Gemeente Groningen

Onderwerp: Beantwoording mondelinge vragen over privacy in het sociale domein

Steller: K.C.M. van Engelenhoven - Eijkelkamp

De leden van de raad van de gemeente Groningen
te
GRONINGEN

Telefoon (050) 367 76 40 Bijlage(n) 2 Ons kenmerk 5754539

Datum 07-07-2016 Uw brief van Uw kenmerk

Geachte heer, mevrouw,

Hierbij doen wij u toekomen onze antwoorden op de door mevrouw Paulusma (D66) tijdens de commissievergadering Onderwijs en Welzijn d.d. 11 mei jl. gestelde vragen over de bescherming van privacy in het sociale domein.

Er is gevraagd om een update van de openstaande punten uit onze brief van 4 november 2015 over dit onderwerp. In die brief is antwoord gegeven op een twintigtal vragen. In de raadscommissie is gevraagd om aandacht te besteden aan de volgende drie punten:

1. Wel of niet een privacyfunctionaris.
2. Ontwikkeling van de logische toegangsbeveiliging.
3. Betrokkenheid bewoners/betrekken bewoners door middel van een burgerdossier.

Uit de brief van 4 november jl. hebben wij voorts de volgende onderwerpen gedestilleerd die een update behoeven:

4. Intern auditschema (vraag 10).
5. Uitkomst onderzoek Autoriteit persoonsgegevens (vraag 11).
6. Kan de privacytoets uit Amsterdam een aanvulling zijn op onze vraag of we goed met privacy bezig zijn (vraag 12).
7. Stand van zaken bewustwordingscampagne (vraag 13).
8. Aangegeven dat de folder in ontwikkeling is (vraag 14).
9. Amsterdamse benadering/ zeggenschap burger over de informatie die over hem aanwezig is (vraag 16).
10. Online inzage geven (vraag 17).
11. Nader in te richten ondersteuningsstructuur (vraag 18 en ook vraag 20).

Hieronder treft u onze reactie aan op deze 11 punten. Ter inleiding daarop eerst het volgende:

Ons uitgangspunt is dat de burger in beginsel zelf eigenaar is van zijn persoonsgegevens en van zijn dossier. Vanuit dit oogpunt doen wij niets zonder toestemming/instemming van de burger. Wij betrekken de cliënt zoveel mogelijk bij de hulpverlening, omdat we

uitgaan van de eigen verantwoordelijkheid en regie van betrokkene. We hanteren bij de uitvoering van taken in het sociaal domein het transparantiebeginsel en informeren de cliënt over zijn rechten. Toestemming voor hulpverlening is een andere dan toestemming (als grondslag) voor de gegevensverwerking. Het feit dat betrokkene instemt met bijvoorbeeld een plan van aanpak voor de hulpverlening of zijn handtekening zet onder een aanvraagformulier zegt dus niet dat dat ook de grondslag is voor de bijbehorende verwerking van persoonsgegevens. Voor toestemming voor gegevensverwerking als grondslag voor rechtmatige verwerking dient er immers sprake te zijn van vrije, specifieke en op informatie berustende toestemming. Toestemming is echter niet de enige grondslag voor gegevensverwerking. Voor de verwerking van persoonsgegevens voor hulpverlening is er vaak een andere grondslag aanwezig, zoals nakoming van een wettelijke verplichting of uitvoering van een publiekrechtelijke taak.

Sinds de brief van 4 november jl.is op het terrein van privacybescherming veel gebeurd. Zo is in december 2015 de samenwerkingsovereenkomst tussen de gemeente Groningen en de samenwerkingspartners in de WIJteams getekend. Het geactualiseerde privacyprotocol voor de WIJteams en sociale teams maakt onderdeel uit van dat convenant. De folder "Uw privacy en bescherming van (persoons)gegevens" is gedrukt en wordt door de medewerkers uitgereikt aan de cliënt.

Er is een zelfscan gedaan met behulp van het door de VNG ontwikkelde instrument om gemeenten te ondersteunen bij het formuleren van privacy-acties voor het sociaal domein.

De zelfscan is een instrument om als gemeente in korte tijd zelf te kunnen beoordelen wat er al is geregeld in het kader van de privacy en indien nodig op welke manier de zorgvuldige omgang met persoonsgegevens van burgers in het sociaal domein kan worden verbeterd. Als uitgangspunt voor deze zelfscan is het Raamwerk Privacy genomen, dat door de VNG is opgesteld. De vijf onderdelen van dit raamwerk zijn: Governance, Beleid, Bewustwording en communicatie, Werkprocessen en triage en Beheer en opslag van gegevens. Op al deze terreinen moeten zaken worden ingericht om de privacy goed te borgen. Uit de zelfscan kan geconcludeerd worden dat er in de gemeente Groningen al veel is geregeld op het gebied van privacybescherming. Zo is er bij de inrichting van werkprocessen aandacht voor informatiebeveiliging/privacy. Er zijn echter nog wel ontwikkelpunten, zo kan meer aandacht besteed worden aan controle op de naleving van de wetten, regels en afspraken. De resultaten van de zelfscan hebben geleid tot een actieplan en prioritering.

Dit jaar is gestart met privacytrainingen voor de medewerkers in het sociaal domein. Bij alle WIJteams worden deze trainingen gegeven. De professionals worden daarin getraind over hoe zij met privacyvraagstukken om moeten gaan in hun functie en/of rol. Het is van belang dat zij zich bewust zijn van het privacybeleid en bijbehorende reglementen en dit kunnen vertalen naar de dagelijkse praktijk. In de trainingen wordt aandacht geschonken aan de wet- en regelgeving, het triage-instrument en er worden casussen behandeld. Vanzelfsprekend zijn dit anonieme casussen waarin geen persoonsgegevens gebruikt worden. De casussen zijn dus niet herleidbaar tot personen. Om er voor te zorgen dat medewerkers zich bewust blijven van het zorgvuldig omgaan met persoonsgegevens wordt met regelmaat een vervolgtraining gegeven. Ook wordt regelmatig geëvalueerd bijvoorbeeld door middel van intervisie en tijdens werkoverleg. Medewerkers kunnen

met vragen terecht bij de interim privacyfunctionaris, werkzaam bij juridische zaken. Najaar 2016 wordt een functionaris gegevensverwerking (FG) aangesteld.

