Comité de sécurité de l'information
Chambre sécurité sociale et santé

CSI/CSSS/23/024

DÉLIBÉRATION N° 23/032 DU 7 MARS 2023 PORTANT SUR L'ÉCHANGE ET LE COUPLAGE DE DONNÉES À CARACTÈRE PERSONNEL PSEUDONYMISÉES RELATIVES À LA SANTÉ ENTRE L'INSTITUT NATIONAL DE CRIMINALISTIQUE ET DE CRIMINOLOGIE, LES CENTRES BELGES DE PRISE EN CHARGE DES VIOLENCES SEXUELLES ET L'INSTITUT POUR L'ÉGALITÉ DES FEMMES ET DES HOMMES, VIA LA PLATEFORME DE HEALTHDATA.BE ET DE HEALTHSTAT.BE, DANS LE CADRE D'UN MONITORING ET D'UNE ÉVALUATION

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

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);

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* ;

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

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

Vu la délibération n° 15/009 du 17 février 2015, modifiée en dernier lieu le 5 juin 2018, relative à la méthode générique d'échange de données à caractère personnel codées ou non relatives à la santé, dans le cadre de healthdata.be et healthstat.be ;

Vu la délibération n° 17/042 du 16 mai 2017, modifiée en dernier lieu le 3 mars 2020, relative à la communication de données à caractère personnel relatives à la santé codées par les prestataires de soins, dans le cadre de healthdata.be et healthstat.be ;

Vu la demande de l'Institut pour l'égalité des femmes et des hommes, de healthdata et de l'l'Institut national de Criminalistique et de Criminologie (INCC);

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 mars 2023:

I. OBJET DE LA DEMANDE

1. L'Institut pour l'égalité des femmes et des hommes (IEFH) souhaite réaliser un monitoring et une évaluation des Centres belges de prise en charge des violences sexuelles[1].

Les personnes concernées sont toutes les victimes de violence sexuelle qui s'adressent, en personne, à un des centres belges de prise en charge des violences sexuelles[2]. Le nombre de patients concernés est estimé à au moins 3200 victimes par an.

2. Les données à caractère personnel pseudonymisées relatives à la santé sont communiquées par les Centres belges de prise en charge des violences sexuelles. L'IEFH interviendra comme responsable du traitement et l'INCC comme sous-traitant.

3. Les chercheurs de l'Institut pour l'égalité des femmes et des hommes et les chercheurs de l'INCC reçoivent accès au datawarehouse de healthdata.be contenant les données historiques et les nouvelles données, selon le mandat attribué, de sorte que les données puissent être validées et utilisées à des fins d'analyse.

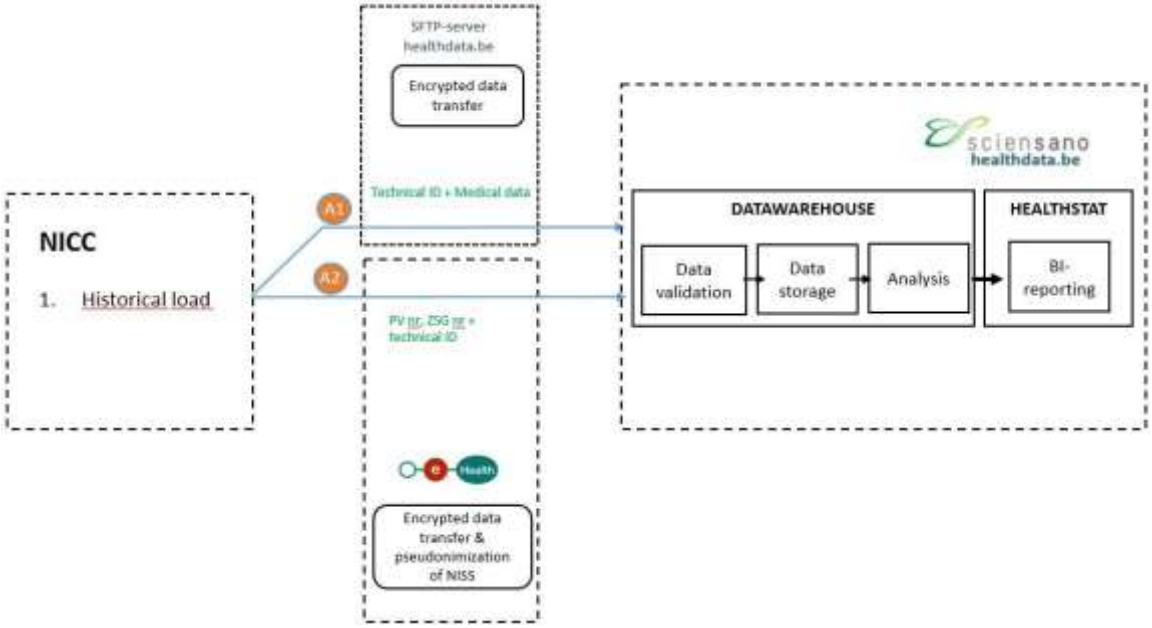
Les données concernées sont communiquées aux instances suivantes selon des modalités spécifiques :

