

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

CSI/CSSS/22/086

DÉLIBÉRATION N° 21/148 DU 26 AOÛT 2021, MODIFIÉE LE 28 SEPTEMBRE 2021 ET LE 25 JANVIER 2022 RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PAR L'OFFICE NATIONAL DE SÉCURITÉ SOCIALE ET VACCINET+ À LA PLATE-FORME EHEALTH EN VUE DE DÉTERMINER LE TAUX DE VACCINATION CONTRE LA COVID-19 DES TRAVAILLEURS DES ÉTABLISSEMENTS DE SOINS

Le Comité de sécurité de l'information,

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 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 le Règlement (UE) n° 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 RGPD);

Vu la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant dispositions diverses*;

Vu la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, en particulier l'article 42, § 2, 3°, modifié par la loi du 5 septembre 2018;

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, notamment l'article 37;

Vu la demande du Centre fédéral d'expertise des soins de santé;

Vu les rapports d'auditorat conjoints de la Banque Carrefour de la sécurité sociale et de la Plate-forme eHealth;

Vu le rapport de monsieur Bart Viaene;

Émet, après délibération, la décision suivante, le 25 janvier 2022:

I. OBJET DE LA DEMANDE

1. Le Centre fédéral d'expertise des soins de santé introduit une demande visant à obtenir une délibération du Comité de sécurité de l'information afin de permettre à la Plate-forme eHealth de traiter des données à caractère personnel de travailleurs des établissements de soins provenant de l'Office national de sécurité sociale et de Vaccinnet+, en vue de la détermination et de la publication (anonymes) du taux de vaccination contre la Covid-19 par établissement de soins et par groupe d'âges (quatre groupes au total: (moins de) 34 ans, entre 35 et 44 ans, entre 45 et 54 ans, 55 ans ou plus). La publication serait effectuée par le Centre fédéral d'expertise des soins de santé et les diverses entités fédérées.
2. L'analyse du taux de vaccination dans les établissements de soins (par groupe d'âges) permet de comprendre l'attitude du personnel vis-à-vis de la vaccination et également d'identifier les lacunes éventuelles dans les programmes de vaccination. Par ailleurs, la publication du taux de vaccination (anonyme) promeut la transparence. Les organisations seront également encouragées à publier leurs informations, d'une manière transparente, sur leur propre site web et dans leur communication.
3. Pour déterminer le taux de vaccination (anonyme) du personnel des établissements de soins, plusieurs données à caractère personnel du réseau de la sécurité sociale seront traitées. L'Office national de sécurité sociale réalisera, sur la base de son répertoire des employeurs et de quelques données à caractère personnel de la DMFA du deuxième trimestre de 2021, une sélection des organisations concernées, au moyen de la Commission paritaire compétente, de la catégorie employeurs et du code NACE. Une liste des numéros d'entreprise des unités d'établissement des établissements de soins sera ensuite transmise pour validation au Centre fédéral d'expertise des soins de santé. Ensuite, l'Office national de sécurité sociale recherchera, par unité d'établissement, l'identité des travailleurs et transmettra leur numéro d'identification de la sécurité sociale à la Plate-forme eHealth. La Plate-forme eHealth recherchera ensuite, par travailleur concerné, l'âge et le statut de vaccination dans la banque de données Vaccinnet+ et, mettra, par employeur (personne morale), quelques informations agrégées relatives aux travailleurs à la disposition du Centre fédéral d'expertise des soins de santé et des entités fédérées.
4. Ainsi, le Centre fédéral d'expertise des soins de santé et les entités fédérées disposeront, par établissement de soins (personne morale), du numéro d'entreprise, de la dénomination, du code commune, du code NACE et du secteur, données qui sont complétées pour chaque unité d'établissement par le numéro d'entreprise, la dénomination, le code commune, l'adresse, le code NACE, le nombre de travailleurs par groupe d'âges précité et le taux de vaccination par groupe d'âges précité (uniquement l'indication du pourcentage de personnes totalement vaccinées, du pourcentage de personnes partiellement vaccinées, du pourcentage de personnes ayant reçu une dose de rappel et du pourcentage de personnes non vaccinées, avec une distinction supplémentaire selon lequel il s'agit ou non d'un étudiant jobiste). Seules quatre catégories d'âges (suffisamment larges) seront utilisées (âgés (de moins) de 34 ans, entre 35 et 44 ans, entre 45 et 54 ans, 55 ans ou plus), ce qui empêche la réidentification des travailleurs. Le résultat final contient par conséquent des données anonymes au niveau de l'employeur,

c'est-à-dire des données qui, en aucune façon, ne peuvent être mises en relation avec des personnes physiques. Les employeurs concernés sont, sans distinction, des personnes morales. Chaque entité fédérée recevra uniquement les informations des établissements de soins situés sur son territoire de compétence.

