

A. Privacy en informatiebeveiliging in het sociaal domein

Sinds 2015 is de gemeente verantwoordelijk voor taken in het sociaal domein. Deze taken zijn vastgelegd in de Wet maatschappelijke ondersteuning (Wmo), de Jeugdwet en de Participatiewet. De drie wetten bevatten verschillende eisen voor het opvragen en uitwisselen van persoonsgegevens.

Gemeenten dienen al het mogelijk te doen om de privacy van burgers te beschermen en de ingewonnen informatie beveiligen. Uit diverse onderzoeken blijkt, dat nog niet alle gemeenten zich hier voldoende van bewust zijn.

Normenkader ten aanzien van privacy is vaag

De persoonsbescherming in de nieuwe opzet van het sociaal domein staat onder stevige druk. Deze druk wordt onder meer veroorzaakt door het opereren van wijkteams en het uitgangspunt van eigen burgerkracht. Hulpverlening in de sfeer van jeugdzorg en Wmo wordt pas geboden als duidelijk is dat de hulpbehoevende (cliënt) niet kan terugvallen op de eigen omgeving (familie, burens, vrienden). In opdracht van de gemeente moet een consulent of een lid van een wijkteam de afwezigheid van eigen kracht vaststellen. Deze kan dat alleen als hij of zij informatie verzamelt over de burens, de kinderen, het vriendennetwerk, de financiële situatie, de huisvesting, de lichamelijke en psychische gesteldheid en de verstandelijke zelfredzaamheid van de betrokkene.

Consulenten en wijkteams beschikken nauwelijks een normenkader over welke vragen zij wel of niet mogen stellen en over hoe om te gaan met de informatie die ze inwinnen. Ze leveren maatwerk op basis van eigen inzicht. en criteria.

Medische privacy van burgers loopt gevaar

Gemeenten gebruiken privacygevoelige medische gegevens van burgers om te bepalen wie wel en wie niet in aanmerking komt voor zorg. Dit roept enkele vragen op. Gaan niet-medisch geschoolde ambtenaren wel voldoende accuraat om met gezondheidgegevens van burgers als ze moeten uitzoeken wat deze burgers nodig hebben? Gaan ze, als ze zorgaanvragen moeten beoordelen zonder eenduidige criteria, niet op de stoel van de behandelaar zitten en zich bemoeien met diagnoses of deze beoordelen? Soms vraagt degene die namens de gemeente optreedt om een schriftelijk 'bewijs' van wat de cliënt mankeert. Die denkt er niet over na of meent verplicht te zijn om die informatie te geven, omdat hij of zij anders geen of minder zorg ontvangt. Wat ook werkelijk gebeurt.

Volgens de Autoriteit Persoonsgegevens zijn gemeenten nauwelijks op de hoogte van wat ze wel of niet mogen opvragen en waar ze toestemming voor nodig hebben. Ook beseffen ze niet dat toestemming nog geen grondslag is om 'bijzondere persoonsgegevens' te verzamelen. Burgers zijn namelijk afhankelijk van zorg en kunnen niet in vrijheid toestemming geven.

Een gemeente heeft geen recht op bijzondere persoonsgegevens

Hoe gemeenten de medische privacy moeten handhaven, blijft in de wet vaag. Volgens de Wet maatschappelijke ondersteuning en de Jeugdwet mogen ambtenaren persoonsgegevens over de gezondheid verwerken voor zover deze 'noodzakelijk zijn' voor de uitvoering van hun taken. Dat schuurt met bestaande privacywetten, te weten de Wet Bescherming Persoonsgegevens en het Europees Verdrag voor de Rechten van de Mens. Die stellen dat gegevens over gezondheid 'bijzondere persoonsgegevens' zijn, net als die over seksuele geaardheid of politieke voorkeur. Volgens de Autoriteit Persoonsgegevens valt onder 'medische gegevens' alles waaruit iemands lichamelijke of geestelijke gezondheid blijkt. Dus ook of iemand bijvoorbeeld veel drinkt of bij een uroloog loopt. Veel gemeenten vinden medische informatie noodzakelijk voor hun werk en rekenen hun aantekeningen niet strikt tot medisch. Zo sluipen diagnoses, ziekteprocessen enzovoort de dossiers binnen.