[1] Loi du 16 décembre 2002 portant création de l'Institut pour l'égalité des femmes et des hommes (MB du 31 décembre 2002): l'Institut est chargé de veiller au respect de l'égalité des genres ainsi que de préparer et appliquer les décisions du gouvernement en matière de suivi de l'égalité des genres sous l'autorité du/de la ministre chargé(e) de la politique d'égalité des femmes et des hommes

[2] Articles 4, 1° et 5, de la loi du 16 décembre 2002 portant création de l'Institut pour l'égalité des femmes et des hommes (*MB* 31 décembre 2002): L'Institut est habilité à : 1° faire, développer, soutenir et coordonner les études et recherches en matière de genre et d'égalité des femmes et des hommes et évaluer l'impact en terme de genre des politiques, programmes et mesures mis en œuvre. L'Institut est chargé de la préparation et de l'application des décisions du gouvernement et du suivi des politiques européennes et internationales, en matière d'égalité des femmes et des hommes.

1) Données historiques présentes auprès de l'INCC (période depuis 2017). Il s'agit d'un chargement de données unique (1 time shot) à l'occasion duquel quelque 5000 enregistrements (contacts patient) seront fournis via SFTP.

Figure 1: données historiques



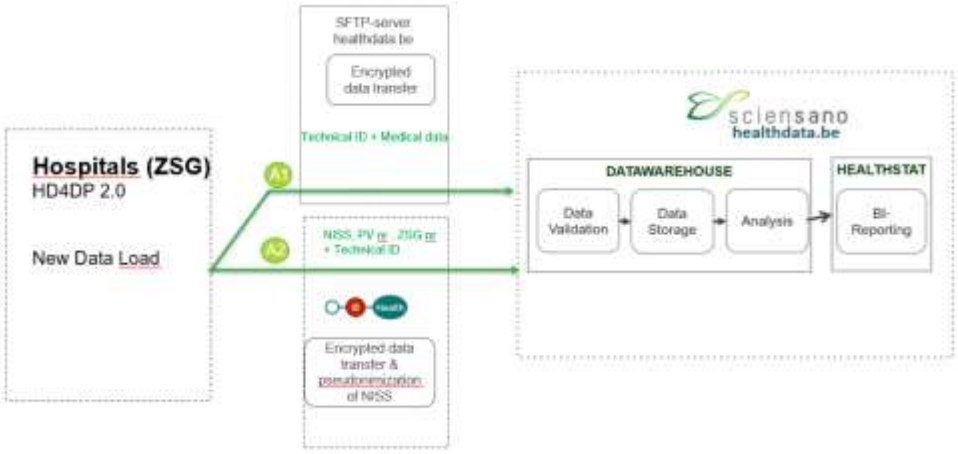
Ces données provenant de l'INCC sont transmises à healthdata.be dans deux flux séparés:

- Le flux A1 contenant des données médicales avec un identifiant technique (technical ID). Les données sont transférées via SFTP vers l'entrepôt de données healthdata.be (HD-DWH). Étant donné que ce fichier ne contient pas de données à pseudonymiser, le fichier est directement envoyé par les fournisseurs de données au DWH HD via SFTP ou toute autre méthode de transfert.
- Le flux A2 avec le même identifiant technique, le numéro de PV et le numéro CSVS. Les données sont transférées, via eHealth (en vue de la pseudonymisation des données d'identification du patient par codage eHBox), vers l'entrepôt de données healthdata.be (HD-DWH). Le numéro de PV et le numéro CPVS sont pseudonymisés par la Plate-forme eHealth en tant que TTP.

