

Conseiller en sécurité CPAS : mutualisation

Une première note sur le fonctionnement de la connexion des CPAS à la BCSS a été élaborée par la Fédération et fournie au cabinet en préparation à la réunion du GT informatisation du 11 mars 2015.

Complémentairement à celle-ci, nous détaillons dans cette note sur le conseiller en sécurité en CPAS les missions qui lui incombent eût égard à la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale et à l'arrêté royal du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les organisations de sécurité sociale.

Nous détaillerons ensuite les situations de terrain en Wallonie et en Flandre et, partant, les raisons permettant d'envisager différentes formes de mutualisation du conseiller en sécurité.

Les expériences de terrain du côté de la Flandre révèlent que la mutualisation du conseiller en sécurité entre CPAS (via l'association Titre VIII, Chapitre 1) et avec la Province est pertinente en termes de taille critique et de fonctionnement.

Des informations que nous avons reçues du SPP IS, les mutualisations ayant pour taille critique le regroupement d'une dizaine de CPAS sont idéales en ce qu'elles rencontrent ainsi l'exigence de terrain qu'un professionnel soit affecté à la sécurité à temps plein, et qu'elles permettent également, par la concentration des acteurs, d'organiser plus facilement les nécessaires relais entre les CPAS, le SPP IS et la BCSS (notamment sur le plan de la formation).

S'appuyant sur ces expériences, trois formes de mutualisation seront plus particulièrement détaillées.

Ces formes sont :

- la mutualisation dans un service provincial
- la mutualisation inter-CPAS
- la mutualisation au niveau régional

Dans tous les cas de mutualisation envisagés, le lien entre le responsable de la gestion journalière de l'institution et le service chargé de la sécurité doit être au centre afin de garantir une réactivité optimale du travail et, dès lors, la pertinence de la mutualisation.

Cette note n'est pas exhaustive. La Fédération des CPAS continue le travail, en lien avec le terrain, afin d'analyser les meilleures manières d'opérationnaliser cette mutualisation du conseiller en sécurité pour qu'elle réponde aux besoins des CPAS et aux obligations qu'ils ont à respecter dans le cadre de leur connexion à la BCSS. Elle reviendra donc avec des éléments plus concrets après analyse.

A. Le CPAS et la connexion à la BCSS

1. Intégration des CPAS dans le réseau de la BCSS

Depuis le 1^{er} janvier 2006, les CPAS appartiennent au réseau de la BCSS:

- en leur qualité d'*institution de la sécurité sociale* : voir la **loi du 15 janvier 1990** relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale ;
- en leur qualité de personnes auxquelles le réseau de la sécurité sociale a été étendu : voir **arrêté royal du 4 mars 2005** relatif à l'extension du réseau de la sécurité sociale aux centres publics d'action sociale.

Moyennant une autorisation du Comité sectoriel de la sécurité sociale et de la santé, les CPAS peuvent faire appel à des données à caractère personnel disponibles dans le réseau BCSS, en tenant compte des principes de finalité et de proportionnalité 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.

2. Obligations de sécurité découlant de l'intégration des CPAS dans le réseau de la BCSS

Outre le respect des législations en termes d'enregistrement, de communication et de traitement des données, les CPAS sont tenus également de développer une politique de sécurité importante, notamment en vertu de l'article 22 de la loi du 15 janvier 1990 qui stipule que « *la Banque-carrefour et les institutions de sécurité sociale sont tenues de prendre toutes les mesures qui permettent de garantir la parfaite conservation des données sociales à caractère personnel* ».

Les CPAS sont donc tenus de prendre les mesures techniques et organisationnelles qui s'imposent pour protéger les données à caractère personnel.

a) Directives de sécurité

Des directives de sécurité sont disponibles sur le site de la BCSS. Elles établissent des objectifs de sécurité à atteindre par tout organisme dans le domaine de la sécurité de l'information. Chaque institution doit les mettre le plus adéquatement en œuvre en fonction des risques spécifiques qu'elle encoure.

