Van

Postbus 60055, 6800 JB Arnhem
Westervoortsedijk 73, 6827 AV Arnhem
Telefoon (026) 355 13 55
info@kplusv.nl
www.kplusv.nl

Rapport

Bescherming van privacygevoelige gegevens in de drie decentralisaties in de gemeente Losser

Opdrachtgever
Rekenkamercommissie
gemeente Losser

Referentie

Arnhem, 12 november 2015
Ons kenmerk 1015101-018/lri/jba

Inhoud

Bijlagen

Samenvatting

De Rekenkamercommissie Losser heeft een onderzoek uitgevoerd naar het beleid van de gemeente inzake de bescherming van de persoonsgegevens bij de drie decentralisaties in het sociaal domein. Dit onderzoek is uitgevoerd tijdens de doorvoering van de drie decentralisaties vanwege het leerdoel van de commissie: concrete verbeterpunten in het proces waar de gemeenteraad, de gemeente en uiteindelijk dus de inwoners wat aan hebben.
Privacy in samenhang met de nieuwe taken van de gemeente is een onderwerp dat, terwijl de uitvoering van de taken zelf begint te lopen, landelijk ook aandacht krijgt. Het onderwerp is daarnaast interessant omdat de uitvoering van de decentralisaties een taak is die Losser deels samen met de gemeente Enschede uitvoert en werkwijzen en protocollen toepast die in de gemeente Enschede zijn ontwikkeld.
De centrale onderzoeksvraag is als volgt geformuleerd:

"Wat is het privacybeleid van de gemeente inzake de drie decentralisaties, hoe vindt de uitvoering in de praktijk plaats en hoe is de beoordeling waar het gaat om rechtmatigheid doeltreffendheid?"

Het onderzoek is uitgevoerd in de maanden juni, juli en augustus van 2015. In het onderzoek zijn beleids- en uitvoeringsdocumenten bestudeerd en zijn interviews gehouden met de bij het de bescherming van de privacy direct betrokken medewerkers, waaronder medewerkers uit de uitvoering van de nieuwe gemeentelijke taken uit de decentralisaties, en bestuurders.

De nota van bevindingen is voorgelegd aan de ambtelijke organisatie van de gemeente voor een technisch wederhoor. De reacties zijn in de rapportage verwerkt. Zowel de technische reactie als de verwerking in de rapportage treft u in de bijlagen onder bijlage 5.

De bevindingen uit het onderzoek zijn in de onderstaande tabel kernachtig getoetst aan het normenkader dat de rekenkamercommissie voor het onderzoek heeft vastgesteld.

Toetsing aan het normenkader

Norm	Toetsing
1. Op welke uitgangspunten, risico's en normen is het privacybeleid van de gemeente Losser gebaseerd?	
De uitgangspunten voor het privacybeleid van de gemeente Losser zijn beschreven en vastgesteld. De risico's voor het beheer, gebruik en de uitwisseling van persoonsgegevens (ten behoeve van de drie decentralisaties) zijn onderzocht. De gemeente heeft duidelijke normen voor het beheer, het gebruik en de uitwisseling van persoonsgegevens door medewerkers van de gemeente en andere betrokken partijen.	De gemeente heeft geen vastgesteld privacybeleid (het WAT en WAAROM). De gemeente heeft een aantal vastgestelde documenten die de uitvoering van de bescherming van informatie waaronder persoonsgegevens en gegevens uit de drie decentralisaties betreffen (het HOE), Deze maatregelen zijn door het college vastgesteld op basis van een door het door gemeenten gezamenlijk ontwikkelde VNG-model (BIG) en zijn risicogestuurd.
2. Wat zijn de algemeen geldende vereisten, interne richtlijnen en formele en informele afspraken voor het privacybeleid en hoe sluiten deze aan bij de bredere beleidsdoelen van de gemeente?	
De gemeente heeft interne en externe richtlijnen voor het beheer, het gebruik en de uitwisseling van persoonsgegevens	Ja. Het door het college vastgestelde beleid bevat richtlijnen over hoe gegevens die in de gemeente worden beheerd behoren te worden beschermd, zowel voor de dataopslag, het interne gebruik als voor de uitwisseling
3. Voldoet de formulering van het privacybeleid van de gemeente Losser aan de Europese en nationale regelgeving?	
Het beleid voldoet aan de Europese en Nederlandse wet en regelgeving met betrekking tot het gebruik van persoonsgegevens. Het beleid is afgestemd op de laatste inzichten met betrekking tot beheer, gebruik en uitwisseling van persoonsgegevens zoals dit is vastgelegd in landelijke onderzoeken en handreikingen.	Ja. Het beleid voldoet aan de wetgeving.
4. Op welke wijze is het beleid geïmplementeerd in interne procesafspraken en waarborgen?	
De gemeente heeft ter bescherming van de gegevens werkvoorschriften, procedures en protocollen opgesteld voor het gebruiken, uitwisselen en bewaren van persoonsgegevens. De verantwoordelijkheden en bevoegdheden voor het nakomen van de werkvoorschriften en procedures inzake de bescherming zijn vastgelegd, onder meer wie toezicht houdt	Ja. voor toegang tot persoonsgegevens zijn werkvoorschriften, procedures en protocollen opgesteld. Voor uitwisseling van gegevens zijn geen aparte protocollen. Advies vanuit Samen14 tot anoniem betalen facturen is niet overgenomen. Hierdoor op afd. financiën ook privacygevoelige informatie. Er zijn hiervoor geen protocollen. Documenten zijn nog niet aangepast op de situatie van na 1 januari 2015. Er is geen afspraak over de bewaartermijn van digitale dossiers. Verantwoordelijkheden en bevoegdheden zijn toegewezen, inclusief toezichthouding.
5. In hoeverre is de uitvoeringspraktijk conform het vastgestelde beleid?	
Medewerkers zijn op de hoogte van het privacybeleid en de daarbij behorende werkvoorschriften en procedures en passen deze aantoonbaar toe.	Ja, medewerkers zijn onbewust bekwaam, leidinggevenden zijn bewust bekwaam[1].
De beveiliging van digitale gegevensopslag wordt bewaakt en periodiek up-to-date gehouden.	Ja. De beveiliging van digitale gegevensopslag wordt bewaakt.

[1] Onbewust bekwaam: Dingen lijken als vanzelf goed te gaan, gevoelsmatig goed handelen.
Bewust bekwaam: Bewust goed handelen.

Norm	Toetsing
6. Op welke wijze vindt verantwoording en controle plaats over het privacybeleid?	
Periodiek vindt controle, bijvoorbeeld door middel van audit, plaats op het beheer, gebruik en de uitwisseling van persoonsgegevens.	Ja. Inloggegevens SUWI-net worden opgevraagd door leidinggevenden en gecontroleerd. Er worden audits gehouden op de uitvoering van de beschermingsmaatregelen die op basis van het BIG zijn genomen.
Leidinggevenden en medewerkers spreken elkaar aan op het niet nakomen van procedures inzake de bescherming van persoonsgegevens.	Ja. Medewerkers en leidinggevenden passen regels van privacybeleid toe.
Over de resultaten van controles van het privacybeleid wordt de verantwoordelijke wethouder en de raad periodiek geïnformeerd.	Nee. De raad wordt niet periodiek geïnformeerd over de resultaten van controles.
7. Hoe wordt de samenwerking met de gemeente Enschede in praktijk gebracht en welke ervaringen zijn daarmee tot nu toe?	
De door de gemeente Losser vastgelegde beleidsuitgangspunten, normen en interne richtlijnen en protocollen worden in de samenwerking gehanteerd (voor zover het gegevens van inwoners van Losser betreft).	Het beleid dat het college heeft vastgesteld is overeenkomstig het door gemeenten gezamenlijk opgestelde VNG-model. Ditzelfde model is in de gemeente Enschede gebruikt als basis. Voor de uitvoering van de maatregelen die de bedrijfsvoeringssamenwerking betreffen is geen onderscheid.
8. Hoe wordt de gemeenteraad geïnformeerd over de uitvoering van het privacybeleid?	
Er is een heldere vastgelegde afspraak over de wijze waarop de raad wordt geïnformeerd over de uitvoering van beheer, gebruik en uitwisseling van persoonsgegevens en daarbij optredende knelpunten.	De raad heeft een verordening BRP vastgesteld voor de gemeente. Deze verordening betreft niet de gegevens uit de drie decentralisaties.
De raad wordt periodiek en in hoofdlijnen op de hoogte gesteld van de resultaten van audits op de uitvoering van beheer, gebruik en uitwisseling van persoonsgegevens.	Nee. De raad wordt niet geïnformeerd over de bescherming van persoonsgegevens als zodanig. De raad wordt geïnformeerd over verschillende dossiers die zijdelings raken aan het onderwerp privacy en bescherming van persoonsgegevens.

1 Inleiding

1.1 Doel en vraagstelling voor het onderzoek

De Rekenkamercommissie (RKC) heeft in de maanden juni tot en met september een onderzoek uitgevoerd naar de rechtmatigheid en doeltreffendheid van het privacybeleid van de gemeente. De RKC heeft het onderzoek uitgevoerd om inzicht te krijgen in het gemeentelijk beleid met betrekking tot bescherming van de privacy en de borging van het beleid in de uitvoering. Het onderzoek betreft met name de bescherming van de bij de gemeente aanwezige en te verkrijgen privacygevoelige gegevens uit de drie decentralisaties in het sociaal domein.

