiées dans les registres Banque-Carrefour, ainsi que les institutions de sécurité sociale ou autorités publiques belges, personnes physiques et organismes publics ou privés de droit belge, qui sont habilités à enregistrer ou modifier des données d'identification dans les registres Banque-Carrefour sur la base de ces pièces justificatives » (article 4 § 3 de la loi BCSS). Il est également prévu que les institutions de sécurité sociale sont tenues de tenir à jour leurs données. Selon la loi BCSS, en effet, « la Banque-carrefour peut, après avoir pris l'avis de son Comité général de coordination, répartir les tâches d'enregistrement des données sociales de manière fonctionnelle entre les institutions de sécurité sociale. Ces institutions sont dans ce cas tenues d'enregistrer dans leurs banques de données sociales et de tenir à jour les données dont la conservation leur est confiée » (article 9 de la loi BCSS). Selon la lecture de l'Autorité, il ne découle toutefois pas des dispositions précitées que le législateur bruxellois soit compétent pour imposer à des institutions de la BCSS, tels que les OR bruxellois, de prévoir une procédure pour intégrer des données complétées ou corrigées dans la source authentique RN. Si tel était toutefois le cas, l'Autorité estime nécessaire de justifier cette compétence dans l'exposé des motifs.

29. En ce qui concerne le mécanisme de mise à jour des sources authentiques concernées, tel que prévu à l'article 11 § 4 de l'avant-projet, l'Autorité recommande donc de prévoir à tout le moins une réserve concernant la légalité des procédures envisagées, et de ne maintenir cette obligation de mise à jour de la source authentique à charge des OA bruxellois qu'à condition et pour autant que la législation relative à chaque source authentique concernée le permette. L'Autorité recommande d'apporter des clarifications à cet égard dans l'exposé des motifs.

4.3. Conclusion sur la proportionnalité

30. Faute de disposer d'une listes des catégories de données que les OR bruxellois sont susceptibles de traiter, l'Autorité ne peut se prononcer sur la proportionnalité du traitement de données envisagé.

5. Conservation des données

31. L'article 12 prévoit des délais de conservation pour les données collectées. L'Autorité en prend bonne note.

6. Destinataires des données

32. L'article 13 de l'avant-projet prévoit que dans le cadre de l'application du projet d'ordonnance, les OA bruxellois échangent les données nécessaires avec les unions nationales de mutualités, les mutualités, la Caisse auxiliaire d'assurance maladie-invalidité et la Caisse de soins de santé de HR Rail (ci-après, les « *destinataires* »).

6.1 Finalités et données traitées

33. L'article 13 § 2 de l'avant-projet prévoit que les données ainsi échangées doivent être nécessaires dans le cadre de l'application de l'avant-projet d'ordonnance, et précise les données qui peuvent être concernées par cet échange, notamment, le statut d'assurance des assurés bruxellois dans le cadre de l'assurance obligatoire soins de santé et indemnités, ainsi que les données nécessaires pour éviter le double financement des mêmes coûts de prestation et d'intervention.

34. L'Autorité prend note de ces précisions visant à satisfaire les exigences de légalité et de prévisibilité consacrés à l'article 22 de la Constitution belge et à l'article 8 de la CEDH¹⁵.

6.2 Autorisation préalable

- *Communication de données à une autre institution de sécurité sociale, ou à une instance autre qu'un service public fédéral*

35. L'article 13 prévoit que l'échange de données envisagé aura lieu conformément à une convention à conclure entre les OA bruxellois et les destinataires. Comme indiqué précédemment, en tant que membres de la Banque-Carrefour de la sécurité sociale, les OA bruxellois devront en principe appliquer la loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement 2016/679 (ci-après la « *loi Comité de sécurité de l'information* »). L'Autorité renvoie à ses développements à ce sujet sous le titre 2 « *légalité* », et recommande de faire référence, à

¹⁵ Dans le domaine eHealth notamment, voir Cour constitutionnelle, arrêt n° 29/2010 du 18 mars 2010, point B.16.3 : « *Compte tenu de l'objectif poursuivi par le législateur, la délégation au Roi est suffisamment précise pour répondre à la condition du respect du principe de la légalité, tel qu'il découle de l'article 22 de la Constitution. Elle ne porte pas sur une mission qui consisterait à déterminer les données auxquelles chaque institution aurait accès. C'est en effet la loi qui fixe les missions de la plate-forme eHealth.* »

tout le moins dans l'exposé des motifs, à l'application de la loi BCSS telle que modifiée par la loi Comité de sécurité de l'information.

