

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

CSI/CSSS/20/314

DÉLIBÉRATION N° 20/132 DU 3 MAI 2020, MODIFIÉE LE 13 MAI 2020, LE 2 JUIN 2020 ET LE 7 JUILLET 2020, RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PAR DIVERS PRESTATAIRES DE SOINS OU ORGANISATIONS ACTIVES DANS LE DOMAINE DE LA SANTÉ OU DES SOINS À SCIENSANO ET À LEUR COMMUNICATION ULTÉRIEURE DANS LE CADRE DE LA LUTTE CONTRE LA PROPAGATION DU CORONAVIRUS COVID-19

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

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, en particulier l'article 15, § 1^{er} ;

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

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 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* ;

Vu la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, notamment l'article 42, §2, 3°;

Vu la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*, notamment l'article 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 la demande de Sciensano visant à obtenir une autorisation;

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

Vu le rapport de monsieur Bart Viaene.

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

I. OBJET DE LA DEMANDE

1. Sciensano est une institution scientifique de l'Etat fédéral belge, qui a été créée par la loi du 25 février 2018 portant création de Sciensano. Elle a pour principale mission de réaliser des études scientifiques en vue de soutenir la politique de la santé. Sciensano fournit également une expertise et des services d'intérêt public dans le domaine de la santé publique.
2. En vertu 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* (ci-après l'arrêté royal n° 44 du 26 juin 2020) , sont créées la Base de données I, gérée par Sciensano, et les Bases de données III¹ et IV², gérées par les autorités régionales compétentes ou les agences désignées par les autorités compétentes, dans le cadre de la lutte contre la propagation du coronavirus COVID-19.
3. La Base de données I contient des données à caractère personnel que les prestataires de soins et les établissements de soins communiquent à Sciensano. Toutefois, aux fins énoncées dans le présent arrêté, il sera également nécessaire que le personnel des centres de contact (y compris les chercheurs sur le terrain) et les équipes mobiles partagent avec la Base de données I les données qu'ils ont recueillies. Ensuite, un échange de données entre les Bases de données I et III est prévu, le cas échéant également avec la Base de données IV. Ces deux dernières Bases de données ont été créées en vue de l'échange de données avec les services d'inspection sanitaire régionaux, les équipes mobiles et/ou les centres de contact désignés par les agences compétentes.
4. Ces catégories de données à caractère personnel recueillies dans le cadre de l'arrêté royal n° 44 du 26 juin 2020 concernent des données d'identification et de contact, des données de tests, des prescriptions, des résultats de CT-scans, des diagnostics présumés de personnes, d'une part, et des données de personnes infectées ou de personnes pour lesquelles il existe un soupçon sérieux d'infection ainsi que les patients hospitalisés avec un diagnostic confirmé du coronavirus auprès des hôpitaux, d'autre part. Nombre de ces données sont collectées par les laboratoires, les centres de triage, les hôpitaux et les médecins, les MCC (médecins

¹ La base de données contenant les demandes d'appel et les demandes pour le personnel du centre de contact.

² La base de données contenant les coordonnées des collectivités.

coordinateurs et conseillers) dans les collectivités (par exemple, les maisons de repos et de soins, les centres d'asile et les prisons).

5. Dans un premier temps, sont recueillies les données à caractère personnel décrites dans l'arrêté royal n° 44 du 26 juin 2020 relatives aux personnes pour lesquelles un test médical a été prescrit, qui ont subi un test ou pour lesquelles un test n'était pas possible mais pour lesquelles le médecin considère un diagnostic positif comme fort probable, notamment;

- le numéro d'identification visé à l'article 8, § 1^{er}, 1° ou 2°, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale;
- le nom & le prénom du patient;
- le sexe;
- la date de naissance & le statut vital (date de décès);
- la rue et le numéro de la maison;
- le code postal du domicile;
- la date d'apparition des symptômes ;
- le type, la date, le numéro de l'échantillon et le résultat du test ou le diagnostic présumé en l'absence de test;
- le service hospitalier, le numéro d'identification et les coordonnées de l'hôpital, si la personne concernée est hospitalisée ;
- le résultat du CT-scan, si la personne concernée est hospitalisée ;
- le numéro INAMI du médecin prescripteur et, si d'application, le numéro INAMI du médecin qui a décidé d'annuler un test négatif ;
- les informations de contact (numéros de téléphone et adresse électronique) de la personne concernée et du représentant légal ou, en cas d'urgence, de la personne à contacter;
- la relation avec le représentant légal ou, en cas d'urgence, avec la personne à contacter (p.ex. partenaire, parent, tuteur, administrateur, ...);
- des informations facilitant le contact (p.ex. langue) ;
- l'exercice ou non de la profession de prestataire de soins;
- la collectivité dont la personne fait partie ou avec laquelle elle est entrée en contact: par exemple, école, lieu de travail, centre d'asile, prison, centre de services de soins, institution pour personnes handicapées, accueil pour enfants, centre de rééducation, hôpital psychiatrique, caserne, autres.