Les directives sont essentiellement préventives et concernent la prévention des menaces physiques (incendie, inondation, humidité, alimentation électrique...), humaines (sabotage, vol, intrusion, accès aux bâtiments...), logiques (accès aux programmes et aux données, sécurisation des applications...).

Des directives sont également édictées en cas de reprise des activités après sinistre total ou partiel¹.

¹ BCSS, Directives en matière de sécurité au niveau des institutions participant au réseau géré par la BCSS.
V. : <https://www.ksz-bcss.fgov.be/binaries/documentation/fr/securete/directives.pdf> [consulté le 3 mars 2015].

b) Normes minimales

Pour accéder à la BCSS, les institutions de sécurité sociale doivent obligatoirement respecter des normes minimales établies à partir de la norme ISO 27002 : 2013. Ces normes minimales ont une valeur contraignante. Le respect de celles-ci est vérifié annuellement par la complétion d'un questionnaire émis par la BCSS. Ainsi, tous les ans, les CPAS reçoivent ce questionnaire, par l'intermédiaire du SPP IS.

Le Comité sectoriel de la sécurité sociale veille au respect des normes. En cas de non-respect de celles-ci, l'accès par l'institution à la BCSS peut être interdit. A cet égard, le conseiller en sécurité du CPAS doit remplir annuellement un questionnaire de la BCSS qui lui est adressé par l'intermédiaire du SPP IS et qui vérifie la mise en œuvre concrète des normes.

Les normes minimales sont régulièrement adaptées en fonction des évolutions légales et techniques. La version 2015 des normes minimales est disponible sur le site de la BCSS².

Ces normes minimales portent sur les aspects suivants:

- la politique de sécurité de l'information
- l'organisation de la sécurité
- la sécurité liée aux collaborateurs
- la gestion des ressources de l'entreprise
- la protection d'accès logique,
- la cryptographie
- la sécurité physique et la protection de l'environnement,
- la gestion opérationnelle (logging, protection contre des logiciels malveillants, ...),
- La sécurité des communications
- L'acquisition, le développement et la maintenance de systèmes,
- La relation avec les fournisseurs
- la gestion des incidents,
- L'aspect de la sécurité de l'information dans la gestion de la continuité,
- La conformité (contrôle/audit).

² BCSS, Normes minimales. Version 2015 (ISO27000 :2013). V. https://www.ksz-bcss.fgov.be/binaries/documentation/fr/securite/normes_minimales_securite_2015.pdf [consulté le 3 mars 2015].

c) Désignation d'un conseiller en sécurité par le CPAS³

L'article 24 de la loi du 15 janvier 1990 prévoit la désignation, pour toute institution de sécurité sociale, d'un conseiller en sécurité.

L'arrêté royal du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les organisations de sécurité sociale impose à toutes ces institutions d'instaurer un service de sécurité de l'information placé sous la direction d'un conseiller en sécurité.

• Modalités de désignation

Pour les CPAS, la désignation du conseiller en sécurité se fait par le Conseil de l'action sociale et doit être communiquée au SPP IS.

La personne désignée doit ensuite compléter le « questionnaire d'évaluation pour le candidat conseiller en sécurité » sur le site de la Commission de la protection de la vie privée. La candidature du conseiller sera évaluée par la Section Sécurité Sociale du Comité sectoriel de la Sécurité Sociale. Le candidat doit y renseigner son parcours éducatif et professionnel, les fonctions/mandats exercés en dehors de l'organisme demandeur, ses connaissances (concepts de base de l'informatique, informatique médicale, lois et règlements en vigueur, sécurité de l'information). Ce questionnaire vise à évaluer si le candidat répond aux conditions suivantes :

- ne pas exercer de fonctions incompatible avec sa mission (principe qu'une personne ne peut pas à la fois être contrôleur et contrôlé) ;
- doit être objectif et impartial lors de la réalisation et l'appréciation d'analyses faisant l'objet d'un rapport ;
- doit être suffisamment formé pour exercer la fonction ;
- doit disposer de suffisamment de temps pour réaliser ses missions relatives à la sécurité.