Gemeenten hebben geen recht op inzage in of beschikking over medische dossiers. Ook hebben ze geen kennis in huis om een medische dossiers te beoordelen. Zo bestaan er alleen al van reuma meer dan honderd vormen, elk met specifieke gevolgen voor de patiënt. Welke ambtenaar of consulent

Te veel mensen kunnen medische informatie onder ogen krijgen

Behalve Wmo-consulenten kijken soms ook juridische medewerkers, telefonisten, medewerkers van administratie en klachtenteams mee in medische dossiers met gevoelige informatie. Soms is zelfs die informatie in te zien door ICT'ers en gemeentebestuurders.

Bij de WIA (Wet werk en inkomen naar arbeidsvermogen) en de UWV (Uitvoeringsinstituut Werknemersverzekeringen, een overheidsinstelling die belast is met de uitvoering van alle werknemersverzekeringen) is de

privacy strak geregeld: medewerkers noteren geen medische gegevens van werkzoekenden, zelfs niet als zij spontaan over hun gezondheidsomstandigheden vertellen.

Databeveiliging

Bij veel gemeenten staat de databeveiliging nog in de kinderschoenen: e-mails worden onversleuteld via onbeveiligde lijnen verstuurd of gaan cc. Voor correspondentie over gevoelige zaken hebben ze vaak een algemeen post- of e-mailadres van de gemeente beschikbaar. Wmo-medewerkers werken soms vanuit hun huis en gebruiken laptops en usb-sticks die verloren of gestolen kunnen raken.

Uit een steekproef bleek dat tot april 2016 slechts 6% van de gemeenten voldeed aan de verplichte beveiligingsstandaarden voor e-mail. Door het niet toepassen van de standaarden bleef het mogelijk om phishing e-mails te versturen vanuit en naar de gemeenten en zo argeloze ontvangers een bijlage of link met malware te bezorgen. Bovendien bleef het mogelijk om het gemeentelijk e-maildomein te gebruiken, waardoor iedereen zich kon voordoen als vertegenwoordiger van de gemeente. Ook de beveiligde gegevensuitwisseling was voor veel gemeenten een probleem, omdat er geen START-TLS-standaard (een cryptografische beveiliging van een internetverbinding) werd aangehouden.

Steeds meer gemeenten werken proberen momenteel internetbeveiliging op orde te krijgen en steeds meer gemeenten hebben die grotendeels of geheel op orde. Maar zelfs als gemeenten persoonsgegevens digitaal beveiligd wegzetten, is dit geen garantie tegen datalekken of hacken. Het sluit ook niet uit dat bestanden op enig moment door de gemeente of voor commerciële doeleinden kunnen worden gekoppeld .

Er valt in veel gemeenten nog heel wat te verbeteren

1. Bij werkoverleggen van allen die werkzaam zijn in het sociaal domein is privacybescherming en informatieveiligheid nog geen vast agendapunt.
2. Zorgverleners hebben verschillende visies op het delen van gegevens. Voor sommigen is nadrukkelijke toestemming van cliënten altijd nodig. Voor anderen geldt dat in bepaalde gevallen niet, of verschilt de wijze waarop toestemming wordt verkregen (bijvoorbeeld schriftelijk of mondeling).
3. De werkafspraken met betrekking tot privacy zijn onvoldoende bekend onder alle medewerkers.
4. Samenwerkende (zorg)partners missen een eenvoudig protocol waarop ze elkaar en de gemeente kunnen aanspreken.
5. Inwoners zijn onvoldoende op de hoogte van de wijze waarop de gemeente gegevens verzamelt en deelt. Op de gemeentelijke website staat niet wat de gemeente doet met de gegevens van inwoners.
6. Mensen met een beperking moeten een beroep op de gemeente kunnen doen. Het moet een gemeente niet uitmaken, waardoor een beperking wordt veroorzaakt. Bij twijfel kan een gemeente altijd een onafhankelijk arts vragen om een indicatie te bevestigen. Een medisch deskundige kan zijn of haar bevindingen vertalen naar een begrijpelijke conclusie voor de gemeente, zonder dat daar medische informatie bij wordt geleverd.
7. Er zijn geen vormen van controle bekend onder gecontracteerde zorgpartners (Formeel heeft de gemeente geen verantwoordelijkheid voor de manier waarom gecontracteerde zorgpartners met informatiebeveiliging en privacybescherming omgaan. Materieel blijft de gemeente aanspreekbaar op wat er met de gegevens van haar burgers gebeurt.
8. Binnen de ambtelijke organisatie is het bewustzijn op het gebied van privacy en informatieveiligheid nog geen gemeengoed.
9. Er vindt nog altijd onbeveiligd e-mailverkeer met persoonsgegevens plaats.
10. Veel raadsleden weten onvoldoende om te bepalen of de gemeente en de samenwerkende partijen de privacy en informatiebeveiliging op orde hebben. Het college van B&W biedt hen weinig of geen eenduidige en overzichtelijke informatie op dit punt. Raadsleden kunnen zo het college onvoldoende sturen en controleren op het thema privacy en informatiebeveiliging.

