SECURITE DE L'INFORMATION LORS DES EXERCICES D'INTEGRATION CPAS-COMMUNE

1. Le cadre et le contexte dans lesquels les exercices d'intégration ont lieu

Le décret Politique sociale locale (2004) obligeait les administrations communales et des CPAS à convenir des tâches et de la répartition de celles-ci. Les administrations étaient également obligées de développer un concept de « maison sociale » offrant au moins un accès intégré à l'aide et aux services sociaux de l'administration communale et du CPAS. Ce décret lançait une évolution locale permettant, via toutes sortes de méthodes, de travailler à cet accès intégré, comme par exemple :

- Des formes de services sociaux individuels ont été dans de nombreuses communes transférées de l'administration communale à celle du CPAS (par exemple toutes sortes de primes sociales) ;

- Les collaborateurs de l'administration communale ont été détachés ou mis à la disposition des CPAS pour exécuter des tâches communales sur les sites des CPAS (par exemple les demandes de pensions, les demandes d'intervention pour les personnes handicapées, etc.) ;

- Les collaborateurs de l'administration communale ont tenu des jours d'audience dans les locaux des CPAS.

Lors de la discussion sur la coopération au niveau du contenu, les opportunités financières possibles que la coopération entre les deux administrations peut générer sont souvent abordées (via la réalisation d'avantages d'échelle). Une meilleure coopération entre les deux administrations locales dans le domaine des services de support (informatique, communication, services techniques, entretien, infrastructure, etc.) peut entraîner une plus grande efficacité. Cela semble être dans la pratique une importante motivation pour travailler à une plus grande coopération .[1]

[1] SELS P., 'Samenwerking tussen OCMW- en gemeentebestuur op het vlak van de ondersteunende diensten', dans: *Verzelfstandiging en samenwerking op lokaal vlak*, Bruxelles, Politeia, feuillets mobiles, avril 2008, II/10/65.

L'introduction du décret communal et du décret CPAS visait aussi une plus grande coopération. Plus concrètement, nous visons les passages sur la possibilité de conclure des accords de gestion entre le CPAS et la commune comme stipulé à l'article 271 du Décret communal et à l'article 271 du Décret CPAS.

« Les conventions de gestion peuvent être signées entre la commune et le centre public d'action sociale en ce qui concerne l'utilisation commune des services réciproques. La convention de gestion peut par ailleurs stipuler que la commune et le centre public d'action sociale peuvent pour certaines fonctions faire appel à leurs membres du personnel réciproques ». Sécurité de l'information lors des exercices d'intégration CPAS-commune – VVSG – Boens C., Callens H., Sels P. - 8 mars 2010 - 2/11

Tant l'évolution dans le domaine de la Politique sociale locale que la recherche locale d'avantages d'échelle via la coopération entre les deux administrations entraînent des situations locales où la distinction physique entre les deux organisations, leurs tâches et leurs collaborateurs s'estompe. La législation régulant le fonctionnement des deux administrations tient peu, voire pas du tout compte de ces évolutions. Bien que la première partie de l'article 2 du Décret communal et du Décret CPAS soit identique[2], les administrations communale et du CPAS n'ont pas la même mission ni les mêmes tâches. C'est pourquoi de nombreux pièges sont liés à ces exercices. Nous exposons ci-dessous quelques-unes des questions prioritaires.

[2] L'art. 2 du Décret communal stipule : '*Les communes s'efforcent de contribuer au niveau local au bien-être des citoyens et au développement durable du territoire communal. Conformément à l'article 41 de la Constitution, elles sont compétentes pour les matières d'intérêt communal pour la réalisation desquelles elles peuvent prendre toutes les initiatives*.'
L'art. 2 du Décret CPAS stipule : '*Les centres publics d'action sociale visent au niveau local à contribuer durablement au bien-être des citoyens, tout en conservant les missions visées aux articles 1 et 57 de la loi organique du 8 juillet 1976 relative aux centres publics d'action sociale, et les autres affaires qui leur sont imposées par ou en vertu d'une loi ou d'un décret.*'

3 Le CPAS est décrit comme tel dans le texte de vision de la VVSG (Union des villes et communes flamandes) : vers un rapport optimal entre la commune et le CPAS, http://www.vvsg.be/sociaal_beleid/Documents/Verhouding gemeente-OCMW.doc .