La plateforme healthdata.be consolide ensuite les communications séparées dès leur réception sur la base de l'identifiant technique. Après consolidation et contrôle de qualité technique, l'identifiant technique est immédiatement et définitivement supprimé de l'infrastructure healthdata.be. La plateforme healthdata.be tiendra un journal de ces processus techniques.

2) nouvelles collectes de données au moyen du logiciel de collecte de données HD4DP 2.0 de healthdata.be

Figure 2: nouvelles données



Ces données provenant des CPVS (centres de soins violence sexuelle) sont collectées par le logiciel de collecte des données HD4DP 2.0 et transmises à healthdata.be dans deux flux séparés:

- Le flux A1 contenant des données médicales avec un identifiant technique (technical ID). Les données sont transférées via SFTP vers l'entrepôt de données healthdata.be (HD-DWH). Étant donné que ce fichier ne contient pas de données à pseudonymiser, le fichier est directement envoyé par les fournisseurs de données au DWH HD via SFTP ou toute autre méthode de transfert.
- Le flux A2 avec le NISS du patient, le même identifiant technique, le numéro de PV et le numéro CPVS. Les données sont transférées à l'intervention de la Plate-forme eHealth (en vue de la pseudonymisation des données d'identification du patient par codage eHBox) vers l'entrepôt de données healthdata.be (HD-DWH). L'ID technique est crypté par l'expéditeur tandis que le NISS est pseudonymisé par la Plate-forme eHealth en tant que TTP.

La plateforme healthdata.be consolide ensuite les communications séparées dès leur réception sur la base de l'identifiant technique. Après consolidation et contrôle de qualité technique, l'identifiant technique est immédiatement et définitivement supprimé de l'infrastructure healthdata.be. La plateforme healthdata.be tiendra un journal de ces processus techniques.

Validation, analyse et rapportage des données historiques et des nouvelles données

Les chercheurs de l'Institut pour l'égalité des femmes et des hommes et les collaborateurs de l'INCC reçoivent accès au datawarehouse de healthdata.be contenant les données historiques et les nouvelles données, selon le mandat attribué, de sorte que les données puissent être validées et utilisées à des fins d'analyse.

Healthdata.be peut être utilisé comme une application web sécurisée pour le partage de rapports scientifiques, de diagrammes et de statistiques consolidées provenant du registre avec le monde extérieur.

4. Healthdata.be peut être utilisé comme une application web sécurisée pour le partage de rapports scientifiques, de diagrammes et de statistiques consolidées provenant du registre avec le monde extérieur.

Les données à caractère personnel relatives à la santé pseudonymisées et couplées suivantes seront communiquées: les données qui ont trait à l'identité de la personne telles le NISS (numéro national ou numéro BCSS). Le numéro CPVS et le numéro de PV seront également recueillis. Le nom et l'adresse ne seront pas transmis à Sciensano ou à l'IEFH. Ces données restent disponibles, au niveau local, dans le CPVS.

5. Les données à caractère personnel relatives à la santé seront conservées pendant 30 ans dans le datawarehouse de Healthdata afin d'identifier les glissements et évolutions épidémiologiques et d'évaluer la politique/le fonctionnement des CPVS pendant une longue période. Par ailleurs, ce délai fournit des informations relatives à la re-victimisation. Il ressort d'études que les victimes de violence sexuelle courent un risque accru d'à nouveau être victime de violences. Les enfants qui sont la victime de violences sexuelles courent en particulier un risque accru d'à nouveau être victime à l'âge adulte. En conservant les données, sous forme pseudonymisée, pendant une période de 30 ans, il serait possible de cartographier, à plus long terme, la re-victimisation de victimes, lorsqu'ils s'adressent à différents moments dans leur vie à un centre de prise en charge des violences sexuelles. Seuls les collaborateurs associés au CPVS, à l'Institut ou le(s) sous-traitant(s) désignés par l'Institut, sous le contrôle de l'Institut, y ont accès. Ces données seront ensuite conservées sous forme anonyme.

6. Une analyse de risque « small cell » (SCRA) théorique sera réalisée par le Centre fédéral d'expertise des soins de santé. Le rapport SCRA final sera communiqué au CSI.

7. Le Comité prend, par ailleurs, acte du fait que le Comité d'éthique hospitalo-facultaire des cliniques universitaires Saint-Luc a formulé, le 9 mai 2022, un avis positif pour cette étude.