Voorts hebben wij in kaart gebracht welke externe bewerkers (degenen die ten behoeve van de verantwoordelijke persoonsgegevens verwerken, zonder aan zijn rechtstreeks gezag te zijn onderworpen, zoals de leveranciers van applicaties) door ons worden ingeschakeld en hebben wij nagegaan of er in bewerkersovereenkomsten afspraken zijn gemaakt over de zorgvuldige omgang met persoonsgegevens. Wij hebben daarbij vooral aandacht besteed aan de eisen rondom privacy, datalekken en informatiebeveiliging. Waar nodig hebben wij nieuwe bewerkersovereenkomsten gesloten.

Momenteel wordt een externe audit uitgevoerd. Deze audit geeft inzicht in hoeverre de gemeente Groningen voldoet aan huidige en toekomstige privacy wet- en regelgeving en wat de gemeente nog zou moeten doen om hier op termijn volledig aan te voldoen. De eindrapportage van deze audit wordt in augustus opgeleverd. Aanbevelingen uit deze rapportage pakken wij natuurlijk zo snel mogelijk op.

Sinds 1 januari 2016 is de Wet meldplicht datalekken in werking getreden. Deze meldplicht houdt in dat organisaties, waaronder dus de gemeente, direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP), zodra zij een ernstig datalek hebben. Wij hebben een proces ingericht voor het melden van datalekken: het protocol meldplicht datalekken. Dit protocol is bekend gemaakt en via het Intranet van de gemeente Groningen en posters die op de locaties zijn opgehangen zijn de medewerkers op de hoogte gebracht van de acties die zij moeten nemen in geval van een datalek.

Onze reactie op de hierboven genoemde 11 punten is als volgt:

*1. Wel of niet een privacyfunctionaris.*

Momenteel is er een interim privacyfunctionaris bij de afdeling juridische zaken. Wij zien het belang van een structurele oplossing en benoemen daarom dit najaar nog een definitieve FG, die de regie voert op de borging van privacy in het sociaal domein, maar ook op de andere terreinen. Op 24 mei 2016 is de Algemene verordening gegevensbescherming (Avg) van het Europees parlement en de Raad van de Europese unie in werking getreden. Zij is van toepassing met ingang van 25 mei 2018. De Avg is voortaan de wet die de bescherming van persoonsgegevens regelt. Op grond van deze Europese privacyverordening, die rechtstreeks bindend is in alle lidstaten, moeten overheidsinstanties, dus ook de gemeente Groningen, een FG aanwijzen (artikel 37, lid 1 aanhef en onder a). De Avg geeft regels over de positie en taken van een dergelijke FG. Dus ook wettelijk is er een verplichting om een FG te benoemen.

*2. Ontwikkeling van de logische toegangsbeveiliging.*

Onze systemen zijn zo ingericht dat de gebruiker alleen toegang krijgt tot de persoonsgegevens die noodzakelijk zijn voor zijn specifieke rol en verantwoordelijkheid. We hebben een goedgekeurde autorisatiematrix (met functierollen en autorisaties). Daarnaast is er een geformaliseerd proces dat alleen een WIJ-manager nieuwe medewerkers autoriseert voor de toegang tot het WIZ-portaal.

Autorisaties moeten via een standaard proces worden uitgegeven (logische toegangsbeveiliging (LTB)), maar de LTB is nog onvoldoende ingeregeld. Inmiddels is een verbetertraject gestart om dit proces verder aan te scherpen. Voor de applicaties met geheime of vertrouwelijke informatie worden nu verbeterplannen opgesteld om het autorisatiebeheer op orde te krijgen.

Het opstellen en invoeren van het autorisatiemodel voor het WIZ- Portaal is reeds uitgevoerd. WIJ-medewerkers hebben autorisaties in WIZ- Portaal die afgestemd zijn op de gewenste handelingsvrijheid en er is een procedure voor het aanvragen en toekennen van autorisaties. Alle acties die een gebruiker uitvoert in het systeem worden gelogd aan de achterkant. Er wordt bijvoorbeeld gelogd op het raadplegen door gebruikers van registraties/voorzieningen die zijn ingelezen, het raadplegen van het plan, raadplegen van producten en raadplegen van productbestellingen.
Maandelijks worden er logbestanden gegenereerd en geanalyseerd. De opvallende loggings worden besproken. Daarnaast zijn de logbestanden een informatiebron voor de periodieke audits in het kader van privacy. De loggings en het autorisatiemodel gaan ook gebruikt worden om te toetsen of de autorisaties en rollen (nog) passend zijn bij de activiteiten die uitgevoerd worden door de medewerkers.

*3. Betrokkenheid bewoners/betrekken bewoners door middel van een burgerdossier.*

Op dit moment hebben we geen (technische) burgermodule ingericht in WIZ. Het onderdeel bestaat wel, maar wordt momenteel niet gebruikt. We willen hier in de vorm van een pilot wel mee gaan experimenteren. De randvoorwaarden zijn nog niet duidelijk (hoe en wanneer). In de overige systemen, zoals het systeem dat gebruikt wordt voor uitvoering van de Participatiewet, is een dergelijke module niet ingebouwd. Wel kan iedere burger natuurlijk gebruik maken van zijn recht tot inzage van zijn dossier.

Op dit moment is een digitaal burgerdossier, waarbij de burger online inzage heeft in zijn gegevens, nog niet haalbaar. Rond de zomer wordt de laatste hand gelegd aan geautomatiseerde koppeling tussen de WIZ- en de backofficesystemen van de gemeente m.b.t. bestellingen voor zorg in het kader van de WMO en Jeugdzorg. Dit is een opmaat naar zaakgericht werken. Burgers kunnen dan eenvoudig via een burgermodule (of mijnloket) de afhandeling van een aanvraag volgen. De bedoeling is om deze ontwikkeling begin 2017 vorm te gaan geven. Hiermee krijgen de burgers dan rechtstreeks inzage in hun dossier.