De RKC is zich bewust dat de drie decentralisaties pas sinds begin dit jaar door de gemeente worden uitgevoerd en dat de aandacht nu nog vooral uitgaat naar het daadwerkelijk zorgen dat de inwoners van Losser de benodigde zorg ontvangen. Zaken als gegevensbescherming worden in zo'n beginperiode vaak niet als eerste prioriteit gezien. Toch heeft de RKC dit onderzoek nu uitgevoerd, omdat juist in de beginperiode het meest geleerd kan worden. Het doen leren uit de rekenkameronderzoeken is voor de RKC de belangrijkste taak.

De centrale onderzoeksvraag voor het onderzoek is als volgt geformuleerd:
"Wat is het privacybeleid van de gemeente inzake de drie decentralisaties, hoe vindt de uitvoering in de praktijk plaats en hoe is de beoordeling waar het gaat om rechtmatigheid doeltreffendheid?"

Om de centrale onderzoeksvraag te beantwoorden zijn 8 deelvragen voor het onderzoek vastgesteld:

Beleidsbeschrijving

1. Op welke uitgangspunten, risico's en normen is het privacybeleid van de gemeente Losser gebaseerd?
2. Wat zijn de algemeen geldende vereisten, interne richtlijnen en formele en informele afspraken voor het privacybeleid en hoe sluiten deze aan bij de bredere beleidsdoelen van de gemeente?
3. Voldoet de formulering van het privacybeleid van de gemeente Losser aan de nationale regelgeving (en eventueel Europese)?

Beleidsuitvoering

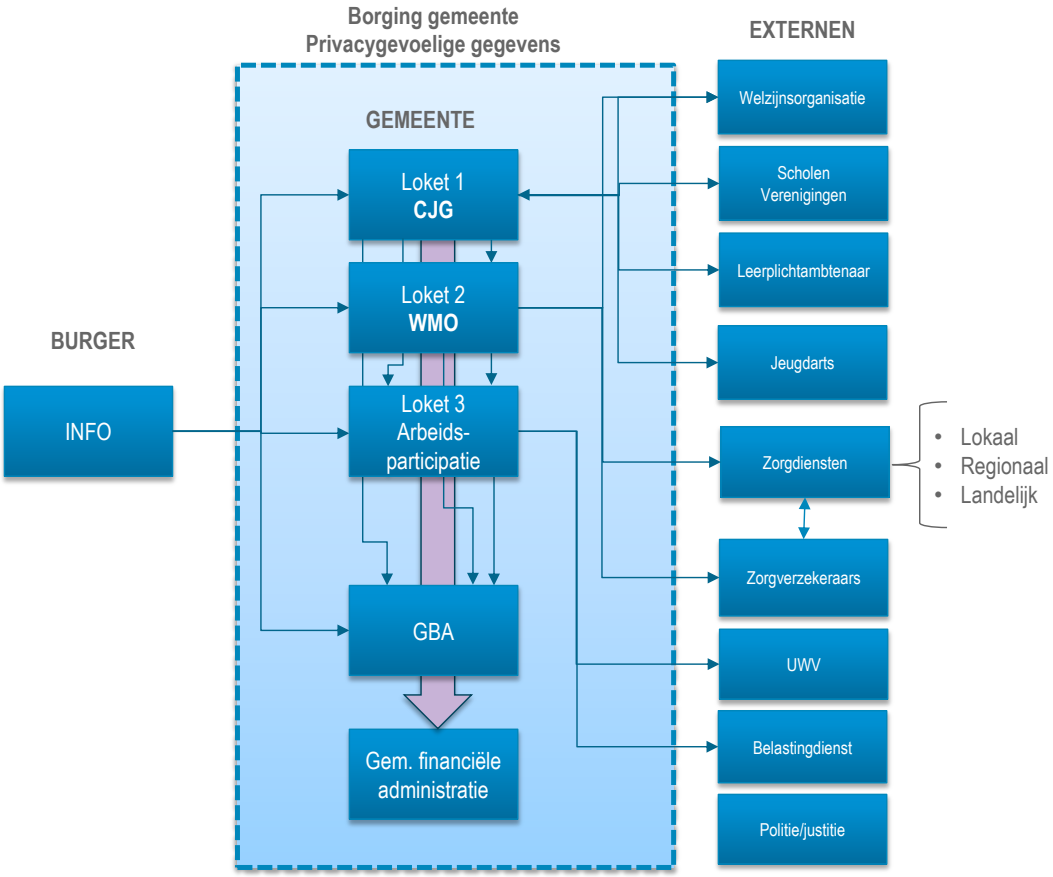
4. Op welke wijze is het beleid geïmplementeerd in interne procesafspraken en te waarborgen?
5. In hoeverre is de uitvoeringspraktijk conform het vastgestelde beleid?
6. Op welke wijze vindt verantwoording en controle plaats over het privacybeleid?
7. Hoe wordt de samenwerking met de gemeente Enschede in praktijk gebracht en welke ervaringen zijn daarmee tot nu toe?

Controlerende taak

8. Hoe wordt de gemeenteraad geïnformeerd over de uitvoering van het privacybeleid?

Afbakening

Uit de onderzoeksvragen is af te leiden dat het onderzoek de borging van de bescherming van de privacygevoelige gegevens betreft die door de gemeente worden beheerd. Het onderzoek is afgebakend tot de voor de gemeente uitvoerende organisaties inzake de drie decentralisaties. In de onderstaande figuur is de afbakening schematisch weergegeven.



Leeswijzer

Hoofdstuk 2 beschrijft de opzet en aanpak van het onderzoek en normenkader dat door de RKC hiervoor is vastgesteld.
In hoofdstuk 3 zijn de bevindingen (feiten en analyse) uit het onderzoek opgenomen. Dit zijn de feiten zoals deze op basis van het feitenonderzoek en confrontatie van de bevindingen met het normenkader zijn aangetroffen. Het hoofdstuk behandelt achtereenvolgens in paragrafen: Het privacybeleid; de uitvoering; de controle en verantwoording en de rol van de raad. Elke paragraaf begint met de feitelijke constateringen vanuit documentstudie en interviews. Daarnaast worden de waarnemingen in de gemeente geconfronteerd met het normenkader. De conclusies en de aanbevelingen die de rekenkamercommissie aan de bevindingen verbindt, vormen hoofdstuk 4. Dit hoofdstuk is na het ambtelijk wederhoor toegevoegd.

2 Opzet en aanpak van het onderzoek

2.1 Uitvoering van het onderzoek

In het onderzoek zijn twee bronnen gebruikt voor de gegevensverzameling. De eerste bron is het bestuderen van de gemeentelijke documenten, de tweede bron zijn gesprekken met een aantal sleutelfunctionarissen.

Het onderzoek is gestart met een startbijeenkomst met de betrokkenen uit de ambtelijke organisatie. Tijdens deze bijeenkomst is het onderzoek toegelicht en zijn afspraken gemaakt over de medewerking van de organisatie. Daarna is de documentstudie uitgevoerd. De lijst met bestudeerde documenten treft u aan in bijlage 1 bij deze nota van bevindingen. In de documentstudie is aandacht besteed aan het vastgestelde beleid en de uitwerking daarvan voor de uitvoerende medewerkers.

Na de documentenanalyse hebben interviews met een aantal sleutelpersonen plaatsgehad. Tijdens deze gesprekken zijn de onderzoeksvragen en het normenkader leidend geweest. Tevens zijn de interviews gebruikt om een organisatiebreed beeld krijgen hoe wordt omgegaan met het beleid ten aanzien van de persoonsgegevens uit de decentralisaties. Met name is gekeken naar de wijze waarop daarbinnen borging van privacy een plaats krijgt alsmede de dilemma's waarvoor de medewerkers komen te staan in de praktijk.

Zowel in de ook de documentstudie als in de gesprekken is de rol van de samenwerking met de gemeente Enschede voor de bedrijfsvoeringstaken een aandachtspunt geweest.

Vervolgens is de nota van bevindingen aan de ambtelijke organisatie van de gemeente gezonden voor een technisch wederhoor. Daarin is de feitelijke juistheid van de bevindingen gecheckt. De reacties zijn in de rapportage verwerkt.

2.2 Normenkader

De rekenkamercommissie heeft voor het onderzoek een aantal normen vastgesteld die gebruikt zijn om de bevindingen te toetsen. De normen zijn per deelvraag voor het onderzoek gerubriceerd. Dit normenkader en de confrontatie van het normenkader met de bevindingen is opgenomen in de samenvatting (pagina 1-3).

3 Bevindingen

In dit hoofdstuk worden de bevindingen (feiten en analyse) uit het onderzoek beschreven. Dit zijn de feiten zoals deze op basis van het feitenonderzoek en confrontatie van de feiten met het normenkader zijn aangetroffen.

3.1 Het privacybeleid

De gemeente heeft diverse beleidsdocumenten die betrekking hebben op de bescherming van privacygevoelige gegevens van burgers die de gemeente beheert. Al voor de start van het decentralisaties werd er in algemene zin nagedacht over de bescherming van informatie. Specifiek voor de transities spreekt de gemeente zich in 2014 uit over de bescherming van de privacygevoelige gegevens:
"Om invulling te kunnen geven aan de integrale aanpak volgens één gezin, één plan, één regisseur moet informatie tussen actoren in het sociaal domein gedeeld worden. Dat vraagt dat we zorgdragen voor een goede borging van de privacy en veiligheid van informatie van onze inwoners[2]."