2. Questions prioritaires générales au niveau de cette évolution

La recherche d'avantages d'échelle et la réalisation d'une fourniture de service plus intégrée sont des motifs légitimes pour une plus grande coopération. Les deux objectifs et les actions destinées à les atteindre ne doivent cependant pas être mélangés. Les actions proposées pour obtenir des avantages d'échelles ne peuvent pas porter préjudice à la mission et à la combativité de l'une des deux administrations. L'administration du CPAS est selon la VVSG responsable de la politique tactique et opérationnelle au niveau des affaires sociales. L'application de la politique sociale stratégique est d'après la VVSG une tâche essentielle du conseil communal[3]. Cela se situe au niveau des processus de coopération dans le domaine des services de soutien dans ce sens que le CPAS doit pouvoir disposer des services de soutien nécessaires (soit au sein du CPAS, soit des services fournis par la commune ou d'autres parties externes) pour pouvoir donner forme de manière autonome à la politique tactique et opérationnelle en matière de politique sociale.
Les exercices d'intégration destinés à accroître l'accessibilité concernent principalement sur le plan physique l'intégration dans le front-office. Il convient de tenir compte à ce niveau des compétences légales du CPAS et de la commune ainsi que de l'expertise de chacun. L'intégration dans le front-office ne suppose pas nécessairement un transfert des compétences et des

tâches d'une administration à l'autre. Cela est problématique pour les tâches attribuées par la loi (demande de pensions par le CPAS, demande d'intervention pour les personnes handicapées), bien que de nombreuses administrations semblent dans la pratique faire preuve de créativité à ce niveau. Un service plus intégré pour le citoyen peut également être fourni sans transfert de la tâche principale. Grâce à l'attribution de certains modules du processus de fourniture de service au front office (par exemple l'information, l'éclaircissement des demandes, la fourniture du produit), cela peut être réalisé dans une certaine mesure. Un CPAS peut sans aucun problème donner des informations sur la demande de pension et aider à compléter la demande tandis que la demande proprement dite est officiellement réalisée via un membre du personnel communal. On peut également travailler à une plus grande intégration au point de vue du citoyen via des jours d'audience de membres du personnel d'une administration dans les locaux de l'autre administration ou via la mise à disposition d'un détachement.

3. Tâches ne pouvant pas être transférées et sécurité de l'information en tant que limites de l'intégration

Les évolutions susmentionnées débouchent de plus en plus souvent sur des situations où les membres du personnel de différentes administrations ou d'organisations externes donnent forme ensemble et sous un même toit à une (certaine mesure de) aide ou de service intégré. On se demande dès lors où se situe le besoin de coopération que la fourniture de service intégré exige par rapport :

- Aux compétences légales définies et à l'expertise des différentes organisations ;

- A l'accès à l'information et aux obligations de confidentialité ou de discrétion de leurs membres du personnel qui y sont liées.

Nous essayons ci-dessous d'apporter des éclaircissements en ce qui concerne le personnel du CPAS et le personnel communal.

3.1 Respecter les compétences légales délimitées et l'expertise spécifique de chacun

3.1.1 Accueil : demande et service sociaux administratifs et non liés à la vie privée

L'accueil sur un site où l'aide ou le service de la commune et du CPAS est intégré dans une certaine mesure (cf. concept de maison sociale) est l'endroit où le citoyen peut formuler pour la première fois ses problèmes, ses besoins ou ses demandes de service. S'il s'agit d'une demande d'information à laquelle le/la réceptionniste peut répondre ou d'un simple « produit » qui peut rapidement être fourni, le/la réceptionniste (souvent un collaborateur de niveau administratif) traite la demande à l'accueil (par exemple une attestation de composition de ménage). L'accueil peut selon nous être assuré aussi bien par le personnel du CPAS que celui de la commune.