II. COMPETENCE

8. Conformément à l'article 42, § 2, 3°, de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé*, toute communication de données à caractère personnel relatives à la santé requiert, sauf les exceptions prévues, une délibération de principe de la chambre sécurité sociale et santé du Comité de sécurité de l'information.

9. Le Comité estime dès lors qu'il est compétent pour se prononcer sur cette communication de données à caractère personnel relatives à la santé.

III. EXAMEN DE LA DEMANDE

A. ADMISSIBILITÉ

10. Le traitement de données à caractère personnel relatives à la santé est en principe interdit conformément à l'article 9, § 1er, du RGPD[3]. 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, §1er, 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.

11. 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. Ceci est le cas en l'espèce.

12. 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 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.

13. Le Comité fait observer qu'il existe un cadre réglementaire pour différentes activités de traitement et/ou finalités.

14. Ce traitement de données à caractère personnel trouve un fondement dans
- les articles 3 (mission légale), 4 § 1 (réaliser des études et des recherches), 5 (préparer et exécuter les décisions du gouvernement) de la loi du 16 décembre 2002 portant création de l'Institut pour l'égalité des femmes et des hommes (*M.B.* 31/12/2002);

[3]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 (RGPD) .

- l'article 2 (la Convention d'Istanbul est suivie strictement) de la loi du 1er mars 2016 portant assentiment à la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, faite à Istanbul le 11 mai 2011 (*M.B.* 9/06/2016);
- article 3 (définition de la violence à l'égard des femmes et de la violence liée au genre), l'article 10 (Organe de coordination pour la Belgique = l'Institut), l'article 11 (Réalisation d'une étude sur les causes et les conséquences et sur l'efficacité des mesures d'exécution de la Convention + recueillir des données statistiques sur les cas de violence qui tombent sous la portée de la Convention), article 25 (centres multidisciplinaires pour les victimes de violence sexuelle) de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, faite à Istanbul le 11 mai 2011;
- article 2 de l'AR du 5 novembre 1971 portant création de l'Institut national de criminalistique[4]

15. Le Comité prend, par ailleurs, acte du fait que le Comité d'éthique hospitalo-facultaire des cliniques universitaires Saint-Luc a formulé, le 9 mai 2022, un avis positif pour cette étude.

16. A la lumière de ce qui précède, le Comité estime par conséquent qu'il existe un fondement admissible pour le traitement des données à caractère personnel relatives à la santé envisagé.

B. FINALITÉ

17. 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. Elles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Le traitement a lieu dans le cadre d'une mission d'intérêt public et est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, à savoir l'exécution de l'obligation vis-à-vis de l'Institut mentionnée à l'article 10 de la Convention d'Istanbul qui a été ratifiée par la Belgique[5].

18. Le traitement des données permet de veiller à la prestation de soins de qualité aux victimes de violence sexuelle dans les Centres belges de prise en charge des violences sexuelles au moyen de la collecte de caractéristiques des victimes, de caractéristiques de la violence sexuelle subie, de caractéristiques des soins et du traitement reçus ainsi qu'à l'impact de la violence sexuelle sur la santé physique, mentale et sexuelle des victimes. Ce traitement des données permet également un suivi épidémiologique de la violence sexuelle au moyen du traitement de données relatives au profil des victimes et aux caractéristiques de la violence sexuelle. Ce traitement de données permet donc de poursuivre l'optimalisation des Centres belges de prise en charge des violences sexuelles et de mettre en place des politiques

[4] Articles 4, 1° et 5, de la loi du 16 décembre 2002 portant création de l'Institut pour l'égalité des femmes et des hommes (*MB* 31 décembre 2002): L'Institut est habilité à : 1° faire, développer, soutenir et coordonner les études et recherches en matière de genre et d'égalité des femmes et des hommes et évaluer l'impact en terme de genre des politiques, programmes et mesures mis en œuvre. L'Institut est chargé de la préparation et de l'application des décisions du gouvernement et du suivi des politiques européennes et internationales, en matière d'égalité des femmes et des hommes.

[5] Art. 6, 1, e) et c) RGPD

préventives et curatives scientifiquement prouvées en matière de violence sexuelle en Belgique.

19. Le Comité prend, par ailleurs, acte du fait que le Comité d'éthique hospitalo-facultaire des cliniques universitaires Saint-Luc a formulé, le 9 mai 2022, un avis positif pour cette étude.

20. Au vu des objectifs, le Comité considère que le traitement des données à caractère personnel envisagé poursuit bien des finalités déterminées, explicites et légitimes.