Omdat in de WIJteams gewerkt wordt volgens het transparantiebeginsel is de burger nu al uitdrukkelijk betrokken bij de aanpak van zijn hulpvraag, omdat zoveel mogelijk uit wordt gegaan van de eigen verantwoordelijkheid en regie van betrokkene. De professionals zijn open over het delen van informatie en het voeren van overleg.

Wat betreft de burgerbetrokkenheid kunnen we u ook nog het volgende meedelen. De gemeente is vanuit de Jeugdwet en vanuit de Wmo verplicht om vanaf 2016 jaarlijks een cliëntervaringsonderzoek uit te voeren. De enquêtes daarvoor zijn in mei jl. verzonden. De uitkomsten worden in het najaar verwacht.

*4. Intern auditschema (vraag 10)*

Er is een auditschema opgesteld voor logische toegangsbeveiliging/ autorisatiebeheer. Er zijn reeds diverse audits uitgevoerd. De uitkomsten zijn gedeeld met de verantwoordelijken en de aanbevelingen worden opgepakt.

*5. Uitkomst onderzoek Autoriteit persoonsgegevens (vraag 11).*

De AP onderkent in het rapport de complexiteit van de taak van gemeenten in het sociaal domein: zij moeten helderheid scheppen zonder verdere handreikingen van de wetgever en terwijl de praktijk zich nog aan het ontwikkelen is. De AP heeft daarom besloten geen onderzoeksrapport per gemeente te publiceren, maar een overkoepelend rapport op te stellen.

De AP geeft in het rapport aan dat gemeenten een overzicht nodig hebben van de doelen, grondslagen en persoonsgegevens in het sociaal domein. Dit overzicht is onder meer noodzakelijk om de taken in het sociaal domein te onderkennen die niet wettelijk zijn geregeld. Voor verwerking van persoonsgegevens bij deze taken kan toestemming namelijk de énige mogelijke grondslag zijn, maar alleen als deze toestemming voldoet aan de randvoorwaarden die de Wbp daaraan stelt. De AP gaat ervan uit dat gemeenten in 2016 alsnog het gespecificeerde overzicht opstellen van de doelen, grondslagen en persoonsgegevens in het sociaal domein. De AP verwacht bovendien dat gemeenten op basis van dit overzicht de professionals in het sociaal domein beter ondersteunen bij het conform de Wbp verwerken van persoonsgegevens én dat gemeenten hun inwoners beter informeren.

Er wordt in onze gemeente nu gewerkt aan het opstellen van dat overzicht. Het overzicht wordt opgesteld met WIJ-medewerkers waarin per doel (zoals entree, signalering, onderzoek, casemanagement en uitvoering) in kaart gebracht wordt welke persoonsgegevens vastgelegd worden, met welk doel en op basis van welke grondslag. Op deze manier wordt direct getoetst hoe in de praktijk omgegaan wordt met de bescherming van de persoonsgegevens van de bewoners en of dit aansluit bij wet- en regelgeving en protocollen. Daar waar geen aansluiting is wordt actie ondernomen en worden afspraken gemaakt gericht op correcte en zorgvuldige omgang met persoonsgegevens, welke ingevoerd (en geëvalueerd) worden in de praktijk.

*6. Kan de privacytoets uit Amsterdam een aanvulling zijn op onze vraag of we goed met privacy bezig zijn (vraag 12).*

De privacytoets m.b.t. jeugdprocessen die in Amsterdam is gedaan is in vier fasen uitgevoerd:

1. Nulmeting: een inventarisatie van de processen waarin (en hoe) persoonsgegevens worden verwerkt.
2. Herstelperiode: deels overlappend met fase 1, waarbij verbeteringen worden verwerkt.
3. Privacyschouw door externe partij.
4. Eindrapportage.

Het doel is om te kunnen vaststellen hoe privacy in de betreffende jeugdprocessen geregeld is. Uit navraag bij de gemeente Amsterdam blijkt dat de adviezen/constateringen vanuit verschillende bronnen in het afgelopen najaar en begin dit jaar opgeleverd zijn. Intussen is het rapport van de Privacyschouw wel intern opgeleverd, maar nog niet openbaar. De uitkomsten worden vertaald naar mogelijke concrete activiteiten. Dat wordt in zijn geheel opgenomen in het Jeugd Implementatie Plan (JIP), waarbij de belangrijkste ketenpartners betrokken worden. Dit implementatieplan ligt naar verwachting in juli 2016 in het college van Amsterdam. Daarbij wordt het rapport over de Privacyschouw ook een bijlage en daarmee openbaar. Wij gaan met Amsterdam ervaringen uitwisselen en afstemmen of we elkaar een hand kunnen toesteken in de uitvoering of de resultaten.

De Privacyschouw in Amsterdam is gedaan op het jeugddomein. De resultaten van het JIP-traject worden daar als input gebruikt voor vervolgstappen voor de rest van het sociaal domein. Uit de nulmeting in Amsterdam blijkt dat er zich daar geen grote tekortkomingen voordoen, maar dat er wel verbeterpunten zijn. Diezelfde bevindingen komen uit onze zelfscan, die op het gehele sociaal domein betrekking heeft, en verbeteringen in onze processen worden en zijn aangebracht. Ook in Groningen wordt binnenkort een privacy-audit door een externe partij gedaan.

Het actief aanreiken van informatie en het op begrijpelijke wijze transparant maken van de gegevensverwerking is een wezenlijk onderdeel van de Amsterdamse Privacyschouw. Veel van de adviezen uit de Privacyschouw zeggen hier wat over, maar het Amsterdamse college heeft daar nog geen formele positie over ingenomen. In de advisering komt vooralsnog naar voren enerzijds begrip voor de positie en rechten van burgers ten aanzien van het gebruik van hun gegevens. Anderzijds staat veiligheid van en hulp aan jeugdigen voorop. Meestal zijn de keuzes daardoor helder en is discussie daarover niet aan de orde. Een visie kan daarin wel als een richtingaanwijzer werken.