Gemeente is verantwoordelijk

Om haar taken goed uit te kunnen voeren, moet de gemeente overeenkomsten sluiten met zorgpartners. Dit brengt met zich mee dat gegevens moeten worden gedeeld. Als het goed is, is er binnen iedere gemeente een controlemechanisme dat er voor zorgt dat op de juiste wijze wordt omgegaan met privacygevoelige gegevens. Dit houdt in dat de gemeente

- a. met de zorgpartners afspraken maakt over het omgaan met privacygevoelige gegevens,
- b. de gemeenteraad informeert over de wijze waarop zorgpartners de privacy waarborgen.

Medewerkers moeten weten hoe ze dienen te handelen

Zij die in het sociaal domein werkzaam zijn, moeten duidelijk weten wat hun taken en bevoegdheden zijn. De afspraken die met hen gemaakt worden, moeten getoetst worden op werkbaarheid en risico's. Uit de werkprocessen moet op te maken zijn wanneer, door wie en om welke reden privacygevoelige informatie is geraadpleegd. Leidinggevendenden moeten periodiek aandacht besteden aan het bewustzijn van medewerkers in het sociaal domein met betrekking tot privacy en informatieveiligheid.

Basisprincipes bij het verzamelen en delen van persoonsgegevens

- a. Persoonsgegevens worden alleen verwerkt (verzameld, gedeeld) voor zover er een noodzaak toe bestaat.
- b. Persoonsgegevens worden alleen verzameld voor een van te voren bepaald, concreet omschreven doel. Nooit wordt meer verzameld dan strikt nodig is voor dat doel. Er wordt niet verzameld als er een manier voorhanden is om informatie te krijgen die minder inbreuk maakt op de privacy.
- c. Persoonsgegevens worden slechts verwerkt met toestemming van de betrokkene.
- d. Persoonsgegevens worden niet langer bewaard dan strikt noodzakelijk is.
- e. Onjuiste persoonsgegevens worden zo snel mogelijk gewist of gerectificeerd.
- f. Ieder die werkzaam is in het sociaal domein moet een medewerker bij het al dan niet verzamelen of delen van persoonsgegevens een afweging maken tussen belangen van zorg, veiligheid, privacy en bijvoorbeeld bedrijfsvoering. Belangrijk is dat iedere medewerker
 - (1) een goede basiskennis van de regelgeving heeft,
 - (2) houvast heeft bij het maken van afwegingen,
 - (3) gemaakte keuzes goed kan uitleggen en verantwoorden en
 - (4) afwegingen die een rol speelden bij het maken van een keuze later kan reproduceren om deze gezamenlijk te evalueren.
- g. De gemeente is open over het feit dat ze persoonsgegevens verwerkt en voor welke doeleinden. Ze informeert inwoners over hun rechten, zoals klachtrecht en inzagerecht. Ze is open over haar standpunt vanuit privacy-oogpunt over bepaalde (technologische) ontwikkelingen en over de afweging van belangen.
- h. De gemeente neemt passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
- i. De gemeente heeft een beleidsplan informatieveiligheid vastgesteld aan de hand van Baseline Informatiebeveiliging Gemeenten (BIG) en houdt zich hieraan. Het college van B&W is verantwoordelijk voor de waarborging van de privacy.
- j. Het college van B&W informeert de gemeenteraad periodiek over wezenlijke aspecten van het privacybeleid en incidenten van ernstige aard. Het college legt periodiek (tenminste een maal per jaar) verantwoording af aan de raad over de wijze waarop uitvoering is gegeven aan het privacybeleid, gehouden evaluaties en eventueel genomen maatregelen ter verbetering.

Grondhouding

Zonder een hoog privacybewustzijn bij allen die in het sociaal domein werkzaam zijn, blijft iedere privacymaatregel zonder werkelijk effect.

Bronnen

'Klik hier, alles kwijt', in: *Binnenlands Bestuur* 37 (22 april 2016), 30-32.

