

**Comité sectoriel de la sécurité sociale et de la santé
Section "Santé"**

SCSZG/13/149

**DÉLIBÉRATION N° 13/068 DU 18 JUI 2013 RELATIVE À LA COMMUNICATION DE
DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ DANS LE
CADRE DE L'AIDE INTÉGRALE À LA JEUNESSE ORGANISÉE AU SEIN DE
L'AGENCE FLAMANDE 'JONGERENWELZIJN'**

Le Comité sectoriel de la sécurité sociale et de la santé (dénommé ci-après : "le Comité sectoriel");

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

Vu la demande d'autorisation de l'Agence flamande "Zorg en Gezondheid";

Vu la demande d'autorisation de l'Agence flamande "Personen met een handicap";

Vu la demande d'autorisation de l'Agence flamande "Kind en Gezin";

Vu le rapport d'auditorat du 13 juin 2013;

Vu le rapport de monsieur Yves Roger;

Émet, après délibération, la décision suivante, le 18 juin 2013:

I. OBJET DE LA DEMANDE

1. En exécution du décret du Gouvernement flamand relatif à l'aide intégrale à la jeunesse¹, un système d'échange de données a été développé sous la responsabilité de l'Agence flamande 'Jongerenwelzijn' dans le but d'offrir de l'aide et des soins sur mesure aux enfants mineurs, à leurs parents et, le cas échéant, à leurs responsables de l'éducation et aux personnes concernées de leur entourage. Ce système est réalisé moyennant une analyse commune de la demande d'aide et ceci par le biais d'une collaboration intersectorielle entre les offreurs d'aide à la jeunesse, ainsi que d'une harmonisation intersectorielle de l'offre d'aide à la jeunesse. À cet effet, les secteurs suivants collaborent: l'Agence flamande 'Jongerenwelzijn', l'Agence flamande 'Kind en Gezin', l'Agence flamande pour les personnes handicapées (Vlaams Agentschap voor Personen met een Handicap), les centres d'encadrement des élèves, les centres de soins de santé mentale, les centres d'aide aux familles intégrée et les centres d'action sociale globale.

L'aide intégrale à la jeunesse porte tant sur l'offre d'aide directement accessible² et sur l'offre d'aide indirectement accessible³ aux enfants mineurs, aux parents et aux responsables de l'éducation dans un contexte volontaire ou extrajudiciaire, que sur l'aide à la jeunesse imposée par le juge de la jeunesse.

2. L'Agence flamande 'Jongerenwelzijn' soumet actuellement la communication de données à caractère personnel relatives à la santé à l'approbation du Comité sectoriel dans le cadre de deux applications relatives à l'aide intégrale à la jeunesse, plus précisément INSISTO et Domino OCJ.

1) INSISTO

3. INSISTO permet le traitement électronique de demandes d'obtention d'une aide indirectement accessible introduites auprès de la "porte d'entrée" intersectorielle. Cette procédure devrait permettre d'introduire une demande d'obtention d'une aide à la jeunesse d'une manière intersectorielle et administrativement simple, d'analyser la situation, d'élaborer un plan d'aide approprié et, enfin, d'aider les intéressés à trouver les offreurs d'aide à la jeunesse les plus appropriés.
4. Par région, une porte d'entrée est instaurée⁴. La porte d'entrée est un organe qui fonctionne indépendamment des offreurs d'aide à la jeunesse. Cet organe se compose de deux équipes: une équipe indication et une équipe régie de l'aide à la jeunesse (aussi appelée équipe d'affectation).

¹ Le projet de décret relatif à l'aide intégrale à la jeunesse a été approuvé par le Gouvernement flamand le 1er mars 2013. Il doit encore être approuvé par le Parlement flamand. La présente délibération demeure dès lors sous réserve de l'approbation et de l'entrée en vigueur du décret précité.

² Il s'agit de l'aide à laquelle la personne concernée ou son entourage peut faire appel.

³ Il s'agit de l'aide qui doit être demandée par des services spécialisés.

⁴ Le décret prévoit que le Gouvernement flamand délimite les régions d'aide intégrale à la jeunesse.