Ook in Groningen spelen deze aspecten een belangrijke rol. In onze WIJteams worden burgers met behulp van de folder die aan hen wordt uitgereikt actief geïnformeerd over hoe wij omgaan met hun persoonsgegevens. Transparantie is het uitgangspunt bij het omgaan met persoonsgegevens. Ook in de privacytrainingen aan de medewerkers van de WIJteams is daar veel aandacht voor. In de werkoverleggen en intervisiebijeenkomsten komen de complexiteit van de afwegingen en het transparantiebeginsel aan de orde. Indien cliënten of hun vertegenwoordigers vragen, klachten of zorgen over de bescherming van de persoonsgegevens uiten, gaan wij daar altijd serieus op in.

*7. Stand van zaken bewustwordingscampagne (vraag 13).*

In het Jaarplan I-beveiliging staat e.e.a. over de bewustwordingscampagne. Er is gecommuniceerd over het clean-deskbeleid en ook zijn de medewerkers geïnformeerd over de meldplicht datalekken. Er worden sessies met de leidinggevenden gepland, waarin zij worden meegenomen in het belang van informatiebeveiliging. Voorts worden speciale thema's, zoals werken in de trein, uitgewerkt en wordt er een checklist ontwikkeld. Door de privacytrainingen van de medewerkers van de WIJteams worden de medewerkers zich ook bewuster van het feit dat er risico's kleven aan de veelheid aan persoonsgegevens die zij verwerken en dat zij zorgvuldig met die gegevens om dienen te gaan.

*8. Aangegeven dat de folder in ontwikkeling is (vraag 14).*
Inmiddels is de folder in gebruik. In de folder is vermeld hoe wij met de (persoons)gegevens van de burgers omgaan. Aangegeven is hoe er wordt samengewerkt en dat er afspraken tussen de gemeente en de verschillende organisaties zijn gemaakt over het omgaan met privacygevoelige gegevens en dat een privacyprotocol geldt. De rechten van betrokkenen, zoals het inzage recht en het recht om een klacht in te dienen, zijn er ook in opgenomen. De folder treft u aan als bijlage.

*9. Amsterdamse benadering/ zeggenschap burger over de informatie die over hem aanwezig is (vraag 16).*

Uit informatie van de gemeente Amsterdam blijkt dat de feitelijke invoering van inzage e.d. nog vooral in de planning/ voornemens zit. Er is dus in Amsterdam vooralsnog hoofdzakelijk visievorming geweest. Op stedelijk niveau (Amsterdamse visie en kader van het beleid) is het formuleren daar nu gaande, met stuur- en werkgroepen. Dit traject wordt in de loop van dit jaar afgerond. In het JIP-traject (zie antwoord bij punt 6) wordt momenteel een klankbordgroep voorbereid, die in de uitvoering van de activiteiten meekijkt en commentaar geeft op wat in Amsterdam ontwikkeld en uitgevoerd wordt. In die klankbordgroep zijn jongeren en ouders dan zeker deelnemer.

Wij houden contact met Amsterdam en de wijze waarop zij hiermee omgaan. De deelname van burgers uit de doelgroep aan een klankbordgroep voor de verdere ontwikkeling en uitvoering spreekt ons zeer aan. Wij kijken hoe dit navolging kan krijgen in de Groningse situatie. Eigenaarschap, zeggenschap en betrokkenheid van burgers bij hun eigen dossier is, zoals hiervoor ook al genoemd, voor ons in ieder geval uitgangspunt.

*10. Online inzage geven (vraag 17).*
Zie het antwoord bij punt 3.

Wij gaan er van uit hiermee uw vragen voldoende te hebben beantwoord.

Met vriendelijke groet,
burgemeester en wethouders van Groningen,

de burgemeester,
Peter den Oudsten

de secretaris,
Peter Teesink

## NIET TEVREDEN?

Bent u niet tevreden over de manier waarop wij met uw gegevens omgaan? Bespreek dit dan met de medewerker die uw vraag behandelt. Komt u er samen niet uit? Neem dan contact op met de klachtenfunctionaris van de gemeente. Schrijf kort op waarover u niet tevreden bent en waarom. Stuur dit naar:
Klachtenfunctionaris Sociaal Domein
Postbus 400
9700 AK Groningen.

## BEWAREN

We bewaren uw gegevens niet langer dan nodig is. Hoe lang dat is, verschilt per situatie. Meestal bewaren we gegevens tot dat u weer (zelfstandig) verder kunt.

## MEER INFORMATIE OVER PRIVACY

Meer informatie over privacy en uw rechten staat op de website van de Autoriteit Persoonsgegevens:
**autoriteitpersoonsgegevens.nl**

## CONTACT

Met uw vragen over het WIJ-team of over privacy kunt u altijd terecht bij het WIJ-team.
De contactgegevens van het WIJ-team bij u in de buurt vindt u op: **wij.groningen.nl/wij-in-de-wijk**

# UW PRIVACY EN BESCHERMING VAN (PERSOONS)GEGEVENS

**WIJ GRONINGEN**
**ONDERSTEUNING EN ZORG**

**MET ELKAAR VOOR ELKAAR**

BIJLAGE

## UW PRIVACY EN BESCHERMING VAN (PERSOONS)GEGEVENS

In deze folder leest u hoe wij met uw (persoons) gegevens omgaan.

Voor uw privacy, houden we bij de WIJ-teams de volgende regels aan :

- We gebruiken alleen (persoons)gegevens die te maken hebben met uw vraag. Deze gegevens zijn echt nodig om uw vraag te beantwoorden.;
- We vertellen duidelijk wat we met uw vraag doen: alles gebeurt in overleg.

### WAT GEBEURT ER MET UW GEGEVENS?

Om u zo goed mogelijk te helpen en uw vraag te beantwoorden, hebben wij gegevens van u nodig. Uw gegevens komen in de computer. Onze medewerker bespreekt met u welke gegevens dat zijn.

### TOESTEMMING

Soms is het nodig of beter om uw vraag te laten beantwoorden door iemand die niet bij het team hoort. Dan vragen we uw toestemming voor het doorgeven van de gegevens. Dat doen we ook als we informatie moeten opvragen bij een andere organisatie. U mag uw toestemming voor het gebruiken van uw gegevens op elk moment weer intrekken. Maar dat kan betekenen dat het moeilijker wordt om u te helpen. Zeker als het gaat om noodzakelijke gegevens.
Alleen als het echt niet anders kan, gebruiken we gegevens zonder dit eerst met u te bespreken. Bijvoorbeeld bij levensgevaar.

