

INFORMATIEVEILIGHEID BIJ INTEGRATIEOEFENINGEN OCMW-GEMEENTE

Gevalideerd door de Kruispuntbank Sociale Zekerheid

Update: 25/05/2010: Deze nota werd ondertussen ook onderschreven door de diensten van de Kruispuntbank Sociale Zekerheid en de POD Maatschappelijke Integratie. Hij zal weldra ook ter beschikking gesteld worden via de website van de POD Maatschappelijke Integratie. Aan de inhoud is niets gewijzigd.

1. Het kader en de context waarbinnen integratieoefeningen plaats vinden

Het decreet Lokaal Sociaal Beleid (2004) verplichtte OCMW- en gemeentebesturen tot taakafspraken en taakverdeling. Besturen werden eveneens verplicht een 'sociaal huis'-concept uit te werken dat minimaal een geïntegreerde toegang zou verschaffen tot de sociale dienst- en hulpverlening van gemeente- en OCMW-bestuur. Dit decreet vormde de aanzet tot een lokale evolutie waarbij via allerlei methoden gewerkt werd aan die geïntegreerde toegang, zoals bv.:

- vormen van individuele sociale dienstverlening werden in vele gemeenten overgeheveld van het gemeente- naar het OCMW-bestuur (bv. allerhande sociale premies),
- medewerkers van het gemeentebestuur werden gedetacheerd of ter beschikking gesteld van OCMW's om gemeentelijke taken uit te voeren op OCMW-locaties (bv. aanvraag pensioenen, aanvraag tegemoetkomingen personen met een handicap, ...),
- medewerkers van het gemeentebestuur gingen zitdagen houden in OCMW-gebouwen

Tijdens de discussie over samenwerking op het inhoudelijke vlak, komen vaak ook de mogelijke financiële opportuniteiten aan bod die de samenwerking tussen beide besturen kan genereren (via realisatie van schaalvoordelen). Meer samenwerking tussen beide lokale besturen op het vlak van de ondersteunende diensten (informatica, communicatie, technische diensten, onderhoud, infrastructuur, ...), kan leiden tot meer efficiëntie en tot meer effectiviteit. In de praktijk lijkt dit ook een sterke motivatie om te werken aan meer samenwerking.¹

¹ SELS P., 'Samenwerking tussen OCMW- en gemeentebestuur op het vlak van de ondersteunende diensten', in: *Verzelfstandiging en samenwerking op lokaal vlak*, Brussel, Politeia, losbladig, april 2008, II/10/65.

De invoering van het gemeentedecreet en het OCMW-decreet sturden eveneens aan op meer samenwerking. Meer concreet doelen we op de passages over de mogelijkheid tot het afsluiten van beheersovereenkomsten tussen OCMW en gemeente zoals weergegeven in artikel 271 van het gemeentedecreet en artikel 271 van het OCMW-decreet.

“Tussen de gemeente en het openbaar centrum voor maatschappelijk welzijn kunnen beheersovereenkomsten worden gesloten over het gemeenschappelijk gebruik van elkaars diensten. In de beheersovereenkomst kan tevens opgenomen worden dat de gemeente en het openbaar centrum voor maatschappelijk welzijn voor bepaalde functies een beroep kunnen doen op elkaars personeelsleden.”

Zowel de evolutie op het vlak van het Lokaal Sociaal Beleid als de lokale zoektocht naar schaalvoordelen via samenwerking tussen beide besturen, leiden tot lokale situaties waarbij het fysieke onderscheid tussen de beide organisaties, hun taken en hun medewerkers vervaagt. De wetgeving die het functioneren van beide besturen regelt houdt weinig tot geen rekening met deze evoluties. OCMW- en gemeentebesturen hebben –ongeacht het feit dat het eerste deel van artikel 2 in zowel gemeente- als OCMW-decreet identiek is²– nog steeds een andere missie en taakhoud. Daarom zijn er een heel aantal valkuilen verbonden aan deze oefeningen. We zetten hieronder een aantal aandachtspunten op een rij.