S'il s'agit de collaborateurs communaux, nous conseillons (par précaution) de leur imposer la confidentialité en reprenant une clause dans le code déontologique pour

le personnel (cf. plus loin). Nous plaidons pour cette mesure de précaution car, malgré une procédure claire, il est pour ainsi dire inévitable que le citoyen divulgue dès l'accueil et à sa propre initiative des informations d'ordre privé, et ce sans que le/la réceptionniste ne puisse l'en empêcher.

3.1.2 Service et aide sociaux individuels non administratifs et liés à la vie privée

Dans une démarche active, certaines tâches socio-administratives peuvent parfois être attribuées aux collaborateurs administratifs ou il faut au moins prévoir la possibilité de demander l'aide d'un travailleur social. Une demande administrative sociale peut en effet être associée à des besoins sociaux plus larges auxquels un travailleur social répondra mieux (par exemple une attestation de salaire)[4]. Dans cette même logique, l'accueil est actuellement renforcé dans de nombreux CPAS et maisons sociales. On estime qu'un accueil fort exige un personnel mieux formé, plus d'instruments de soutien, un autre profil de réceptionnistes, des travailleurs sociaux mobilisables et certains choisissent même d'engager des travailleurs sociaux pour assurer la fonction de réceptionniste.

[4] SELS P., GOUBIN E., e.a., *Het sociaal huis, werken aan een toegankelijke dienst- en hulpverlening*, VVSG-Politeia, Bruxelles, 2008.

L'embauche de profils plus compréhensifs pour assurer la fonction de réceptionniste ne peut toutefois selon nous pas déboucher sur le traitement de toutes les demandes à l'accueil. Si le besoin du client n'est pas clair, la demande doit être éclaircie. S'il semble s'agir d'une demande non administrative, de nature sociale et liée à la vie privée, il convient d'éclaircir la demande :

- Via un travailleur social du CPAS (puisque celui-ci - contrairement aux autres collaborateurs du CPAS - y est formé) ; et

- Dans un espace permettant un entretien lié à la vie privée.

3.1.3 Entretien préliminaire et accès aux données de la Banque-Carrefour de la Sécurité sociale (BCSS)

Lors de l'entretien préliminaire, on procède au diagnostic ou à l'analyse de la situation du client. Cela suppose que l'on rassemble les données nécessaires via un entretien et la consultation d'autres sources. La Banque-Carrefour de la Sécurité sociale est une source de plus en plus importante. Les CPAS ont accès à certaines données de la BCSS une fois que le Comité sectoriel de la Sécurité sociale et de la Santé, département Sécurité sociale (de la Commission pour la protection de la vie privée) fournit les habilitations aux institutions affiliées de la Sécurité sociale pour cette mise à disposition aux CPAS. Vous trouverez des exemples de ces habilitations sur : http://www.ksz-

bcss.fgov.be/nl/bcss/page/content/websites/belgium/security/security_06/security_06_01.html .5

5 Ex. 08/65 est une habilitation du comité à l'Office national des allocations familiales accordée en 2008 pour, sous certaines conditions et à certaines fins, la mise à disposition de données personnelles aux CPAS via la BCSS.

6 http://www.ksz-bcss.fgov.be/nl/bcss/page/content/websites/belgium/security/security_01.html

7 article 23, second alinéa, Loi sur la Banque-Carrefour.

8 articles 61 à 71 inclus de la Loi sur la Banque-Carrefour

Les habilitations sont uniquement accordées à certaines conditions et si les données sont utilisées à des fins préalablement définies et approuvées. L'accès aux données pour les CPAS est également soumis à diverses conditions, qui sont principalement liées à la sécurité des informations[6].