### GEGEVENS BEKIJKEN

Alleen de mensen die aan uw vraag werken, mogen uw gegevens zien. Wie dat zijn, hangt van de vraag af. De medewerker die met uw vraag aan de slag gaat, kan al uw gegevens zien. Dit is nodig omdat deze medewerker uw situatie moet beoordelen. Hij of zij beslist of er nog iemand anders naar uw vraag moet kijken. Bijvoorbeeld iemand die meer weet van de zorg die u misschien nodig heeft. Deze medewerker mag dan alleen de gegevens bekijken die hij of zij moet weten om te kunnen helpen.

### GEMEENTE GRONINGEN

De gemeente Groningen neemt uw vraag op in de administratie en zorgt dat u geholpen wordt. De gemeente krijgt daarvoor alleen de gegevens die daarvoor noodzakelijk zijn. Het gaat hierbij niet om vertrouwelijke informatie over u.

### COMPUTER

Om goede hulp te kunnen geven, verwerken de medewerkers alle informatie in een goed beveiligd computersysteem. In de computer houden ze bij hoe het met u, uw kind of uw gezin gaat. Alleen de mensen waar u hulp van krijgt, mogen deze gegevens bekijken. Ook zij mogen niet alle gegevens bekijken. Ze zien alleen de gegevens die nodig zijn voor de hulp die zij geven. We kijken ook regelmatig of de computer nog wel goed beveiligd is.

### AFSPRAKEN

Het is erg belangrijk dat de medewerkers netjes met uw gegevens omgaan. Daarom hebben de gemeente en de verschillende organisaties die in het team werken afspraken gemaakt. Ook gebruiken de medewerkers een privacyprotocol. Dat is een lijst van afspraken waaraan de medewerkers van het WIJ-team zich moeten houden bij uw gegevens. De gemeente heeft deze lijst gemaakt.

### WIL U WETEN WELKE GEGEVENS WIJ VAN U HEBBEN?

Vraag dit dan aan de medewerker van het WIJ-team. Bij kinderen onder de 16 jaar, kunnen de ouders of hun wettelijke vertegenwoordiger hierom vragen. Ben je 16 jaar of ouder? Dan mogen jouw ouders of jouw wettelijke vertegenwoordigers alleen weten welke gegevens wij hebben als je hier zelf toestemming voor geeft.

### FOUT

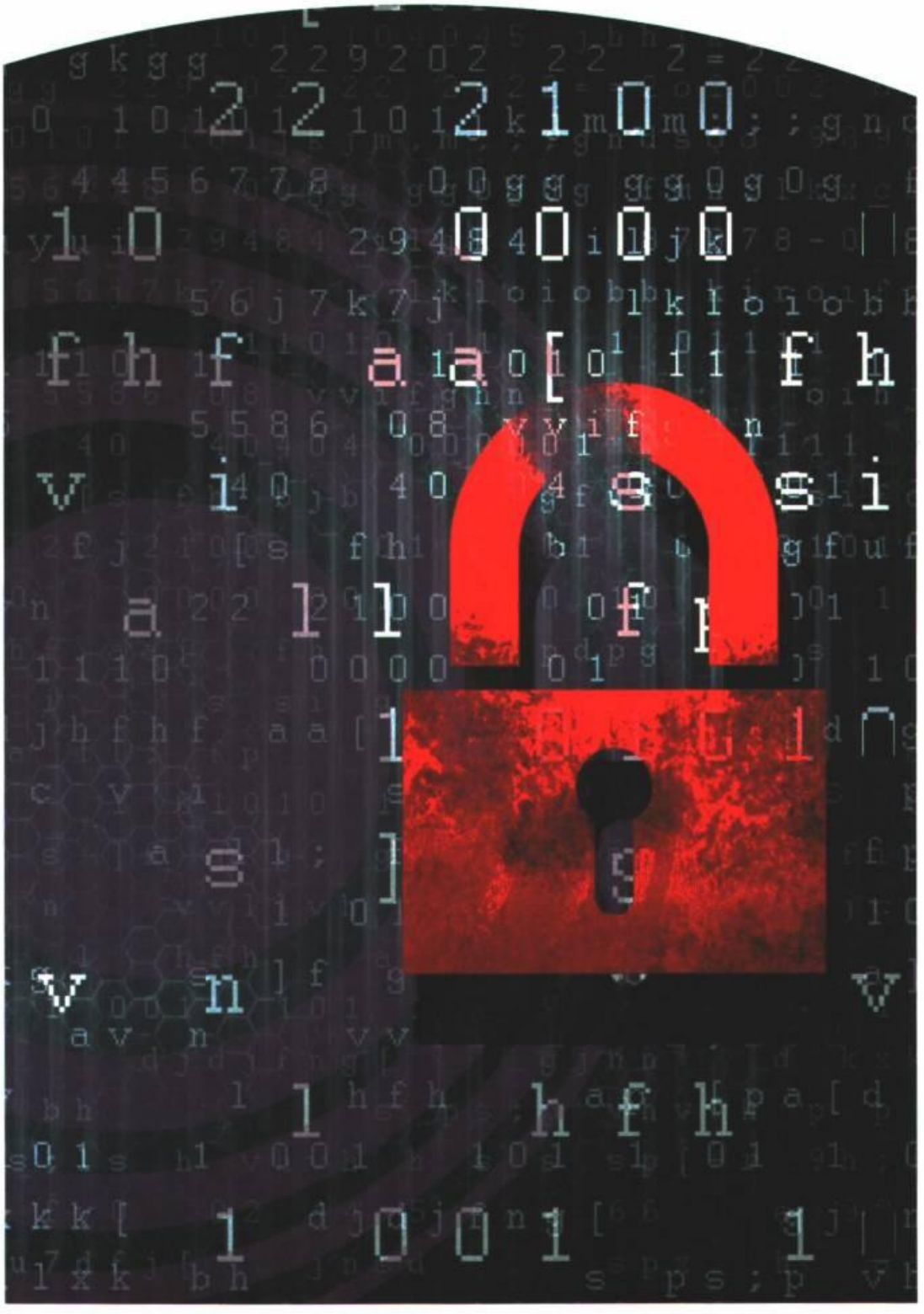
Denkt u dat er een fout in uw gegevens staat? Of ontbreekt er volgens u iets? Laat dit het WIJ-team dan weten. Doe dit ook als wij gegevens hebben die volgens u niets met de vraag te maken hebben. Vraag de medewerker van het WIJ-team dan om de gegevens te verbeteren, aan te vullen of te verwijderen.