6. Sont ensuite enregistrées les données à caractère personnel décrites dans l'arrêté royal n° 44 du 26 juin 2020 concernant les personnes avec lesquelles le patient est entré en contact, qui sont communiquées par le centre de contact après avoir contacté les personnes concernées, notamment:

- le numéro d'identification visé à l'article 8, § 1^{er}, 1° ou 2°, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale;
- le nom et le prénom;
- l'adresse;
- le sexe;
- la date de naissance et le cas échéant la date de décès;
- les données de contact, en ce compris le numéro de téléphone et l'adresse électronique ;
- d'autres informations facilitant le contact (p.ex. langue et code postal) ;

- des informations permettant d'évaluer les risques de contamination : p.ex. date d'apparition et type de symptômes, application de mesures préventives, suivi des conseils (p.ex. consultation d'un médecin), déplacements, ;
- la collectivité dont la personne fait partie ou avec laquelle elle est entrée en contact : p.ex. école, lieu de travail, centre d'asile, prison, maison de repos et de soins, institution pour personnes handicapées, garderie, centre de réadaptation, hôpital psychiatrique, autre.
- le lien entre le patient et les personnes avec lesquelles il est entré en contact (p.ex. colocataire) ;
- des informations permettant de suivre le statut, la nature et le résultat des prises de contact ;
- l'utilisation ou non d'une application de traçage de contacts.

7. La communication des fournisseurs de données (laboratoires, médecins généralistes, MCC & hôpitaux) à la banque de données centrale se compose de quatre types de messages pouvant contenir les données à caractère personnel précitées. Ces types de messages sont les suivants:
- prescription de test de laboratoire;
 - résultat du test de laboratoire;
 - réévaluation du test de laboratoire par le médecin (dans le cadre de résultats faux positifs);
 - cas suspects dans lesquels aucun test n'a été réalisé (par exemple, suite à un refus ou un décès).

Ces messages sont envoyés de manière cryptée au moyen d'un eFORM qui est disponible dans certains logiciels médicaux. Les données enregistrées dans l'eForm seront converties en un fichier csv qui sera ensuite envoyé via la eHealthBox à la banque de données centrale. Si un eForm ne constitue pas une option pour le fournisseur de données concerné, il pourra directement transmettre un fichier json ou un fichier cvs via la eHealthBox. Par ailleurs, Sciensano prévoit aussi la possibilité d'envoyer des fichiers directement via le serveur SFTP. Ce n'est que lorsque les autres solutions ne sont pas possibles que le fournisseur de données aura la possibilité de charger manuellement les fichiers csv sur une page HTTPS au moyen d'un compte et d'un mot de passe.

La banque de données COVID-19 pourra appeler, grâce au service ConsultRN de la plateforme eHealth, le registre national et les registres Banque Carrefour afin d'obtenir, de cette manière, les données les plus exactes possibles concernant a) les patients et b) les personnes avec lesquelles le patient a été en contact. Le numéro de registre national de ces personnes permet de faire appel au service web IdentifyPerson auprès du registre national pour obtenir des données démographiques relatives à ces personnes ainsi que les mises à jour de ces données. Il s'agit à cet égard des données suivantes: le nom, le prénom, le sexe, l'adresse, la date de naissance & la date de décès.

Sciensano a également demandé au ministre de l'Intérieur l'accès aux données du registre national, en vue de la création et de la gestion d'une banque de données dans le cadre de la crise de santé sanitaire liée au COVID-19 et de la lutte contre sa propagation. Etant donné que l'organisation est également confrontée à des personnes qui ne sont pas inscrites au registre national ou dont toutes les données à caractère personnel nécessaires ne sont pas systématiquement mises à jour dans le registre national, elle demande, pour la même finalité, un accès aux mêmes données à caractère personnel dans les registres Banque Carrefour, visés

à l'article 4 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, pour autant que ces données soient disponibles.