In april 2008 stelt het college het Beveiligingsplan voor de ICT-applicatie SUWInet voor de afdeling Werk, Zorg en Inkomen (WIZ) vast. Dit beveiligingsplan gaat over het beheer en de uitwisseling van gegevens in het kader van de Wet Werk en Bijstand (WWB).
Voor de uitvoering van de WWB worden gegevens uitgewisseld met het Centrum voor Werk en Inkomen (CWI) en het UWV, de belastingdienst en andere gemeenten. Met deze ketenpartners zijn beveiligingsafspraken gemaakt ter bescherming van de privacygevoelige informatie. In dit beveiligingsplan wordt aangegeven hoe medewerkers van de gemeente met het gebruik van SUWInet en het raadplegen van het Inlichtingenbureau moeten omgaan.

De kern van het vastgestelde beveiligingsplan bestaat uit een aantal maatregelen:
- er wordt gewerkt met verschillende autorisaties;
- medewerkers worden alleen geautoriseerd om de gegevens in te zien die zij voor hun taak nodig hebben;
- het afdelingshoofd Werk, Zorg en Inkomen kent de autorisaties toe;
- informatie mag nooit voor privédoeleinden worden ingezien of opgevraagd;
- alleen de applicatiebeheerder mag gegevens ophalen;
- voor het uitwisselen van gegevens wordt alleen gebruik gemaakt van het beveiligde SUWImail;
- het gebruik van SUWInet en SUWImail wordt gemonitord en de inloggegevens worden geregistreerd.

[2] Uitvoeringsplan transities sociaal domein, oktober 2014, gemeente Losser.

Voor de medewerkers gelden als maatregelen:

- authenticatie door middel van wachtwoord;
- melden van beveiligingsincidenten;
- geheimhoudingsplicht;
- geen vertrouwelijke informatie aan derden per telefoon;
- clean desk / clear screen policy;
- geen vertrouwelijke informatie in de prullenbak.

In 2013 is het Informatiebeveiligingsbeleid[3] van de gemeente vastgelegd. Voor dit beleid sluit de gemeente aan bij het landelijk ontwikkelde beleid voor het beschermen van persoonsgegevens. Dit beleid is door het Kwaliteitsinstituut Nederlandse Gemeenten in opdracht van de VNG opgesteld[4]. Uitgangspunten voor dit beleid zijn:

- De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels volgens het principe van Verplichtende Zelfregulering.
- Hierbij geldt: Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: GBA, SUWI, BAG en PUN, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het ‘pas toe of leg uit’ principe.
- Het systeem van verplichtende zelfregulering wordt geborgd door het onderdeel te maken van een interne cyclus, door transparantie en door toezicht.

In dit beleid heeft het begrip ‘informatiebeveiliging’ betrekking op:

1. vertrouwelijkheid / exclusiviteit: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
2. betrouwbaarheid / integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
3. beschikbaarheid / continuïteit: het zorg dragen voor het beschikbaar zijn van informatie en informatieverwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.

Het beleid behandelt alle aspecten die met de beveiliging van gegevens en informatie die de gemeente beheert. Dit betekent dat er hoofdstukken zijn over de informatietechnische beveiliging, maar ook over de beveiliging van locaties waar de gegevens zijn, de beveiliging van gegevens tijdens de uitwisseling en de beveiliging van gegevens in het gebruik van gemeentelijke medewerkers. Het beleid is risicogebaseerd. De risico's voor de beveiliging worden hierin geïdentificeerd en vervolgens worden de maatregelen ontworpen om de risico's tegen te gaan. Deze maatregelen zijn als eisen verder uitgewerkt. In feite is het een uitgewerkt gemeentelijk specifiek informatiemanagementsysteem. Het systeem volgt voor de te nemen maatregelen de 'plan – do – check – act' cyclus, waarbinnen continu moet worden bekeken of de maatregelen afdoende zijn.

[3] Informatiebeveiligingsbeleid, augustus 2013, Gemeente Losser.

[4] Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Twee uitgangspunten zijn gericht op het gebruik van informatie en informatiesystemen door medewerkers:

- medewerkers gebruiken gemeentelijke informatie primair voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- privégebruik van gemeentelijke informatie en bestanden is niet toegestaan.

Medewerkers moeten dezelfde bescherming bieden aan gemeentelijke informatie als ze elders (bijvoorbeeld thuiswerkplek) werken. Dat betekent onder andere opletten op niet geautoriseerd gebruik, clean desk, et cetera.
Dit gemeentelijke beleid is de basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen. Genoemd worden bijvoorbeeld SUWI en de gemeentelijke basisregistraties.
Om te bepalen welk beschermingsniveau nodig is wordt een classificatiesysteem gebruikt. Er zijn drie niveaus van bescherming, naast het niveau 'geen'. Dit is in een matrix weergegeven.

Niveau	vertrouwelijkheid	integriteit	beschikbaarheid
Geen	**Openbaar** informatie mag door iedereen worden ingezien (bv: algemene informatie op de externe website van de gemeente	**Niet zeker** informatie mag worden veranderd (bv: templates en sjablonen)	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn (bv: ondersteunende tools als routeplanner)
Laag	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie (bv: informatie op het intranet)	**Beschermd** het bedrijfsproces staat enkele (integriteits-)fouten toe (bv: rapportages)	**Noodzakelijk** informatie mag incidenteel niet beschikbaar zijn (bv: administratieve gegevens)
Midden	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers (bv: persoonsgegevens, financiële gegevens	**Hoog** het bedrijfsproces staat zeer weinig fouten toe (bv: bedrijfsvoerings-informatie en primaire procesinformatie zoals vergunningen)	**Belangrijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk (bv: primaire procesinformatie)
Hoog	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) (bv: zorggegevens en strafrechtelijke informatie)	**Absoluut** het bedrijfsproces staat geen fouten toe (bv: gemeentelijke informatie op de website)	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten (bv: basisregistraties)

Tabel 1: Matrix classificatie beschermingsniveau (tussen haakjes voorbeelden van informatie).

Uit de tabel valt af te leiden dat de gegevens die de gemeente beheert over burgers in het kader van de 3D-transitie vallen onder beschermingsniveau 'Hoog' als het gaat om zorggegevens. Het beleid verwijst voor de maatregelen bij persoonsgegevens naar het richtsnoer Beveiliging van Persoonsgegevens van het College Bescherming Persoonsgegevens (CBP 2013).

In 2007 is in de gemeente Enschede al de Nota Informatiebeleid vastgesteld. deze nota doet uitspraken over de informatisering van de gemeente. Twee van de uitgangspunten voor de bescherming van de gegevens in deze nota raken de beveilig borging van de beveiliging van persoonsgegevens zoals in dit onderzoek bedoeld. Het zijn uitgangspunten voor management en bedrijfsvoering:

- centrale sturing op Informatisering en ICT (automatisering);
- informatiehuishouding voldoet aan eisen van beveiliging, privacy.

Deze nota kan als voorloper van het in 2013 vastgestelde beleid worden gezien. De nota wordt hier genoemd vanwege de samenwerking in de bedrijfsvoering die de gemeente Losser met de gemeente Enschede heeft.
In 2014 zijn over de drie decentralisaties door de gemeente een drietal nota's vastgesteld:

- Beleidsplan Participatiewet Gemeente Losser (11 november 2014)
- Beleidsplan maatschappelijke ondersteuning Gemeente Losser 2015-2018 (2014)
- Beleidsregels Jeugdzorg Gemeente Losser (december 2014)

De nota's behandelen vooral wat de gemeente in de drie decentralisaties wil doen, wat ze voor de burgers van Lossen wil betekenen. Het hoe wordt niet in de nota's behandeld. In deze nota's wordt het beheren en beschermen van privacygevoelige gegevens als zodanig niet behandeld. Wel wordt een denkrichting beschreven die de gemeente hanteert als dienstverlener voor de burger. De gemeente zet in op één integraal werkende organisatie.

In het visiedocument op het sociaal domein[5] is er wel aandacht voor de bedrijfsvoerings-vraagstukken die de drie decentralisaties met zich brengen. De gemeente Losser wil de transitie gebruiken om een transformatie in de bedrijfsvoering te bereiken[6] naar een vraaggerichte organisatie. Vanuit de visie op de drie decentralisaties, geldt voor de uitwerking op de taakvelden het volgende op privacy van toepassing zijnde uitgangspunt:

- *"We gaan als gemeente Losser meer persoonsgegevens van meer inwoners verwerken. We gaan zorgvuldig om met privacy gevoelige gegevens en volgen de wettelijke voorschriften."*

Dit is uiteindelijk in het plan voor de drie decentralisaties ook verwoord, zoals aan het begin van de paragraaf is vermeld. Ook daarin komt echter de bescherming van de privacy niet uitgewerkt voor. Dit sluit aan bij het op een na laatste uitgangspunt in het visiedocument:

- *"We kennen onze beperkingen: onze ambities passen we aan op de capaciteit van onze organisatie en die van onze partners. Het betekent dat we dankbaar gebruik maken van de ervaringen en deskundigheid van anderen in onze regio en daarbuiten. We vinden zo mogelijk niet zelf het wiel uit, maar vertalen "best practices" en voorbeelden naar de Losserse situatie[7]"*

Eveneens in 2014 heeft de raad van de gemeente een verordening vastgesteld die mede de bescherming van persoonsgegevens als onderwerp heeft: Verordening basisregistratie personen gemeente Losser. Deze verordening betreft niet rechtstreeks de gegevens die de gemeente uit de drie decentralisaties verkrijgt en beheert, maar de gegevens uit de gemeentelijke basisregistratie.