2. Algemene aandachtspunten bij deze evolutie

Zowel het streven naar schaalvoordelen als het realiseren van een meer geïntegreerde dienstverlening zijn legitieme motieven om meer samen te werken. Beide doelstellingen en de acties om ze te bereiken mogen echter wel niet vermengd worden. Voorgestelde acties vanuit de motivatie van schaalvoordelen mogen geen afbreuk doen aan de missie en de slagkracht van één van beide besturen. Het OCMW-bestuur is volgens de VVSG verantwoordelijk voor het tactisch en operationeel beleid op het vlak van sociale aangelegenheden. Het voeren van het strategisch sociaal beleid is volgens de VVSG een kerntaak van de gemeenteraad³. Dit speelt in samenwerkingsprocessen op het vlak van ondersteunende diensten in die mate dat

² Art. 2 in het gemeentedecreet: *‘De gemeenten beogen op het lokale niveau bij te dragen tot het welzijn van de burgers en tot de duurzame ontwikkeling van het gebied. Overeenkomstig artikel 41 van de Grondwet zijn ze bevoegd voor de aangelegenheden van gemeentelijk belang voor de verwezenlijking waarvan ze alle initiatieven kunnen nemen.’*

Art. 2 in het OCMW-decreet: *‘De openbare centra voor maatschappelijk welzijn beogen om op het lokale niveau duurzaam bij te dragen tot het welzijn van de burgers, met behoud van de opdracht, vermeld in artikelen 1 en 57 van de organieke wet van 8 juli 1976 betreffende de openbare centra voor maatschappelijk welzijn, en de andere gelegenheden die hen door of krachtens een wet of een decreet worden opgelegd.’*

³ Het OCMW wordt als dusdanig omschreven in de VVSG-visietekst: naar een optimale verhouding tussen Gemeente en OCMW, http://www.vvsg.be/sociaal_beleid/Documents/Verhouding_gemeente-OCMW.doc.

het OCMW uiteraard moet kunnen beschikken over de nodige ondersteunende diensten (ofwel binnen het OCMW, ofwel aangeleverd door de gemeente of door andere externen) om autonoom het tactisch en operationeel beleid inzake sociaal beleid te kunnen vorm geven.

Integratieoefeningen vanuit de motivatie van het verhogen van de toegankelijkheid, betreffen op het fysieke vlak voornamelijk integratie in de front-office. Daarbij moet wel rekening gehouden worden met de wettelijke bevoegdheden van OCMW en gemeente en met elkaars expertise. Integratie in de front-office veronderstelt niet noodzakelijk overdracht van bevoegdheden en taken van het ene naar het andere bestuur. Voor bij wet toegewezen taken is dit zelfs problematisch (aanvraag pensioenen door OCMW, aanvraag tegemoetkoming personen met een handicap), alhoewel vele besturen daar in de praktijk creatief mee blijken om te springen. Een meer geïntegreerde dienstverlening voor de burger kan ook gerealiseerd worden zonder dat de kerntaak wordt overgedragen. Via het toewijzen van bepaalde modules van het proces van dienstverlening naar de frontoffice (bv. informatie, vraagverheldering, aflevering van product), kan dit eveneens in zekere mate gerealiseerd worden. Een OCMW kan zonder problemen informatie geven over de pensioenaanvraag en de aanvraag mee helpen invullen, terwijl de eigenlijke aanvraag formeel nog gebeurt via een gemeentelijk personeelslid. Ook via zitdagen van personeelsleden van het ene bestuur in de gebouwen van het andere bestuur of via ter beschikking stelling of detachering, kan er gewerkt worden aan meer integratie vanuit het standpunt van de burger.

3. Niet verschuifbare taken en informatieveiligheid als grenzen aan de integratie

Bovenstaande evoluties leiden steeds vaker tot situaties waarbij personeelsleden van verschillende besturen of zelfs van externe organisaties samen onder één dak vorm geven aan een (bepaalde mate van) geïntegreerde dienst- of hulpverlening. Hierbij stelt zich de vraag hoe de nood tot samenwerking die de geïntegreerde dienstverlening vereist, zich verhoudt tot:

- de afgebakende wettelijke bevoegdheden en de deskundigheid van de diverse organisaties,
- de toegang tot informatie en de eraan gekoppelde geheimhoudings- of discretieplicht van hun personeelsleden.

We trachten hieronder enige duidelijkheid te verschaffen voor wat betreft gemeentelijk en OCMW-personeel.