Les CPAS ne peuvent ainsi disposer que des coordonnées acquises pendant la période nécessaire pour l'application de la sécurité sociale ; ils doivent prendre des mesures pour assurer le caractère confidentiel des données personnelles et veiller à ce que celles-ci ne soient utilisées que pour l'exercice de leurs missions légales[7]. Toute violation des dispositions est sanctionnée pénalement[8]. Les CPAS doivent aussi respecter plusieurs normes minimales afin d'obtenir et de conserver un accès au réseau de la Banque-Carrefour. Par conséquent, les données relatives aux clients que le CPAS obtient via la BCSS peuvent uniquement être consultées et manipulées par les membres du personnel du CPAS. Donc actuellement, dans la pratique, seuls les travailleurs sociaux du CPAS peuvent réaliser un entretien préliminaire pour une aide ou un service social individuel et gérer l'ensemble du parcours.

En cas de détachement (statutaires) ou de mise à disposition (contractuels), le personnel communal travaillera au sein du CPAS pour exercer les tâches d'intérêt communal. Si l'on veut confier les tâches du CPAS au personnel communal, ce n'est pas possible avec la mise à disposition. Le personnel communal (même les travailleurs sociaux communaux) ne peut pas être engagé pour la tâche essentielle du CPAS, l'aide et le service social individuel puisque, contrairement au personnel du CPAS, il n'a pas accès aux données de la BCSS. La mutation (licenciement de la commune et embauche au CPAS) est l'unique solution. Sécurité de l'information lors des exercices d'intégration CPAS-commune – VVSG – Boens C., Callens H., Sels P. - 8 mars 2010 - 6/11

3.2 Garantir la sécurité de l'information dans un contexte de service intégré

Dans le contexte du fonctionnement du CPAS, la sécurité des informations porte sur la protection des données de nature personnelle, des données de personnes physiques identifiables ou identifiées. Nous retrouvons ces données au niveau du CPAS dans :

- Le logiciel que les CPAS utilisent pour leurs recherches dans le cadre du droit à l'intégration sociale, la loi du 4 avril 1965, le fonds mazout, etc. ;

- Les fichiers numériques que les travailleurs sociaux créent en vue de la présentation des demandes au Conseil de l'Action sociale ;

- Le logiciel de comptabilité ;

- Sur des supports de sauvegardes (USB, disques durs externes, DVD, etc.) ;

- Sur le portail de la sécurité sociale ;

- Sur le serveur ;

- Sous la forme de supports sur papier (dans des dossiers, dans des courriers, dans les archives, etc.) qui découlent de fichiers numériques.

Il est évident qu'une politique de sécurité de l'information doit accorder de l'attention à la sûreté de tous ces supports d'information. Vous trouverez de plus amples informations sur les normes de sécurité à respecter en général sur le site Web de la VVSG[9] et sur celui de la Banque-Carrefour de la Sécurité sociale[10].

[9] http://www.vvsg.be/sociaal_beleid/Kruispuntbank/Pages/kruispuntbankdefault.aspx

[10] http://www.ksz-bcss.fgov.be/nl/bcss/home/index.html

Depuis le point de vue de la sécurité des informations, le plus facile serait bien entendu de décider que seuls le personnel du CPAS et la clientèle du CPAS (avec accompagnement) puissent avoir accès aux bâtiments dans lesquels tous ces supports se trouvent. Il s'agit cependant d'une approche allant à l'encontre et rendant impossible la coopération croissante entre les administrations communales et les CPAS. Elle n'est ni réalisable, ni souhaitable. Il s'agit également d'une mesure disproportionnée puisque ce sont les données personnelles qui doivent faire l'objet d'une protection et non pas l'accès à tout un bâtiment. La coopération au niveau des services de soutien crée des situations où les femmes de ménage, les hommes à tout faire, les réceptionnistes, les archivistes, les collaborateurs du helpdesk informatique ou encore les responsables informatiques communaux travaillent dans des bâtiments et des locaux dans lesquels se trouvent les données de nature personnelle. Sécurité de l'information lors des exercices d'intégration CPAS-commune – VVSG – Boens C., Callens H., Sels P. - 8 mars 2010 - 7/11

On part du principe (et il faut partir du principe) que toutes ces personnes n'ont pas accès aux données des clients du CPAS parce que :

- Elles ne bénéficient pas d'un accès légal à celles-ci ;

- Ces données ne sont pas nécessaires à l'exercice de leur fonction.