---

[5] Visie Sociaal Domein, gemeente Loser, 4 juni 2014.

[6] Visie Sociaal Domein, gemeente Loser, 4 juni 2014, § 2.5, pagina 8.

[7] Visie Sociaal Domein, gemeente Loser, 4 juni 2014, § 3, pagina 10.

Overeenkomstig de verordening kan de gemeente voor bepaalde werkzaamheden van een gewichtig maatschappelijk belang en aan bepaalde organisaties[8] een gelimiteerd aantal gegevens uit de basisregistratie[9] verstrekken over personen uit de gemeente Losser. Daarnaast kan de gemeente een instantie gegevens over een inwoner van Losser verstrekken indien de instantie daarvoor toestemming heeft gekregen van de betreffende inwoner.
In 2012 heeft de Rekenkamercommissie een onderzoek uitgevoerd naar de uitvoering van de WMO in de gemeente. Hierbij is onder meer het zorgloket onderzocht en is naar de klanttevredenheid gekeken. Het rekenkameronderzoek heeft geleid tot een project om de WMO-prestatievelden meetbaarder te maken.

Deze is in een raadsinformatiebrief op 9 september 2013 naar de gemeenteraad gestuurd. Onderdeel van de meting van de klanttevredenheid is dat de gegevens van alle personen die contact opnemen met het zorgloket worden vastgelegd, ook als er geen aanvraag voor een voorziening wordt gedaan.

De gemeente heeft een aantal beleidsnota's die de drie decentralisaties en de visie van de gemeente daarop betreffen. In die nota's ligt de nadruk op de uitvoering van de decentralisatietaken. De bedrijfsvoering daarvoor komt alleen zijdelings als randvoorwaarde ter sprake.
De gemeente heeft voorts een aantal beleidsnota's en documenten die de bescherming van gegevens behandelen. Deze documenten zijn in het college vastgesteld en betreffen de uitvoering van beschermingsmaatregelen voor gegevens, waaronder privacy gevoelige gegevens van personen die de gemeente in het kader van de transities in het sociaal domein onder zich heeft.
De gemeente heeft de Verordening basisregistratie personen gemeente Losser. Deze handelt over de bescherming van persoonsgegevens uit de BRP.
De gemeente heeft geen beleidsnota's over de bescherming van de privacy van de inwoners van de gemeente in samenhang met de 3D-transitie.

[8] Deze zijn limitatief opgenomen in de bijlage 1 bij artikel 3 van de verordening.

[9] De gegevens die uitgewisseld mogen worden staan in artikel 2 lid 3 van de verordening.

3.2 Uitvoering: organisatie, bevoegdheden en verantwoordelijkheden, samenwerking

3.2.1 Organisatie en verantwoordelijkheden

De gemeente Losser heeft ter bescherming van persoonsgegevens meerdere werkvoorschriften, procedures en protocollen opgesteld voor de toegang tot en beveiliging van persoonsgegevens. De gemeente heeft een procedure voor account- en wachtwoordbeleid bij toegang tot het gemeentelijke netwerk[10], en een procedure voor de autorisatie tot het GBA systeem[11]. Het beveiligingsplan SUWInet behandelt de autorisatie tot gebruik van het SUWIsysteem, regels rond beveiligd gebruik van de informatie en de monitoring ervan[12].

Voor SUWInet zijn 16 medewerkers geautoriseerd, waaronder een medewerker van de administratie. Voor het programma voor de jeugdwet zijn 14 gebruikers geautoriseerd.
In het document Informatiebeveiliging[13] zijn functies en verantwoordelijkheden bij informatiebeveiliging binnen de gemeente Losser beschreven. De BMO-ICT Change Management procedures[14] beschrijven de te volgen protocollen bij gewenste wijzigingen in de verschillende ICT-systemen. Veel van de gebruikte protocollen zijn nog niet aangepast aan de situatie van na 1 januari 2015.
Over het gebruik, uitwisselen en bewaren van gegevens zijn geen aparte protocollen opgesteld. Papieren dossiers worden bewaard volgens de regels van de archiefwet, digitale dossiers worden in principe oneindig bewaard.

Privacy in de gemeente Losser is geborgd in de materiewetten en in de systeemwetten van de gemeente. Uit de interviews komt naar voren dat medewerkers van de gemeente zichzelf zien als professionele en integere medewerkers, die, met het afleggen van de gemeentelijke eed, zichzelf en collega's beschouwen als betrouwbaar onderdeel van dit systeem. Dit geldt voor zowel de professionals, de leidinggevenden, bestuurders als de staffunctionarissen.

De professionals in de gemeente Losser gaan deels onbewust bekwaam om met privacy. Zij handelen niet bewust gevoelsmatig juist. Protocollen worden niet consequent gebruikt, maar medewerkers weten over het algemeen welke bedrijfsregels gelden in het beschermen van persoonsgegevens. De opzet en het gebruik van papieren en digitale formulieren is hierin mede bepalend, want zij geven kaders aan de hoeveelheid benodigde informatie. In het Handboek Maatwerkvoorzieningen voor WMO en Jeugdwet[15] staat in diverse werkinstructies dat een omschrijving van de indicatie dient te worden toegevoegd in het dossier almede een mogelijke zorgverlener. Dit betreft uitwisseling van privacygevoelige informatie, maar dit valt volgens het handboek binnen de geldende geheimhouding.
Medewerkers hanteren een clean desk policy, en casuïstiek wordt onderling anoniem besproken.

---

[10] Account en wachtwoordbeleid en procedure – memo 6-12-2012, afdeling DV/IM.

[11] Proces autorisatie GBA systeem – status, versie en afdeling niet bekend.

[12] Beleidsplan SUWINET, april 2008, afdeling WIZ.

[13] Informatiebeveiliging, functies en rolbeschrijvingen, juli 2103 – auteur A.H. de Kleine.

[14] De BMO-ICT Change Management, gemeente Enschede.

[15] Handboek Maatwerkvoorzieningen alle leeftijden WMO 2015 en Jeugdwet, versie 11-05-2015.

Uit de interviews komt naar voren dat de algemene houding ten opzichte van informatiebeveiliging is:

Als het niet nodig is ten behoeve van de aanvraag, schrijf je de informatie niet op en als je twijfelt over de waarborging van de privacy of informatiebeveiliging, bespreek je dit geanonimiseerd met iemand binnen de afdeling.

Leidinggevenden gaan bewust bekwaam om met privacy. Bij het inwerken van (2 tijdelijke medewerkers, zoals nodig bij het inhaaltraject om bestaande zorgtrajecten om te vormen naar de regels van de drie decentralisaties), worden zij hierover geïnstrueerd door hun leidinggevende. Op werkoverlegniveau vindt casusoverleg plaats (nieuwe meldingen). Daar wordt ook besproken hoe er mee om te gaan, inclusief houding- en gedragsaspecten. Ook hier geldt het uitgangspunt dat informatie die niet met inwoners kan worden besproken geen aanvullende waarde heeft en niet wordt bewaard. Daarnaast geldt bij het toewijzen van autorisaties door leidinggevenden het principe: Als het niet nodig is ten behoeve van de functie of het functioneren, heb je geen toegang. Door de inrichting van de ICT-informatiesystemen is dit gericht toe te wijzen. Aansturing gebeurt niet overal eenduidig en niet alle relevante protocollen, procedures en werkinstructies worden door leidinggevenden actief uitgelegd.
Op hoger managementniveau wordt vertrouwd op de deskundigheid van de uitvoering door de professionals, de opbouw van en sturing vanuit de informatiesystemen en de daarbij behorende richtlijnen. Ook hoger management hanteert hetzelfde uitgangspunt: Gegevens worden alleen gebruikt waarvoor ze zijn bedoeld.

In collegeoverleg komt af en toe privacygevoelige informatie ter sprake. Hierop wordt geanticipeerd door in deze gevallen in besloten kring te vergaderen en/of informatie te anonimiseren. Het maakt het bestuur extra kritisch op openbare vergaderstukken met persoonsgevoelige informatie en ze zijn zich bewust dat dit ook juist in een kleinere gemeenschap van groot belang is.

Bestuurlijk wordt gezien dat rond privacy vooral discussie ontstaat door de drie decentralisaties wanneer signalering en preventie belangrijk zijn. Sociale teams worden steeds meer de ogen en oren van de wijk. Om als gemeente de regiefunctie uit te kunnen voeren, is overzicht vanuit verschillende taakvelden nodig. Hiervoor is overleg en uitwisseling van persoonsgegevens van belang. Er is bewustzijn dat dit een grijs gebied is. Wat betreft informatievergaring en informatie-uitwisseling speelt de intentie van handelen hierin een belangrijke rol. Daarnaast is terugkoppeling aan de inwoner van belang. De vorming van beleid hierin is gewenst. Door de uitvoering van de drie decentralisaties is hier nog geen tijd voor geweest, maar het bestuur is zich bewust van de behoefte hieraan.