• Missions

L'arrêté royal du 12 août 1993 précise, dans son article 3, les missions du service chargé de la sécurité de l'information. Celui-ci a une mission d'avis de stimulation, de documentation et de contrôle. Nous reprendrons dans un tableau les missions du service et la manière dont l'arrêté précise, le cas échéant, leurs modalités d'opérationnalisation.

Missions	Opérationnalisation
<p><i>Conseiller le responsable de la gestion journalière de l'institution, à la demande de celui-ci ou de sa propre initiative, au sujet de tous les aspects de la sécurité de l'information.</i></p>	<p><i>Sauf si les risques ne sont pas suffisamment importants, les avis s'expriment par écrit et sont motivés. Dans le délai requis par les circonstances, mais avec un maximum de trois mois, le responsable de la gestion journalière décide de suivre ou non les avis et informe le service chargé de la sécurité de la décision adoptée. Si la décision déroge à un avis exprimé par écrit, elle doit être communiquée de façon écrite et motivée.</i></p>
<p><i>Promouvoir le respect des règles de sécurité imposées par une disposition légale ou réglementaire ou en vertu d'une telle disposition, ainsi que l'adoption, par les</i></p>	

³ BCSS, Procédure concernant la désignation d'un conseiller en sécurité par les CPAS. V. https://www.ksz-bcss.fgov.be/binaries/documentation/fr/securite/policies/isms_031_ocmw_cpas_fr.pdf [consulté le 3 mars 2015.]

<i>personnes employées dans l'institution, d'un comportement favorisant la sécurité.</i>	
<i>Rassembler la documentation utile à ce sujet.</i>	
<i>Veiller au respect, dans l'institution, des règles de sécurité imposées par une disposition légale ou réglementaire ou en vertu d'une telle disposition.</i>	<i>Toutes les infractions constatées sont communiquées par écrit et exclusivement au responsable de la gestion journalière de l'institution, accompagnées des avis nécessaires en vue d'éviter de telles infractions à venir.</i>

- **Autorité fonctionnelle**

Conformément à l'article 4 de l'arrêté royal du 12 août 1993, le service chargé de la sécurité de l'information est placé sous la direction du conseiller en sécurité et, suivant l'article 5, sous l'autorité fonctionnelle directe du responsable de la gestion journalière de l'institution à savoir, dans le cas du CPAS, le Directeur général.

Comme on le voit, l'article 3 de l'arrêté royal du 12 août 1993 prévoit une étroite collaboration entre le conseiller en sécurité et le responsable de la gestion journalière de l'institution. Il s'agit de garder cela à l'esprit dans les formes de mutualisation que nous envisagerons par la suite, afin de ne pas rompre ce lien indispensable en cas d'externalisation du service chargé de la sécurité de l'information.

- **Travail du conseiller⁴**

Le conseiller s'occupe de l'ensemble des mesures de sécurité appliquées aux données à caractère social. Il est donc amené à veiller à la sécurité :