3.1 Afgebakende wettelijke bevoegdheden en elkaars specifieke deskundigheid respecteren

3.1.1 Onthaal: administratieve sociale dienstverlening en niet privacy-gevoelige vragen
Het onthaal op een locatie waar de dienst- of hulpverlening van gemeente en OCMW in een bepaalde mate geïntegreerd zijn (cfr. concept sociaal huis) is de plaats waar de burger zijn

probleem, behoefte of vraag naar dienstverlening voor het eerst formuleert. Betreft het een informatievraag die de onthaalmedewerker kan beantwoorden of een eenvoudig 'product' dat snel kan afgeleverd worden, dan handelt de onthaalmedewerker (vaak van niveau administratief medewerker) dit af aan het onthaal (bv. attest van gezinssamenstelling). Het onthaal kan ons inziens gebeuren door zowel gemeente- of OCMW-personeel.

Indien het gaat om gemeentelijke medewerkers raden wij aan deze – uit voorzorg- te verbinden tot geheimhouding via het opnemen van een clause in de deontologische code voor het personeel (zie verder). Wij pleiten voor deze voorzorgsmaatregel omdat het –ondanks een duidelijke procedure- bijna onvermijdelijk is dat de burger reeds aan het onthaal op eigen initiatief privacygevoelige informatie vrijgeeft, zonder dat de onthaalmedewerker dit kan verhinderen.

3.1.2 Niet-administratieve en privacygevoelige individuele sociale dienst- en hulpverlening

Vanuit een actieve houding kunnen bepaalde sociaal-administratieve taken soms beter evenmin helemaal toegewezen worden aan administratieve medewerkers of moet er minstens de mogelijkheid voorzien zijn om de hulp van een maatschappelijk werker in te roepen. Een sociaal administratieve vraag kan immers samenhangen met een breder sociaal behoeftepatroon waar best naar wordt gepeild en wat best wordt uitgeklaard door een maatschappelijk werker⁴ (bv. attest leefloon). Vanuit dezelfde logica wordt momenteel in veel OCMW's en sociale huizen het onthaal versterkt. Men ziet in dat een sterk onthaal beter opgeleid personeel vereist, meer ondersteunende instrumenten, een ander profiel van onthaalbedienden, maatschappelijk werkers die oproepbaar zijn en sommige verkiezen zelfs maatschappelijk werkers in te zetten voor het vervullen van de onthaalfunctie op zich.

Het inzetten van meer inhoudelijke profielen voor het vervullen van de onthaalfunctie mag er ons inziens echter niet toe leiden dat de gehele hulpverlening zich aan het onthaal gaat afspelen. Indien de behoefte van de cliënt niet duidelijk is, is er nood aan vraagverduidelijking. Indien het lijkt te gaan over een niet-administratieve vraag, van sociale aard en privacygevoelig, dan dient de vraagverduidelijking zeker te gebeuren:

- door een OCMW-maatschappelijk werker (gezien zij -in tegenstelling tot andere medewerkers van het OCMW- daartoe opgeleid zijn) én
- in een ruimte die een privacygevoelig gesprek toelaat.

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

3.1.3 Intake en toegang tot gegevens van de Kruispuntbank van de Sociale Zekerheid (KSZ)

Tijdens de intake wordt de diagnose of analyse van de situatie van de cliënt gemaakt. Dit veronderstelt dat men de nodige gegevens verzamelt via een vraaggesprek en via het raadplegen van andere bronnen. Een bron van toenemend belang is de Kruispuntbank van de Sociale Zekerheid. De OCMW's krijgen toegang tot bepaalde KSZ-gegevens nadat het Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid, afdeling Sociale Zekerheid (van de Commissie voor de bescherming van de persoonlijke levenssfeer) machtigingen verleent aan de aangesloten instellingen van Sociale Zekerheid om deze ter beschikking te stellen aan de OCMW's. U vindt voorbeelden van deze machtigingen op: http://www.ksz-bcss.fgov.be/nl/bcss/page/content/websites/belgium/security/security_06/security_06_01.html.⁵

De machtigingen worden slechts verleend onder bepaalde voorwaarden en enkel indien de gegevens gebruikt worden voor op voorhand vastgelegde en goedgekeurde doeleinden. Ook de toegang tot de gegevens voor OCMW's is onderworpen aan heel wat voorwaarden, vnl. in verband met informatieveiligheid⁶.