Vanuit de Twentse samenwerking Samen14 is op 30 juni 2015 het ongevraagd advies gegeven om anonieme facturen die zorgaanbieders de gemeente momenteel ter betaling aanbieden, in het belang van de continuïteit van zorg toch te verwerken[16].
Dit advies is door de gemeente Losser niet overgenomen, vanuit het bestuurlijke standpunt van gewenste transparante verantwoording voor de uitgaven van de gemeente. Door de financiële afdeling worden geen geanonimiseerde betalingen gedaan. Op de afdeling financiën geldt geen geheimhoudingsplicht en hiervoor worden geen specifieke protocollen gebruikt. Wel wordt ook op deze afdeling vertrouwd op de professionaliteit en integriteit van de medewerkers.

[16] OZJT/Samen14: Memo – persoonsgegevens jeugd- en facturatie, 30-06-2015.

Er is 1 ambtenaar verantwoordelijk voor controle leverantie van facturen. Een andere ambtenaar, zijnde de budgethouder, is verantwoordelijk voor de accordering van betalingen. Het kleinschalige karakter van de gemeente Losser maakt privacy van inwoners extra gevoelig. Bestuur, management en uitvoering zijn zich hier terdege van bewust. Op een schaal van 1-10 scoort zowel de privacygevoeligheid als het geschatte bewustzijn ervan een 8-9. Sociale teams leggen bij voorkeur huisbezoeken af. Inwoners die naar de verschillende loketten komen op het gemeentehuis wordt de mogelijkheid geboden om in een aparte ruimte te gaan zitten. De komst van het CJG naar de locatie van het gemeentehuis wordt vanwege samenwerking door medewerkers positief ervaren, maar de gescheiden ingang in het gemeentehuis zou, gezien de schaalgrootte van Losser, tot precaire situaties voor inwoners kunnen leiden. Het CJG speelt hierop in door bewoners van Losser de keuze te geven om zowel via de hoofdingang- als de achteringang van het gemeentehuis naar het CJG te gaan.

Scholing, intervisie en evaluatie van privacybeleid en gestructureerde aandacht voor privacy in de uitvoering (zoals bij signalering en preventie) zijn nog niet structureel georganiseerd. De uitvoering en het management wijzen nadrukkelijk op de hectiek die de voorbereiding van en implementaties van de decentralisaties heeft betekend. Hierin is een pragmatische houding gehanteerd: Eerst doen en dan regelen, om te zorgen voor continuering van zorg voor inwoners van Losser. Men is zich bewust van, en heeft behoefte aan meer aandacht voor privacy, met name in de overgangen tussen de verschillende materiewetten: Jeugdwet, WMO, participatiewet en passend onderwijs.

3.2.2 Organisatie samenwerking met zorgaanbieders

Vanuit de samenwerking Samen14 is een handboek opgesteld voor regisseurs van WMO en Jeugd in de gemeente Losser. Het handboek beschrijft een aantal werkafspraken tussen de gemeente en zorgaanbieders. Over privacy is een aparte werkafspraak opgenomen: "Aanbieder behandelt cliënten respectvol en de privacy van cliënten wordt gerespecteerd conform wettelijke eisen. Dit betekent:

- de medewerker respecteert de levenssfeer en de leefpatronen van de cliënt; dit uit zich bijvoorbeeld in het zich niet ongevraagd bemoeien met diens privézaken, vertrouwelijk omgaan met privé-gegevens, zorgvuldig omgaan met eigendommen van de cliënt, rekening houden met de dagelijkse leefpatronen van de cliënt, respect hebben voor geloofsovertuiging en voor seksuele diversiteit;
- de medewerker staat open voor wensen, aanwijzingen, vragen en kritiek van de cliënt met betrekking tot de ondersteuning."

Daaronder is een werkafspraak opgenomen over de omgang met cliëntgegevens waarbij de Wet gebruik Burgerservicenummer in de zorg (Wbsn-z) leidend is.[17]

Ook binnen deze samenwerkingsafspraken is de basishouding terug te vinden dat informatie die niet met inwoners gedeeld kan worden, geen aanvullende waarde heeft en niet wordt bewaard. Uitzonderingen zijn wanneer er een (sterk) vermoeden is van een onveilige kind-situatie, of van fraude. Momenteel is nog niet al het e-mailverkeer tussen de verschillende betrokken samenwerkingspartners beveiligd mogelijk. Voor werk- en inkomen gaat dit grotendeels via (onbeveiligde) e-mail.

[17] Handboek Maatwerkvoorzieningen alle leeftijden WMO 2015 en Jeugdwet, versie 11-05-2015, blz. 8

De informatie-uitwisseling in de zorgsector is grotendeels beschermd en het berichtenverkeer beveiligd. Zorgaanbieders leveren nu informatie aan via de VBO-module, daar kan 1 persoon in. Soms wordt via e-mail aanvullende gegevens opgevraagd.

Deze situaties is ontstaan doordat niet iedereen in de VBO-module kan en deze module eenrichtingsverkeer is. Medewerkers communiceren in dit geval de BSN-nummers van cliënten om aanvullende informatie aan te vragen. De informatie die hierop teruggekoppeld wordt, vindt wel plaats via de beveiligde VBO-module.

3.2.3 Samenwerking met gemeente Enschede

De samenwerking met de gemeente Enschede wordt door bestuur, management, uitvoering en ondersteuning hoog gewaardeerd. De gemeente Losser voelt genoeg autonomie in de samenwerking bij de voorbereiding en implementatie van de drie decentralisaties. Het beleid dat het college heeft vastgesteld is overeenkomstig het door gemeenten gezamenlijk opgestelde VNG-model. Ditzelfde model is in de gemeente Enschede gebruikt als basis. Voor de uitvoering van de maatregelen die de bedrijfvoeringssamenwerking betreffen is geen onderscheid. Voor de praktische organisatie van de uitvoering geeft Gemeente Losser aan gemeente Enschede aan wat ze wil, en Enschede geeft aan hoe ze dat kunnen organiseren. De uitkomsten hiervan worden door de gemeente Losser positief ontvangen. Medewerkers van de gemeente vinden dat ze goed worden geholpen.
Door de samenwerking met Enschede is de informatiebeveiliging verbeterd, mede ook door de mogelijkheid van verdere functiescheiding in toekennen en controle op autorisaties.

De gemeente Losser heeft ter bescherming van persoonsgegevens meerdere werk-voorschriften, procedures en protocollen opgesteld. Deze betreffen onderdelen van het gebruik (met name toegang tot) en is niet compleet voor alle processen rondom gegevensgebruik. Papieren dossiers worden bewaard volgens de regels van de archiefwet, digitale dossiers worden in principe oneindig bewaard.
Privacy in de gemeente Losser is geborgd in de materiewetten en in de systeemwetten van de gemeente.
De professionals in de gemeente Losser gaan deels onbewust bekwaam om met privacy. Leidinggevenden gaan bewust bekwaam om met privacy. Op hoger management-niveau wordt vertrouwd op de deskundigheid van de uitvoering door de professionals, de opbouw van en sturing vanuit de informatiesystemen en de daarbij behorende richtlijnen.
Door de afdeling financiën worden alleen niet geanonimiseerde facturen betaald. Hier bevindt zich ook privacygevoelige informatie.
Discussie ontstaat vooral door de drie decentralisaties wanneer signalering en preventie belangrijk zijn. De vorming van beleid hierin is gewenst. Door de uitvoering van de drie decentralisaties is hier nog geen tijd voor geweest, maar het bestuur is zich bewust van de behoefte hieraan.
Het kleinschalige karakter van de gemeente Losser maakt privacy van inwoners extra gevoelig. Bestuur, management en uitvoering zijn zich hier terdege van bewust.
Scholing, intervisie en evaluatie van privacybeleid en gestructureerde aandacht voor privacy in de uitvoering (zoals bij signalering en preventie) zijn nog niet structureel georganiseerd.
Momenteel is nog niet alle emailverkeer tussen de verschillende betrokken samenwerkingspartners beveiligd mogelijk.
De samenwerking met de gemeente Enschede wordt door bestuur, management, uitvoering en ondersteuning hoog gewaardeerd.

3.3 Controle en verantwoording

Het lijnmanagement is verantwoordelijk voor de sturing op informatieveiligheid en controle op naleving. Elke drie maanden tot half jaar worden er door het hoofd van de afdeling WIZ rapportages gemaakt op basis van de inloggegevens van SUWI-net inkijk. Onregelmatigheden hierin worden nauwelijks gevonden, uit de interviews komt naar voren dat leidinggevenden weten volgens protocollen te handelen bij eventuele onregelmatigheden, en daarbij de privacy gevoeligheid te respecteren. Eenmalig heeft de controle geleid tot een disciplinair gesprek met een medewerker van de gemeente.

De verantwoordelijkheid voor de 'interne' toetsing en control van de Informatiebeveiliging is belegd bij het IT Bedrijf Enschede. Voor de control-functie komt in verband met de functiescheiding een positie in de staf (van het 'IT-Bedrijf') in aanmerking.

Momenteel betreft dat de periodieke audits zoals de GBA-audit, de DigiD-audit en de SUWInet-audit. Beveiliging van informatie wordt steeds meer regionaal opgepakt, zoals vanuit Shared Service Netwerk Twente, ook om kleinere gemeenten te ontlasten.