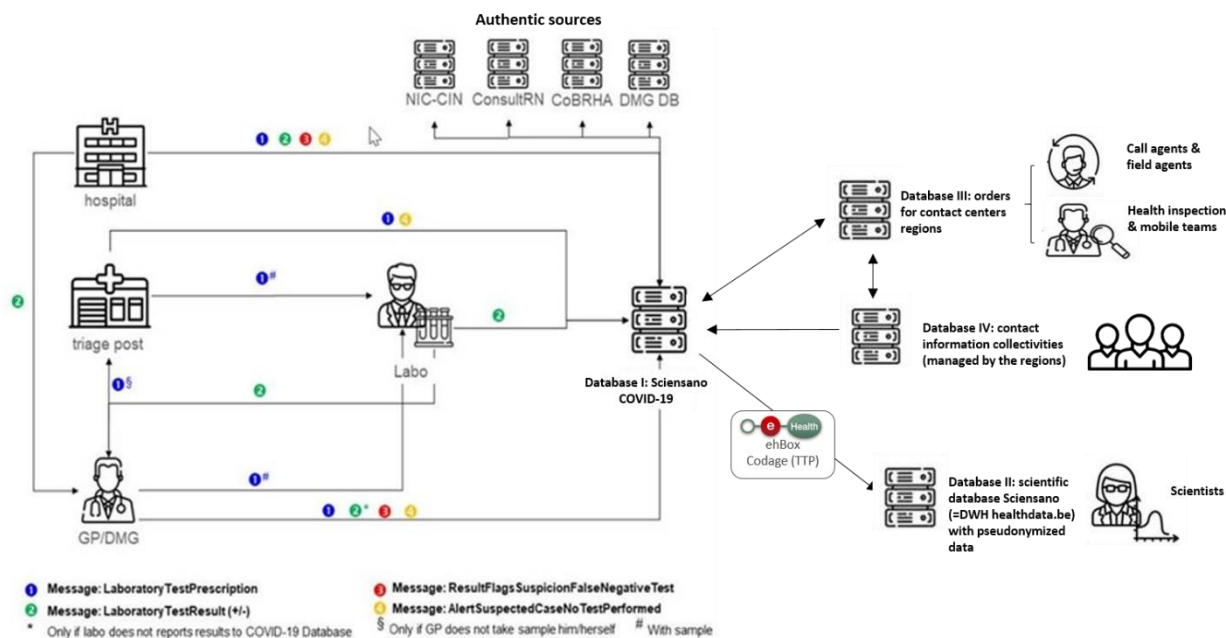
Dans la mesure où le ministre de l'Intérieur accède à la demande de Sciensano et autorise effectivement l'accès au registre national, Sciensano peut aussi accéder aux registres Banque Carrefour. Par sa délibération n° 12/13 du 6 mars 2012, le Comité sectoriel de la sécurité sociale et de la santé jadis compétent a, en effet, jugé qu'il semblait légitime et opportun que des instances soient autorisées à accéder aux registres Banque Carrefour dans la mesure où elles répondent aux conditions d'accès au registre national et aussi longtemps qu'elles y satisfont. Dans cette délibération, il a aussi fixé le cadre général pour l'accès aux registres Banque Carrefour dans le chef des instances qui ont accès au Registre national. L'accès aux registres Banque Carrefour intervient, le cas échéant, dans le respect de la décision du ministre de l'Intérieur relative à l'accès au registre national et des mesures de protection des données définies dans la délibération précitée n° 12/13 du 6 mars 2012.

Par ailleurs, la banque de données pourra aussi faire appel à la source authentique CoBRHA pour obtenir des données d'identification exactes relatives aux médecins et établissement de soins concernés. La source authentique DMG DB qui peut être consultée par les utilisateurs de la banque de données permet, en cas de présomptions d'infection sans test ou dans des situations d'urgence dans lesquelles il n'est pas possible de joindre une personne, d'identifier le médecin généraliste.

Dans le cadre du *contact tracing* prévu, les centres de contact prendront contact avec les personnes chez qui le médecin présume une infection et les personnes dont le test médical était positif et ils s'informeront auprès de ces personnes de leurs fréquentations physiques avec d'autres personnes au cours d'une période déterminée. Ces dernières seront alors contactées à leur tour afin de leur fournir des conseils adéquats quant aux actions à prendre. L'objectif de ce système est d'avertir les personnes qui ont été en contact avec des personnes (potentiellement ou effectivement) infectées, de sorte que ces personnes puissent elles-mêmes se protéger et prendre les mesures visant à protéger les autres personnes (par exemple auto-isolement). Ceci devrait permettre d'éviter une résurgence de la propagation du coronavirus Covid-19 et de réagir instantanément à tout nouveau foyer de contamination lorsque les mesures de confinement seront progressivement levées. Un problème peut toutefois surgir lorsque le centre de contact ne dispose pas du numéro de téléphone ou de l'adresse e-mail corrects pour une personne qu'il doit contacter en tant que personne (potentiellement ou effectivement) infectée ou pour une personne ayant été en contact avec une personne atteinte du Covid-19. Dans ce cas, il serait fait appel, à l'intervention du Collège intermutualiste national, au numéro de téléphone ou à l'adresse électronique dont disposent les organismes assureurs dans le cadre des contacts avec leurs membres. Ceci signifie que les organismes assureurs communiquent à Sciensano le numéro de téléphone ou l'adresse e-mail – sur la base évidemment d'un strict minimum de données à caractère personnel d'identification des intéressés (telles que leur nom et prénom et/ou domicile). Dans les listes d'appels à effectuer par le centre de contact, Sciensano peut alors inclure ce numéro de téléphone ou cette adresse e-mail, de sorte que les intéressés puissent être contactés.

Les organismes assureurs communiquent dès lors les données mentionnées à Sciensano de sorte que leurs membres puissent, le cas échéant, être contactés par les centres de contact.