'Génant slechte beveiliging e-mail' in: *Binnenlands Bestuur* 37 (3 juni 2016) 16-18.

Jan Elzinga, 'Privacy-lek in sociaal domein', in: *Binnenlands Bestuur* 27(18 november 2016), 13

Rapport Rekenkamer Arnhem, Privacy en informatieveiligheid in het sociaal domein, 13 februari 2017.

Marieke Sjeerps, 'Onderzoek: Privacy in de zorg', in: *De Groene Amsterdammer*, 4 mei 2017, 22-25.

<https://vng.nl/onderwerpenindex/sociaal-domein/isd-informatievoorziening-sociaal-domein/privacybeleid-sociaal-domein>

<https://zoek.officielebekendmakingen.nl/gmb-2017-5553.html>

B. Privacybescherming en informatiebeveiliging in de gemeente Zevenaar

Stand van zaken

Om te weten hoe de privacybescherming en informatiebeveiliging ervoor staan in de gemeente Zevenaar, hebben wij (Peter van Schijndel en Leen den Besten) namens de Participatieraad Zevenaar het gemeentelijk apparaat de volgende vragen voorgelegd. Op 24 mei gaf dhr. Jules Lauwerier (Teamleider S&O/IBDIV)¹ hierop een mondelinge toelichting. Hier volgt een samenvatting.

1. *Is privacy en informatiebeveiliging een vast agendapunt bij werkoverleggen van de ambtenaren die werkzaam zijn in het sociaal domein?* ja/nee/weet niet

Toelichting:

Een vast agendapunt kan met zich meebrengen dat de zaak waarom het draait minder in plaats van meer aandacht krijgt. Privacybescherming en informatiebeveiliging komen regelmatig aan de orde in het managementteam. Lauwerier geeft gevraagd en ongevraagd advies. Leidinggevend zijn alert op zaken van privacybescherming en informatiebeveiliging.

2. *Hebben de ketenpartners van de gemeente Zevenaar een zelfde visie op het delen van gegevens?*

ja/nee/weet niet

Toelichting:

De verantwoordelijke ambtenaren hebben directe contacten op organisatieniveau. Zij proberen beleidsafspraken te maken. De ketenpartners zijn zich ervan bewust dat gegevens van een cliënt niet zonder dwingende noodzaak mogen worden gedeeld.

3. *Hebben de door de gemeente gecontracteerde zorg- en welzijnsorganisaties eenzelfde visie op het delen van gegevens?*

ja/nee/weet niet

Toelichting:

In contracten is de privacybescherming opgenomen. Er is direct contact tussen de accounthouders van de gemeente met gecontracteerde zorginstellingen waarin dit onderwerp aandacht heeft.

4. *Zijn werkafspraken met betrekking tot privacy bij eenieder binnen de gemeentelijke organisatie voldoende bekend?*

ja/nee/weet niet

Toelichting:

Periodiek zijn er privacysessies. Door de vele wisselingen van ambtenaren, is het noodzakelijk privacybescherming telkens opnieuw aan de orde te stellen. Medewerkers moeten van de Functionaris Gegevensbescherming toestemming krijgen om gegevens te mogen inzien en krijgen bij die gelegenheid meteen nog een-op-een-instructie/-advies.

5. *Hebben de door de gemeente gecontracteerde zorg- en welzijnsorganisatie c.q. haar ketenpartners een protocol waarop ze elkaar en de gemeente kunnen aanspreken?*

ja/nee/weet niet

Toelichting:

Er zijn afspraken tussen partners en het sociaal team en er zijn zakelijke contracten met vastgelegde werkafspraken, bv. dat gegevens van cliënten niet via internet worden verstuurd.

6. *Zijn de cliënten (sociaal domein) op de hoogte van de wijze waarop gegevens worden verzameld en gedeeld?*

ja/nee/weet niet

Toelichting:

Bij de intakegesprekken komt dit aan de orde. Degene die de intakegesprekken voert, heeft de volgende instructie:

I. Vraag je af of gegevensuitwisseling inzake de cliënt van evident belang is (a. er is een dringend gezondheidsbelang? b. bestaat de vrees voor ernstig nadeel? c. is er mogelijk sprake van ernstig overlast?)

II Denk aan subsidiariteit: als het anders kan, doe het dan ook.

III Denk aan proportionaliteit: alles met mate.

IV Leg vast of cliënt ondubbelzinnig toestemming geeft.