3.4 Rol van de raad

De gemeenteraad heeft zich in de afgelopen jaren enkele malen beraadslaagd over de drie decentralisaties en over de bescherming van persoonsgegevens, maar niet met elkaar in verband staand. Over de decentralisaties heeft de raad zowel de beleidsnota's over de onderscheiden gebieden Participatiewet, Jeugdzorg en AWBZ behandeld als het visiedocument van de gemeente. In de raadsvergadering van 1 juli 2014 heeft de raad ten aanzien van de uitwerking van het visiedocument besloten:

1. De raad besluit om de visie sociaal domein gemeente Losser vast te stellen en de visie uit te laten werken in het uitvoeringsplan;
2. De raad besluit om het college te mandateren voor het maken en uitvoeren van het uitvoeringsplan[18].

Het SUWI plan[19] dat door het college is vastgesteld is ook niet in de raad behandeld. Dit sluit aan op de meer algemene gedachte dat de wijze waarop de uitvoering van gemeentelijke taken geregeld wordt een taak is die het college is toebedeeld.

Over de wijze waarop de gemeente handelt met persoonsgegevens heeft de raad in januari 2014 een verordening aangenomen: de Verordening basisregistratie personen gemeente Losser. Deze verordening betreft echter niet de gegevens uit de drie decentralisaties.

Er zijn geen afspraken gemaakt met de raad over de wijze waarop de raad wordt geïnformeerd over de resultaten van uitvoering van beheer, gebruik en uitwisseling van persoonsgegevens. De raad wordt hier niet periodiek in hoofdlijnen van op de hoogte gebracht.
Op andere terreinen die raakvlakken hebben met de privacy wordt de raad wel geïnformeerd. Als voorbeeld de raadsinformatiebrief van 9 september 2013 over de uitvoering van de aanbevelingen van het onderzoek van de Rekenkamercommissie naar uitvoering van de WMO.

[18] Raadsbesluit Visie sociaal domein, 1 juli 2014

[19] Vaststellingsbesluit SUWInet, 2008

De raad van de gemeente is op verschillende momenten en in verschillende dossiers betrokken bij beleid dat direct of indirect de bescherming van de privacy van de inwoners raakt. Het raakvlak is echter klein, de nadruk in de raadsbehandeling ligt op de inhoud van het beleid. Privacy als afzonderlijk thema is niet in de raad aan de orde geweest anders dan bij de verordening basisregistratie persoonsgegevens.
De diverse en verspreide informatie aan de raad heeft nog niet geleid tot een raadbesluit over de bescherming van de privacy van de inwoners van Losser in verband met de drie decentralisaties.

4 Conclusies en aanbevelingen

4.1 Conclusies

1. De rekenkamercommissie stelt vast dat de gemeente Losser bij de uitvoering van de drie decentralisaties voorrang heeft gegeven aan het doorgaan van de noodzakelijke ondersteuning van de inwoners boven het op orde brengen van het systeem.
2. De gemeente Losser heeft het 'hoe' geregeld, het 'wat' en het 'waarom' nog niet. De wijze waarop de gemeente persoonlijke gegevens beheert is grotendeels geregeld. De gemeente heeft nog geen beleidsmatige uitspraken gedaan (anders dan algemene uitspraken) waarom en met welke doelstellingen dit moet worden geregeld. Ook de grens tot waar en waarvoor de gemeente persoonlijke gegevens mag opvragen is niet beleidsmatig beantwoord. Er is sprake van ad hoc-beleid.
3. Voor de bescherming van de privacy gevoelige persoonsgegevens is adequaat uitvoeringsbeleid opgesteld voor zover het de beveiliging en borging daarvan betreft van de gegevens die worden opgeslagen in de gemeentelijke digitale bestanden. Hiervoor zijn verantwoordelijkheid, toegang, werkwijze en uitwisseling geregeld, alsmede het toezicht hierop.
4. De gemeente is voor de uitvoering van deze beveiliging gedeeltelijk afhankelijk van de werking van landelijke systemen en werkwijzen.
5. De werkwijze ten aanzien van privacygevoelige gegevens is bij intakegesprekken en onderlinge (schriftelijke) uitwisseling afhankelijk van de houding van de direct betrokken medewerkers van de gemeente. Deze zijn doordrongen van de bescherming van de persoonlijke levenssfeer van de inwoners, maar dit is niet geborgd in protocollen of werkbeschrijvingen.
6. Hetzelfde geldt ten aanzien van de niet direct betrokken medewerkers van de gemeente, bijvoorbeeld de financiële afdeling, de postafdeling of de balie, die privacygevoelige persoonsgegevens onder ogen krijgen. Ook hiervoor zijn geen protocollen en is de toegang tot gegevens niet geregeld met het oog op bescherming van de persoonlijke gegevens.
7. Met de raad zijn geen afspraken gemaakt over de wijze waarop hij geïnformeerd wordt over de resultaten van uitvoering van beheer, gebruik en uitwisseling van persoonsgegevens. De raad wordt hier niet periodiek in hoofdlijnen van op de hoogte gebracht.

4.2 Aanbevelingen

1. Stel een beleidsnota op met de grenzen waarvan de gemeente vindt dat zij de persoonlijke gegevens van inwoners nodig heeft voor de uitvoering van de drie decentralisaties en welke gegevens dus mogen worden gevraagd. Stel hierbij de hulpvraag centraal, niet de persoon. Binnen de samenwerking van de 14 Twentse gemeenten zijn hiervoor al richtinggevende ideeën aanwezig, ook landelijk wordt hierover nagedacht.
2. Ook de overheid en VNG zijn bezig met visie en beleidsvorming op dit domein. Het is niet noodzakelijk voor de troepen uit te lopen. Wellicht is het mogelijk en wenselijk de gemeente Losser als pilotproject bij VNG aan te dragen voor de vorming van nieuw landelijk beleid.
3. Zorg dat er richtlijnen komen over de bescherming van de privacy en privacygevoelige persoonlijke gegevens voor de uitvoering van de gesprekken die medewerkers van de gemeente voeren met (potentiële) cliënten.

4. Zorg dat er richtlijnen komen over de bescherming van de privacy en privacygevoelige persoonlijke gegevens bij de uitwisseling van gegevens, met name intern (extern zijn ze er wel).
5. Zorg dat er richtlijnen komen ter bescherming van de privacygevoelige gegevens voor de niet direct bij de uitvoering van de drie decentralisaties betrokken medewerkers.
6. Zorg daarbij dat privacy gevoelige gegevens bij niet meer mensen onder ogen komen als noodzakelijk.
7. Beperk het gebruik van (landelijke) systemen en werkwijzen die niet aan de beveiligingsgraad voldoen die de gemeente stelt. Zorg dat het verzenden van privacy-gevoelige gegevens volgens geldende richtlijnen verzonden worden, zowel per post als digitaal.
8. Zorg voor training en intervisie bij de medewerkers die met privacygevoelige gegevens werken.

Bijlage 1

Bestudeerde documenten

- Beleidsplan Participatiewet Losser
- Beleidsplan Wmo (1)
- Concept bestuurlijke reactie op escalatieprotocol
- Escalatieprotocol SUWInet
- Brief VNG escalatieprotocol SUWInet
- Memo privacy tbv gs
- Beleid BIG Gemeente Losser
- BMO-ICT - Proces - Change Management
- Procedure Autorisatie tot GBA systeem
- Account en wachtwoordbeleid en procedure
- Functies en rolbeschrijvingen beveiliging
- Informatiebeleid 2007 (Koenders en Bal)
- IT Bedrijf Totaal
- RE ICT rekenkamercommissie
- Voorlichtingsfolder rechten en plichten uitkering 2015
- antwoordbrief D66 14.0000604
- Autorisatie suwinet 2015 06 29
- B&W besluit beveiligingsplan Suwi
- Beveiligingsplan Suwinet 2008
- Losser april tm september 2014
- Mutatieformulier 2015
- werkinstructie UA bij melding uitkering
- WIZ Kwartaalrapport controle 1e kwartaal 2014
- WIZ Kwartaalrapport controle 2014 07 tm 09
- Inlichtingenformulier bijz bijst deel_1
- Inlichtingenformulier bijz bijst deel_2
- Aanvraagformulier uitkering Pwet deel 1
- Aanvraagformulier uitkering Pwet deel 2
- Aanvraagformulier loaw
- Aanvraagformulier koopkrachttegemoetkoming 2014
- aanvraagformulier Kortingsregeling 2015
- Aanvraagformulier bijzondere bijstand
- aanvraagformulier inkomenstoeslag 2015
- Overeenkomst Cannock Chase 2008
- Beleidsplan Participatiewet Losser v 2 oktober_S_14.0015082_3
- Proces afhandeling aanvraag levensonderhoud
- Proces intake aanvraag levensonderhoud
- Proces melding uitkering levensonderhoud
- Van Wet op de jeugdzorg naar de Jeugdwet
- Individueel taxivervoer 2015
- jeugdaanmeldingen via arts
- Procesbeschrijving huishoudelijke ondersteuning 2015
- Procesbeschrijving Aanmelding CJG
- procesbeschrijving jeugdzorg
- rapportage deel 1 en 2
- 150501 Contactformulier met aanvraagformulier
- 20150312 Mailing PGB TR_Bijlage Werkinstructie vervoer
- Aanmaken aanmelding Jeugdwet bij zorginstelling
- Dyslexiezorg
- HANDBOEK - LAATSTE VERSIE
- LOSSER Jaarrekening 2014 DEF
- Kadernota 2016-2019def
- LOSSER Programmabegroting 2015-2018
- visie sociaal domein
- 20150731_informatieveiligheid-en-intergemeentelijke
- raadsbesluit visie sociaal domein
- raadsvoorstel visie 4 juni 2014
- rs_2013_richtsnoeren-beveiliging-persoonsgegevens
- visie sociaal domein (1)