Zo mogen de OCMW's slechts beschikken over de verkregen persoonsgegevens gedurende de tijd die nodig is voor de toepassing van de sociale zekerheid; ze moeten maatregelen treffen om het vertrouwelijke karakter van de persoonsgegevens te verzekeren en ze moeten ervoor zorgen dat de persoonsgegevens uitsluitend worden gebruikt voor het uitvoeren van hun wettelijke opdrachten⁷. De schending van de bepalingen wordt gesanctioneerd met strafsancties⁸. De OCMW's moeten ook een heel aantal minimumnormen naleven teneinde toegang te kunnen krijgen en behouden tot het netwerk van de Kruispuntbank.

Dit alles maakt dat de cliëntgegevens die door het OCMW bekomen werden via de KSZ uitsluitend door OCMW-personeelsleden kunnen geraadpleegd en gehanteerd worden. Dit heeft tot gevolg dat momenteel -in de praktijk- enkel de OCMW-maatschappelijk werkers een intake individuele sociale dienst- en hulpverlening kunnen doen en het gehele traject beheeren.

Bij detachering (statutairen) of ter beschikkingstelling (contractuelen) gaat gemeentepersoneel in het OCMW werken om taken van gemeentelijk belang uit te oefenen. Indien men gemeentepersoneel OCMW-taken wil laten uitvoeren, dan kan dat dus sowieso niet met ter

⁵ bv. 08/65 is een machtiging van het comité aan de Rijksdienst voor Kinderbijslag, verleend in 2008, om onder bepaalde voorwaarden, voor bepaalde doeleinden, persoonsgegevens ter beschikking te stellen aan de OCMW's, via de KSZ.

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

⁷ artikel 23, tweede lid, Kruispuntbankwet.

⁸ artikelen 61 tot en met 71 Kruispuntbankwet

beschikkingstelling. Voor de kerntaak van het OCMW, de individuele sociale dienst- en hulpverlening, kan gemeentepersoneel niet ingezet worden (zelfs geen gemeentelijke maatschappelijk werkers), gezien zij in tegenstelling tot OCMW-personeel geen toegang hebben tot de gegevens van de KSZ. Mutatie (ontslag bij de gemeente en aanwerving bij het OCMW) is dan de enige weg.

3.2 Informatieveiligheid garanderen in de context van geïntegreerde dienstverlening

Informatieveiligheid heeft in de context van de OCMW-werking betrekking op de beveiliging van gegevens van persoonlijke aard, gegevens van geïdentificeerde of identificeerbare natuurlijke personen. Deze gegevens vindt men in het OCMW in:

- De software die gebruikt wordt door OCMW's voor onderzoeken in het kader van het recht op maatschappelijke integratie, de wet van 4 april 1965, het stookoliefonds, etc. ...
- Digitale bestanden die maatschappelijk werkers zelf aanmaken in functie van het voorleggen van aanvragen op de Raad voor Maatschappelijk Welzijn
- De boekhoudingssoftware
- Op dragers van back-ups (usb, externe harde schijven, dvd's, ...)
- Op het portaal van de sociale zekerheid
- Op de server
- In de vorm van papieren dragers (in mappen, in de post, in de archieven, enz. ...) die voorstpruiten uit de digitale bestanden.

Het weze duidelijk dat een informatieveiligheidsbeleid aandacht moet hebben voor de veiligheid van al deze dragers van informatie. Meer informatie over de na te leven veiligheidsnormen in het algemeen vindt u op de VVSG-website⁹ en op de website van de Kruispuntbank Sociale Zekerheid¹⁰.

Vanuit het standpunt van informatieveiligheid zou het uiteraard het makkelijkste zijn om als regel te hanteren dat enkel OCMW-personeel en (onder begeleiding) ook OCMW-cliënteel toegang zou hebben tot de gebouwen waarbinnen al deze dragers zich bevinden. Dit is echter een benadering die de toenemende mate van samenwerking tussen OCMW en gemeentebeheer negeert en onmogelijk maakt. Ze is realiseerbaar, noch wenselijk. Het is ook een bui-

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

¹⁰ <http://www.ksz-bcss.fgov.be/nl/bcss/home/index.html>

tenproportionele maatregel, gegeven de essentie, namelijk dat het de persoonlijke gegevens zijn die het object van beveiliging moeten zijn en niet de toegang tot een heel gebouw.