BIJLAGE

VNG

Vereniging van
Nederlandse Gemeenten

# Zelfscan privacy sociaal domein



**Colofon**

Dit instrument is tot stand gekomen in nauwe samenwerking met de Gemeente Zaanstad

**Opmaak**

Chris Koning (VNG)

december 2015

# Inhoudsopgave

# Achtergrond en toepassing instrument

- Dit instrument is ontwikkeld om gemeenten te ondersteunen bij het formuleren van privacy-acties voor het sociaal domein
- Het betreft een instrument om als gemeente in korte tijd zelf te kunnen beoordelen wat er al is ingeregeld in het kader van de privacy en indien nodig op welke manier de zorgvuldige omgang met persoonsgegevens van burgers in het sociaal domein kan worden verbeterd (NB. Het betreft geen officiële audit of Privacy Impact Assessment (PIA))
- Als uitgangspunt is het Raamwerk Privacy genomen, dat door de VNG is opgesteld. De vijf onderdelen van dit raamwerk zijn: Governance, Beleid, Bewustwording en communicatie, Werkprocessen en triage en Beheer en opslag van gegevens. Uit de praktijk blijkt dat op al deze terreinen zaken moeten worden ingericht om de privacy goed te borgen.
- Noteer naast elke vraag van de scan uw antwoord, een toelichting op uw antwoord en uw eigen acties. Per vraag wordt aangegeven wat de gemeente op dit gebied zou moeten inrichten vanuit wettelijke vereisten of op basis van best practices in het land.
- Bepaal met de betrokkenen in de gemeente de prioriteiten en stel een actieplan op

# Beleid

| | Vraag | Ja/ nee | Toelichting bij antwoord | Aanbevolen acties | Eigen acties |
|---|---|---|---|---|---|
| 1 | Is er een algemeen privacybeleid in uw gemeente aanwezig? | Ja | Collegebesluit 24 mei 2011 Privacybeleid en bijbehorend Privacyprotocol | Veel gemeenten kiezen er voor om een gemeentebreed privacybeleid op te stellen. Hierin worden de gemeentebrede uitgangspunten beschreven op het gebied van de zorgvuldige omgang met persoonsgegevens. Houd dit beleid actueel, en controleer of er nieuwe vereisten zijn vanuit wet- en regelgeving. De Europese Privacyverordening (verwacht in 2016) stelt strengere privacyvereisten. Pas hier uw beleid tijdig op aan. | Zowel beleid als protocol kunnen geactualiseerd worden. |
| 2 | Is er specifiek voor de situatie in het sociaal domein een privacybeleid opgesteld voor uw gemeente (gebaseerd op de inhoudelijke beleidskeuzes die er gemaakt zijn)? | Ja | In grote lijnen in Beleidsplan VSD 2014/2015 en in Uitvoeringsplan VSD 2014/2015 en uitgewerkt in Samenwerkingsconvenant WIJteams en sociale teams en bijbehorend privacyprotocol<br>Daarnaast worden gegevens in de backoffice uitgewisseld met zorgaanbieders, woningbouwverenigingen, deurwaarders, huisartsen, andere gemeenten etc. De beleidsuitgangspunten zijn daarbij niet altijd gedeeld. | Het is aan te bevelen voor de situatie in het sociaal domein een aantal aparte beleidsuitgangspunten te formuleren. In dit beleid beschrijft u de kaders waarbinnen gegevensverwerking plaatsvindt, waarbij u de inhoudelijke beleidskeuzes beschrijft (bijv. mate van integraal werken, taken en werkzaamheden gemeente) in relatie tot de relevante (nieuwe) wettelijke kaders. Maak hierbij eventueel gebruik van bestaand privacybeleid binnen uw gemeente en betrek juridische zaken en de betrokken 3D-beleidsdirecties hierbij. Het formuleren van beleidsuitgangspunten kan helpen bij het opstellen van een handreiking voor de professional en in de communicatie naar de burger. | Folder voor de burger beschikbaar<br><br>Nagaan of met de derden waarmee vanuit de backoffice gegevens worden uitgewisseld de beleidsuitgangspunten zijn gedeeld; evt. bewerkersovereenkomsten mee afsluiten. |
| 3 | Zijn de beleidsuitgangspunten privacy gedeeld met externe partijenuitbesteed aan wie taken worden, bij wie u zorg inkoopt of met wie u samenwerkt? | Ja | Staan in convenant | Draag zorg dat de privacybeleidsuitgangspunten van de gemeente worden gedeeld met alle externe partijen aan wie taken worden uitbesteed, bij wie u zorg inkoopt of met wie u samenwerkt. Op die manier is voor alle partijen (inclusief voor de burger) duidelijk op welke manier met persoonsgegevens wordt omgegaan. | |

