

<p>Comité de sécurité de l'information Chambre sécurité sociale et santé</p>
--

CSI/CSSS/20/322

DÉLIBÉRATION N° 20/134 DU 3 MAI 2020, MODIFIÉE LE 7 JUILLET 2020, RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PAR LES COLLECTIVITÉS À LA PLATE-FORME E-HEALTH ET À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PAR LA PLATE-FORME E-HEALTH À SCIENSANO DANS LE CADRE DE LA LUTTE CONTRE LE COVID-19 – CRÉATION DE LA BASE DE DONNÉES IV « COORDONNÉES DES COLLECTIVITÉS »

Le Comité de sécurité de l'information, chambre sécurité sociale et santé (dénommé ci-après « le Comité »),

Vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général relatif à la protection des données ou GDPR) ;

Vu la loi du 3 décembre 2017 *relative à la création de l'Autorité de protection des données*, en particulier l'article 114, modifié par la loi du 25 mai 2018 ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ;

Vu 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 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*, notamment l'article 97;

Vu la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions*, en particulier les articles 5,5° et 11 ;

Vu l'arrêté royal n° 18 portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19 ;

Vu l'arrêté royal n°25 du 28 mai 2020 modifiant l'arrêté royal n°18 du 4 mai 2020 portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19 ;

Vu l'arrêté royal n°44 concernant le traitement conjoint de données par Sciensano et les centres de contacts désignés par les autorités régionales compétentes ou par les agences compétentes, par les

inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano ;

Vu le rapport d'auditorat de la Plate-forme eHealth ;

Vu le rapport de monsieur Bart Viaene.

Émet, après délibération, la délibération suivante, le 7 juillet 2020 :

I. OBJET DE LA DEMANDE

1. La Plate-forme eHealth a été chargée, dans le cadre de ses missions légales, de mettre en place une base de données contenant les coordonnées des collectivités. Selon l'article 1^{er}, §1^{er}, 3^o de l'arrêté royal n°44, une collectivité est « une communauté de personnes pour lesquelles les inspections sanitaires compétentes jugent qu'il existe un risque accru de propagation du coronavirus COVID-19 ».
2. Cette base de données IV¹ contient² les coordonnées du médecin de référence d'une collectivité³ ou à défaut, du responsable administratif de cette collectivité en vue d'apporter un soutien à l'initiative gouvernementale de suivi des personnes positives au COVID-19 (tracing) dans le but de lutter contre la propagation du COVID-19 au sein des collectivités et de protéger la population évoluant au sein de ces collectivités. Il est également prévu par l'article 8 de l'A.R. n°44 du 26 juin 2020 que la banque de données IV contient les données de contact des Personnes de catégories V⁴ à savoir les médecins traitants des Personnes de catégories I, II, III.
3. Les informations relatives aux coordinateurs (médecin de référence de la collectivité ou, à défaut de médecin de référence, un responsable administratif de cette collectivité) sont communiquées par les sources authentiques dont dépendent celles-ci. En l'occurrence il s'agit des services publics fédéraux ou des services publics des entités fédérées.
4. Cette base de données, dite « base de données collectivités » sera alimentée par les sources authentiques du fédéral et des entités fédérées de collectivités de manière hebdomadaire au moyen d'un formulaire standardisé par la Plate-forme eHealth. Cette base de données sera mise à disposition du call center de Smals désigné comme opérateur par les entités fédérées en charge de la prévention et du tracing des patients atteints de COVID-19.

¹ Article 1^{er}, §1^{er}, 8^o de l'arrêté royal n°44 du 26 juin 2020 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano, *M.B.*, 29 juin 2020, p. 48424.

² Art. 8 de l'arrêté royal n°44 précité.

³ Il y a 3 catégories de champs pour les personnes de contact : un responsable administratif, un responsable back-up et un responsable médical.