De samenwerking op het vlak van de ondersteunende diensten creëert situaties waarbij gemeentelijke poetsvrouwen, klusjesmannen, onthaalbedienden, archiefbeheerders, ict-hulpdeskmedewerkers of ICT leidinggevenden werkzaamheden verrichten in gebouwen en lokalen waarin zich de gegevens van persoonlijke aard bevinden.

Het uitgangspunt is en dient te zijn dat al deze personen geen toegang hebben tot OCMW-cliëntgegevens omdat zij:

- er wettelijk geen toegang toe hebben,
- deze niet nodig hebben voor hun taakuitoefening

Op dat vlak is er overigens geen enkel verschil met een externe firma die diensten levert aan het OCMW en vanuit die hoedanigheid werkzaamheden verricht in het gebouw waar zich de te beveiligen persoonsgegevens bevinden.

Het is dus zaak om alle nodige maatregelen te nemen zodanig dat de informatieveiligheid verzekerd is, zonder dat dit de samenwerking op het inhoudelijke vlak of op het vlak van de ondersteunende diensten in het gedrang brengt.

Wij stellen volgende maatregelen voor:

- In de deontologische code die de gemeenteraad vaststelt voor het gemeentepersoneel¹¹ wordt een bijzondere clausule opgenomen betreffende informatieveiligheid. Deze clausule heeft tot doel om al de gemeentelijke personeelsleden die zich in functie van hun taakuitoefening moeten begeven in ruimtes waarin zich te beveiligen gegevens van persoonlijke aard bevinden, te verbinden tot geheimhouding.

Clausule i.v.m. informatieveiligheid:

Indien u niet geautoriseerd bent om kennis te hebben van of toegang te hebben tot persoonlijke gegevens van dossiers betreffende individuele dienstverlening van het OCMW tracht u zichzelf nooit die toegang te verschaffen. Indien u ongewild wel in aanraking komt met deze gegevens, hetzij op fysische wijze, hetzij elektronisch of allebei, verbindt u zich tot strikte geheimhouding.

In de deontologische code die de Raad voor Maatschappelijk Welzijn vaststelt¹, wordt deze clausule uitgebreid met onderstaande passage:

Wie uit hoofde van zijn functie wel toegang heeft tot genoemde gegevens, hetzij op fysische wijze, hetzij elektronisch of allebei, hanteert een strikte geheimhoudingsplicht

¹¹ Gemeentedecreet, art. 112.

ten aanzien van deze gegevens en onderschrijft de naleving van de minimale veiligheidsnormen waarvan u door de OCMW-secretaris in kennis gesteld wordt.

- Gemeentelijke ICT-medewerkers die ook voor het OCMW werken, worden vanuit het standpunt van informatieveiligheid door de Kruispuntbank Sociale Zekerheid beschouwd als ‘externe leveranciers’ en vallen dus –indien zij vanuit hun werkzaamheden toegang hebben tot gegevens van persoonlijke aard- onder de verantwoordelijkheid van de OCMW-secretaris. In ons voorstel -gegeven de clausule in de gemeentelijke deontologische code- kan echter ook de gemeentesecretaris hen aanspreken op hun plicht tot geheimhouding. Bijkomend kan voor de gemeentelijke ICT-medewerkers die ook voor het OCMW werken in de clausule i.v.m. informatieveiligheid verwezen worden naar de ‘gedragscode voor informatiebeheerders binnen het netwerk van de sociale zekerheid’. Onder informatiebeheerder wordt hier verstaan: *eenieder die toegangsrechten heeft die dat van het functioneel gebruik van de gegevens overschrijden. Het gaat met name om systeembeheerders, databeheerders, applicatiebeheerders, netwerkbeheerders, consultants, veiligheidsbeheerders enz..*¹²
- Indien er lokaal ook gewerkt wordt met een gemeenschappelijke informatica-infrastructuur, bv. een gemeenschappelijke server, dan is het vanuit informatieveiligheid noodzakelijk dat op netwerkniveau de nodige technische en organisatorische maatregelen voorzien worden opdat enkel geautoriseerde personen toegang hebben tot de voor hen bestemde sociale persoonsgegevens (bijv. door het voorzien van twee domeinen, segmentatie, acces controls en access policy’s.)
- Tenslotte dient het OCMW-personeel dat met cliëntgegevens werkt, het in het OCMW uitgestippelde veiligheidsbeleid na te leven. Essentieel in een context van integratie of samenwerking met de gemeente zijn: het clean desk-principe waardoor cliëntgegevens niet rondslingeren op fysieke dragers en een goed systeem van schermbeveiliging en een wachtwoordenbeleid (zie hieronder).