Bijlage 2

Interviews

Gemeentesecretaris:	J. van Dam
Portefeuillehouder Werk & Inkomen:	J. Hassink (decentralisatie participatiewet)
Portefeuillehouder Dienstverlening& Jeugd en Wmo: (inclusief decentralisatie AWBZ)	J. van Rees
Afdelingshoofd Werk, Inkomen en Zorg:	S. Hagen-Kroeze
Afdelingshoofd Welzijn/BSP:	I. Kamp-Kolner (interim)
Controller / regiefunctionaris samenwerking:	H. ten Voorde
IT Bedrijf:	H. Ellenbroek (contactpersoon)
Programmadirecteur dienstverlening / CIO:	C. Koman (Enschede)
Projectleider facturatie & declaratie jeugd en WMO	E. Braskamp

Groepsinterviews

Gemeentelijke medewerkers (beleid, uitvoering en/of vertegenwoordiging partners gemeente in uitvoering van decentralisaties):	E. Liefaard-Gerberink, K. Wassen, F. Beumers, D. Kanbar-Bos, P. Bosman, M. Perik

Bijlage 3

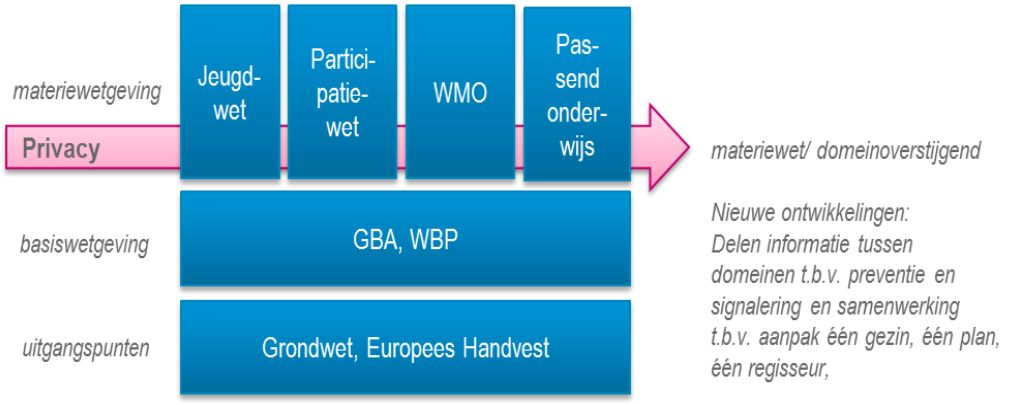
Gebruikte afkortingen

BAG:	Basisregistratie Adressen en Gebouwen
BIG:	Baseline Informatiebeveiliging Nederlandse Gemeenten
BRP:	Basis Registratie Persoonsgegevens
CBP:	College Bescherming Persoonsgegevens
CJG:	Centrum voor Jeugd en Gezin
CWI:	Centrum voor Werk en Inkomen
GBA:	Gemeentelijke Basis Administratie
SUWI:	Structuur Werk en Inkomen
UVW:	Uitvoeringsinstituut werknemersverzekeringen
VNG:	Vereniging Nederlandse Gemeenten
WMO:	Wet Maatschappelijke Ondersteuning

Bijlage 4

Drie decentralisaties en privacy: plan van aanpak

Gemeenten hebben de verantwoordelijkheid om goed en zorgvuldig om te gaan met persoonsgegevens van burgers. Er moet vertrouwen zijn voor inwoners, met name zij die dienstverlening of zorg krijgen, dat hun gegevens bij de gemeente in goede handen zijn, binnen de kaders van de wet.
In wet- en regelgeving is daar op verschillende niveaus vorm aan gegeven. In de uitvoeringspraktijk doen zich echter dagelijks nieuwe situaties voor waarin de generieke normen uit deze wet- en regelgeving vertaald moeten worden naar de specifieke en soms ook eigen lokale situatie.
Juist door de decentralisaties worden gegevens van burgers over verschillende domeinen heen met elkaar gedeeld. Om integrale dienstverlening te kunnen bieden (één gezin, één plan) is het noodzakelijk voor gemeenten informatie te delen, ook met partners in de uitvoeringspraktijk buiten de gemeente, zoals woningcorporaties, zorgaanbieders en zorgverzekeraars.
Dat roept vragen op bijvoorbeeld over het delen van gegevens tussen professionals in een wijkteam, en bijvoorbeeld de afhandeling van verleende zorg door zorgaanbieders door de (financiële) administratie.



In dit plan van aanpak[20] schetsen we hoe een gemeente systematisch aandacht kan geven aan het formuleren van een eigen privacybeleid en de manier waarop dat in de uitvoering kan worden vormgegeven. Het gaat niet alleen afspraken over het verkrijgen van informatie en met welk oogmerk, maar ook om het borgen van privacy in toegang en beheer van die informatie. Het is noodzakelijk hiervoor naast organisatie en 'governance' ook gestructureerde aandacht te besteden aan training en opleiding van betrokken professionals en medewerkers.
Het inzichtelijk maken aan inwoners van de manier waarop de gemeente met persoonsgegevens om gaat is belangrijk voor de betreffende inwoners, maar natuurlijk ook essentieel voor de gemeenteraad en de eerder genoemde professionals in de uitvoering.

[20] Voor dit plan van aanpak is gebruik gemaakt van het stappenplan privacybeleid van de Informatie Voorziening Sociaal Domein (VISD).

Voor deze laatste groep vormt het lokale privacybeleid het kader voor de omgang met persoonsgegevens.

Dit plan van aanpak biedt een methodische aanpak voor het formuleren van een gemeentelijk privacybeleid. Want generieke wet- en regelgeving volstaan niet voor de diversiteit van de alledaagse uitvoeringspraktijk, die sterk lokaal wordt ingekleurd.

1. **Formeer een team op gemeenteniveau met de juiste mensen: management, juridisch advies, uitvoering en bestuur**
   Beleid moet uitvoerbaar zijn. Het is daarom erg belangrijk om privacybeleid van het begin af aan op te zetten met voldoende juridische kennis aan tafel, maar ook met professionals die de uitvoeringspraktijk kennen. Samen met management en bij voorkeur bestuurders kan er privacy beleid worden opgesteld dat kan rekenen op draagvlak, inhoud en uitvoerbaarheid. Stel een proces op waarin betrokkenen aan bod komen, en er confrontatie van ideeën en opvattingen kan plaats vinden.
   Een overweging is nog dat privacy een belangrijk maatschappelijk vraagstuk is. Dat maakt het onderwerp ook geschikt om met de raad vooraf over de gemeentelijke eigenheid en daaruit voortkomende wensen en ideeën te spreken, en pas daarna het voorstel op te stellen.

2. **De basis is: de Wet bescherming persoonsgegevens (Wbp)**
   De WBP geeft het kader voor het goed en zorgvuldig omgaan met persoonsgegevens. Voor het sociaal domein zijn verder de verschillende materiewetten (Jeugdwet, WMO en Participatiewet) van belang. Voor de lokale kaders is het erg belangrijk te inventariseren met welke partners wordt samengewerkt, en welke wet- of regelgeving voor hen van belang is, en welk privacy beleid zij zelf mogelijk hebben opgesteld en hanteren. Tot slot is het van belang te checken welke gemeentelijke privacy beleidsregels er mogelijk in het verleden al zijn vastgelegd.

   Bouw voort op bestaande kennis. Die kan zijn vastgelegd in (samenwerkings-) convenanten, of specifiek geformuleerd op bijvoorbeeld informatiebeveiliging voor gehanteerde ICT-systemen.

3. **Maak gebruik van landelijke richtlijnen: er zijn al een paar wielen uitgevonden!**
   Het kabinet heeft een visie gepubliceerd ("Zorgvuldig en bewust: gegevensverwerking en privacy in een gedecentraliseerd sociaal domein”21). Deze visie is gebouwd op drie pijlers:
   1. De balans tussen noodzakelijke gegevensverwerking vanuit de maatschappelijke opgave in het sociaal domein en borging van de privacy.
   2. Versterking van de positie van de bewoner.
   3. Het versterken van de democratische verantwoording over gegevensverwerking en privacy op lokaal niveau.

In deze visie zijn belangrijke uitgangspunten geformuleerd waaraan het gemeentelijk privacy beleid moet voldoen.

[21] Ministerie van BZK in overleg met de ministeries van VWS, VenJ, SZW, OCW en de VNG.

4. Vertaal: van algemeen naar specifiek, van generiek naar lokaal

Hoe het lokale privacybeleid wordt ingevuld is afhankelijk van de manier waarop lokale beleidskeuzes voor het sociaal domein zijn gemaakt en hoe ze zijn vertaald in de lokale uitvoeringspraktijk. De gemeentelijke visie op de eigen maatschappelijke opgave is een tweede belangrijke uitgangspunt.