Cette communication s'inscrit dans le cadre des missions des organismes assureurs d'octroi d'aide, d'information, de guidance et d'assistance en vue de promouvoir le bien-être physique de leurs membres, telles que visées dans la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités.



La base de données I de Sciensano transmet via serveur SFTP les données nécessaires à la base de données III des régions de sorte que leur centre de contact puisse, sur base des ordres d'appels, contacter les patients avec un diagnostic confirmé ou présumé et/ou en cas d'urgence leurs personnes de contact. Le centre de contact fournit, à son tour, à la Base de données I via serveur SFTP les données de contact des personnes avec lesquelles le patient a été en contact ainsi que d'autres informations concernant l'exécution et le suivi de la mission du centre de contact. Ces informations complétées peuvent ensuite être reprises dans le nouveau flux des ordres d'appel. Les services d'inspection sanitaire et les équipes mobiles des régions ont également recours à cet échange entre la Base de données I et la Base de données III. Via un transfert de la Base de données I à la Base de données III, ils obtiennent les informations nécessaires en provenance des acteurs de soins et du centre de contact pour l'exécution de leurs missions en matière de lutte contre la propagation des effets néfastes causés par les maladies infectieuses. A l'inverse, les services d'inspection régionaux ou leurs équipes mobiles recueilleront des données complémentaires des personnes appartenant à un cluster au sein de la banque de données III et échangeront ces informations avec la Base de données I de sorte à pouvoir intégrer ces informations complémentaires dans les nouveaux ordres d'appels pour les centres de contact.

Etant donné que les personnes avec un diagnostic confirmé ou présumé de COVID-19 peuvent faire partie d'une collectivité (p.ex. établissement d'enseignement, maison de repos et de soins, ...), il est important, dans le contexte du danger de contamination, de pouvoir contacter un médecin de référence ou un responsable administratif de cette collectivité. Pour

faciliter ces contacts, les régions se chargeront de la gestion d'une Base de données contenant les données de contact des collectivités (= banque de données IV dans le schéma) qui sera partagée avec la Base de données I dans le cadre des ordres d'appels.

En ce qui concerne le volet scientifique, les données de la base de données COVID-19 seront envoyées via l'eHealthbox Codage vers le datawarehouse de healthdata.be (= la Base de données II dans le schéma) de sorte qu'elles soient conservées sous forme pseudonymisée à des fins de recherche épidémiologique.

8. En ce qui concerne la banque de données, une gestion des utilisateurs et des accès en cascade est installée, ce qui permet de garantir que seule un nombre limité de collaborateurs de Sciensano aura accès aux informations les plus sensibles. Ces collaborateurs sont tenus contractuellement de respecter strictement le secret professionnel par la signature d'un accord de confidentialité lors de l'entrée en service et de traiter les données d'une manière déontologique et éthique. Dans la banque de données, un logiciel a été installé qui permet de surveiller et de protéger en temps réel l'activité de la banque de données. Ce logiciel d'audit permet de créer des loggings qui enregistrent de manière permanente tout utilisateur, accès, période d'accès, activité et résultat de cette activité et les rendent consultables. Pour les transferts de données provenant de la banque de données, des traces seront également conservées concernant la date et l'heure des transferts de données, le contenu du transfert et l'identification des destinataires. En ce qui concerne l'utilisation des serveurs SFTP et la page HTTPS, un système adéquat d'accès et d'utilisation est mis au point afin d'identifier les acteurs autorisés à y accéder.

II. COMPÉTENCE

9. Le Comité a pris connaissance de l'arrêté royal n° 44 du 26 juin 2020 et rend une délibération pour la durée déterminée dans cet arrêté.
10. En vertu de l'article 11, § 1^{er}, du présent arrêté, la chambre sécurité sociale et santé du Comité de sécurité de l'information est compétente pour rendre une délibération, tant pour la communication de données à caractère personnel à Sciensano en vue du traitement dans la Base de données I que pour la communication ultérieure de ces données à caractère personnel par Sciensano à des tiers, dans la mesure où cela n'est pas repris dans le présent arrêté. À l'exception de ce qui précède, la chambre sécurité sociale et santé du Comité de sécurité de l'information ne délibère sur les communications à ou par la Base de données I de Sciensano que dans la mesure où elles servent les fins visées à l'article 3 du présent arrêté, sans qu'elle puisse déterminer elle-même une autre fin³. En outre, la chambre sécurité sociale et santé du Comité de sécurité de l'information peut préciser, pour chaque finalité de traitement définie à l'article 3, quelles données à caractère personnel spécifiques peuvent être traitées dans le

³ Art. 11, § 2, 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 (ci-après : AR n° 44 du 26 juin 2020).

cadre d'une certaine catégorie de données à caractère personnel et qui sont communiquées à l'une des Bases de données II, III ou IV ou qui doivent être communiquées à partir de la Base de données IV à la Base de données I, dans la mesure où cela est utile pour atteindre la finalité du traitement en question⁴

11. En vertu de l'article 42, § 2, 3° de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, la chambre sécurité sociale et santé du Comité de sécurité de l'information est compétente pour rendre une délibération de principe concernant toute communication de données à caractère personnel relatives à la santé.
12. L'article 11 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la Plate-forme eHealth dispose que 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.
13. En application de l'article 15, § 1^{er}, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, la communication de données à caractère personnel par les institutions de sécurité sociale (telles que le Collège intermutualiste national et les organismes assureurs) à des tiers (tels que les centres de contact précités) requiert en principe une délibération préalable de la chambre sécurité sociale et santé du Comité de sécurité de l'information.
14. Le comité s'estime dès lors compétent pour se prononcer sur la présente demande d'autorisation.