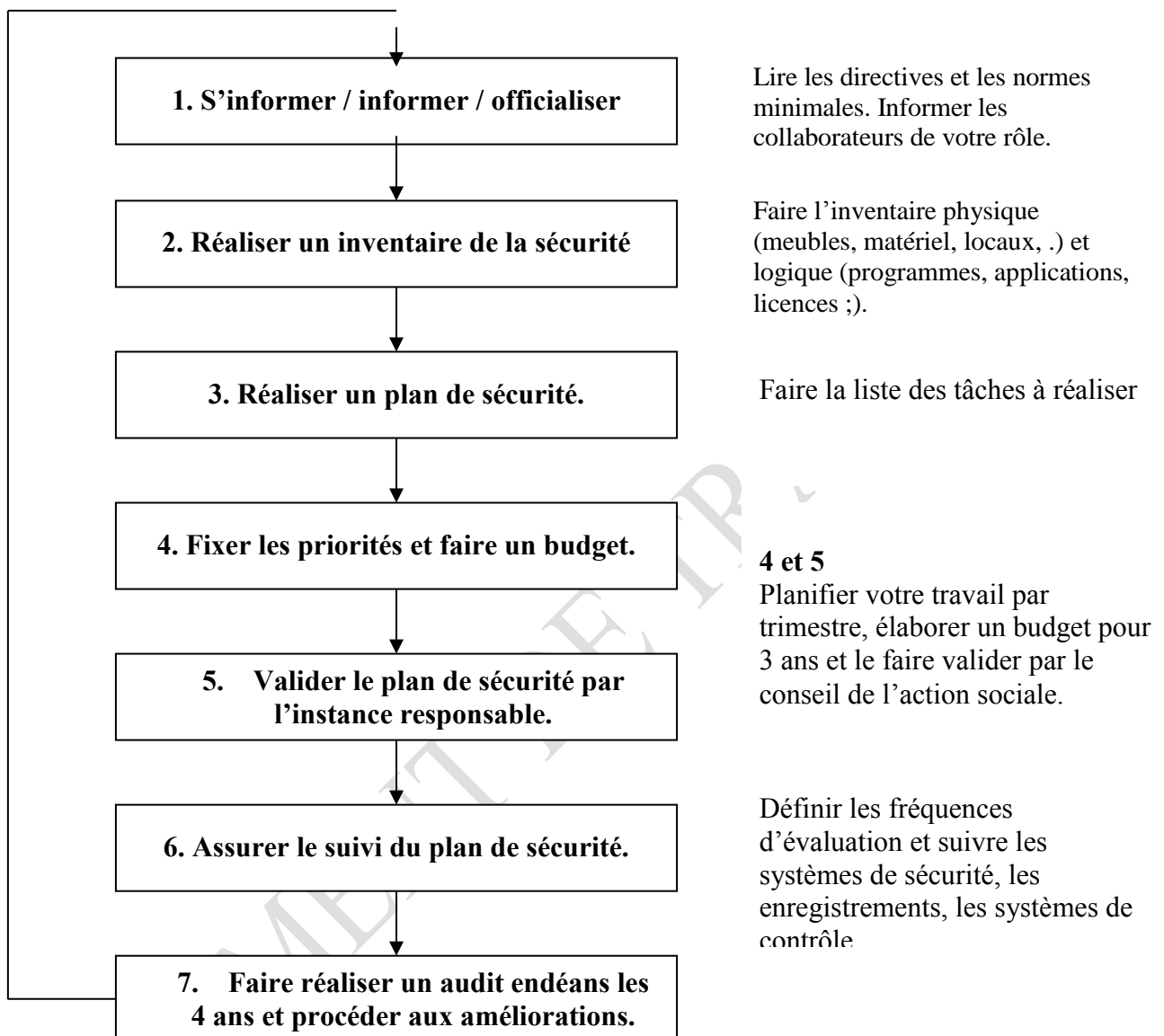
- des accès aux données à caractère social (logiciel social, logiciel comptable, dossiers avec des documents contenant des données à caractère social, etc.) ;
- de leur utilisation ;
- du stockage physique et informatique ;
- des utilisateurs de ces données ;
- de la restauration de ces données ;
- du respect de la loi sur la protection de la vie privée

Il veillera aussi à :

- organiser les mesures à prendre pour répondre aux conditions minimales de sécurité: rédiger le plan de sécurité, coordonner les actions du CPAS, prendre contact avec les services spécialisés (firmes informatiques, services de sécurité, etc.), sensibiliser les utilisateurs de la connexion aux aspects de sécurité, etc.;
- apporter au Conseil de l'Action sociale un éclairage sur la politique de sécurité qui soit le plus pertinent pour le centre, dans le respect des normes définies par la BCSS;
- servir de relais entre le Conseil de l'Action sociale, le Directeur général, les différents services, les travailleurs sociaux ou administratifs utilisateurs de la connexion, la BCSS, le SPP Intégration sociale, les firmes informatiques, etc.;
- contrôler que les règles édictées en matière de sécurité soient respectées.