II. COMPÉTENCE

5. Conformément à l'article 5 de l'accord de coopération du 12 mars 2021 entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française *concernant le traitement de données relatives aux vaccinations contre la COVID-19*, les données visées à l'article 3 peuvent uniquement être communiquées pour la réalisation des finalités énumérées à l'article 4 et, après délibération de la chambre sécurité sociale et santé du Comité de sécurité de l'information, aux instances chargées d'une mission d'intérêt public par ou en vertu d'une loi, d'un décret ou d'une ordonnance.
6. Conformément à l'article 5, 8°, de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la Plate-forme eHealth et portant dispositions diverses*, l'intervention de la Plate-forme eHealth en tant qu'organisation intermédiaire pour le couplage et le codage de données à caractère personnel requiert l'autorisation du Comité de sécurité de l'information.
7. La communication des données à caractère personnel par l'Office national de sécurité sociale à la Plate-forme eHealth, en vue de leur traitement ultérieur, doit faire l'objet d'une délibération préalable de la chambre sécurité sociale et santé du Comité de sécurité de l'information, conformément à l'article 15 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*.
8. Le Comité de sécurité de l'information estime par conséquent qu'il est compétent.

III. EXAMEN

A. ADMISSIBILITÉ

9. Le traitement de données à caractère personnelle 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 traitement; voir l'article 6, 1, alinéa 1^{er}, e), du RGPD.
10. 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.

11. La finalité décrite dans la présente délibération correspond à la finalité de traitement définie à l'article 4, § 2, point 6°, de l'accord de coopération du 12 mars 2021, à savoir déterminer le taux de vaccination anonyme de la population contre la COVID-19. Il y a lieu d'observer que le taux de vaccination contre la COVID-19 doit pouvoir être déterminé de manière granulaire (par exemple, dans les centres de services de soins avec une distinction entre le personnel soignant et les résidents) et que ceci n'est pas toujours possible sur la base de données anonymes ou à tout le moins de données à caractère personnel pseudonymisées dans le cas où l'anonymisation ne permettrait pas de réaliser la finalité visée¹.
12. Le Comité de sécurité de l'information estime par conséquent qu'il existe un fondement pour le traitement des données à caractère personnel relatives à la santé envisagé.

B. FINALITÉ

13. Conformément à l'article 5, b), du RGPD, le traitement de données à caractère personnel est uniquement autorisé pour des finalités déterminées, explicites et légitimes.
14. La finalité consiste à vérifier le taux de vaccination anonyme par établissement de soins et par catégorie d'âges et de publier ce taux. Ceci permet de savoir combien de membres du personnel dans les soins de santé se sont fait vacciner. L'analyse de ce taux de vaccination anonyme par établissement de soins et par groupe d'âges permet ensuite de comprendre l'attitude des membres du personnel par région et par catégorie d'âges vis-à-vis des vaccins et permettra d'identifier des lacunes dans les programmes de vaccination. Par ailleurs, la publication du taux de vaccination anonyme promeut la transparence.
15. Au vu de cet objectif, le Comité de sécurité de l'information considère que le traitement des données à caractère personnel envisagé poursuit bien des finalités déterminées, explicites et légitimes.
16. Ensuite, conformément à l'article 5, 1, b), du RGPD, le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales. L'utilisation des données de la DMFA sous forme anonyme, à des fins scientifiques ou en vue de l'établissement de statistiques, constitue par conséquent un usage compatible et autorisé en vertu du RGPD.

C. PROPORTIONNALITÉ

17. Conformément à l'article 5, b) et c), du RGPD, 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.

¹ Ces explications sont reprises dans le commentaire des articles: article 4 de l'accord de coopération du 12 mars 2021 entre l'Etat fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, la Commission communautaire commune, la Région wallonne et la Commission communautaire française *concernant le traitement de données relatives aux vaccinations contre la COVID-19*.