En ce domaine, il n'y a d'ailleurs aucune différence avec une entreprise externe qui fournit des services au CPAS et exécute en cette qualité des activités dans le bâtiment où les données personnelles à protéger se trouvent.
Il convient donc de prendre toutes les mesures nécessaires pour que la sécurité des informations soit assurée, sans que cela ne menace la coopération sur le plan du contenu ou au niveau des services de support.
Nous proposons les mesures suivantes :

- Reprendre dans le code déontologique que le conseil communal définit pour le personnel communal[11] une clause particulière concernant la sécurité de l'information. Cette clause a pour but d'imposer la confidentialité à tous les membres du personnel communal qui doivent, dans le cadre de l'exercice de leur fonction, accéder à des espaces dans lesquels se trouvent des données de nature personnelle à protéger.

11 Décret communal, art. 112.
Clause liée à la sécurité des informations :
Si vous n'est pas autorisé à prendre connaissance ou à avoir accès à des données personnelles de dossiers concernant les services individuels du CPAS, n'essayez jamais d'y avoir accès. Si vous entrez involontairement en contact avec ces données, que ce soit physiquement, par voie électronique ou les deux, vous vous engagez à strictement conserver la nature confidentielle de ces informations.
Le code déontologique que le Conseil pour l'Action sociale définit élargit cette clause avec le passage suivant :
Toute personne ayant accès aux données visées dans le cadre de sa fonction, que ce soit physiquement, par voie électronique ou les deux, respectera strictement le caractère confidentiel de ces données et s'engage à respecter les normes de sécurité minimales que le secrétaire du CPAS a communiquées.

- Au niveau de la protection des informations, les collaborateurs ICT communaux qui travaillent également pour le CPAS sont considérés par la Banque-Carrefour de la Sécurité sociale comme des "fournisseurs externes" et ils ressortent donc (s'ils ont accès dans le cadre de leurs activités à des données de nature personnelle) de la responsabilité du secrétaire du CPAS. Dans notre proposition (étant donné la clause reprise dans le code déontologique communal),

le secrétaire communal peut également leur demander des comptes par rapport à leur obligation de confidentialité. En ce qui concerne les collaborateurs ICT communaux qui travaillent également pour le CPAS, la clause sur la sécurité des informations peut également renvoyer au « code de conduite pour les gestionnaires des informations dans le réseau de la sécurité sociale ». Nous entendons ici par gestionnaire des informations : *toute personne disposant de droits d'accès dépassant celui de l'usage fonctionnel des données. Il s'agit notamment des administrateurs du système, des gestionnaires de données, des gestionnaires des applications, des administrateurs de réseau, des consultants, des gestionnaires de la sécurité, etc.* [12]

- Si l'on travaille aussi localement avec une infrastructure informatique commune, par exemple un serveur commun, il convient, au niveau du réseau et afin d'assurer la sécurité des informations, que les mesures organisationnelles et techniques nécessaires soient prévues pour que seules les personnes autorisées aient accès aux données personnelles sociales qui leur sont destinées (par exemple par la prévision de deux domaines, la segmentation, les contrôles d'accès, les politiques d'accès, etc.).

- Enfin, le personnel du CPAS travaillant avec des données sur la clientèle doit respecter la politique de sécurité en vigueur dans le CPAS. Les éléments suivants sont essentiels dans un contexte d'intégration ou de coopération avec la commune : le principe du clean desk, en vertu duquel les données sur les clients ne doivent pas traîner pas sur des supports physiques et garantissant un bon système de protection d'écran ainsi qu'une politique de mot de passe (cf. ci-dessous).