C. PROPORTIONNALITÉ

21. En vertu de l'article 5 b) et c) 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.

22. Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées uniquement pendant la durée nécessaire à la réalisation des finalités pour lesquelles les données à caractère personnel sont traitées[6]. 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, §1er, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par ce règlement afin de garantir les droits et libertés de la personne concernée (« limitation de la conservation »).

23. En l'espèce, cette délibération sera valable aussi longtemps que le cadre réglementaire autorise l'existence des Centres de soins et le monitoring et l'évaluation des centres de soins.

24. Le délai de conservation dans le datawarehouse de Healthdata s'élève à 30 ans afin d'identifier les glissements et évolutions épidémiologiques et d'évaluer la politique/le fonctionnement des CPVS au cours d'une longue période. Par ailleurs, ce délai fournit des informations relatives à la re-victimisation. Il ressort d'études que les victimes de violence sexuelle courent un risque accru d'à nouveau être victime de violences. Les enfants qui sont la victime de violences sexuelles courent en particulier un risque accru d'à nouveau être victime à l'âge adulte. En conservant les données, sous forme pseudonymisée, pendant une période de 30 ans, il serait possible de cartographier, à plus long terme, la re-victimisation de victimes, lorsqu'ils s'adressent à différents moments dans leur vie à un centre de prise en charge des violences sexuelles. Seuls les collaborateurs associés au CPVS, à l'Institut ou le(s) sous-traitant(s) désigné(s) par l'Institut, sous le contrôle de l'Institut, y ont accès. Après un délai de 30 ans, les données peuvent être conservées sous une forme anonyme.

25. Les données à caractère personnel générales collectées sont notamment les codes d'identification (NISS pseudonymisé, numéro de dossier CPVS pseudonymisé, numéro de PV pseudonymisé). Ces informations sont nécessaires afin de pouvoir créer un profil identique par déclaration et de coupler les données de la section CPVS, dans une phase

[6] Article 5,§ 1, e) du RGPD.

ultérieure, aux données de la police moyennant autorisation des organes compétents tels la chambre sécurité sociale et santé du Comité de sécurité de l'information. Ces codes d'identification sont pseudonymisés par un tiers de confiance (= la Plate-forme eHealth).

26. En outre, des caractéristiques démographiques générales (date de naissance, uniquement l'année de naissance sera disponible pour les chercheurs; pays de naissance; sexe; pays du domicile; code postal du domicile). Ces informations sont nécessaires pour mesurer la prévalence de la violence sexuelle en Belgique sur la base de données démographiques (âge, répartition géographique, sexe) et déterminer le profil des victimes qui s'adressent à un CPVS. La date de naissance est convertie en l'âge et la date de naissance exacte n'est donc pas affichée. Le code postal du domicile est converti en le niveau de l'arrondissement.

27. En ce qui concerne les données générales, il est aussi tenu compte de la vie privée, en particulier de la situation au niveau du logement/du ménage et du statut légal. Ces informations sont nécessaires pour mesurer la prévalence de la violence sexuelle en Belgique sur la base de données démographiques (situation de logement, statut de réfugié/sans-papier, européen/non européen, ...), vu la plus grande vulnérabilité de certains groupes cibles + déterminer le profil des victimes qui s'adressent à un CPVS.

28. Il est aussi tenu compte de la vie professionnelle (le niveau de formation le plus élevé et la situation en matière de travail). Ces informations sont nécessaires pour mesurer la prévalence de la violence sexuelle en Belgique sur la base de données démographiques (niveau de l'enseignement, situation en matière de travail) et déterminer le profil des victimes qui s'adressent à un CPVS.

29. Enfin, les données sociales relatives aux soins administrés par le CPVS (aide linguistique; présence d'une personne aidante; renvoi aux services d'aide; contacts gestion de cas (date, heure, personne concernée) concernant l'encadrement social prévu pendant les soins administrés par le CPVS et pendant les 6 mois après le premier contact avec le centre. Les données à caractère personnel des personnes aidantes ne sont pas enregistrées et toutes les dates sont converties en un délai (X nombre de jours/semaines) entre la date enregistrée et la date des premiers contacts avec le CPVS. Toutes les périodes sont aussi converties en une partie de la journée (matin, midi, après-midi, soir, nuit).