III. EXAMEN

A. ADMISSIBILITÉ

15. 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, §1^{er}, du RGPD est remplie. Ceci est notamment le cas lorsque le traitement est nécessaire à une obligation légale à laquelle le responsable du traitement est soumis.
16. Le traitement de données à caractère personnel relatives à la santé est en principe interdit. Conformément à l'article 9, 2, i) du RGPD, l'interdiction ne s'applique cependant pas lorsque le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel. C'est le cas en l'espèce.

Conformément à l'article 9, 2, j) du RGPD, l'interdiction ne s'applique pas non plus lorsque le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de

⁴ Art. 11, § 3, de l'AR n° 44 du 26 juin 2020.

recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

17. Le Comité estime par conséquent qu'il existe un fondement pour le traitement des données à caractère personnel relatives à la santé envisagé.

B. FINALITÉ

18. L'article 5 du RGPD autorise le traitement de données à caractère personnel uniquement pour des finalités déterminées, explicites et légitimes.

19. En vertu de l'article 2 de l'arrêté royal n° 44 du 26 juin 2020, sont créées la Base de données I, gérée par Sciensano, ainsi que les Bases de données III et IV, gérées par autorités régionales compétentes ou par les agences désignées par les autorités régionales compétentes, dans le cadre de la lutte contre la propagation du coronavirus COVID-19.

20. Étant donné que la détection des infections par le coronavirus Covid-19 relève de la compétence des Communautés, la création d'une banque de données centrale s'avère nécessaire compte tenu de la mobilité des citoyens entre les différentes entités fédérées. Par ailleurs, la collecte et l'échange de données servent à identifier précocement et à contacter les personnes infectées par le coronavirus Covid-19 ou pour lesquelles il existe un sérieux soupçon d'infection, afin de leur prodiguer les recommandations nécessaires pour éviter que ces personnes n'infectent d'autres personnes. Cette collecte et cet échange de données servent ensuite à contacter les personnes avec lesquelles les personnes infectées ou suspectées d'être infectées ont été en contact pour fournir des consignes en matière d'hygiène et de prévention, pour proposer une quarantaine et/ou pour les inviter à subir un test de dépistage du coronavirus Covid-19 et son suivi ultérieur. Afin d'atteindre ces finalités de traitement, un échange de données entre les Bases de données I et III est prévu, le cas échéant également avec la Base de données IV.

21. En outre, un échange de données est prévu entre la Base de données I et les équipes mobiles, ainsi que les services d'inspection sanitaire, afin de permettre à ces équipes et services d'exercer correctement les tâches leur confiées, à savoir identifier et détecter des foyers et clusters de Covid-19 et adopter des mesures sur place pour contenir les foyers et clusters de Covid-19. Enfin, la Base de données I fournit des données pseudonymisées à la banque de données qui existe déjà auprès de Sciensano et qui est utilisée à des fins d'étude scientifique (Base de données II). Ceci doit permettre aux institutions de recherche d'effectuer des études scientifiques ou statistiques sur la lutte contre la propagation du coronavirus Covid-19 et/ou de soutenir la politique de lutte contre ce virus.

22. Le Comité estime que le traitement de données à caractère personnel envisagé poursuit effectivement des finalités déterminées, explicites et légitimes.

C. PROPORTIONNALITÉ

23. L'article 5 du RGPD dispose que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.
24. Sciensano justifie le traitement des données à caractère personnel par finalité comme suit:

Finalité traçage des contacts par le centre de contact (destinataire des données = collaborateurs du centre de contact)