5. Les offreurs d'aide à la jeunesse admis au système (tant des personnes individuelles que des structures) peuvent inscrire un enfant mineur auprès d'une porte d'entrée en vue d'une indication et de la réalisation de l'aide à la jeunesse indirectement accessible.
6. L'inscription doit se faire moyennant le consentement et l'engagement maximal de l'enfant mineur, de ses parents ou, le cas échéant, de ses responsables de l'éducation. Elle contient toutes les informations disponibles et requises relatives aux personnes précitées, un rapport sur l'aide déjà fournie à l'enfant mineur, ainsi qu'un rapport sur l'aide à la jeunesse directement accessible qui est déjà offerte (cf. infra).
7. Après l'introduction d'une demande d'obtention d'une aide indirectement accessible par un des demandeurs agréés, l'équipe indication déterminera l'aide à la jeunesse souhaitable au maximum et rédigera un rapport d'indication dans lequel l'aide à la jeunesse proposée est décrite de façon modulaire. Des données diagnostiques supplémentaires relatives à l'enfant mineur peuvent, si nécessaire, être recueillies à l'intervention d'une équipe multidisciplinaire agréée.
8. Ensuite, l'équipe régie de l'aide à la jeunesse:
 - transformera le rapport d'indication en un ou plusieurs modules d'aide à la jeunesse indirectement accessible ou en financement afin de permettre l'aide à la jeunesse;
 - négociera avec les offreurs d'aide à la jeunesse;
 - fixera les modules convenus ou le financement dans une décision sur l'aide à la jeunesse et transmettra cette décision aux intéressés;
 - établira une proposition d'aide à la jeunesse si les modules ne sont pas immédiatement disponibles, et transmettra cette proposition aux intéressés;
 - transmettra le dossier à la Commission régionale intersectorielle des priorités si les modules ne peuvent pas être réalisés et qu'une proposition d'aide à la jeunesse a été établie et transmise;
 - demandera aux offreurs d'aide à la jeunesse d'exécuter, en fonction de la capacité disponible, un ou plusieurs modules d'aide à la jeunesse indirectement accessible pour les dossiers ayant la priorité la plus élevée.
9. Un schéma de l'échange de données entre toutes les parties concernées est présenté comme suit par le demandeur:

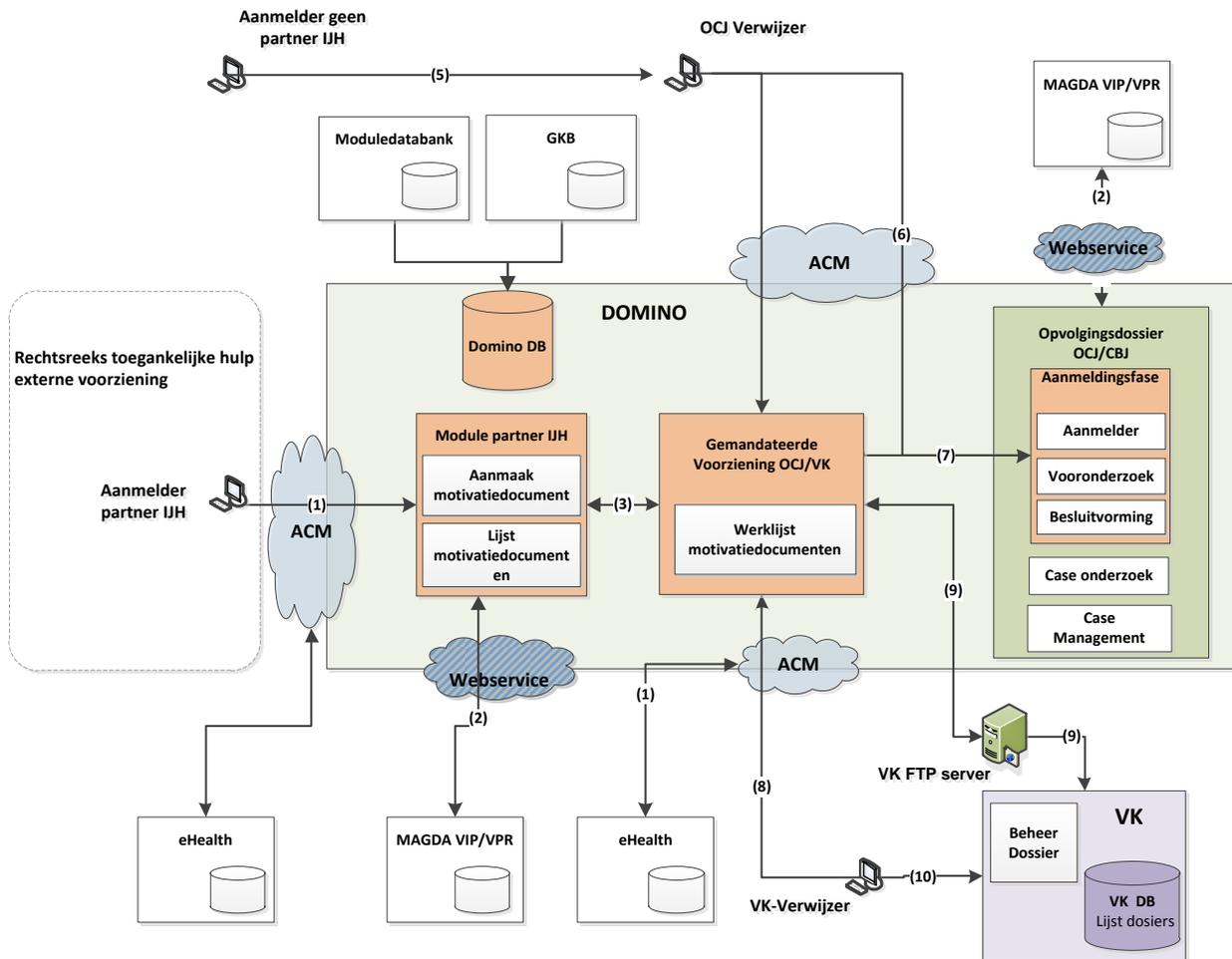
- la vision des prestataires d'aide concernés, éventuellement complétée par des données diagnostiques en relation avec le besoin d'aide provenant d'une équipe multidisciplinaire agréée et ceci à la demande de l'équipe indication; la proposition de l'aide requise provenant de la structure qui inscrit l'enfant mineur; le procès-verbal pertinent de l'entretien avec les intéressés et le procès-verbal pertinent de la discussion du dossier au sein de l'équipe indication;
- l'interrogation relative au besoin d'aide du point de vue de l'enfant mineur inscrit et des autres personnes concernées;
- les données nécessaires à la réalisation d'une indication de qualité par la porte d'entrée, y compris – le cas échéant – les données à caractère personnel nécessaires relatives à la santé;
- le rapport d'indication;
- la décision en matière d'aide à la jeunesse ou la proposition en matière d'aide à la jeunesse.