30. Dans un second temps, pour autant que les sections des CPVS disposent de ces informations, des données de la police sont aussi collectées concernant l'intervention de la police (déclaration antérieure, déclaration via le CPVS), l'intervention du parquet (action en justice); le parquet compétent; la date de l'audition + type d'audition + l'intervention ZIP; le type d'intervention, la date et l'heure de l'intervention, le lieu et la date de la déclaration. Ces informations sont nécessaires à l'identification du fonctionnement politionnel et judiciaire du CPVS et à son évaluation. Toutes les dates sont converties en un délai (X nombre de jours/semaines) entre la date enregistrée et la date de la première prise de contact avec le CPVS. Toutes les périodes sont aussi converties en une partie de la journée (matin, midi, après-midi, soir, nuit). Le lieu de l'audition est dans le CPVS, dans le bureau de police d'une zone coopérante ou d'une autre zone ou à un autre endroit. L'endroit exact de la zone où l'audition a eu lieu, n'est pas enregistré.

Le Comité de sécurité de l'information n'est toutefois pas compétent pour se prononcer sur la communication de données à caractère personnel politionnelles. La communication envisagée n'est cependant pas impossible, pour autant que les principes du RGPD soient respectés et que les dispositions contractuelles nécessaires soient établies entre les parties concernées.

31. Troisièmement, des catégories de données à caractère personnel spécifiques relatives à la sexualité et à la perception du genre (orientation sexuelle, identité transgenre, antécédents sexuels) sont traitées. Ces informations sont nécessaires pour mesurer la prévalence de la violence sexuelle en Belgique (orientation sexuelle et identité transgenre, ...), vu la plus grande vulnérabilité de certains groupes cibles + déterminer le profil des victimes qui s'adressent à un CPVS. Ces informations relatives au comportement sexuel sont aussi nécessaires en cas d'antécédents de violence sexuelle (victimisation multiple).

32. Des <u>données relatives à la santé</u> sont également traitées:

- Handicap
- Profil de risque psychologique
- Antécédents santé mentale
- Médicaments et allergies
- Antécédents menstruels et obstétricaux
- Informations relatives à l'expertise médicolégale (participants, date, heure, consentement)
- Expertise médicolégale: description des lésions
- Expertise médicolégale: échantillons corps et vêtement
- Expertise médicolégale: examen clinique anogénital
- Expertise médicolégale: échantillons toxicologie - Expertise médicolégale: autres pistes
- Échantillon de référence ADN
- Soins médicaux: jour 0: tests, médicaments/vaccins administrés et résultats de test
- Soins médicaux: suivi: date, heure, tests, médicaments/vaccins administrés et résultats de test - Renvoi soins médicaux
- Suivi psychologique: date et heure, présence, personne concernée, type d'intervention
- Suivi psychologique: thérapie et instruments + résultats.

Ces informations sont nécessaires pour mesurer la prévalence de la violence sexuelle en Belgique (handicap, profil de risque psychologique), vu la plus grande vulnérabilité de certains groupes cibles + déterminer le profil des victimes qui s'adressent à un CPVS. Ces informations sont nécessaires pour identifier et évaluer le fonctionnement médical et médicolégal du CPVS.

Toutes les dates sont, à cet égard, converties en un délai (X nombre de jours/semaines) entre la date enregistrée et la date de la première prise de contact avec le CPVS. Toutes les périodes sont aussi converties en une partie de la journée (matin, midi, après-midi, soir, nuit).

Les données à caractère personnel spécifiques comprennent aussi des données relatives à la violence sexuelle (date et heure violence sexuelle, antécédents en matière de violence, informations relatives à la prise de contact avec le CPVS, type de contacts pendant la violence sexuelle, plaintes physiques et psychiques suite à la violence sexuelle, alcool et consommation de drogues, actes posés après la violence sexuelle). Ces informations sont nécessaires pour mesurer la prévalence de la violence sexuelle en Belgique (type de violence sexuelle, agression sexuelle facilitée par la drogue, violence sexuelle et violence physique, ...) et pour identifier les formes de violence sexuelle dont sont victimes les personnes qui s'adressent à un CPVS. En outre, ces informations sont également nécessaires pour évaluer les principes de base du CPVS (violence sexuelle en phase aiguë/non aiguë, viol/agression) et les associer aux soins/services fournis. Toutes les dates sont, à cet égard, converties en un délai (X nombre de jours/semaines) entre la date enregistrée et la date de la première prise de contact avec le CPVS.