4. In de praktijk: enkele richtlijnen

Om de beschreven samenwerking tussen gemeente en OCMW op een voldoende veilige manier te kunnen uitvoeren gelden er een aantal elementaire richtlijnen.

4.1 Wachtwoordbeleid

Uiteraard zal in de toekomst elke medewerker die toegang heeft tot beveiligde data zich moeten kenbaar maken en inloggen door middel van zijn/haar elektronische identiteitskaart. Het is immers hét middel bij uitstek om door middel van de certificaten op de elektronische

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

identiteitskaart (eID) en de bijhorende pincode in te loggen op alle mogelijke systemen. Bij de gemeentebesturen is men nu ook van start gegaan met het lokaal veiligheidsbeheer én het gebruik van de eID. Omdat nog niet alle leveranciers en niet alle toepassingen geschikt zijn voor het gebruik van de eID, zal er voorlopig nog moeten gewerkt worden met het traditionele gebruikersnaam/wachtwoord concept.

Het is van het grootste belang dat enerzijds alle toepassingen beveiligd zijn door middel van een login-systeem én anderzijds dat er een wachtwoordbeleid wordt gevoerd dat voldoet aan een aantal minimumeisen:

- Iedereen (iedereen !) die toegang heeft of moet hebben tot beveiligde data, kan dit alleen verkrijgen mits een wachtwoord/gebruikersnaam dat aan hem verleend wordt in opdracht van de lokale veiligheidsbeheerder.
- Dit wachtwoord moet aan minimale voorwaarden voldoen en (concreet) liefst uit minimum 8 tekens bestaan en zowel hoofd- als kleine letters bevatten, cijfers bevatten en niet voor de hand liggende tekens (zoals \$,{,&,...). Vermijd voor de hand liggende combinaties en/of woorden. De lokale veiligheidsbeheerder is -in samenwerking met de systeembeheerder-, verantwoordelijk voor het opstellen van de richtlijnen in dit verband.
- Schrijf je wachtwoord nooit op, zeker niet op een Post-It aan je computer.
- Geef je wachtwoord nooit door. Als iemand anders in het bezit komt van jouw wachtwoord, verander het dan zo snel mogelijk.
- Verander op tijd je wachtwoord als je dat zelf wilt, het veiligheidsbeheer moet er voor zorgen dat je verplicht wordt om regelmatig een nieuwe wachtwoord te definiëren. Het systeem moet ook een controle kunnen uitvoeren dat het oude en het nieuwe wachtwoord niet te veel op elkaar lijken.
- Kijk na of je wachtwoorden niet kan koppelen aan werktijden, vaak is het niet nodig in het weekeinde toegang te verlenen...

4.2 Het loggen van verrichtingen en de controle ervan

Hoewel dit in de beginfase van de informatisering anders was, wordt er sinds de aansluiting op het netwerk van de KSZ aandacht besteed aan het loggen van de verrichtingen. Onder loggen verstaan we 'het geautomatiseerd bijhouden van wie, wat, wanneer deed'. Dit loggen is belangrijk om misbruiken op te sporen. In die zin is het belangrijk op welke wijze met het loggen van verrichtingen wordt omgegaan:

- Communiceer zo helder en open mogelijk over het feit dat verrichtingen gelogd worden. Communiceer welke verrichtingen gelogd worden. Voorkomen is immers steeds beter dan genezen.

- Communiceer tevens dat de bevoegde personen op regelmatige basis steekproeven zullen nemen en dat medewerkers kunnen gevraagd worden uitleg te verschaffen over verrichtingen, zonder dat dit hoeft te impliceren dat er fouten gebeurd zijn.
- Communiceer dat bij het vermoeden van misbruiken deze logging gebruikt zal worden ter controle.
- Communiceer dat deze methodiek (loggen, steekproeven, controle) niet enkel op het niveau van het lokale bestuur gebeurt, maar tevens op het niveau van de aanbieder van de data (in casu de KSZ).