11. Les offreurs d'aide à la jeunesse individuels qui introduisent une demande n'ont accès qu'aux dossiers de leurs propres clients. Les collaborateurs des structures qui introduisent une demande ont accès aux dossiers de leur propre groupe d'utilisateurs au sein de la structure. Un groupe d'utilisateurs est défini préalablement, en collaboration avec la Plate-forme eHealth, dans le cadre de la gestion des utilisateurs et des accès.
12. Les personnes chargées de l'inscription qui sont titulaires d'un diplôme de médecin peuvent ajouter des données à caractère personnel relatives à la santé à une demande et lire de telles données ajoutées par d'autres médecins. Lors de la phase d'indication, seules les personnes concernées chargées de l'indication avec un diplôme de médecin ont accès aux données à caractère personnel relatives à la santé. Lors de la phase de la régie de l'aide à la jeunesse ou la phase d'affectation, seules les personnes chargées de la régie de l'aide à la jeunesse avec un diplôme de médecin ont accès aux données à caractère personnel relatives à la santé.
13. Si le traitement d'une demande introduite via la porte d'entrée donne lieu à une intervention de l'Agence flamande "Personen met een handicap" (VAPH), les données à caractère personnel enregistrées dans le dossier électronique d'INSISTO seront communiquées à la VAPH afin de permettre à cette agence de réaliser ses missions légales.
14. En effet, s'il ressort du besoin d'assistance que la personne concernée a besoin d'adaptations, de moyens auxiliaires, d'une intervention dans les frais de déplacement et de séjour dans le cadre de l'enseignement ordinaire ou de l'assistance d'une structure subventionnée, il y a lieu d'analyser la demande sur le plan du contenu, à la lumière de la nécessité de l'assistance ou de la subvention demandées en raison du handicap, en vue de l'intégration sociale. La communication de données enregistrées dans le dossier électronique d'INSISTO est par conséquent nécessaire pour informer la VAPH sur le handicap de l'enfant mineur concerné, sur ses possibilités et ses limites, afin de se faire une idée de ses besoins.

2) Domino OCJ

15. Domino OCJ permet le traitement électronique de déclarations de situations inquiétantes à certaines structures mandatées: le Centre de soutien d'aide à la jeunesse (Ondersteuningscentrum Jeugdzorg) et le Centre de confiance pour enfants maltraités (Vertrouwenscentrum Kindermishandeling).
16. Si les offreurs d'aide à la jeunesse constatent qu'ils ne peuvent plus garantir eux-mêmes les possibilités de développement ou l'intégrité de l'enfant mineur ou d'un ou plusieurs membres de son ménage, ils peuvent s'adresser aux structures mandatées précitées.
17. Le Centre de soutien d'aide à la jeunesse a pour mission:
 - de conseiller, à leur demande, les offreurs d'aide à la jeunesse confrontés à des situations inquiétantes;
 - d'examiner les situations inquiétantes et d'en assurer le suivi à la demande des offreurs d'aide à la jeunesse ou du ministère public. Ceci donne lieu à une décision motivée sur l'existence ou non de la nécessité sociale d'aide à la jeunesse;
 - de renvoyer, au besoin, l'enfant mineur à l'aide à la jeunesse directement accessible ou, par le biais de la porte d'entrée, à l'aide à la jeunesse indirectement accessible;
 - de renvoyer l'enfant mineur au ministère public si l'aide à la jeunesse s'avère nécessaire, mais que les personnes concernées n'apportent pas leur collaboration volontaire.
18. Dans le cadre du décret précité, le Centre de confiance pour enfants maltraités (VK) a pour mission:
 - d'examiner les déclarations et les présomptions de maltraitance d'enfants à la demande de toute personne ou institution;
 - de fournir une aide à la jeunesse appropriée à l'enfant mineur victime de maltraitance, ainsi qu'à sa famille;
 - de conseiller, à leur demande, les offreurs d'aide à la jeunesse qui sont confrontés à une situation inquiétante où l'offre d'aide à la jeunesse semble nécessaire d'un point de vue social, ou d'examiner la situation inquiétante.
19. Un schéma de l'échange de données entre toutes les parties concernées dans le cadre de l'application Domino OCJ est présenté comme suit par le demandeur:

AANMELDINGSFASE DOMINO IJH



(1) : Authentification et autorisation via l'Access Control Management de Corve et l'UAM de la plate-forme eHealth dans Domino afin de procéder à une déclaration ou un renvoi pour nécessité sociale (MaNo).

(2) : Extraction des données d'identification du client dans le Registre national (via l'application Magda VIP/VPR).

(3) : Envoi de la déclaration, à l'aide du formulaire de motivation, à la personne chargée du renvoi au sein de la structure mandatée en vue du suivi. La structure mandatée envoie un feed-back au déclarant.

(4) : La personne chargée du renvoi au sein du Centre de soutien d'aide à la jeunesse (OCJ) se connecte à l'application Domino via ACM afin de valider la liste de travail contenant les documents de motivation .

(5) : Le déclarant (pas un partenaire IJH) contactera la personne chargée du renvoi au sein de l'OCJ afin de démarrer un nouveau dossier pour MaNo

(6) : Authentification via ACM/eHealth dans l'application Domino afin de créer manuellement un nouveau dossier OCJ du déclarant (pas un partenaire IJH)

(7) : La personne chargée du renvoi au sein d'OCJ déclare la déclaration recevable. Le suivi démarre automatiquement en complétant la phase de déclaration par des données provenant du document de motivation.

(8) : Authentification et autorisation via l'ACM/plate-forme eHealth afin de permettre au Centre de confiance pour enfants maltraités de consulter la liste de travail contenant les documents de motivation.

(9) : La personne chargée du renvoi au sein du VK déclare la déclaration recevable. Un message XML est envoyé en mode batch au serveur FTP VK afin de télécharger le dossier. Un feed-back concernant le téléchargement réussi ou non est envoyé en mode batch.

(10) : La personne chargée du renvoi au sein du VK consulte le dossier

20. La déclaration est effectuée à l'aide d'un document de motivation contenant toutes les données à caractère personnel qui démontrent que les conditions pour la réalisation d'une déclaration sont remplies. Étant donné qu'il s'agit d'une situation inquiétante, le consentement préalable des intéressés n'est pas requis. Cependant, les intéressés sont en principe préalablement informés. Ce n'est que dans des circonstances spécifiques et dans l'intérêt de l'enfant mineur que les intéressés ne sont pas (immédiatement) mis au courant du traitement de données.
21. Les données à caractère personnel suivantes, y compris des données à caractère personnel relatives à la santé, sont communiquées aux structures mandatées précitées via l'application Domino OCJ, dans le cadre de la déclaration :
- les données d'identification de l'enfant mineur (nom, prénom, sexe, date et lieu de naissance, numéro de Registre national, adresse de domicile et de résidence);
 - les données d'identification du représentant légal et/ou de la personne qui assure l'éducation de l'enfant mineur, les membres du ménage pertinents et les autres personnes concernées pertinentes vis-à-vis de l'enfant mineur;
 - esquisse de la problématique par le prestataire d'aide concerné qui effectue la déclaration;
 - esquisse de la problématique du point de vue de la personne concernée;
 - vision de la personne concernée par rapport à la déclaration;
 - description du caractère inquiétant et motivation de la déclaration;
 - esquisse de l'historique de l'aide du point de vue du prestataire d'aide;
 - toutes les informations supplémentaires pertinentes;
 - indication selon laquelle le client a été informé;
 - date de la décision de l'équipe à laquelle appartient l'offreur d'aide à la jeunesse qui approuve la déclaration.

II. COMPÉTENCE

22. Conformément à la loi du 13 décembre 2006, toute communication de données à caractère personnel relatives à la santé doit faire l'objet d'une autorisation de principe de la section santé du Comité sectoriel de la sécurité sociale et de la santé.⁶

⁶ Article 42, § 2, 3°, de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, *M.B.* du 22 décembre 2006.