Enfin, les données relatives à l'auteur de la violence sexuelle sont aussi recueillies (nombre d'auteurs, sexe de l'auteur (des auteurs), relation, relation entre l'auteur (les auteurs) et la victime). Ces informations sont nécessaires pour établir un profil des auteurs de la violence sexuelle ainsi que pour mesurer la prévalence de la violence sexuelle dans le ménage, par le partenaire ou par des inconnus. La relation entre l'auteur et la victime est définie comme: partenaire/ancien partenaire, membre de la famille, connaissance, inconnu. Les données exactes de l'auteur ne sont pas traitées.

33. Certaines données sont demandées une seule fois, il s'agit de données rétrospectives depuis l'année 2017 et d'autres données sont demandées sur une base périodique (à des intervalles réguliers), à savoir sur base trimestrielle.

34. Conformément à l'article 5, 1, e) du RGPD, les données 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, alinéa 1er, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation).

35. Ces données à caractère personnel relatives à la santé sont traitées, conservées, supprimées et/ou dépersonnalisées, conformément aux délais de conservation mentionnés dans la délibération de la chambre sécurité sociale et santé du Comité de sécurité de l'information au moyen de l'infrastructure qui est développée par la Plateforme Healthdata.be. L'Institut national de criminalistique et de criminologie (INCC) validera, nettoiera et analysera par ailleurs ces données et générera des rapports sur la base de ces données.[7]

[7] Article 2, 6° de l'AR du 5 novembre 1971 portant création et érection en établissement scientifique de l'Etat de l'Institut national de criminalistique: effectuer ou faire effectuer par des tiers toutes études ou recherches criminologiques, juridiques ou statistiques en rapport avec la politique criminelle, la politique à l'égard des victimes d'infractions et la politique d'exécution des peines et mesures, à la requête ou avec l'accord du Ministre de la Justice,

36. Le Comité fait observer que les hôpitaux communiqueront les données concernées au datawarehouse de Healthdata via HD4DP. Ces données seront ensuite mises à la disposition de l'INCC et de l'Institut. La Plate-forme eHealth est chargée de l'exécution des mesures de pseudonymisation vis-à-vis des données.

37. Le Comité fait observer que le NISS pseudonymisé du patient sera communiqué. Ce NISS correspond au numéro d'identification du Registre national, au numéro d'identification de la sécurité sociale ou au numéro Banque Carrefour.

38. La Plate-forme eHealth est, en tant que « tierce partie de confiance », chargée de la pseudonymisation des numéros d'identification des personnes concernées.[8]

39. Le Comité autorise la Plate-forme eHealth à conserver la clé de codage utilisée afin de réaliser un contrôle de qualité des données. Lorsque le sous-traitant des données présume que les informations relatives à un patient déterminé présentes dans le registre ne sont peut-être pas correctes, il doit pouvoir communiquer avec le centre au sujet de ce patient afin de vérifier si les informations sont correctes et de pouvoir apporter les corrections.

40. Une analyse de risque « small cell » (SCRA) théorique sera réalisée par le Centre fédéral d'expertise des soins de santé. Le rapport SCRA final sera communiqué au CSI.

41. A cet égard, le Comité rappelle que conformément à la délibération n° 15/099, cette analyse est réalisée sous la responsabilité du Comité directeur de la plateforme healthdata.be.

D. TRANSPARENCE

42. 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.

43. Les articles 13 et 14 du RGPD fixent les conditions auxquelles le responsable du traitement doit satisfaire lorsque des données à caractère personnel sont collectées concernant la personne concernée. Ainsi, les informations suivantes doivent notamment être communiquées: les coordonnées du responsable du traitement et du délégué à la protection des données, les catégories de données à caractère personnel si les données ne sont pas

---

du Président du Service public fédéral Justice ou du Conseiller général à la politique criminelle, ou à la requête d'un directeur général du Service public fédéral Justice ou du Collège des procureurs généraux. La mise en œuvre de cette disposition se déroule selon une procédure fixée par arrêté ministériel.

[8] Par le passé, la Plate-forme eHealth a été autorisée à conserver le lien entre le numéro d'identification réel d'une personne concernée et le numéro d'identification pseudonymisé qui lui a été attribué, conformément à la délibération n° 15/009 du 17 février 2015, modifiée en dernier lieu le 5 juin 2018, relative à la méthode générique d'échange de données à caractère personnel codées et non codées relatives à la santé, dans le cadre de healthdata.be et healthstat.be.