[12] http://www.ksz-bcss.fgov.be/binaries/documentation/nl/securite/policies/isms_024_code_info-nl.pdf

4. Dans la pratique : quelques directives

Afin de pouvoir exécuter la coopération décrite entre la commune et le CPAS d'une manière assez sûre, quelques directives élémentaires sont d'application.

4.1 La politique du mot de passe

Bien entendu, à l'avenir, chaque collaborateur ayant accès à des données protégées devra s'identifier et se connecter via sa carte d'identité électronique. Il s'agit en effet du moyen par excellence pour se connecter à tous les systèmes possibles à l'aide des certificats sur la carte d'identité électronique (eID) et du code PIN correspondant. Dans les administrations communales, on a également lancé la gestion de la sécurité locale et l'utilisation des eID. Etant donné que tous les fournisseurs et toutes les applications ne permettent pas encore l'utilisation de l'eID, on devra temporairement encore travailler avec le concept traditionnel du nom d'utilisateur/mot de passe.

Il est extrêmement important, d'une part, que toutes les applications soient protégées par un système de login, et d'autre part, qu'une politique du mot de passe soit appliquée et réponde à plusieurs exigences minimales :

- Toutes les personnes (sans exception !) ayant accès ou devant avoir accès aux données protégées ne peuvent y accéder que via un mot de passe/nom d'utilisateur qui leur sont attribués sur l'ordre du responsable local de la sécurité.

- Ce mot de passe doit satisfaire à des conditions minimales et (concrètement) se composer de préférence d'au moins 8 caractères comprenant des majuscules, des minuscules, des chiffres et aucun signe élémentaire (comme §,{,&, etc.). Il convient d'éviter les combinaisons et/ou les mots élémentaires. Le responsable local de la sécurité est (en collaboration avec l'administrateur du système) responsable de la définition des directives à ce propos.

- N'écrivez jamais votre mot de passe, surtout pas sur un Post-It placé à côté de votre ordinateur.

- Ne communiquez jamais votre mot de passe. Si une autre personne en prend connaissance, modifiez-le dans les plus brefs délais.

- Modifiez votre mot de passe à temps si vous le désirez. Le responsable de la sécurité doit veiller à ce que vous soyez régulièrement obligé de définir un nouveau mot de passe. Le système doit aussi pouvoir réaliser un contrôle pour s'assurer que l'ancien et le nouveau mots de passe ne sont pas trop similaires.

- Vérifiez si votre mot de passe ne peut pas être associé à des heures de travail. Il est souvent inutile d'avoir un accès pendant le week-end.

4.2 L'enregistrement d'opérations et leur contrôle

Même s'il en allait autrement durant la phase de lancement de l'informatisation, depuis le raccordement au réseau de la BCSS, on accorde de l'attention à l'enregistrement des opérations. Nous entendons par enregistrement "l'enregistrement automatisé de qui a fait quoi et quand". Cet enregistrement est important pour tracer les abus. Dans ce sens, la manière dont on aborde l'enregistrement des opérations est importante :

- Signalez aussi clairement et ouvertement que possible que les opérations sont enregistrées. Signalez quelles sont les opérations enregistrées. Mieux vaut prévenir que guérir.

- Signalez que les personnes compétentes prélèveront régulièrement des échantillons et que les collaborateurs peuvent être invités à fournir des explications sur leurs opérations sans que cela n'implique que des erreurs ont été commises.

- Signalez qu'en cas de présomption d'abus, cet enregistrement sera utilisé pour contrôle.

• Signalez que cette méthode de travail (enregistrement, échantillons, contrôle) n'est pas uniquement appliquée au niveau de la gestion locale, mais aussi au niveau du fournisseur des données (in casu la BCSS).

4.3 Des procédures plus claires

Veillez à ce que les procédures soient plus claires au niveau de la gestion de la sécurité :

• Intégrez la gestion et l'octroi des accès à la procédure d'accueil des nouveaux collaborateurs. Concertez-vous avec le service du personnel à ce propos.

• Idem dito en cas de démission/licenciement (!) et/ou d'absence de longue durée (toutes sortes d'interruptions de carrière).