- NISS du patient ou des personnes avec lesquelles il/elle est entrée en contact: identification unique des patients et établissement du lien entre les données recueillies et les sources authentiques ;
- Nom, prénom, adresse (électronique), numéros de téléphone, date de naissance, sexe et informations facilitant le contact (p.ex. langue) du patient ou des personnes avec lesquelles le patient a été en contact: données en vue de faciliter les prises de contact afin d'obtenir des informations pour le traçage des contacts ;
- Nom, prénom et numéro de téléphone du représentant légal ou de la personne de contact du patient à contacter en cas d'urgence et sa relation avec le patient (p.ex. partenaire, parent, tuteur, administrateur, ...) : données en vue de faciliter les prises de contact du patient afin d'obtenir des informations pour le traçage des contacts ;
- Date de décès: nécessaire pour éviter que le call center ne contacte des personnes qui sont entre temps décédées ;
- Le diagnostic présumé d'infection par le coronavirus Covid-19 ; si le résultat du test n'a pas permis d'établir une contamination, l'éventuelle décision d'annulation prise par un médecin ; le résultat du test ; données facilitant l'entretien avec le patient indice ;
- Collectivité dont le patient fait partie ou avec laquelle il est entré en contact et données de contact du médecin de référence ou du responsable administratif de la collectivité: nécessaire à l'évaluation du contexte des risques de contamination en vue du traçage des contacts ;
- Date d'apparition et type de symptômes, application des règles d'hygiène, suivi des conseils (p.ex. consultation d'un médecin, isolement, distanciation sociale), informations sur les déplacements, etc. : informations nécessaires pour l'évaluation du risque de contamination et l'organisation du suivi ;
- Les critères pertinents pour évaluer si le risque de contamination est faible ou élevé : informations nécessaires pour l'évaluation du risque de contamination et l'organisation du suivi ;
- Le simple fait qu'un contact ait eu lieu entre le patient et les personnes de contact, y compris le fait de faire partie du ménage du patient : informations nécessaires pour l'évaluation du risque de contamination et l'organisation du suivi ;
- L'indication de l'exercice ou non de la profession de prestataire de soins : informations nécessaires pour l'évaluation du risque de contamination et l'organisation du suivi ;
- Numéro, statut, résultat, durée des prises de contact avec le patient, avec son représentant légal ou sa personne de contact en cas d'urgence ou avec les personnes avec lesquelles il a été en contact par le centre de contact, le service d'inspection sanitaire et/ou les équipes mobiles : informations nécessaires pour le planning et le suivi des activités de traçage de contacts par les acteurs mandatés des régions ;

- L'utilisation ou non d'une application de traçage de contacts : informations utiles pour savoir si les personnes avec qui le patient a été en contact pourront être averties via l'application.

Finalité initiatives services d'inspection sanitaire & équipes mobiles (destinataire des données = services d'inspection de la santé & équipes mobiles des communautés)

- Numéro INAMI du médecin prescripteur ou du médecin qui a annulé un résultat de test négatif : identification unique du médecin afin d'obtenir, en cas d'urgence, des informations supplémentaires relatives aux données fournies lors de la prise de contact ;
- L'exercice ou non de la profession de prestataire de: variable fournissant des informations sur la propagation potentielle du virus au sein du secteur des soins et du secteur social) ;
- Numéro INAMI, service et localisation de l'hôpital: identification unique de l'hôpital afin d'obtenir, en cas d'urgence, des informations supplémentaires relatives aux données fournies lors de la prise de contact ou de permettre des actions préventives au niveau de santé à l'égard de l'hôpital ;
- Numéro INAMI du laboratoire : identification univoque du laboratoire permettant, le cas échéant, d'obtenir des informations complémentaires concernant les données fournies lors de la prise de contact ;
- Nom, prénom, adresse, numéro(s) de téléphone, date de naissance, langue et sexe du patient ou des personnes avec lesquelles il a été en contact : données permettant de faciliter la prise de contact avec le patient, traçage de personnes que l'on ne peut joindre et/ou suivi dans le cadre des mesures de prévention de la santé ;
- Données d'identification et de contact du représentant légal ou des personnes à contacter en cas d'urgence pour le patient ou des personnes avec lesquelles le patient est entré en contact: données permettant de faciliter la prise de contact, traçage de personnes que l'on ne peut joindre et/ou suivi dans le cadre des mesures de prévention de la santé ;
- Date de décès: informations nécessaires dans le cadre des actions de traçage des contacts et en vue du suivi de l'état de santé des groupes cibles concernés et des risques de contamination y liés.
- Collectivité dont la personne fait partie ou avec laquelle il est entré en contact et données de contact du médecin de référence ou du responsable administratif de la collectivité : nécessaire à l'évaluation de la nature des risques de contamination et des mesures de prévention requises ;
- Numéro, statut, résultat, durée des prises de contact avec le patient, avec son représentant légal ou sa personne de contact en cas d'urgence ou avec les personnes avec lesquelles il a été en contact par le centre de contact, le service d'inspection sanitaire et/ou les équipes mobiles : nécessaires pour le planning et le suivi des activités de traçage des contacts par les acteurs mandatés des régions ;
- Date d'apparition et type de symptômes, application des mesures d'hygiène, suivi des conseils (p.ex. consultation d'un médecin, isolement, distanciation sociale), informations sur les déplacements, etc. : informations nécessaires pour évaluer le risque de contamination, définir des actions préventives et organiser le suivi ;
- Les critères pertinents permettant d'évaluer si le risque de contamination est faible ou élevé : informations nécessaires pour évaluer le risque de contamination et organiser le suivi des contacts ;

- Données relatives aux tests de laboratoire & aux CT scans: nécessaire afin de pouvoir suivre le contenu, le timing et les résultats des tests dans le but d'entamer des mesures de prévention en matière de santé sur la base de connaissances objectives ;
- Données relatives à des présomptions d'infection (réévaluation des faux positifs et des cas sans test): nécessaires pour parvenir à une approche inclusive totale en matière de traçage des contacts et de prévention de la santé qui ne se limite pas aux cas confirmés ;
- L'utilisation ou non d'une application de traçage de contacts : informations utiles pour savoir si les personnes avec qui le patient a été en contact pourront être averties via l'application.