[9] Délibération n° 15/009 du 17 février 2015, dernièrement modifiée le 3 mars 2020, relative à la méthode générique d'échange de données à caractère personnel codées et non codées relatives à la santé, dans le cadre de healthdata.be et healthstat.be

obtenues auprès des personnes concernées, les finalités du traitement et le fondement du traitement, les catégories de destinataires et, si le responsable du traitement a l'intention de transmettre les données à caractère personnel à un destinataire dans un pays tiers, les garanties appropriées.

44. Ensuite, afin de garantir un traitement équitable et transparent, le responsable du traitement doit notamment informer la personne concernée sur ses droits (droit d'introduire une plainte, droit de consultation, droit d'opposition, droit de rectification, etc.), le cas échéant, sur la source des données à caractère personnel et l'existence d'une prise de décision automatisée.

45. En l'espèce, après approbation du projet par la chambre sécurité sociale et santé du Comité de sécurité de l'information, une déclaration de confidentialité sera mise à la disposition des victimes par le biais des CPVS et par le biais du site internet violencessexuelles.be. Ce site contient des informations pertinentes relatives au traitement et aux droits de la personne concernée.

46. Le Comité estime par conséquent que la demande répond aux exigences de transparence.

E. MESURES DE SÉCURITÉ

47. 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 doivent garantir 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.

48. 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 conseiller en sécurité de l'information; 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.

49. Le Comité constate qu'une analyse d'impact relative à la protection des données[10] a été réalisée. Une version définitive a été validée par le DPO.

50. Le Comité fait observer que Sciensano, l'INCC ainsi que l'Institut ont désigné un délégué à la protection des données. Lorsque des données relatives à la santé sont traitées, un professionnel des soins de santé responsable est aussi désigné.

[10] En exécution de l'article 23 du la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*

51. Une analyse de risque « small cell » (SCRA) théorique sera réalisée par le Centre fédéral d'expertise des soins de santé. Le rapport SCRA final sera communiqué au CSI.

52. Le Comité observe que tous les collaborateurs internes et externes ont conclu un contrat de confidentialité (NDA) avec Sciensano. Les collaborateurs de l'INCC et de l'Institut[11] sont tenus par une obligation de confidentialité vis-à-vis des données qu'ils traitent dans le cadre de leur fonction. Les médecins et leurs collaborateurs sont aussi tenus par une obligation de confidentialité dans le cadre du secret professionnel.

53. Des services de protection sont aussi prévus, à savoir des certificats eHealth, la pseudonymisation, l'anonymisation et la tierce partie de confiance, la gestion intégrée des utilisateurs et des accès et un système de chiffrement de bout-en-bout.

54. Le Comité souligne qu'en vertu de l'article 111, alinéa 1er, de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, sans préjudice des pouvoirs de contrôle de l'Autorité de protection des données, les autorisations accordées par les comités sectoriels de la Commission de la protection de la vie privée avant l'entrée en vigueur de cette loi gardent leur validité juridique. Les modalités de la délibération n° 15/009 du 17 février 2015, modifiée en dernier lieu le 3 mars 2020, relative à la méthode générique d'échange de données à caractère personnel codées et non codées relatives à la santé, dans le cadre de healthdata.be et healthstat.be restent donc d'application.

55. 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 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.

56. Le Comité estime nécessaire de rappeler que depuis le 25 mai 2018, la plateforme healthdata.be, Sciensano et l'Institut sont tenus de respecter les dispositions et les principes 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 sur la protection des données). Ces instances sont également tenues de

[11] Article 458 du Code pénal; article 28quinquies, § 1er, et article 57, § 1er, du Code d'instruction criminelle: fiche « confidentialité dans le cadre de l'accès à long terme » (Annexe 5 a: P&O/A.01/verN.8); circulaire n° 573 relative au cadre déontologique des agents de la fonction publique administrative fédérale; circulaire n° 706. - Une attention renouvelée pour le cadre déontologique des fonctionnaires fédéraux (annexe 7: code déontologique agents fédéraux)

respecter les dispositions 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

vu la délibération n° 15/009 du 17 février 2015, dernièrement modifiée le 3 mars 2020, relative à la méthode générique d'échange de données à caractère personnel codées et non codées relatives à la santé, dans le cadre de healthdata.be et healthstat.be ;

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 des données 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