⁴ SPP IS, Kit de sécurité. Guide de mise en pratique des normes minimales. Voir : <http://www.mi-is.be/be-fr/cpas/securite-dinformation>

Schématiquement, les différentes étapes de son travail peuvent être résumées comme suit⁵ :



⁵ SPP IS, Kit de sécurité. Guide de mise en pratique des normes minimales, p.5. Voir : <http://www.mi-is.be/be-fr/cpas/securite-dinformation>

B. Les possibilités de mutualisation du conseiller en sécurité

1. Pourquoi mutualiser ?

Si, au départ de la connexion des CPAS à la BCSS, la fonction de conseiller en sécurité pouvait s'envisager sans compétences informatiques particulièrement poussées, l'évolution et la complexification des technologies, des risques informatiques et des textes réglementaires relatifs à la sécurité font qu'aujourd'hui, une professionnalisation de cette fonction s'avère nécessaire.

Or, sur le terrain, les conseillers en sécurité actuellement désignés occupent cette fonction en sus de la fonction administrative, sociale, ou managériale qu'ils exercent par ailleurs au sein du CPAS. Dans la majorité des cas, ils ne disposent ni du temps suffisant pour se mettre à jour en terme de formation ou de documentation, ni de toute la compétence requise pour implémenter les normes techniques de sécurité.

L'informatique en CPAS est un outil de travail fondamental, mais doit bel et bien rester un outil au service des missions sociales. Vu les spécificités des missions des CPAS, les règles de sécurité doivent être consciencieusement respectées. Ces deux domaines représentent une charge financière importante que des mutualisations optimales et réfléchies sur la mesure des réalités de terrain permettraient de diminuer.

D'autres avantages sont encore à noter aux mutualisations. Comme décrit dans la précédente note rendue par la Fédération des CPAS dans le cadre du GT informatisation et qui consistait en la présentation générale de la BCSS, les CPAS font partie du réseau secondaire de la BCSS. C'est le SPP IS qui se profile comme institution du réseau primaire et qui est chargé, vis-à-vis de la BCSS, de la gestion du réseau secondaire (CPAS) en suivant les tâches définies par l'article 6 de l'Arrêté royal du 4 février 1997 organisant la communication de données sociales à caractère personnel entre institutions de sécurité sociale. Une mutualisation des conseillers en sécurité de CPAS permettrait de faciliter et favoriser la communication avec le conseiller en sécurité du SPP IS qui s'adresserait ainsi à un nombre plus limité d'interlocuteurs. Il y aurait donc certainement là un gain d'efficacité.

De plus, les mutualisations permettraient de renforcer les acteurs de terrain face à la situation monopolistique informatique en Wallonie en faisant levier non seulement sur le plan des coûts, mais également des exigences de sécurité propres à la connexion à la BCSS.

2. Situation en Wallonie

Selon les informations reçues par le SPP IS, sur les 262 CPAS wallons, 252 conseillers en sécurité sont recensés. Les quelques exemples de conseillers en sécurité communs ne concernent pas toujours des mutualisations à proprement parler. Il peut s'agir en effet d'un Directeur général travaillant à temps partiel dans deux petits CPAS et qui assume cette fonction dans les deux entités. Il peut également s'agir d'un même conseiller en sécurité travaillant pour une société informatique privée avec laquelle plusieurs CPAS travaillent.