Finalité étude scientifique et d'appui à la politique (destinataire des données = épidémiologistes associés à Sciensano ou aux institutions de recherche qui reçoivent une autorisation du Comité de sécurité de l'information, chambre sécurité sociale et santé

- Numéro INAMI, service et localisation de l'hôpital: identification univoque de l'hôpital afin de pouvoir traiter des informations pertinentes relatives à la propagation des infections et à la prise en charge des patients COVID19 ;
- Numéro INAMI du laboratoire : identification univoque du laboratoire afin de pouvoir traiter des informations pertinentes sur la propagation des infections et les prestations médicales pour les patients atteints de COVID-19 ;
- Le numéro INAMI du médecin prescripteur ou du médecin qui a décidé d'annuler un résultat de test négatif : identification univoque des (cabinets de) médecins afin de pouvoir traiter des informations pertinentes sur la propagation des infections et les soins administrés aux patients atteints de COVID-19 ;
- L'exercice ou non de la profession de prestataire de soins et les contacts avec des groupes vulnérables : variable fournissant des informations sur la propagation potentielle du virus au sein du secteur de la santé et du secteur social (par exemple dans les maisons de repos et de soins et les institutions pour personnes handicapées) ;
- Numéros NISS pseudonymisés des patients ou des personnes avec lesquelles le patient est entré en contact: identification unique de personnes ainsi que la possibilité d'établir un lien avec d'autres banques de données si autorisation du Comité de sécurité de l'information ;
- Année de naissance, sexe, code postal et année et mois de décès du patient ou des personnes avec lesquelles le patient est entré en contact: ces données démographiques sont pertinentes pour les connaissances scientifiques et les statistiques d'appui à la politique concernant les groupes cibles dans lesquels le virus s'est ou non manifesté, les groupes cibles qui ont subi des tests, les entités géographiques où le virus est présent, etc.
- Le simple fait qu'un contact ait eu lieu entre le patient et les personnes de contact, y compris le fait de faire partie du ménage du patient : informations utiles pour mieux comprendre les clusters d'infections ;
- Type et code postal de la collectivité dont le patient fait partie: variable permettant d'acquérir des connaissances sur la propagation du virus ;
- Données relatives aux tests de laboratoire & aux CT scans (date du test, type de test, résultats) : acquisition de connaissances concernant l'utilisation de tests et d'examens en Belgique (notamment le nombre, les groupes atteints, les médecins-prescripteurs) ;
- Données relatives à des présomptions d'infection (réévaluation des faux positifs et des cas sans test): nécessaires afin de disposer des informations les plus complètes possibles

pour des activités scientifiques et d'appui à la politique qui ne se limite pas aux seuls cas confirmés ;

- Données communiquées au centre de contact, y compris symptômes, date d'apparition des premiers symptômes, déplacements, respect des mesures d'isolement et d'hygiène : données nécessaires pour comprendre la propagation de COVID-19 à la lumière des signaux médicaux et du comportement ;
- Données relative à la prise de contact, y compris la date du ticket du centre de contact et le résultat général de la prise de contact sous forme d'un code : nécessaire pour l'évaluation scientifique et d'appui à la politique du traçage des contacts.
- Données relatives à l'évaluation du risque de contamination des personnes avec lesquelles le patient a été en contact (e.a. distance physique) : nécessaire pour comprendre la propagation du virus.

25. En outre, il est absolument nécessaire d'enregistrer le numéro d'identification de la sécurité sociale, en vue d'une identification univoque des patients et de l'établissement d'un lien avec les données collectées.
26. Les données à caractère personnel ne peuvent être conservées sous une forme permettant l'identification des personnes concernées au-delà du délai nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement.
27. La suppression de données à caractère personnel dans les Bases de données I, II, III et IV intervient conformément aux dispositions de l'arrêté royal n° 44 du 26 juin 2020. En toute hypothèse, les données à caractère personnel reçues sont supprimées par le responsable du traitement dans un délai de cinq jours à compter du jour où le présent arrêté cesse de produire ses effets, à savoir au plus tard le 20 octobre 2020. À cet égard, les données pertinentes restantes sont tout d'abord transférées au datawarehouse de la plateforme healthdata-be via le service eHealthbox Codage, de sorte à garantir la disponibilité des données pseudonymisées à des fins scientifiques. La suppression des données a aussi trait à l'ensemble des back-ups et peut aussi être contrôlée au moyen d'audits.
28. Compte tenu de l'objectif, le Comité estime que le traitement de ces données à caractère personnel est en principe adéquat, pertinent et non excessif.