KING/VNG onderscheiden in het programma VNG- Informatievoorziening Sociaal Domein (VISD) een aantal 'archetypen' modellen voor de uitvoeringsorganisatie in het sociaal domein:

1. Transitieproof: De gemeente voldoet aan de transitie maar stelt het transformeren uit tot er meer duidelijkheid is over de kaders.
2. Totaal integraal: burgers hebben één toegang tot het sociaal domein. Veel gemeenten die dit archetype ambiëren, migreren hier geleidelijk naartoe.
3. Geclusterd integraal: integraal werken in verschillende clusters (bijvoorbeeld jeugd, werk- en financiën, zorg).
4. Integraal in tweede instantie: alleen integraal werken als daar aanleiding voor is, bij meervoudige vragen en multi-probleemsituaties.
5. Geclusterd integraal elders: gespecialiseerde partijen voeren taken uit in clusters.

Elk van de beschreven archetypen kennen eigen uitwerkingsvragen.

Neem in het lokale privacybeleid in elk geval de volgende punten op:

- **Visie:** De privacy van de burger in relatie tot de gemeentelijke maatschappelijke opgave in het sociaal domein. Welke gegevens heeft de gemeente echt nodig en waarvoor? Welke uitgangspunten worden lokaal gehanteerd? Welke keuzes worden gemaakt? Welke dilemma's zijn er?
- **Governance:** de verantwoording aan de Gemeenteraad, wijze van inrichting en controle op waarborgen privacy, bij voorkeur een functionaris gegevensverwerking als interne toezichthouder, de afspraken met derden (leveranciers/samenwerkingspartners/derden) inclusief de verantwoording door hen.
- **Organisatorische borging van de privacy:** autorisatie (specifiek), mandatering van taken, kennis en bewustwording van medewerkers, expertondersteuning over privacy voor medewerkers, sturing en monitoring (indicatoren), auditing.
- **Samenwerking en uitbesteding:** eisen die je aan samenwerkingspartners stelt om de privacy te borgen.
- **Werkprocessen:** omgang met gegevens (bij het verkrijgen, het verwerken, het delen), waarborgen voor de privacy, triagemomenten, vroegsignalering.
- **ICT-systemen en informatieveiligheid:** eisen die je vanuit privacy- en informatieveiligheidsperspectief moet stellen aan de gegevensverwerking, bewaren en vernietigen van gegevens.
- **Positie en rechten van de burger:** de rechten zoals het opvragen van de eigen gegevens, klachtenafhandeling en hoe je als gemeente met de burger wilt omgaan in relatie tot de privacy, de vraag hoe de burger hierover wordt geïnformeerd, een eventuele ombudsfunctie.

Belangrijk om te weten is dat voor de ICT-organisatie alle gemeenten gebruik kunnen maken van de producten en dienstverlening van de Informatie Beveiligings Dienst, zoals de Ondersteuningsaanpak voor het ICT-Beveiligingsassessment DigiD, de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en bijbehorende operationele producten ter ondersteuning van implementatie.

5. **Juridische toets**

   Voer een juridische toets uit om er zeker van te zijn dat dit strookt met de verschillende materiewetten en de Wbp, en de aansluiting op het mogelijk bestaande privacybeleid van de gemeente.

6. **Laat de gemeenteraad het privacy beleid vaststellen**

   Juist door de lokale uitwerking in de vormgeving van de decentralisaties is het belangrijk de raad een stem te geven in het vaststellen van het lokale privacybeleid. Deze stap is essentieel voor een transparant privacybeleid. Maak het beleid tot een cyclus: laat bijvoorbeeld het beleidskader elke vier jaar evalueren en stel het bij op basis van voortschrijdend inzicht en mogelijk jurisprudentie.

7. **Breng het beleid naar de praktijk**

   Wanneer het privacybeleid geformuleerd is geef er dan ook vervolgactie aan:
   - afspraken die er over privacy gemaakt worden met derden (bijvoorbeeld de ICT-leverancier, een ketenpartner);
   - communicatie over privacy richting de burger;
   - een gedragscode en werkinstructie of protocol over privacy voor de professionals in het sociaal domein.

Bijlage 5

Technisch wederhoor en verwerking rapport:

In de onderstaande tabel zijn de reacties, uit het technisch wederhoor op de nota van bevindingen "Privacybeleid in de 3 decentralisaties in de gemeente Losser", weergegeven.

Pag.	Tekst	Ambtelijke reactie	Verwerking in de nota van bevindingen
1.	'de gemeente heeft geen vastgesteld privacybeleid'	Dit klopt voor zover het een algemeen, overkoepelend, beleid betreft. Uiteraard, hebben we wel diverse protocollen en reglementen die privacy garanderen. Overigens biedt het hebben van ook dit dan nog op te stellen algemeen beleid en meer protocolleren mi geen “harde-garanties”. Wij zijn blij met de opmerking dat de ambtelijke organisatie vanuit de intrinsieke motivatie zich al vanzelfsprekend hieraan feitelijk al houdt en correct omgaat met privacygevoelige gegevens.	Geen.
3	“De raad wordt niet periodiek geïnformeerd over uitgevoerde controles.”	De raad wordt inderdaad niet geïnformeerd. De vraag is of dit een probleem is. In de huidige rapportages zijn de resultaten van de checks goed te herleiden naar medewerkers c.q. individuele gevallen/dossiers in Losser. Op dit detailniveau kan niet aan de raad worden gerapporteerd. Indien het verder geabstraheerd / geanonimiseerd moet worden blijft er niet veel informatiewaarde meer over voor de raad.	Geen.
14	“Inhoudelijk is 1 ambtenaar verantwoordelijk voor de controle van de facturen en accordering van betalingen.”	Dit is niet correct / voor meer interpretaties vatbaar. De correcte tekst luidt: Er is 1 ambtenaar verantwoordelijk voor controle leverantie van facturen. Een andere ambtenaar, zijnde de budgethouder, is verantwoordelijk voor de accordering van betalingen.	Tekst zal als zodanig worden aangepast.
14	“…… maar de gescheiden ingang in het gemeentehuis zou, gezien de schaalgrootte van Losser, tot precaire situaties voor inwoners kunnen leiden.”	Voor zover relevant is het juist andersom. De correcte tekst luidt: Het gemeentehuis heeft één centrale ingang. Naar het oordeel van het CJG kan dit in sommige gevallen voor bezoekers van het CJG een obstakel zijn. Zodra het CJG in het gemeentehuis wordt gehuisvest, wordt dit opgelost door, in situaties waarin dat wenselijk is, bezoekers bij de achteringang op te halen.	In het interview kwam naar voren dat het voor bewoners van Losser juist een obstakel kan zijn wanneer er een aparte ingang is voor het CJG. Voorstel tot aanpassing: De komst van het CJG naar de locatie van het gemeentehuis wordt vanwege samenwerking door medewerkers positief ervaren, maar de gescheiden ingang in het gemeentehuis zou, gezien de schaalgrootte van Losser, tot precaire situaties voor inwoners kunnen leiden. Het CJG speelt hierop in door bewoners van Losser de keuze te geven om zowel via de hoofdingang- als de achteringang van het gemeentehuis naar het CJG te gaan.

Pag.	Tekst		Ambtelijke reactie		Verwerking in de nota van bevindingen
15	"De samenwerking met de gemeente Enschede wordt door bestuur, management, uitvoering en ondersteuning zeer hoog gewaardeerd."		In deze zin moet het woord "zeer" worden weggelaten.		De tekst zal als zodanig worden aangepast.
Bijlage 1, blz.2	"BMO Control / regie"		moet zijn: Controller / regiefunctionaris samenwerking		Tekst zal worden aangepast.
Bijlage 1, blz.2	"Afdelingshoofd CIO Office"		moet zijn: Programmadirecteur dienstverlening / CIO		Tekst zal worden aangepast.
Bijlage 1, blz.2	"Vertegenwoordigers CJG: i.o.m. BSP"		Vertegenwoordigers CJG: Namen geïnterviewde medewerkers CJG noemen.		Tekst zal worden aangepast.
Bijlage 1, blz.2	"Vertegenwoordigers participatieraad en (beëdigde WMO-raad): is in oprichting, nog niet bekend"		weglaten of de Namen geïnterviewde personen vermelden		Tekst zal worden aangepast.
Bijlage 1, blz.2	"Vertegenwoordigers van partners van de gemeente in uitvoering van decentralisaties: Team Welzijn / P. Bosman; M. Bouman Afdeling WIZ / S. Hagen-Kroeze"		Is onjuist en onduidelijk. Genoemde zijn gemeentelijke medewerkers en geen partners van de gemeente. S.v.p. namen van geïnterviewde vertegenwoordigers vermelden of weglaten, indien P. Bosman en M. Bouman zijn geïnterviewd deze vermelden als zodanig vermelden als gemeentelijk medewerkers. S. Hagen-Kroeze is al eerder vermeld.		Tekst zal worden aangepast.
Bijlage 1, blz.2	Ambtelijk betrokkenen vanuit Enschede: Regiefunctionaris H. ten Voorde		geheel weglaten, is onjuist. en H. ten Voorde is al eerder vermeld.		Akkoord, weglaten.