# Governance: interne afspraken

| | Vraag | Ja/ nee | Toelichting bij antwoord | Aanbevolen acties | Eigen acties |
|---|---|---|---|---|---|
| 1 | Is er binnen uw gemeente iemand aangewezen die expliciet verantwoordelijk is voor het borgen van de privacy van burgers bij de verwerking van persoonsgegevens in het sociaal domein? | Interim | Coördinatie is interim belegd bij juridische zaken. Daarnaast zijn er een concernfunctionaris informatiebeveiliging en een ICT security officer.<br><br>Structureel nog niet belegd. | Het is aan te raden om iemand te benoemen die de regie voert op de borging van privacy in het sociaal domein. Dit zou een Functionaris voor de gegevensbescherming (FG) kunnen zijn, maar dit is niet verplicht. In de praktijk wordt deze rol op verschillende wijzen ingericht. Soms wordt de taak belegd bij informatievoorziening (informatiebeveiliging) soms bij juridische zaken en in sommige gevallen bij een medewerker kwaliteit. Het is in ieder geval van belang dat deze medewerker de ontwikkeling, implementatie en operationele uitvoering overziet van het privacybeleid binnen de gemeente. Wanneer men officieel een FG aanstelt dan heeft deze een aparte juridische status binnen de gemeente en een officiële toezichthoudende taak. (zie handreiking Governance van de VNG voor meer informatie) | Regisseur, coördinator, concernbrede security officer (informele FG) of Functionaris voor de Gegevensbescherming aanwijzen (formele FG) |
| 2 | Is duidelijk wie waarvoor verantwoordelijk is/zijn in de organisatie m.b.t. de verwerking van persoonsgegevens? (zoals wie adviseert, controleert en rapporteert over de verwerking en op welk niveau (binnen het team, directie en/of (deel) gemeente?) | Ja | Is een lijntaak, maar vanuit I&A adviseren/regisseren de domeinfunctionaris I-beveiliging, de concernfunctionaris I-beveiliging en de ICT-security officer. Jaarplannen zijn aanwezig. Protocol melden datalekken is in ontwikkeling. Classificatie van gegevensbronnen heeft plaatsgevonden, inclusief eigenaarschap. | Zorg dat leidinggevenden op de hoogte zijn van hun verantwoordelijkheid m.b.t. de verwerking van persoonsgegevens. Zij moeten op de hoogte zijn van: wat persoonsgegevens zijn, welke persoonsgegevens hun afdeling of team verwerkt, wat zij moeten doen indien er zich incidenten voordoen m.b.t. persoonsgegevens (datalekken of klachten e.d.), wat hun eigen verantwoordelijkheid is ten aanzien van het creëren van bewustzijn en trainen van de eigen medewerkers. | |

| | Vraag | Ja/ nee | Toelichting bij antwoord | Aanbevolen acties | Eigen acties |
|---|---|---|---|---|---|
| 3 | Heeft u afspraken gemaakt met het College en de Raad over de wijze van verantwoording over het privacybeleid? (zowel dat van de gemeente zelf als van partijen aan wie taken in het sociaal domein zijn uitbesteed) | Ja | In het Privacybeleid staat dat er jaarlijks een audit is op dit terrein, maar er is geen duidelijke planning. | Het College moet aan de Raad verantwoording af kunnen leggen over de zorgvuldige omgang met persoonsgegevens van burgers. Maak daarom afspraken (met het College van B&W en de Gemeenteraad) over de wijze van verantwoording. Van belang is dat de politieke discussie over het belang van privacy gescheiden wordt van de vraag of de privacy wettelijk is geborgd. | Helder auditprogramma opstellen. |
| 4 | Beschikken medewerkers waar nodig over een Verklaring Omtrent Gedrag (VOG)? | Ja | Ambtenaren leggen de eed af. Voordat men met werkzaamheden mag/kan beginnen dient er een VOG te zijn. Dit geldt ook voor medewerkers in samenwerkingsverbanden zoals WIJteams.<br><br>De VOG wordt niet regelmatig geactualiseerd.<br><br>Uit recente audits blijkt dat binnen het sociale domein de VOG's een aandachtspunt zijn. Beleid lijkt onduidelijk m.b.t. externen. Externen hebben wel een verklaring van geheimhouding getekend.<br><br>De VOG is opgenomen als eis in het informatiebeveiligingsbeleid. | Breng in kaart welke medewerkers over een Verklaring Omtrent Gedrag (VOG) moeten beschikken. Volgens de Jeugdwet moet elke hoofdbehandelaar een geldige VOG hebben. Vrijgevestigde jeugdhulpaanbieders moeten een VOG overleggen aan de gemeente met wie zij een contract sluiten. Dit is een VOG voor natuurlijke personen. In de verwervingsprocedure aan jeugdhulpaanbieders kunnen gemeenten de eis stellen dat zij voor de medewerkers die zorg verlenen een VOG overleggen. Het is dus van belang om na te gaan welke interne medewerkers een VOG nodig hebben, maar ook jeugdhulpverleners van instellingen waar inkoopafspraken mee zijn gemaakt. | Vanuit I-beveiliging (en suwi) wordt een bewustwordingscampagne opgestart. |
| 5 | Controleert u of het privacybeleid van uw gemeente in de praktijk wordt uitgevoerd en stuurt u daarop? (Denk aan audits, PIA's op systemen etc.) | De els | Kan geïntensiveerd worden. | Het is aan te bevelen om uzelf en samenwerkingspartners periodiek te controleren of het privacybeleid in de praktijk wordt uitgevoerd. Dit kan door middel van audits, maar ook door middel van intervisie onder professionals. Besteed extra aandacht aan organisaties aan wie gemeentelijke taken worden uitbesteed. De gemeente blijft dan namelijk verantwoordelijk. Een Privacy Impact Assessment (PIA) kan vooraf worden uitgevoerd bij het opstellen van nieuwe werkprocessen en inrichten van systemen. | Controleplan opstellen en uitvoeren. Op het gebied van informatiebeveiliging vinden diverse audits plaats onder regie van de concernfunctionaris informatiebeveiliging (CFIB). Denk aan mystery-guestronde, audits op autorisatiebeheer en op het thema bedrijfscontinuïteit. |
| 6 | Heeft u juridische ondersteuning binnen uw organisatie voor privacyvraagstukken en de uitwerking van wet- en regelgeving naar een passend privacybeleid? | Ja | Bij SSC juridische zaken is een kennisteam privacy. | Zorg dat bekend is wie binnen de afdeling Juridische Zaken verantwoordelijk is voor privacyvraagstukken en dat medewerkers hier met privacyvragen terecht kunnen, betrek diegene bij de privacyvraagstukken in het sociaal domein en bij de vertaling van wet- en regelgeving naar een passend privacybeleid. | |