Les conseillers en sécurité exercent cette activité en plus des tâches qu'ils exercent par ailleurs au sein du CPAS. Le temps consacré à ces aspects est donc bien souvent rabaissé par la charge de travail exercée en lien direct avec les missions du CPAS.

Le SPP estime qu'11% des CPAS disposent d'un conseiller ayant des connaissances informatiques.

3. Situation en Flandre

En Flandre, la situation est différente, puisque les CPAS ont davantage recours à la mutualisation des conseillers informatiques (selon le SPP IS, +/- 40% des CPAS y ont recours). Ils le font notamment via l'association Titre VIII, Chapitre I qui est une association inter-CPAS dont les possibilités sont un peu plus larges que dans le cadre de l'association chapitre XII en ce qu'elle permet l'engagement de personnel pour des fonctions dirigeantes de cadres, d'experts et de management⁶.

Ainsi, les possibilités de mutualisation suivantes sont rencontrées sur le terrain :

- certaines provinces disposent d'un service de sécurité informatique et mettent leurs conseillers à disposition des CPAS et des communes ; d'autres n'ont pas de service à proprement parler mais mettent des formations en place pour les conseillers
- création d'une association de CPAS Titre VIII, Chapitre 1⁷ disposant d'un service de conseillers en sécurité
- mise à disposition du conseiller entre CPAS, avec la commune

Nous détaillerons plus particulièrement l'association Titre VIII, Chapitre 1 afin de faire ressortir ses principales caractéristiques.

• Association Titre VIII, Chapitre 1

Cinq associations Titre VIII, Chapitre 1⁸ exerçant notamment des activités liées à la sécurité de l'information existent en Flandre. Elles regroupent de 9 à 27 CPAS. Selon les informations reçues à ce sujet, la taille critique d'une quinzaine de CPAS semble idéale pour cette activité.

Activités⁹

Une association Titre VIII, Chapitre I est une association de droit public.

Elle peut seulement être créée pour la mise en œuvre d'une tâche précise appartenant aux missions du secteur des CPAS. Il n'est pas nécessaire que cette tâche soit déjà organisée par l'un des CPAS fondateurs. Tant les tâches existantes que les activités/services devant encore être créés peuvent entrer en considération. Les tâches internes du CPAS peuvent même entrer en ligne de compte. Une telle association peut également être fondée pour l'exploitation d'un hôpital ou d'une partie d'hôpital. Dans ce dernier cas, il s'agit d'un « établissement de soins autonome »¹⁰. Une association Titre VIII, Chapitre I peut aussi être créée pour assurer des tâches relatives aux fonctions de direction (cadres, experts, management).

⁶ STAFFE, F., « L'externalisation de la gestion des missions du C.P.A.S. », in CABUY, Y., WOLTER, J-M. (dir.), *Externalisation des missions des pouvoirs locaux*, Bruxelles, De Boeck, 2010, p.184.

⁷ Le « OCMW-decreet » ne parle plus d'associations chapitre XII, XII *bis* et XII *ter* mais parle d'associations Titre VIII, Chapitre 1 / Titre VIII, Chapitre 2 / Titre VIII, Chapitre 3 / Titre VIII, Chapitre 4.

⁸ Welzijnskoepel West-Brabant, Welzijnsband Meetjesland, Welzijnsregio Noord-Limburg, Kina, Welzijnszorg Kempen.

⁹ JANSSENS, K., LEROY, P., VANDERSTAPPEN, P., VANHOLSBEECK, D., VAN SCHUYLENBERG, P., 2013, *Het OCMW-decreet ontleed*, Politeia, Bruxelles, pp. 279-284.

¹⁰ Autonome verzorgingsinstelling (AV).