4.3 Heldere procedures

Zorg voor heldere procedures bij het veiligheidsbeheer:

- Integreer het toegangsbeheer en het verlenen van toegang in de onthaalprocedure voor nieuwe werknemers. Overleg met de personeelsdienst in dit verband.
- Idem dito bij uitdienststreding (!) en/of langdurige afwezigheid (allerlei vormen van loopbaanonderbreking).
- Werk aan een procedure die moet toelaten snel én volledig een overzicht te hebben van wie, waar en wanneer toegang moet hebben.
- Werk procedures uit bij vaststelling en/of vermoeden van misbruik. Dit is erg belangrijk omdat dit bv. kan leiden tot schorsing en/of ontslag.
- Communiceer en overleg deze procedures voldoende met alle betrokkenen (inclusief bv. vakbonden !).

4.4 De taken van de veiligheidsconsulent en de lokale veiligheidsbeheerder

De taken van de veiligheidsconsulent zijn beschreven in de regelgeving (waaronder het uitvoeringsbesluit bij de wet op interbestuurlijke gegevensuitwisseling)¹³. Het is belangrijk te

¹³ *Besluit van de Vlaamse Regering betreffende de veiligheidsconsulenten, vermeld in artikel 9 van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer*, 15 mei 2009, B.S.: 2009-07-13 (Ed. 1), nummer: 2009/203137.

Wet van 15/1/90 ter oprichting en organisatie van een kruispuntbank van de sociale zekerheid art. 4 par.5 en art. 24, http://www.ksz-bcss.fgov.be/nl/bcss/anchorpage/content/websites/belgium/legislation/legislation_01/legislation_01_01.html .

noteren dat de veiligheidsconsulent zijn taak op voldoende (tijd) en onafhankelijke wijze kan uitvoeren. Hij is verantwoordelijk voor het opstellen van de nodige verbeterplannen. De adviezen die hij geeft, moeten meegenomen worden bij bv. onderhandelingen met leveranciers. In principe is het niet wenselijk dat de veiligheidsconsulent en de lokale veiligheidsbeheerder (in principe de secretaris, in een aantal gevallen zijn gedelegeerde) dezelfde zijn. Belangenvermenging ligt dan voor de hand, gezien het beheren van de toegangen en het toezien op de informatieveiligheidsnormen best gescheiden worden.

Een veiligheidsconsulent is in de meeste besturen geen voltijdse taak. Samenwerking tussen de veiligheidsconsulenten van gemeente en OCMW ligt voor de hand en is in de context van integratie een must. Maar ook samenwerking tussen verschillende OCMW's en gemeenten is een optie. Het voordeel is dat hierdoor beter competenties kunnen worden opgebouwd en er op langere termijn meer garanties zijn voor een voldoende veiligheidsbeleid.

4.5 Conclusie

Zeker in het licht van de samenwerking tussen gemeente en OCMW wordt het belang van een goed informatieveiligheidsbeleid steeds groter. Niet enkel de fysieke informatieveiligheid (laten rondslingeren van dossiers, papier aan kopieerapparaten e.d.m.) maar ook de digitale informatieveiligheid. De inhoud van 20 meter dossierkasten kan immers gemakkelijk op een USB-stick gestockeerd worden...

5. Algemene conclusies

We beschreven in deze nota twee motivaties die aan de basis lagen van de evolutie naar meer samenwerking tussen OCMW- en gemeentebesturen: de zoektocht naar schaalvoordelen en het streven naar een meer geïntegreerde dienstverlening. Beide zijn legitieme motivaties voor meer samenwerking. In de praktijk echter stuit die evolutie naar meer samenwerking op een wetgeving die aangepast, noch gecoördineerd is (inzake personeelsaangelegenheden en inzake dienstverlening die toegewezen is aan één specifiek bestuur). Bijkomend zijn er een aantal aandachtspunten inzake methodologie en informatieveiligheid. Qua methodologie is het van belang om als bestuur aandacht te hebben voor elkaars specifieke expertise en opdracht.

Informatieveiligheid is cruciaal en dit zowel voor de privacy van de gebruikers, als voor de betrouwbaarheid van de dienst- en hulpverlening. Bovendien is het zo dat zowel gemeente- als OCMW-besturen voor hun dienstverlening meer en meer afhankelijk worden van gegevens die hen door andere instanties verstrekt worden. Deze instanties (bv. KSZ) koppelen terecht voorwaarden inzake informatieveiligheid aan het gebruik van deze gegevens. Het niet naleven van deze veiligheidsvoorwaarden door sommige besturen, zet de toegang tot bestaande en nieuwe gegevens voor alle besturen op de helling.