V. Motiveer en documenteer (zou je deze reden zelf accepteren van een ander?)

VI. Voldoe aan de rechten van de cliënt (a. informeer de cliënt over de gegevensdeling; b. de cliënt mag altijd zijn / haar dossier inzien; de cliënt mag om correctie of verwijdering vragen).

7. *Zijn er bij door de gemeente gecontracteerde zorg- en welzijnspartner c.q. haar ketenpartners vormen van controle t.a.v. privacy en informatiebeveiliging?*

ja/nee/weet niet

Toelichting:

Er is geen actieve controle. Tijdens de periodieke gesprekken met ketenpartners komt hoe om te gaan met vertrouwelijke gegevens regelmatig aan de orde.

¹ S&O = Speur- en Ontwikkelingswerk;

8. *Informeert de gemeente haar inwoners over hun rechten m.b.t. verzamelde persoonsgegevens?*

ja/nee/weet niet

Toelichting: De gemeente is hier niet erg actief in. Op de gemeentelijke website (zoekterm: privacy) informeert de gemeente haar inwoners. Ze stelt dat ze heel voorzichtig omgaat met persoonlijke gegevens en privacy en zich houdt aan de Wet Bescherming Persoonsgegevens. Dat betekent dat de gemeente nooit zomaar gegevens aan anderen geeft, behalve als dat nodig is om de gevraagde dienst uit te voeren en als het volgens de wet verplicht is.

De gemeente geeft persoonsgegevens door als de volgende instellingen erom vragen en er vooraf toestemming van betrokkene of een wettelijke basis is:

- instellingen die wettelijke taken uitvoeren, zoals Politie, Justitie, Belastingdienst, Waterschappen en Sociale Verzekeringsbank,
- notarissen, gerechtsdeurwaarders en advocaten die bezig zijn met een gerechtelijke procedure waarbij een inwoner betrokken is
- Centraal Bureau voor Genealogie
- afdeling Reclassering van het Leger des Heils
- ziekenhuizen die wetenschappelijk onderzoek doen
- pensioenfondsen, kredietinstellingen, effecteninstellingen, verzekeraars en beleggingsinstellingen, maar alleen als zij geld beheren dat zij aan betreffende inwoner moeten uitkeren.

Een inwoner die niet wil dat zijn / haar persoonsgegevens aan maatschappelijke instellingen worden doorgegeven, kan vragen om geheimhouding.

In het sociaal domein mag delen van gegevens alleen in de context van wat aan de orde is en alleen als het in het belang van de cliënt is. Als een cliënt geen toestemming geeft, mag gegevensuitwisseling slechts plaatsvinden a. ter voorkoming van strafbare feiten, b. in het belang van bescherming van de cliënt of c. in het belang van rechten en vrijheden van anderen.

9. *Vindt er (wel eens) onbeveiligd e-mailverkeer plaats door ambtenaren/medewerkers die werkzaam zijn in het sociaal domein?*

ja/nee/weet niet

Toelichting:

Er wordt op toegezien dat er geen onbeveiligd e-mailverkeer plaats vindt. Er is een technische oplossing om beveiligd te mailen met ketenpartners. Zowel medewerkers als cliënten en ketenpartners gebruiken echter de normale e-mail af en toe.

10. *Houdt de gemeente een START-TLS standaard aan?*

ja/nee/weet niet

Toelichting:

De gemeente Zevenaar gebruikt dit. De RID de Liemers verzorgt dit voor alle vier de Liemerse gemeenten en de RSD.

11. *Heeft de gemeente een beleidsplan informatieveiligheid?*

ja/nee/weet niet

Toelichting:

Liemers breed wordt samengewerkt om de informatie- en communicatietechnologie optimaal beveiligd te houden.

12. *Informeert het college van B&W de gemeenteraad periodiek over het privacybeleid?*

ja/nee/weet niet

Toelichting:

De verantwoordelijke beveiligers zoeken naar evenwicht tussen transparantie en beveiliging: het is ongewenst om teveel details over de wijze van beveiliging te geven. De beveiligers zijn blij met het kritisch meedenken door deskundigen vanuit de gemeenteraad.

13. *Legt het college minimaal een keer per jaar verantwoording af over het gevoerde privacybeleid?*

ja/nee/weet niet

Toelichting:

Dit is een van de voorwaarden van de BIG (Baseline Informatiebeveiliging Gemeenten). Het is opgenomen in de planning en controlecyclus (stukken van de begroting en jaarrekening).