Caractéristiques¹¹

Caractéristiques	Association Titre VIII, Chapitre 1
conditions de création	pas de condition spécifique
forme juridique	dispose de la personnalité juridique
partenaires	pas de personnes ayant un but lucratif en cas d'autonomisation: pas de partenaire, uniquement le CPAS
durée maximale	30 ans, renouvelable
représentation du CPAS	membres du Conseil de l'action sociale pour la gestion d'un hôpital : maximum 1/3 des représentants peuvent ne pas être membres du Conseil de l'action sociale
impact du CPAS sur l'association	pour la gestion d'un hôpital : le nombre de voix de chaque partenaire est divisé proportionnellement à l'apport de chacun dans l'association en dehors du secteur hospitalier : la position minoritaire d'un CPAS est possible

4. Comment mutualiser?

Les formes de mutualisation qui rassemblent un plus grand nombre d'acteurs (mutualisation avec les Provinces et mutualisation en association de CPAS) sont privilégiées en ce qu'elles permettent la standardisation des procédures de tous les partenaires concernés, un gain de temps lié à cette standardisation et une amélioration du respect des dispositions relatives à la sécurité par la capitalisation de bonnes pratiques. Elles permettent également d'engager un conseiller en sécurité professionnel, dont les tâches concernent uniquement l'informatique et la gestion de la sécurité de l'information, ce qui ne serait pas possible à plus petite échelle.

En Flandre, dans les cas de mutualisation avec la Province ou sous forme d'une association de CPAS, un service spécifique relatif à la sécurité de l'information est créé. La totalité des missions qui lui incombe est prise en charge par les conseillers en sécurité mutualisés, mais chaque CPAS garde néanmoins en interne un correspondant pour cette matière afin d'assurer le relais entre le CPAS et le personnel du service/de l'association.

Pour préserver le lien de collaboration prévu par l'arrêté royal du 12 août 1993 entre le service chargé de la sécurité de l'information et le responsable de la gestion journalière de l'institution, les CPAS flamands regroupés en Association Titre VIII, Chapitre 1 pour ce service ont prévu des réunions régulières entre les Directeurs généraux des CPAS partenaires, le responsable de l'association et les membres du service. Ainsi, en début d'année, une réunion est organisée afin que chaque Directeur général puisse préciser les besoins de son institution. Un plan de travail est élaboré pour l'année. Ensuite, des réunions trimestrielles sont organisées permettant de réajuster, au besoin, le travail de l'équipe en fonction des priorités, des urgences, des nouveautés.

Au niveau du coût, le SPP IS a pu nous indiquer, sur base des exemples en Flandre, qu'il fallait compter 75 000 euros/an pour un conseiller œuvrant pour 15 à 18 CPAS. Il s'agit évidemment d'une approximation puisque les besoins diffèrent non seulement en fonction de la taille du CPAS mais aussi de l'état initial de leur gestion de la sécurité de l'information dans leur institution. Si une

¹¹ AGENTSCHAP BINNENLANDS BESTUUR, OCMW verenigingen. Voir : <http://binnenland.vlaanderen.be/verzelfstandiging-en-samenwerking/ocmw-verenigingen>

remise à niveau importante est nécessaire, un plus grand temps de travail devra être investi au départ, mais se lissera petit à petit.

Les pistes de mutualisation existantes en Flandre sont intéressantes pour la Wallonie. Dans tous les cas de mutualisation envisagés ci-dessous, le lien entre le responsable de la gestion journalière de l'institution et le service chargé de la sécurité doit être au centre de leur construction afin de garantir une réactivité optimale du travail et, dès lors, la pertinence de la mutualisation.

→ au niveau des **Provinces** wallonnes, il existe déjà certains types de mutualisation à disposition des CPAS : par ex., marchés conjoints en Province du Luxembourg concernant l'électricité, le gaz, la téléphonie ; centrales de marché pour les consommables informatique, fourniture de papier, acquisition/location de photocopieurs ; service interne de prévention et de protection au travail / centrale de marchés en Province de Hainaut /...

En Flandre, les partenariats entre les CPAS et les Provinces portant sur la mutualisation des conseillers en sécurité vont croissants.