18. Le Centre fédéral d'expertise des soins de santé et les entités fédérées recevront de la Plate-forme eHealth uniquement des données agrégées des travailleurs, à savoir le nombre de travailleurs par groupe d'âges, le taux de vaccination par groupe d'âges (uniquement l'indication du pourcentage de personnes totalement vaccinées, du pourcentage de personnes partiellement vaccinées, du pourcentage de personnes ayant reçu une dose de rappel et du pourcentage de personnes non vaccinées) ainsi que l'indication selon laquelle le travailleur est un étudiant jobiste ou non. Les données seront affichées par établissement de soins (personne morale). Les diverses entités fédérées recevront uniquement des informations agrégées des établissements de soins de leur propre territoire pour publication.
19. L'analyse du taux de vaccination anonyme par établissement de soins et par groupe d'âges permet de comprendre l'attitude des membres du personnel par région et par catégorie d'âges vis-à-vis des vaccins et permet d'identifier des lacunes dans les programmes de vaccination. Des classes d'âges suffisamment larges seront utilisées (âgés (de moins) de 34 ans, entre 35 et 44 ans, entre 45 et 54 ans, 55 ans ou plus), ce qui empêche la réidentification des travailleurs. Les destinataires finals (le Centre fédéral d'expertise des soins de santé et les entités fédérées) reçoivent donc uniquement des données anonymes (données relatives aux employeurs-personnes morales identifiés dont les travailleurs ne peuvent pas être réidentifiés).
20. L'indication travail étudiant (étudiant / non étudiant) est nécessaire puisqu'un impact moindre de ce groupe sur le comportement de vaccination est attendu. Par ailleurs, par rapport aux travailleurs fixes, les étudiants travaillent plus souvent dans les liens d'un contrat de courte durée, de sorte que la rotation dans ce groupe est supérieure.
21. La Plate-forme eHealth détruit les listes de numéros d'identification de la sécurité sociale des travailleurs concernés, complétés par les informations précitées de l'Office national de sécurité sociale et de Vaccinnet+, sans tarder, après leur transformation en données anonymes. Pour autant que la Plate-forme eHealth en ait à nouveau besoin pour un traitement légitime complémentaire, elle s'adresse, moyennant une délibération préalable du Comité de sécurité de l'information, aux sources authentiques indiquées.
22. Compte tenu de l'objectif, le Comité de sécurité de l'information estime que le traitement de ces données à caractère personnel est en principe adéquat, pertinent et non excessif.

D. TRANSPARENCE

23. Conformément à l'article 12 du RGPD, le responsable du traitement doit prendre des mesures appropriées pour fournir toute information en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique.
24. Le responsable du traitement de données à caractère personnel, collectées à des fins déterminées, explicites et légitimes ou l'organisation intermédiaire doit, préalablement à la pseudonymisation des données, en principe communiquer certaines informations à la personne concernée. Le Centre fédéral d'expertise des soins de santé et les entités fédérées ne connaissent pas l'identité des travailleurs des établissements de soins, étant donné que

seules des données anonymes sont communiquées. La communication d'informations aux personnes concernées n'est par conséquent pas possible.

25. Le Comité de sécurité de l'information estime par conséquent que la demande répond aux exigences de transparence.

E. MESURES DE SÉCURITÉ

26. Conformément à l'article 5, f) du RGPD, le demandeur doit prendre toutes les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel. 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.
27. Pour garantir la confidentialité et la sécurité du traitement des données à caractère personnel, toute organisation qui conserve, traite ou communique des données à caractère personnel est tenue de prendre des mesures dans les onze domaines d'action suivants liés à la sécurité de l'information: politique de sécurité; désignation d'un conseiller en sécurité de l'information (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.
28. Le Comité de sécurité de l'information renvoie explicitement aux 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 dans la loi du 30 juillet 2018 précitée.
29. Le Comité de sécurité de l'information insiste ensuite sur le fait que 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 et que ce dernier ainsi que ses préposés et mandataires sont soumis au secret lors du traitement des données à caractère personnel.
30. Avant la communication des résultats, des mesures appropriées seront prises pour garantir le caractère anonyme des données en toutes circonstances. Par conséquent, une analyse de risque « small cell » sera préalablement effectuée. Si il apparait que la communication du degré de vaccination du nombre de personnes qui, au sein de l'établissement de soins répondent à une certaine combinaison de critères, entraîne un risque élevé d'identification des personnes concernées (par exemple parce qu'il s'agit d'un petit établissement de soins avec peu de travailleurs), ce nombre ne sera pas rendu disponible, les critères seront alors répartis en classes plus larges ou d'autres mesures appropriées seront prises.
31. Lors du traitement des données à caractère personnel, les parties doivent tenir compte de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-*

carrefour de la sécurité sociale et de toute autre réglementation relative à la protection de la vie privée, en particulier 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.

Par ces motifs,

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

conclut que la communication de données à caractère personnel par l'Office national de sécurité sociale et Vaccinnet+ à la Plate-forme eHealth, en vue de la détermination du taux de vaccination contre la COVID-19 des travailleurs des établissements de soins, telle que décrite dans la présente délibération, est autorisée moyennant le respect des mesures de protection des données 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
Président

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.