➤ *Communication de données aux dispensateurs de soins et offices de tarification*

36. L'article 14 § 2 de la loi BCSS précise qu'une autorisation de principe du Comité de sécurité de l'information est requise pour la communication de données par les organismes assureurs fédéraux (à savoir, une union nationale, la Caisse auxiliaire d'assurance maladie-invalidité et la Caisse des soins de santé de HR Rail) aux dispensateurs de soins et aux offices de tarification, de données à caractère personnel dont ces destinataires ont besoin en vue de l'exécution des missions fixées dans la loi relative à l'assurance obligatoire soins de santé et indemnités coordonnée le 14 juillet 1994 (article 14 § 2 de la loi BCSS *juncto* article 2.i de la loi relative à l'assurance obligatoire soins de santé et indemnités coordonnée le 14 juillet 1994). Cette même disposition de la BCSS précise qu'une telle communication se fait à l'intervention du Collège intermutualiste national et sans intervention de la Banque-Carrefour.

37. L'Autorité recommande de clarifier dans l'avant-projet les règles applicables dans de telles circonstances au niveau régional. L'Autorité renvoie à cet égard à la remarque formulée à ce sujet dans son avis n° 18/2018 du 28 février 2018¹⁶.

7. Transparence

38. L'Autorité constate que l'avant-projet d'ordonnance ne comporte aucune disposition expresse concernant les droits de la personne concernée, outre le renvoi général à l'application de la législation de protection des données personnelles (voir les remarques à cet égard sous le titre 2 « *légalité* »). Elle souhaite attirer l'attention sur deux droits qui peuvent être d'une importance particulière dans le cadre de l'avant-projet de décret et pour lesquels le demandeur doit éventuellement prévoir des garanties légales supplémentaires. L'Autorité se réfère à cet égard aux remarques similaires formulées dans son avis n°45/2017 du 30 août 2017 au sujet de l'avant-projet de décret relatif à la protection sociale flamande, reproduites partiellement ci-dessous (titre 7 de l'avis n° 45/2017 « *droits de la personne concernée* »).

39. Les articles 12-14 du RGPD définissent les informations qui doivent être fournies à la personne concernée et font une distinction selon que les données à caractère personnel ont été obtenues ou non auprès de la personne concernée (collecte directe ou indirecte). L'article

¹⁶ « *Il convient d'encadrer de manière adéquate les flux et/ou couplages de données réalisés entre les organismes assureurs régionaux et les prestataires de soins, notamment du point de vue de la sécurisation des données et de la gestion des accès* », Avis de la CPVP n° 18/2018 du 28 février 2018 sur l'avant-projet de décret du Gouvernement wallon relatif aux organismes assureurs portant modification du Code wallon de l'Action sociale et de la Santé, paragraphe 8.

14.5(c) du RGPD est particulièrement important pour l'avant-projet de décret car il prévoit une possibilité de dérogation lorsque les données à caractère personnel n'ont pas été obtenues auprès de la personne concernée si "*l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis*", mais uniquement si "*[ce droit] prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée*". L'Autorité invite dès lors le demandeur à vérifier la manière dont la transparence des traitements de données envisagés sera assurée et à prendre au besoin des mesures supplémentaires appropriées pour protéger les intérêts légitimes de la personne concernée.¹⁷

40. Outre un cadre légal clair qui expose les informations obligatoires à fournir pour respecter l'obligation de transparence prévue à l'article 14 du RGPD, l'Autorité recommande que le projet prévoie expressément que les OA bruxellois seront responsables de la transmission de ces informations obligatoires dans leurs communications et leurs interactions individuelles avec les personnes concernées, informations qui incluent notamment les coordonnées du délégué à la protection des données à qui elles peuvent s'adresser pour de plus amples informations.