⁴ Art. 1^{er}, 16

5. Les données personnelles contenues dans la base de données « collectivités » seront uniquement consultables par les collaborateurs du centre d'appel.
6. Le personnel, les procédures de travail ou encore l'utilisation des résultats de ces contact tracings (envoyés à Sciensano et aux entités fédérées) relève de la compétence des entités fédérées.
7. Dans l'hypothèse où une personne vivant ou travaillant au sein d'une collectivité est diagnostiquée positive au COVID-19, les agents du centre d'appel⁵ dans le cadre du suivi des personnes infectées (call center tracing) seront alors chargés de contacter le coordinateur de cette collectivité et de l'avertir de la présence d'un cas de coronavirus au sein de la collectivité. Ce coordinateur pourra alors prendre les mesures nécessaires afin de limiter la propagation du virus au sein de la collectivité.
8. Les collectivités⁶ en charge d'une population vulnérable visées sont, notamment :
 - les centres d'hébergement et/ou d'accompagnement de personnes handicapées (centres de jour, habitat accompagné) ;
 - les collectivités actives dans le domaine de la santé (maisons médicales, conventions de revalidation, service de santé mentale (SSM), initiatives d'habitation protégée, maisons de soins psychiatriques (MSP), services de soins palliatifs et continués, services actifs en matière de toxicomanie, les services de soins intégrés à domicile) ;
 - les maisons de repos, maisons de repos et de soins ;
 - les prisons, les maisons de justice ;
 - les crèches, les jardins d'enfants ;
 - les écoles (maternelles, primaires, secondaires) ;
 - les universités et les hautes écoles ;
 - les institutions publiques de protection de la jeunesse (IPPJ) ;
 - les centres d'aide aux adultes en difficulté (accueil de jour, accueil d'urgence, hébergement d'urgence, housing first, maison d'accueil, travail de rue, les services d'aide aux sans-abris,...) ;
 - les centres d'accueil Fedasil ;
 - les centres fermés dépendants de l'Office des étrangers ;
 - les entreprises du secteur privé ;
 - une caserne ;
 - les initiatives ou projets liés au secteur de l'enfance, au secteur de la santé ou lié au secteur social non repris ci-dessus.
9. Les données⁷⁸ reprises dans la base de données hébergée par la Plate-forme eHealth sont :

⁵ La gestion de ces centres d'appels relève de la compétence des entités fédérées.

⁶ Cette liste n'est pas limitative.

⁷ Les données marquées d'un (*) sont obligatoires.

⁸ La Base de données IV contient les catégories suivantes de données à caractère personnel des Personnes de catégorie V et VI aux fins énoncées à l'article 3, § 1^{er}, 2°, B :

1° le numéro d'identification provenant d'une source authentique et le numéro d'identification interne ;

2° le nom, le type, l'adresse, le numéro figurant dans la Banque-Carrefour des Entreprises, de la collectivité à laquelle la personne appartient ou avec laquelle elle a eu des contacts;

- le numéro d'identification de l'organisation donné par la source authentique* ;
- le type d'organisation* ;
- le numéro INAMI (8 digits) ;
- le numéro BCE (10 digits) ;
- le nom de l'organisation* ;
- l'adresse complète de l'organisation (nom de rue*, numéro, code postal*, commune*) ;
- le nom* et le prénom du responsable de l'organisation ;
- le numéro de téléphone du responsable de l'organisation* ;
- le nom et prénom du back-up du responsable de l'organisation ;
- le numéro de téléphone du back-up du responsable de l'organisation ;
- le nom et le prénom du médecin responsable de l'organisation ;
- le numéro de téléphone du médecin responsable de l'organisation ;
- le numéro INAMI du médecin responsable de l'organisation.

10. Ces données personnelles seront utilisées dans le cadre de l'article 3, §1^{er}, 2^o, B de l'arrêté royal n°44 du 26 juin 2020 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano.
11. Les données à caractère personnel de cette base de données sont soit mises à jour tous les 10 ans, soit supprimées⁹.
12. Cette base de données sera hébergée par la Plate-forme eHealth jusqu'au jour de la publication de l'arrêté royal proclamant la fin de l'état d'épidémie du coronavirus COVID-19.

II. COMPÉTENCE

13. Selon l'article 4, 1) du RGPD, on entend par données à caractère personnel toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
14. En vertu de l'article 11 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions*, toute communication de données à caractère personnel par ou à la plate-forme eHealth requiert une autorisation de principe de la chambre sécurité sociale et santé du comité de sécurité de l'information, sauf dans les cas prévus par la loi.

^{3°} les coordonnées du médecin de référence et/ou de la personne responsable de la collectivité, en ce compris le nom, le prénom et le numéro de téléphone.

⁹ Art. 15, §1^{er}, al. 1, A.R. n°44.

15. Le Comité s'estime dès lors compétent pour se prononcer sur cette communication de données à caractère personnel.

III. EXAMEN DE LA DEMANDE

A. ADMISSIBILITÉ

16. Le traitement de données à caractère personnel n'est licite que si, et dans la mesure où, au moins une des conditions mentionnées à l'article 6 du RGPD est remplie. C'est notamment le cas, lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement¹⁰.
17. Selon l'article 5, 5° de la loi eHealth¹¹, la Plate-forme eHealth est chargée, en vue de l'exécution de son objectif, de s'accorder sur une répartition des tâches en ce qui concerne la collecte, la validation, l'enregistrement et la mise à disposition de données échangées au moyen de la plate-forme de collaboration et sur les normes de qualité auxquelles ces données doivent répondre, et contrôler le respect de ces normes de qualité.
18. Le Comité est par conséquent d'avis qu'il existe un fondement acceptable au traitement de données à caractère personnel envisagé.