Comme sur le modèle flamand, il serait intéressant d'analyser quelles Provinces disposent d'un service (de sécurité) informatique et d'envisager, à partir des partenariats déjà existants, les possibilités d'extension de ceux-ci pour la mise en place d'un tel appui pour les CPAS. Sur le terrain, des CPAS ont déjà fait une démarche en ce sens vers une des Provinces.

Cette option nous semble, de plus, aller dans le sens de l'optimalisation du rôle des Provinces inscrite dans la DPR et de la place qui leur est attribuée pour le développement d'actions de supracommunalité.

→ au niveau des **inter-CPAS**, à l'heure où l'allègement de l'association Chapitre XII est envisagé dans le cadre du GT gouvernance, la piste de mutualisation des conseillers en sécurité par le biais de cette structure peut nous éclairer dans la réflexion pour aller dans le sens de plus de souplesse et de flexibilité pour offrir une meilleur réponse aux besoins du terrain.

Une des difficultés rencontrées par les associations chapitre XII est le fait qu'elles disposent de mécanismes de fonctionnement similaires aux CPAS, sans pour autant avoir à leur tête une personne qui, à l'instar du Directeur général, est chargée de la gestion de l'association. Il existe bel et bien dans les associations un coordinateur mais ce poste n'est pas couvert pas un subventionnement structurel et, de plus, il est généralement occupé par une personne dont l'expertise est davantage tournée vers l'action menée par l'association que vers le rôle de direction. Organiser la mise en place d'une fonction dirigeante au sein de ces associations serait incontestablement un moyen de faciliter leur fonctionnement quotidien et de les renforcer sur le plan de la gestion.

Des mutualisations entre CPAS pourraient également être envisagées par le biais de conventions de collaboration ou de création de clusters pour la sécurité de l'information (sur le modèle des 20 clusters existants en Wallonie pour l'insertion socio-professionnelle).

→ enfin, s'il semble important de laisser aux CPAS le choix du modèle de mutualisation qui conviendra au mieux à leurs réalités locales, pourquoi ne pas envisager une réponse plus ambitieuse sur le plan de l'échelle par la mise en place d'un pool de conseillers en sécurité au niveau **régional**¹² ? Ce pool devrait bien sûr être suffisamment mobile (interventions sur place) et composé de suffisamment d'experts pour assurer un réel service aux CPAS.

¹² Par la BCED, l'eWBS possède une expertise en matière d'échange de données, de protection de la vie privée et de sécurité informatique à laquelle il pourrait être intéressant de recourir pour concrétiser cette orientation.

A l'échelle de la Région wallonne, cette mutualisation permettrait tout d'abord de mieux évaluer le rapport coûts/bénéfices des produits sur le marché, d'orienter les CPAS dans leurs achats sur base de leurs besoins et, par l'achat en nombre, de diminuer les coûts.

Ensuite, la concentration de conseillers en sécurité dans un pool permettrait d'éviter le morcellement des interlocuteurs et de faciliter le nécessaire travail partenarial entre le SPP IS, la BCSS et les CPAS autour des exigences de sécurité fixées par la BCSS.

La professionnalisation du service permettrait enfin une meilleure anticipation des développements informatiques à venir et, partant, une meilleure préparation des transitions qui favoriserait l'efficacité du travail.

Quelle que soit la forme de mutualisation envisagée, il est indispensable d'impliquer les autres acteurs concernés par la connexion des CPAS à la BCSS, à savoir le SPP IS et la BCSS elle-même, afin de rester en phase avec les exigences qui découlent de cette connexion.

Il est également indispensable, et la Fédération s'y engage, de mener un travail d'analyse plus approfondi permettant de penser l'opérationnalisation de cette mutualisation afin qu'elle rencontre au mieux les besoins et les obligations des CPAS en la matière.

DOCUMENT DE TRAVAIL