8. Sécurisation et confidentialité des données

41. L'Autorité recommande de préciser, à tout le moins dans l'exposé des motifs, les mesures prises en vue d'assurer la sécurité et la confidentialité des données personnelles traitées, compte tenu des obligations de sécurité prévues à l'article 32 du RGPD, le cas échéant, par référence aux mesures prises dans le cadre de l'affiliation des OA bruxellois à la BCSS.

¹⁷ Voir également à cet égard Cour de Justice, Affaire C-201/14 (*Smaranda Bara e.a. contre Presedintele Casei Nationale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)*), 1^{er} octobre 2015, points 40-41 ("40. Or, outre la circonstance, relevée par la juridiction de renvoi, selon laquelle les données relatives aux revenus ne font pas partie des données personnelles nécessaires à l'établissement de la qualité d'assuré, il y a lieu de souligner que l'article 315 de la loi n° 95/2006 ne fait qu'envisager, en son principe, la transmission de ces dernières données personnelles détenues par des autorités, des institutions publiques et d'autres institutions. Il ressort également de la décision de renvoi que la définition des informations transmissibles ainsi que les modalités de mise en œuvre de la transmission de ces informations ont été élaborées au moyen non pas d'une mesure législative, mais du protocole de 2007 conclu entre l'ANAF et la CNAS, lequel n'aurait pas fait l'objet d'une publication officielle. 41. Dans de telles circonstances, il ne saurait être considéré que les conditions posées à l'article 13 de la directive 95/46 pour qu'un État membre puisse déroger aux droits et aux obligations qui découlent de l'article 10 de cette directive sont réunies.")

PAR CES MOTIFS,

Concernant l'avant-projet d'ordonnance relatif à la qualité de la pratique des soins de santé, l'Autorité émet un avis favorable à condition que soient prise en compte les recommandations suivantes :

- Considérants 10-13 : faire référence, à tout le moins dans l'exposé des motifs, à l'application aux OA bruxellois de la loi BCSS telle que modifiée par la loi Comité de sécurité de l'information ; reformuler l'article 13 de l'avant-projet de manière à tenir compte du fait qu'en aucun cas la convention à conclure entre les OA bruxellois et les destinataires de données sociales à caractère personnel (comme prévu à l'article 13 de l'avant-projet) ne pourra déroger aux règles prescriptives régissant l'accessibilité de données en provenance de certaines sources authentiques comme le Registre national.
- Considérant 14 : adapter la référence à la loi du 8 décembre 1992 relative à la protection de la vie privée, abrogée par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (article 280) ;
- Considérant 20 : préciser les catégories de données traitées par les OA bruxellois en vue de rencontrer les exigences de prévisibilité de l'article 22 de la Constitution;
- Considérants 25-26 : vérifier que la législation applicable à chaque source authentique concernée permet bien les mécanismes d'information ou rectification prévus à l'article 11 de l'avant-projet ; ne maintenir une obligation d'information de la source authentique et de mise à jour de la source authentique à charge des OA bruxellois qu'à condition et pour autant que la législation relative à chaque source authentique concernée le permette;
- Considérant 37 : envisager de clarifier les règles applicables à la communication de données personnelles par les OA bruxellois aux dispensateurs de soins et aux offices de tarification.
- Considérant 40 : clarifier les informations obligatoires à fournir pour respecter les obligations de transparence prévues à l'article 14 du RGPD et rendre les OA bruxellois responsables de la transmission de ces informations obligatoires dans leurs communications et leurs interactions individuelles avec les personnes concernées, informations qui incluent les coordonnées du délégué à la protection des données à qui elles peuvent s'adresser pour de plus amples informations.

- Considérant 41 : préciser, à tout le moins dans l'exposé des motifs, l'impact de l'affiliation des OA bruxellois à la BCSS en termes de sécurité et de confidentialité des données personnelles traitées.

L'Administrateur f.f.,

Le Président

(sé) An Machtens

(sé) Willem Debeuckelaere