23. La communication de données à caractère personnel relatives à la santé ne doit pas faire l'objet d'une autorisation, entre autres, lorsque la communication est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance, après avis de la Commission de la protection de la vie privée.
24. En l'occurrence, la communication de données à caractère personnel relatives à la santé s'inscrit dans le (projet de) décret relatif à l'aide intégrale à la jeunesse concernant lequel la Commission de la protection de la vie privée a rendu un avis (avis n° 27/2012 du 12 septembre 2012). Le Gouvernement flamand peut déterminer les données à caractère personnel que les acteurs traiteront concrètement ainsi que la forme du traitement, comme l'a constaté la Commission dans l'avis précité. Étant donné que ces arrêtés n'ont pas encore été pris, le Comité sectoriel n'est pas en mesure de constater, à l'heure actuelle, si l'exemption d'autorisation s'applique ou non à la communication, conformément à l'exception précitée. Il est dès lors effectivement indiqué que la communication soit soumise à l'approbation du Comité sectoriel.
25. La présente délibération est dès lors subordonnée à l'approbation et à l'entrée en vigueur du décret relatif à l'aide intégrale à la jeunesse. Le Comité sectoriel souligne en outre que la communication de données à caractère personnel dans le cadre de l'aide intégrale à la jeunesse, telle qu'autorisée par la présente délibération, devra évidemment toujours être confrontée aux arrêtés d'exécution futurs et, au besoin, une modification de la présente délibération devra être obtenue.
26. Enfin, le Comité sectoriel constate que l'AJW a déjà reçu, dans le cadre du présent projet, l'autorisation du Comité sectoriel du Registre national ainsi que celle de la Commission de contrôle flamande pour l'échange électronique de données administratives.

III. EXAMEN DE LA DEMANDE

A. ADMISSIBILITÉ

27. Le traitement de données à caractère personnel relatives à la santé est en principe interdit.⁷ Cette interdiction ne s'applique cependant pas, comme c'est le cas en l'espèce, lorsque le traitement est rendu obligatoire par ou en vertu d'une loi, d'un décret ou d'une ordonnance pour des motifs d'intérêt public importants. En outre, il est prévu que l'inscription auprès de la porte d'entrée intersectorielle dans le cadre d'INSISTO ne puisse se faire que moyennant le consentement des personnes concernées (l'enfant mineur, ses parents ou son représentant légal). Dans la mesure où le consentement n'est pas obtenu dans le cadre d'une situation inquiétante (Domino OCJ), le traitement peut être autorisé en vertu du fait qu'il est nécessaire à la prévention d'un danger concret et même à la défense des intérêts vitaux de la personne concernée.

⁷ Article 7er, § 1er, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.* 18 mars 1993 (dénommée ci-après loi relative à la vie privée).

28. Compte tenu de ce qui précède, le traitement de données à caractère personnel relatives à la santé est autorisé.

B. FINALITÉ

29. Les données à caractère personnel doivent être obtenues pour des finalités déterminées, explicites et légitimes.
30. L'objectif du traitement de données dans le cadre des applications INSISTO et Domino OCJ est la réalisation de l'aide intégrale à la jeunesse, telle que prévue dans le (projet de) décret. L'aide intégrale à la jeunesse doit permettre de fournir de l'aide et des soins sur mesure aux enfants mineurs, à leurs parents et, le cas échéant, à leurs responsables de l'éducation et aux personnes concernées de leur entourage qui en ont besoin. Comme mentionné explicitement dans le (projet de) décret, le traitement de données est effectué sous la responsabilité de l'Agence flamande "Jongerenwelzijn". Vu ce qui précède, le Comité sectoriel constate dès lors que le traitement envisagé poursuit une finalité déterminée, explicite et légitime.

C. PROPORTIONNALITÉ

31. Les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement.⁸
32. Dans le cadre de l'enregistrement dans INSISTO et dans DOMINO OCJ, des données à caractère personnel sont communiquées devant permettre d'identifier la personne concernée et son entourage et de décrire les circonstances concrètes justifiant l'aide à la jeunesse indirectement accessible (comme expliqué sous les points 8 et 17). À cet égard, il est également prévu que les déclarants qui sont titulaires d'un diplôme de médecin puissent ajouter des données à caractère personnel relatives à la santé, pour autant que ce soit nécessaire. L'AJW avance les arguments selon lesquels les données à caractère personnel relatives à la santé sont nécessaires afin de pouvoir déterminer le type d'aide à la jeunesse à fournir ou afin de pouvoir tenir compte - lorsqu'un type d'aide déterminé est fourni - des limitations psychiques ou physiques de la personne concernée. L'AJW précise également que les données à caractère personnel relatives à la santé envisagées doivent en principe porter sur la situation actuelle au moment de de l'enregistrement.
33. Les deux systèmes prévoient – via la gestion intégrée des utilisateurs et des accès (cf. infra) – que les utilisateurs n'ont accès qu'aux seules données à caractère personnel dont ils ont besoin pour accomplir leurs tâches et leurs missions. Cela implique que les personnes chargées de l'enregistrement, de l'indication et de la régie de l'aide à la jeunesse n'ont accès qu'aux seules données à caractère personnel de leurs clients. Cela signifie également que les données à caractère personnel relatives à la santé ne peuvent être consultées que par les utilisateurs (les personnes chargées de l'enregistrement, de l'indication et de la régie de l'aide à la jeunesse) qui sont en même temps médecins.