D. TRANSPARANCE

29. Conformément à l'article 14 du RGPD, le responsable du traitement fournit les informations nécessaires à la personne concernée lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée. Cette disposition ne s'applique cependant pas, notamment lorsque la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles.
30. Sciensano en tant que responsable du traitement des Bases de données I et II et les autorités régionales compétentes ou les agences désignées par les autorités compétentes, chacune pour

sa compétence, en tant que responsables des Bases de données III et IV, mettent en œuvre les mesures appropriées, pour que les personnes concernées reçoivent les informations visées aux articles 13 et 14 du RGPD et les communications visées aux articles 15 à 22 inclus et à l'article 34 du RGPD en ce qui concerne les finalités de traitement visées à l'article 3 de l'arrêté royal n° 44 du 26 juin 2020, sous une forme concise, transparente, compréhensible et facilement accessible, dans un langage simple et clair. Par ailleurs, Sciensano gère et assure la maintenance d'un système pour l'exercice des droits prévus aux articles 15 à 22 inclus et à l'article 34 du Règlement Général sur la Protection des Données.

31. Sciensano créera ensuite et tiendra à jour une page web sur laquelle seront publiées des informations adéquates conformément à l'article 14 du RGPD et les données de contact du délégué à la protection des données. Cette page web permet aux différents sujets de données (patients, personnes qui ont été en contact avec le patient et les prestataires de soins) de trouver des renseignements sur le traitement des données ainsi que sur leurs droits dans le cadre de la banque de données.

Enfin, 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.

E. MESURES DE SÉCURITÉ

32. En vertu de 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. 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.
33. Le Comité attire explicitement l'attention sur les dispositions du Titre 6. Sanctions de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui prévoient des sanctions administratives et pénales sévères dans le chef du responsable du traitement et des sous-traitants pour la violation des conditions prévues dans le RGPD et la loi du 30 juillet 2018 précitée.
34. Le Comité souligne par ailleurs que l'article 458 du Code pénal est d'application aux collaborateurs du centre de contact, ainsi qu'aux responsables administratifs des collectivités, qui sont contactés le cas échéant.

« Art. 458. Les médecins, chirurgiens, officiers de santé, pharmaciens, sages-femmes et toutes autres personnes dépositaires, par état ou par profession, des secrets qu'on leur confie, qui, hors le cas où ils sont appelés à rendre témoignage en justice ou devant une commission d'enquête parlementaire et celui où la loi, le décret ou l'ordonnance les oblige ou les autorise à faire connaître ces secrets, les auront révélés, seront punis d'un

emprisonnement d'un an à trois ans et d'une amende de cent euros à mille euros ou d'une de ces peines seulement. »

- 35.** Les données à caractère personnel relatives à la santé peuvent uniquement être traitées sous la surveillance et la responsabilité d'un professionnel des soins de santé. Même si cela n'est pas strictement requis par le RGPD, le Comité estime qu'il est préférable que de telles données soient traitées sous la responsabilité d'un médecin. Ce qui est le cas en l'espèce. Le Comité rappelle que lors du traitement de données à caractère personnel, le professionnel des soins de santé ainsi que ses préposés ou mandataires sont soumis au secret.
- 36.** En vertu de l'article 89, § 1^{er}, du RGPD, le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est soumis, conformément au RGPD, à des garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties garantissent la mise en place de mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données.

Le Comité rappelle également que dans le cadre du traitement à des fins scientifiques, le responsable du traitement doit respecter les dispositions du titre 4 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

- 37.** Les données à caractère personnel sont, toujours après pseudonymisation, communiquées par Sciensano aux épidémiologistes associés au COVID19 Risk Assessment Group à des fins d'étude scientifique, statistique et/ou d'appui à la politique. Conformément à l'article 5 du RGPD, les données à caractère personnel peuvent 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 ou pour lesquelles elles sont traitées ultérieurement. Le Comité estime que les données peuvent être conservées par Sciensano sous forme pseudonymisée pendant une période de 30 ans à compter du décès du patient. À l'issue de cette période, elles peuvent uniquement être conservées sous forme anonyme, c'est-à-dire sous une forme qui ne permet pas de les mettre en relation avec une personne identifiée ou identifiable.
- 38.** Le Comité souligne que les résultats du traitement à des fins scientifiques ne peuvent pas être publiés sous une forme qui permet l'identification de la personne concernée.
- 39.** Le Comité rappelle enfin qu'en vertu 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, 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

conclut

- que les organismes assureurs sont autorisés à communiquer à Sciensano le numéro de téléphone ou l'adresse électronique sur la base d'un minimum de données personnelles d'identification des personnes concernées communiquées (telles que leur nom et prénom et/ou leur domicile), de sorte que leurs membres puissent, le cas échéant, être contactés par le centre de contact.

- que la communication des données à caractère personnel telle que décrite dans la présente délibération est autorisée 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

<p>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).</p>
--