B. PRINCIPES RELATIFS AU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

19. Selon l'article 5 du RGPD, les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence).
20. En vertu de l'article 5, 5° de la loi eHealth précitée, la Plate-forme eHealth peut créer une base de données regroupant des données à caractère personnel en vue d'apporter à un soutien à une initiative dans le domaine de la santé.
21. L'article 3, §1^{er}, 2°, B de l'arrêté royal n°44 du 26 juin 2020 précité prévoit que le centre de contact utilise les données à caractère personnel de la banque de données pour contacter les personnes chez qui le médecin présume une infection et les personnes dont le test médical était positif et pour retrouver l'identité des personnes avec lesquelles elles ont été en contact. Dans la mesure où elles ont été en contact avec des personnes d'une collectivité avec une population fragile, le centre de contact prend contact avec le médecin référent ou, à défaut, avec le responsable administratif de cette collectivité. Dans la mesure où elles ont été en contact avec des personnes individuelles, le centre de contact prend contact individuellement

¹⁰ Art. 6, §1^{er}, e) du RGPD.

¹¹ Loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth, *M.B.* du 13 octobre 2008, p. 54454.

avec ces personnes individuelles et leur fournit ensuite, sur la base des informations qu'elles communiquent, des recommandations adéquates par la voie électronique.

22. Selon l'article 5 du RGPD, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données).
23. La base de données hébergée par la Plate-forme eHealth contient les données d'identification et de contact strictement nécessaires à l'identification et au contact du coordinateur de la collectivité dans laquelle vit ou travaille la personne positive au COVID-19.
24. Le Comité constate que la Plate-forme eHealth ne détiendra aucune donnée à caractère personnel relative à la santé concernant la personne déclarée positive à une infection au coronavirus de type COVID-19.
25. Selon l'article 5 du RGPD, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.
26. Cette base de données a pour but de permettre la consultation par le centre d'appel chargé d'assurer le suivi des personnes des personnes identifiées positives au coronavirus COVID-19 de l'identité et des coordonnées exactes et mises à jour du coordinateur d'une collectivité ou d'une entreprise privée dans laquelle un cas de COVID-19 a été déclaré. Le but est que le collaborateur du centre d'appel prenne contact avec ce coordinateur pour l'informer de la présence d'un cas de Covid-19 au sein de l'organisation afin qu'il puisse mettre en place des mesures de protection du personnel, des travailleurs ou des autres résidents.
27. Selon l'article 5 du RGPD, les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude).
28. Le Comité constate qu'il est prévu que les sources authentiques des collectivités communiquent les mises à jour des données de manière hebdomadaire.
29. Selon l'article 5 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 au regard des finalités pour lesquelles elles sont traitées (limitation de la conservation).
30. Les données contenues dans la base de données collectivités seront conservées selon le délai prévu par l'arrêté royal n°44 du 26 juin 2020 précité.
31. Compte tenu de la finalité de la « base de données collectivités », le Comité estime que la communication envisagée est adéquate, pertinente et non excessive.

C. PRINCIPE DE TRANSPARENCE

32. Conformément à l'article 14 du RGPD, lorsque les données n'ont pas été obtenues auprès de la personne concernée, le responsable du traitement doit fournir certaines informations à la personne concernée. Cette disposition ne s'applique pas, notamment, lorsque 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 et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée.
33. Selon l'article 16, §4, Sciensano, les autorités régionales compétentes et les agences désignées par les autorités régionales compétentes, chacune dans son domaine de compétence, définissent de manière transparente leurs responsabilités respectives, notamment en ce qui concerne l'exercice des droits de la personne concernée et la fourniture d'informations. A cette fin, est conclu un règlement qui fixe les modalités d'une convention de traitement et d'une convention de partage des données à caractère personnel, définissant les rôles et relations respectifs des responsables conjoints du traitement vis-à-vis des personnes concernées.
34. Il est prévu de créer une page web sur laquelle seront publiées, conformément à l'article 14 du RGPD, des informations sur le traitement de données effectué par le centre de contact, le centre d'appel ainsi que la base de données centrale COVID-19. Via cette page web, les personnes concernées (patients, les personnes qui sont entrées en contact avec le patient et les prestataires de soins,) pourront trouver des informations sur le traitement des données ainsi que leurs droits dans le cadre de ce traitement.
35. Le Comité est d'avis que les mesures de transparence envisagées sont suffisantes.