⁸ Article 4, 2°, de la loi relative à la vie privée.

34. Vu ce qui précède, le Comité sectoriel estime que la communication des données à caractère personnel relatives à la santé envisagées est adéquate, pertinente et non excessive à la lumière de la finalité envisagée.
35. Les données à caractère personnel ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant un délai n'excédant pas celui nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. Le demandeur prévoit que les données à caractère personnel pour le dossier électronique seront conservées jusqu'au moment où la personne concernée aura 50 ans (compte tenu du fait qu'il y a moyen de poursuivre l'aide à la jeunesse jusqu'à ce que la personne concernée ait 25 ans).
36. Pour justifier le délai de conservation précité, le demandeur souligne que la porte d'entrée et le Centre de soutien d'aide à la jeunesse participent à la prise de décisions qui ont un impact profond sur la vie des enfants mineurs concernés. Cependant, ceux-ci ne sont pas toujours en mesure de comprendre les raisons des décisions, ni les situations qui ont donné lieu à l'enregistrement. Des événements qui ont un effet profond sur la vie perturbent la stabilité et la continuité d'une personne. Dans ce cas, la vision du monde que l'on a et, par conséquent, de sa place dans le monde est bouleversée. Bref, cela induit le besoin d'une reconstruction narrative. Ce besoin peut encore se manifester plus tard dans la vie, comme le constate 'Jongerenwelzijn' dans la pratique. Un aspect important de la charge psychosociale vécue par les personnes ayant un passé dans l'aide à la jeunesse (souvent accompagnée d'un placement) est la rupture dans la perspective de vie que l'on éprouve. Cette rupture donne lieu à un processus de reconstruction narrative au cours duquel la vision subjective des événements est modifiée. Au cours d'un processus appelé *emplotment*, les événements sont configurés et reliés entre eux de façon à développer des structures significatives. Des études du processus qui incite les délinquants à ne plus commettre des infractions (processus appelé *desistance*) ont par ailleurs démontré que les constructions narratives, subjectives et individuelles que développent les auteurs pour donner une signification à certains moments-clé et à certains changements dans leur vie, jouent un rôle essentiel dans ce processus de *desistance*. Le demandeur est d'avis que la conservation des données jusqu'au moment où le client a 50 ans permettra à ce dernier d'arriver au processus d'*emplotment*.
37. Le Comité sectoriel estime que s'il existe un motif valable pour la conservation des données à caractère personnel jusqu'à l'âge de 50 ans, ce même motif vaut également pour la conservation des données à caractère personnel au-delà de l'âge de 50 ans. Le Comité sectoriel estime que même au-delà de cet âge, les informations conservées dans le système peuvent s'avérer utiles pour le traitement médical ou psychologique de l'intéressé. Le Comité sectoriel conclut dès lors que les données à caractère personnel peuvent être conservées jusqu'au décès de l'intéressé, à la suite duquel elles doivent être détruites. Le Comité sectoriel estime, par ailleurs, qu'à défaut d'un cadre spécifique, il est primordial qu'après la cessation de l'aide à la jeunesse, les données à caractère personnel ne puissent être communiquées qu'à la demande de l'intéressé ou moyennant son consentement écrit. Le demandeur est tenu de prévoir les garanties nécessaires à cet effet.

D. TRANSPARANCE

38. Conformément à l'article 9 de la loi relative à la vie privée, le responsable du traitement doit fournir à la personne concernée des informations concernant les modalités du traitement et ses droits.
39. En ce qui concerne le traitement de données dans le cadre d'INSISTO, le (projet de) décret prévoit que la personne concernée donne son consentement pour le traitement de données. À cette occasion, les personnes concernées recevraient une lettre d'information contenant toutes les informations nécessaires relatives au traitement de données. Le Comité sectoriel estime que le demandeur doit soumettre le contenu de cette lettre d'information, préalablement à son utilisation, à l'approbation du Comité sectoriel.
40. En ce qui concerne le traitement de données dans le cadre de Domino OCJ, le (projet de) décret stipule que les personnes concernées doivent en principe être informées de la déclaration auprès des structures mandatées. Le Comité sectoriel estime que le demandeur doit également soumettre préalablement les informations à fournir à l'approbation du Comité sectoriel.
41. Dans la mesure la situation inquiétante de l'enfant mineur en question le requiert, le (projet de) décret prévoit, dans le cadre de l'enregistrement dans Domino OCJ, de ne pas fournir d'informations ou de ne les fournir qu'à un moment ultérieur. L'article 9, § 2, alinéa 2 de la loi relative à la vie privée prévoit en effet que le responsable du traitement est dispensé de la communication lorsque l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

