

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

CSI/CSSS/22/154

DÉLIBÉRATION N° 22/132 DU 5 JUILLET 2022 RELATIVE AU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ PAR L'INSTITUT VIAS DANS LE CADRE DE L'ÉVALUATION DE L'APTITUDE À LA CONDUITE VIA L'APPLICATION VIAP - CARA

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 RGPD) ;

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 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, articles 5 et 15 ;

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

Vu la demande des organismes assureurs wallons ;

Vu le rapport d'auditorat de la Plate-forme eHealth du 9 mai 2022 ;

Vu le rapport de monsieur Bart Viaene ;

Émet, après délibération, la décision suivante, le 5 juillet 2022 :

I. OBJET DE LA DEMANDE

1. L'institut Vias est un institut de connaissance indépendant qui agit comme une référence pour les citoyens, les instances publiques et les entreprises afin d'améliorer la sécurité routière, la mobilité, la sécurité et la santé.
2. CARA évalue l'aptitude à la conduite des personnes présentant une diminution des capacités fonctionnelles pouvant influencer la conduite en toute sécurité. L'évaluation de l'aptitude à la conduite est une décision médicale et fait partie des conditions légales obligatoires pour disposer d'un permis de conduire valide. Les critères médicaux sont définis par la loi, ainsi que les motifs de renvoi vers CARA. Le résultat de l'évaluation CARA est une attestation d'aptitude à la conduite définie par la loi. Cette attestation est délivrée au patient, qui doit la soumettre au service des permis de conduire de sa commune. Les codes présents sur l'attestation sont repris sur le nouveau permis de conduire.
3. Le médecin (généraliste) qui constate que son patient ne répond plus aux critères médicaux du permis de conduire, définis par la loi, est obligé d'en informer son patient. Dans certains cas, un renvoi vers CARA est obligatoire afin de (re)confirmer l'aptitude à la conduite du patient. Dans les autres cas, le médecin peut renvoyer le patient vers CARA à titre d'appui ou de remplacement de son propre avis en matière d'aptitude à la conduite. Il appartient toutefois au patient de décider du renvoi effectif et dès lors de la mise à disposition de données. Le médecin (généraliste) qui effectue le renvoi décide, d'une part, si les critères médicaux sont applicables et, d'autre part, si le renvoi vers CARA est nécessaire ou simplement souhaitable. Le renvoi se fera en concertation avec le patient. L'initiative est toujours prise par le patient. Toute demande donnera lieu à l'ouverture d'un dossier d'aptitude à la conduite.
4. Les intéressés sont des conducteurs ou candidats-conducteurs avec une diminution des capacités fonctionnelles comme mentionné dans l'arrêté royal du 23 mars 1998 relatif au permis de conduire.
5. Les données sont mises à la disposition via un module auprès du médecin généraliste, comme décrit ci-après. Les données proviennent du DPI. Le médecin généraliste peut demander des informations à des collègues spécialistes.

6. Une notification est envoyée via l'eHealthBox à VIAS, département CARA, indiquant que le questionnaire a été complété par le(s) prestataire(s) de soins. Le département CARA de VIAS peut en outre demander des informations complémentaires au prestataire de soins via un message eHealthBox.
7. Sur la base de la notification mentionnée à l'étape 6, CARA est en mesure de prendre connaissance du questionnaire complété. Via le module de gestion MyBox, CARA peut obtenir un aperçu des différents dossiers et réaliser le suivi des différentes étapes et actions de chaque dossier/questionnaire.
8. Suite à l'examen de l'aptitude à la conduite, CARA transmet par courrier au patient-conducteur les lettres explicatives et attestations résultantes.
9. Les questionnaires d'aptitude à la conduite (formulaire) peuvent être exportés vers le datawarehouse VIAS dans un format au choix (structuré ou non-structuré).
10. Le département CARA de VIAS a recours au datawarehouse VIAS. L'application cliente ouvre le dossier du patient à partir d'un lien contextuel vers MyBox (p.ex. NISS du patient comme clé unique du dossier). L'interface MyBox est affichée via un iFrame à partir de l'application cliente.

II. COMPÉTENCE

7. 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 en principe compétente pour l'octroi d'une autorisation de principe concernant toute communication de données à caractère personnel relatives à la santé.
8. Le Comité attire cependant l'attention sur le fait que la communication de données à caractère personnel relatives à la santé telle que prévue à l'article 42, § 2, 3°, de la loi précitée du 13 décembre 2006 doit être considérée comme une communication entre un responsable du traitement et un tiers autre que la (les) personne(s) concernée(s) ou un sous-traitant au sens du RGPD.
9. Le Comité s'estime dès lors compétent pour se prononcer sur la présente demande d'autorisation.

III. EXAMEN

A. ADMISSIBILITÉ

10. Le traitement de données à caractère personnel relatives à la santé est en principe interdit, et ce conformément au prescrit de l'article 9, § 1^{er}, 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 (Règlement général relatif à la protection des données ou RGPD).

11. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions de l'article 9, § 2 est remplie, notamment lorsque la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques. La personne concernée donne son consentement lors de l'utilisation de l'application.
12. Le traitement des données par l'institut VIAS est basé sur les articles 40 à 46 de l'arrêté royal du 23 mars 1998 relatif au permis de conduire. « Le candidat qui ne s'estime pas autorisé à signer la partie de la déclaration relative à l'aptitude physique et psychique générale subit un examen effectué par un médecin de son choix. Le médecin demande, le cas échéant, le rapport d'un médecin spécialiste conformément aux dispositions de l'annexe 6 ».
13. L'arrêté ministériel du 27 mars 1998 portant exécution de l'article 45 de l'arrêté royal du 23 mars 1998 relatif au permis de conduire précise que le centre visé à l'article 45 de l'arrêté royal du 23 mars 1998 relatif au permis de conduire est l'Institut Belge pour la Sécurité Routière, A.S.B.L., Département CARA - Aptitude à la conduite et adaptation des véhicules.
14. A la lumière de ce qui précède, le Comité est par conséquent d'avis qu'il existe un fondement admissible pour le traitement des données à caractère personnel relatives à la santé envisagé.

B. FINALITÉ

15. Selon l'article 5 du RGPD, les données à caractère personnel doivent être traitées de manière licite, loyale et transparente à l'égard de la personne concernée (licéité, loyauté, transparence). Elles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (limitation des finalités).
16. Au vu des objectifs du traitement tels que décrits ci-dessus, le Comité considère que le traitement des données à caractère personnel envisagé poursuit bien des finalités déterminées, explicites et légitimes.

C. PROPORTIONNALITÉ

17. L'article 5 du RGPD dispose que 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).
18. La nature des informations médicales demandées est déterminée par les troubles fonctionnels et affections mentionnés dans l'arrêté royal du 23 mars 1998.
19. Les informations demandées via le formulaire sont communiquées à la fois par le patient (adresse mail, profession, type de permis de conduire demandé, information sur une éventuelle implication dans un accident de la circulation durant les 5 dernières années, les difficultés éprouvées durant la conduite, d'évaluation de l'aptitude à la conduite, évolution

de la situation médicale après la précédente demande auprès de CARA) et par le médecin. Le médecin communique son adresse mail, son numéro de GSM (nécessaire pour que VIAS puisse le contacter en cas de questions sur le patient). Le médecin communique les données relatives à la médication, à l'historique médical ainsi qu'un bilan médical et ses éventuelles remarques.

20. Conformément à 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. Les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation).
21. La durée de validité d'une évaluation de l'aptitude à la conduite est déterminée par le médecin. Dans ce cadre, ce dernier tient compte de la situation médicale/fonctionnelle du patient, du pronostic et des durées de validité maximales par affection définies par la loi. La décision d'aptitude à la conduite prend fin en cas de modification (importante) de l'état médical, comme déterminé par la loi.
22. En vertu de l'arrêté royal du 23 mars 1998, le médecin est tenu de conserver pendant minimum 6 ans les données sur lesquelles est basée sa décision d'aptitude à la conduite. Etant donné que la décision d'aptitude à la conduite est mentionnée sur le permis de conduire et qu'en cas de perte, de vol ou de renouvellement du permis de conduire, une nouvelle attestation de l'aptitude à la conduite est requise, les données ne sont pas détruites. Lors d'une nouvelle décision de l'aptitude à la conduite, l'historique fournit en effet une indication de la stabilité et/ou de l'évolution des troubles fonctionnels. L'évolution est par ailleurs un des paramètres qui déterminent la durée de validité de la décision. La durée de validité administrative actuelle du permis de conduire belge est de dix ans. Jusqu'il y a peu, la durée de validité était cependant illimitée, ce qui contraignait parfois CARA à réévaluer des dossiers d'il y a 30 ans.
23. Les experts médicaux ne conservent les données communiquées que le temps nécessaire à la durée de la réalisation de l'expertise.

D. TRANSPARENCE

24. Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations mentionnées à l'article 13 du RGPD.
25. Le renvoi et donc la mise à disposition des données médicales est préalablement discuté avec le patient par le médecin généraliste. Généralement, le renvoi a lieu à la demande du patient lui-même et éventuellement à l'initiative du médecin spécialiste.

26. Le Comité est d'avis qu'il existe suffisamment de transparence quant au traitement envisagé.

E. MESURES DE SÉCURITÉ

27. Conformément aux articles 9, §2, h) et 9, §3 du RGPD, le traitement de données à caractère personnel relatives à la santé doit être effectué 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. Même si cela n'est pas strictement requis par le RGPD, le Comité estime qu'il est préférable de traiter de telles données sous la responsabilité d'un médecin, comme c'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.
28. Conformément à l'article 5, §1^{er}, f) 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 doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.
29. 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, ...); documentation¹.
30. Le Comité constate que l'institut VIAS a désigné un délégué à la protection des données.
31. L'institut VIAS prévoit de réaliser une analyse d'impact relative à la protection des données dès que l'application sera activée. Le Comité rappelle que le responsable du traitement des données est tenu de respecter l'article 35 du RGPD.

¹ « Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel », document rédigé par la Commission de la protection de la vie privée.

- 32.** Le Comité constate que l'application VIAP – CARA utilise le service de base eHealthBox de la plateforme eHealth.
- 33.** Le Comité rappelle 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.
- 34.** Le Comité attire 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 sanctions pénales sévères dans le chef du responsable du traitement et des sous-traitants en cas d'infraction aux conditions prévues dans le RGPD et dans la loi précitée du 30 juillet 2018.

Par ces motifs,

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

conclut 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
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 (tél. 32-2-741 83 11).