• Développez une procédure permettant d'avoir un aperçu rapide et complet de qui doit avoir accès, où et comment.

• Développez des procédures à appliquer en cas de constatation et/ou de présomption d'abus. Ce point est très important car cela peut par exemple déboucher sur une suspension et/ou un licenciement.

• Communiquez et concertez-vous assez avec toutes les parties intéressées à propos de ces procédures (dont les syndicats par exemple !).

4.4 Les tâches du consultant en sécurité et du responsable local de la sécurité

Les tâches du consultant en sécurité sont décrites dans la réglementation (dont l'arrêté d'exécution à la loi sur l'échange de données entre les administrations)[13]. Il est important de noter que le consultant en sécurité peut exécuter sa tâche de manière indépendante et en temps voulu. Il est responsable de l'élaboration des plans d'amélioration nécessaires. Les conseils qu'il donne doivent être repris dans les négociations avec les fournisseurs, par exemple. Il n'est en principe pas souhaitable que les fonctions de consultant en sécurité et de responsable local de la sécurité (normalement le secrétaire, et dans certains cas son délégué) soient assurées par la même personne. Des conflits d'intérêt

[13] *Arrêté du Gouvernement flamand concernant les consultants en sécurité, mentionné à l'article 9 du Décret du 18 juillet 2008 relatif à l'échange électronique de données administratives*, 15 mai 2009, M.B.: 2009-07-13 (Ed. 1), numéro: 2009/203137.
Loi du 15/01/1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale, art. 4 par.5 et art. 24, http://www.ksz-bcss.fgov.be/nl/bcss/anchorpage/content/websites/belgium/legislation/legislation_01/legislation_01_01.html .

se présenteraient puisque la gestion des accès et le contrôle des normes de sécurité des informations doivent de préférence être deux activités séparées.
Dans la plupart des administrations, la tâche du consultant en sécurité n'équivaut pas à un temps plein. La coopération entre les consultants en sécurité de la commune et du CPAS est évidente et est un must dans le contexte de l'intégration. La coopération entre différents CPAS et communes est également une option. L'avantage est que cela permet de développer de meilleures compétences et d'offrir à plus long terme plus de garanties pour une politique de sécurité suffisante.

4.5 Conclusion

Assurer une bonne politique de sécurité des informations est de plus en plus important, surtout dans le cadre de la coopération entre la commune et le CPAS. Il est non seulement question de la sécurité physique des informations (laisser traîner des dossiers, des documents près des photocopieuses, etc.), mais aussi de la protection numérique des informations. Le contenu de 20 mètres d'armoires à dossiers peut en effet facilement être enregistré sur une clé USB.

5. Conclusions générales

Nous avons décrit dans cette note deux motivations qui étaient à la base de l'évolution vers une plus grande coopération entre les administrations communales et des CPAS : la recherche d'avantages d'échelle et la recherche d'un service plus intégré. Il s'agit de deux motivations légitimes pour une plus grande coopération. Toutefois, dans la pratique, cette évolution vers une plus grande coopération bute contre une législation qui n'est ni adaptée, ni coordonnée (pour ce qui a trait aux affaires liées au personnel et aux services octroyés à une administration spécifique). Il existe en outre plusieurs questions prioritaires en ce qui concerne la méthodologie et la sécurité des informations. Au niveau de la méthodologie, il convient en tant qu'administration d'accorder de l'attention aux missions et à l'expertise spécifiques de chacun.
D'autre part, la sécurité des informations est cruciale, et ce tant pour protéger la vie privée des utilisateurs que pour garantir la fiabilité du service et de l'aide. De plus, les administrations communales et des CPAS dépendent de plus en plus pour leurs prestations de services des données qui leur sont fournies par d'autres instances. Ces instances (par exemple la BCSS) imposent à juste titre des conditions en matière de sécurité des informations pour l'utilisation de ces données. Or, le non-respect de ces conditions de sécurité par certaines administrations remet en cause l'accès aux données nouvelles et existantes pour toutes les administrations.