E. MESURES DE SÉCURITÉ

42. Le traitement de données à caractère personnel relatives à la santé doit être effectué sous la surveillance et la responsabilité d'un professionnel des soins de santé⁹. Même si ce n'est pas strictement requis, le Comité sectoriel estime qu'il est préférable de traiter de telles données sous la responsabilité d'un médecin¹⁰. Le Comité sectoriel a effectivement reçu l'identité du médecin concerné. Le Comité sectoriel 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.
43. Le responsable du traitement doit prendre les mesures techniques et organisationnelles appropriées qui sont nécessaires à la protection des données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel¹¹. Le Comité sectoriel renvoie à ce propos aux mesures de référence qui sont applicables à la protection de tout traitement de données à caractère personnel, qui ont été

⁹ Article 7, § 4, de la loi relative à la vie privée.

¹⁰ Délibération n° 07/034 du 4 septembre 2007

¹¹ Article 16 de la loi relative à la vie privée.

établies par la Commission de la protection de la vie privée.¹² 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.

44. Pour garantir la confidentialité et la sécurité du traitement de données, tout organisme qui conserve, traite ou communique des données à caractère personnel est, en fonction du contexte et de la nature des données à caractère personnel, 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, ...); respect et documentation. Le Comité sectoriel prend acte du fait que le demandeur confirme qu'il prévoit toutes les mesures de sécurité requises, en ce compris la désignation d'un conseiller en sécurité de l'information.
45. Conformément aux dispositions du (projet de) décret, l'Agence flamande 'Jongerenwelzijn' fait appel à la Plate-forme eHealth et à la Banque Carrefour de la sécurité sociale comme intégrateurs de service. Concrètement, les services de base suivants seront utilisés:
 - le portail: un lien vers les applications concernées sera ajouté sur le portail de la Plate-forme eHealth;
 - la gestion intégrée des utilisateurs et des accès: qui garantit que seuls les utilisateurs autorisés puissent avoir accès aux applications INSISTO et Domino OCJ.
46. La gestion des utilisateurs et des accès qui est prévue, requiert en effet la collaboration entre l'Access Control Management (ACM) de la Cellule de coordination Vlaams e-government (Corve) et la plate-forme eHealth. A cet effet, une solution générique a été élaborée qui permet de rendre une application hébergée sur le portail d'un partenaire déterminé accessible à un ou plusieurs groupes cibles qui ne sont pas connus dans la gestion des utilisateurs de ce partenaire déterminé, mais bien dans celle d'un autre partenaire.

Afin d'éviter de devoir enregistrer un seul groupe cible dans plusieurs systèmes de gestion des utilisateurs différents, il est prévu une collaboration entre les deux partenaires. A cet effet, une communication est établie en fonction d'un protocole déterminé entre les Identity Providers¹³ (IDP) des deux partenaires, de sorte que l'utilisateur puisse s'identifier auprès de

¹²

http://www.privacycommission.be/sites/privacycommission/files/documents/mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel.pdf

¹³ Il s'agit d'un composant qui fournit une interface web permettant à l'utilisateur de s'authentifier et qui met les données d'identification à la disposition du fournisseur d'accès (il s'agit du composant qui contrôle l'accès à l'application web).

cet IDP qui donne accès à la gestion des utilisateurs dans laquelle l'utilisateur et le groupe cible concernés sont connus. Cette solution a recours aux protocoles standard, fixés par la OASIS Security committee. Le Comité sectoriel a reçu une note à ce sujet.

De manière concrète, le processus se déroule comme suit:

- L'utilisateur demande l'accès à l'application sécurisée ;
- Le fournisseur d'accès intercepte la requête de l'utilisateur non encore authentifié et l'envoie au fournisseur d'identité (IDP) ;
- L'utilisateur sélectionne auprès de l'IDP une méthode d'authentification ou un groupe cible qui sera pas traité par l'IDP même ;
- L'IDP intervient comme proxying IDP, crée une nouvelle requête d'authentification et la transmet à l'autre IDP (qui intervient comme authenticating IDP) ;
- L'authenticating IDP renvoie une réponse contenant les données d'identité utiles au proxying IDP ;
- Le proxying IDP effectue si nécessaire un traitement supplémentaire sur les données et renvoie une réponse contenant les données d'identité utiles au fournisseur de services ;
- Un module d'authentification situé chez ou dernière le fournisseur de services traite les données d'identité pour obtenir un Principal object et met l'utilisateur en contact avec l'application qu'il avait demandée au cours de la première étape.