D. MESURES DE SÉCURITÉ

36. Selon l'article 5 du RGPD, les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité). Ces mesures devront assurer un niveau de protection adéquat compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraînent l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.
37. Le Comité constate que l'article 2, 5° de l'arrêté royal n°44 du 26 juin 2020 prévoit que le Vlaams Agentschap Zorg en Gezondheid, l'Agence wallonne pour une Vie de Qualité, le ministère de la Communauté germanophone et la Commission communautaire commune sont, chacun dans son propre domaine de compétence, les responsables du traitement pour leur domaine sanitaire respectif.
38. Le Comité constate que l'Etat fédéral, notamment par l'intermédiaire de Sciensano ou de la Plate-forme eHealth, a été chargé, outre la mise à disposition d'une plateforme technologique

de call center commun aux entités fédérées, d'un rôle de facilitateur afin d'assurer au maximum la cohérence des procédures de travail, de formation du personnel et le respect de la vie privée dans la consultation des données par les call takers dans le cadre strict de leurs fonctions (données d'input) et dans l'utilisation par les entités fédérées en charge de la prévention et tracing du résultat de leurs contacts avec les patients et citoyens potentiellement impactés (données d'output).

39. Le Comité juge souhaitable que la désignation de chaque coordinateur de collectivité se fasse avec une préférence pour les personnes présentant un profil medico-sanitaire. En effet, étant donné que ces coordinateurs auront connaissance d'une information relative à la santé d'un de leurs collaborateurs ou résidents, il y a lieu de respecter les dispositions du RGPD en matière de traitement de données à caractère personnel relatives à la santé. A cet égard, le Comité tient à rappeler les dispositions de l'article 9, §3 du RGPD selon lesquelles « les données à caractère personnel relatives à la santé peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents ».
40. Pour garantir la confidentialité et la sécurité du traitement de données, tout organisme qui conserve, traite ou communique des données à caractère personnel est tenu de prendre des mesures dans les onze domaines d'action suivants liés à la sécurité de l'information: politique de sécurité; désignation d'un délégué à la protection des données; organisation et aspects humains de la sécurité (engagement de confidentialité du personnel, information et formations régulières du personnel sur le thème de la protection de la vie privée et sur les règles de sécurité); sécurité physique et de l'environnement; sécurisation des réseaux; sécurisation logique des accès et des réseaux; journalisation, traçage et analyse des accès; surveillance, revue et maintenance; système de gestion des incidents de sécurité et de la continuité (systèmes de tolérance de panne, de sauvegarde, ...); documentation.
41. Le Comité constate que la Plate-forme eHealth dispose d'un délégué à la protection des données et satisfait à ces exigences de sécurité de l'information.
42. Le Comité rappelle que les collectivités, qu'elles soient sous la responsabilité de l'Etat fédéral ou des entités fédérées (Communautés et Régions), doivent se conformer aux dispositions 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* et de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.
43. Le Comité de sécurité de l'information tient à rappeler à l'adresse de Sciensano ainsi que du médecin de référence d'une collectivité ou, à défaut, du responsable administratif de cette collectivité, ainsi que des entités fédérées, les dispositions de 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, selon lesquelles le responsable du traitement prend les mesures supplémentaires suivantes lors du traitement de données génétiques, biométriques ou des données concernant la santé :

1° les catégories de personnes ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées;

2° la liste des catégories des personnes ainsi désignées est tenue à la disposition de l'autorité de contrôle compétente par le responsable du traitement ou, le cas échéant, par le sous-traitant;

3° il veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

Par ces motifs,

la chambre sécurité sociale et santé du comité de sécurité de l'information

vu l'arrêté royal n°44 du 26 juin 2020 concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus COVID-19 sur la base d'une base de données auprès de Sciensano,

autorise, en vertu des articles 5, 5° et 11 de la loi du 21 août 2008 *relative à la création et à l'organisation de la Plate-forme eHealth*, la création d'une base de données à caractère personnel relatives aux médecins de référence ou aux responsables administratifs des collectivités au sein de la Plate-forme eHealth,

autorise, la communication des données à caractère personnel telle que décrite dans la présente délibération moyennant le respect des mesures de protection de la vie privée qui ont été définies, en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information.

Bart VIAENE

Le siège de la chambre sécurité sociale et santé du comité de sécurité de l'information est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante : Quai de Willebroeck, 38 - 1000 Bruxelles (tél. 32-2-741 83 11).