Lorsque le domaine de destination ne reçoit pas tous les attributs qui ont été transmis par l'Authenticating IDP, un élément dans le domaine du proxying doit offrir la possibilité de demander ces attributs supplémentaires auprès du domaine de l'Authenticating IDP. Cet échange supplémentaire de données doit avoir lieu conformément à un protocole Assertion Query/Request déterminé. Lorsque le proxying et l'authenticating IDP n'utilisent pas les mêmes valeurs, il appartient au Proxying IDP de convertir les valeurs dans le jargon du domaine de destination.

Après authentification via un IDP, un domaine hosting exécutera des règles d'autorisation avant d'accorder l'accès à l'application à un utilisateur (à ce moment, identifié et connu via une liste d'attributs). Ceci intervient par un élément déterminé, le PEP (Policy Enforcement Point). Avant de prendre une décision, le PEP doit contacter le PDP (Policy Decision Point) du domaine qui gère les règles d'autorisation. Si le PDP n'a pas reçu toutes les informations utiles du domaine proxying, il doit être en mesure de faire appel à un PIP (Policy Information Point) auprès du domaine authenticating pour obtenir les informations supplémentaires et ce conformément à un Protocole Query/Request déterminé.

Un des objectifs d'un IDP est d'effectuer le SingleSignOn (SSO) pour l'utilisateur entre toutes les applications pour lesquelles il est contacté en tant qu'IDP pendant une session d'utilisation. En intervenant en tant que proxying IDP, il est cependant fait appel à un nouvel authenticating IDP qui ne connaît peut-être pas encore l'utilisateur pendant cette même session de navigation de l'utilisateur. Si l'utilisateur était déjà connu dans le proxying IDP, il serait à nouveau invité à s'authentifier dans l'authenticating IDP. Pour éviter ceci, les possibilités suivantes ont été élaborées:

- Le proxying IDP peut déclarer que l'utilisateur est déjà connu chez lui après authentification via une méthode d'authentification déterminée.

- Lorsque les IDP des deux partenaires font authentifier les utilisateurs via l'eID Middleware de Fedict, un SSO est automatiquement créé pour le login avec l'eID et ce aussi longtemps que la carte est maintenue dans le lecteur de carte. L'utilisateur sera donc automatiquement admis dans l'Authenticating IDP sans qu'il ne doive à nouveau introduire son code PIN.
- Fedict met également un IDP à la disposition qui permet une identification au moyen de différentes méthodes d'authentification telles que l'eID et le token fédéral. Il s'agit d'un mécanisme de proxying par lequel les IDP des deux partenaires envoient à leur tour une requête de proxying authentication à l'IDP de Fedict en vue d'une authentification au moyen de la méthode demandée. Un SSO est ainsi aussi créé entre les deux partenaires.

Pour obtenir un Single Logout (SLO), il faut qu'il y ait au moins une communication entre les différents IDP qui se sont échangés des informations d'identité pendant une session de navigation de l'utilisateur et éventuellement aussi avec les applications finales auxquelles des informations relatives à l'identité ont été fournies sous la forme de tokens de session. Un protocole Single Logout déterminé est prévu à cet effet. Si tant un proxying qu'un authenticating IDP soutiennent ceci, il est possible d'implémenter, outre un SSO entre les deux IDP, un SLO de sorte qu'un utilisateur qui est authentifié dans les deux domaines pendant une session de navigation active puisse indiquer à l'aide d'un seul clic qu'il souhaite se déconnecter des deux domaines.

Le Comité sectoriel approuve la solution générique décrite dans la note soumise.

47. La consultation des données d'identification de l'enfant mineur concerné dans le Registre national est effectuée à l'intervention de la Banque Carrefour de la sécurité sociale. Le Comité sectoriel souligne que l'utilisation du numéro de Registre national et l'accès aux données du Registre national requièrent l'autorisation du Comité sectoriel du Registre national.

Par ces motifs,

la section Santé du Comité sectoriel de la sécurité sociale et de la santé

autorise, sous réserve de l'approbation et de l'entrée en vigueur du décret relatif à l'aide intégrale à la jeunesse,

selon les modalités de la présente délibération, la communication de données à caractère personnel relatives à la santé, dans le cadre de l'aide intégrale à la jeunesse organisée au sein de l'Agence flamande 'Jongerenwelzijn', dans la mesure où:

- les données à caractère personnel sont conservées jusqu'au décès de l'intéressé, tel que décrit sous le point 37;
- après la cessation de l'aide à la jeunesse, les données à caractère personnel de l'enfant mineur ne seront communiquées qu'à la demande de l'enfant mineur ou moyennant son consentement, tel que décrit sous le point 37;
- le contenu des lettres d'information est soumis, préalablement à leur utilisation, à l'approbation du Comité sectoriel, tel que décrit sous les points 39 et 40.

Yves ROGER
Président

Le siège du comité sectoriel de la sécurité sociale et de la santé est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: Quai de Willebroeck 38 - 1000 Bruxelles.