# Governance: externe afspraken

| | Vraag | Ja/ nee | Toelichting bij antwoord | Aanbevolen acties | Eigen acties |
|---|---|---|---|---|---|
| 1 | Heeft u met alle gemeentelijke afdelingen en/ of organisaties die gemeentelijke taken uitvoeren afspraken gemaakt om de privacy van burgers te borgen? (in contracten, opdrachtverlening, bevoegdheidsverlening) | Ja, goed deels | In het convenant en er is een begin gemaakt met het afsluiten van bewerkersovereenkomsten. | Breng in kaart aan wie de gemeente taken uitbesteedt in het sociaal domein. Ga per organisatie na of afspraken zijn gemaakt over de zorgvuldige omgang met persoonsgegevens. Bepaal welke convenanten of andere overeenkomsten moeten worden aangepast en met welke partijen nog afspraken moeten worden gemaakt over de zorgvuldige omgang met persoonsgegevens in het kader van samenwerking in sociaal domein. (zie VNG-document Governance voor meer informatie en specifieke aandachtspunten) | |
| 2 | Heeft u wanneer u bewerkers inschakelt (bijv. ICT-leveranciers) privacy-afspraken gemaakt? (Bewerker: de bewerker verwerkt gegevens ten behoeve van de verantwoordelijke, dat wil zeggen overeenkomstig diens instructies en onder diens verantwoordelijkheid. De bewerker heeft geen zeggenschap over het doel van en de middelen voor de verwerking van persoonsgegevens. Hij neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens enz.) | Ja | Bewerkersovereenkomsten; deze zijn er niet altijd. | Breng in kaart welke bewerkers worden ingeschakeld en ga na of er in bewerkersovereenkomsten afspraken zijn gemaakt over de zorgvuldige omgang met persoonsgegevens. Bepaal welke bewerkersovereenkomsten nog moeten worden aangepast. Er dient in ieder geval aandacht te worden besteed aan: verantwoordelijkheid persoonsgegevens,<br>afspraken over eventuele goedkeuring van onderaannemers,<br>Incidentenmanagement, teruggave of vernietiging gegevens door de bewerker en subbewerkers, beveiliging systemen, autorisaties, wanneer aan de samenwerking een einde komt, bepalingen over toezicht door de gemeente, eventueel ingrijpen wanneer de bewerker en/of subbewerker zich niet aan de afspraken houdt en aansprakelijkheid. | Nagaan waar bewerkersovereenkomsten ontbreken en deze alsnog sluiten. Zijn de afdeling Inkoop en de afdeling Contractbeheer van I&A mee bezig. Er is met name aandacht voor de eisen rondom privacy, datalekken en informatiebeveiliging. |

| | Vraag | Ja/ nee | Toelichting bij antwoord | Aanbevolen acties | Eigen acties |
|---|---|---|---|---|---|
| 3 | Zijn er afspraken gemaakt bij het inkopen van zorg over privacy, bijvoorbeeld bij het opstellen van inkoopcontracten? | Ja | Maakt onderdeel uit van bestek (de bewerkersovereenkomsten maken er deel van uit) | Doe aantoonbaar navraag naar de privacybeleidsvoering bij partijen bij wie u zorg inkoopt. In bestekteksten of inkoopcontracten kan naar een zorgvuldige omgang met persoonsgegevens verwezen worden. Maak afspraken over:<br>• De uitwisseling (of beperking daarvan) van gegevens in de back office/ factureringsproces<br>• De eventuele samenwerking op casus niveau bij complexe problematiek | |
| 4 | Zijn er afspraken gemaakt met partijen met wie wordt samengewerkt als het gaat om melden van signalen (bijvoorbeeld met onderwijsinstellingen, huisartsen, politie, justitie, woningbouwvereniging) en rondom multiproblematiek? | Ja | WIJteams: met convenantpartners<br><br>Veilig Thuis: privacyreglement<br><br>Schuldhulpverlening: afspraken met woningbouwverenigingen e.d. | Maak met de belangrijkste 'vindplaatsen' (onderwijsinstellingen, woningbouwcorporaties, energiebedrijven, huisarts, wijkverpleging, politie) afspraken over gegevensuitwisseling bij signalen of meldingen aan Jeugd/Wijk/WMO teams. Leg in een convenant vast hoe gegevensuitwisseling plaatsvindt met partijen met wie wordt samengewerkt rondom multiproblematiek. (zie VNG-document Governance voor meer informatie en specifieke aandachtspunten) | |

# Bewustwording en communicatie

| | Vraag | Ja/ nee | Toelichting bij antwoord | Aanbevolen acties | Eigen acties |
|---|---|---|---|---|---|
| 1 | Is er binnen de gemeente een gedragscode voor medewerkers waarin het belang van privacy wordt beschreven en aan welke regels en reglementen uw medewerkers in het sociaal domein (bijvoorbeeld in het sociaal wijkteam en klantcontactcentrum) zich dienen te houden? | Ja | Privacyprotocol (gemeentelijk protocol uit 2011) en privacyprotocol WIJteams | Ga na of er binnen uw gemeente een gedragscode is geïmplementeerd waarin aandacht is voor de manier waarop uw medewerkers om dienen te gaan met de persoonsgegevens van burgers. Medewerkers dienen zich te committeren aan deze gedragscode. Vaak gebeurt dat door middel van een ondertekening bij indiensttreding. Ga na of de gedragscode ook geldig is voor de nieuwe situatie in het sociaal domein. Het is aan te raden om een specifieke handreiking privacy voor professionals op te stellen. (zie VNG document Opstellen handreiking voor de professional) | |
| 2 | Worden de professionals (die gemeentelijke taken uitvoeren in sociaal domein) getraind als het gaat om privacy bewustwording en het maken van een zorgvuldige rondom het verwerken van persoonsgegevens? | Ja | Zie jaarplan I-beveiliging (onderdeel is bewustwordingscampagne). Voor training van medewerkers WIJteams wordt een opleidingsplan ontwikkeld. In april en mei 2016 krijgen alle 11 teams scholing over het omgaan met persoonsgegevens. | Train professionals in het sociaal domein regelmatig over hoe zij met privacyvraagstukken om moeten gaan in hun functie en/of rol. Het is van belang dat zij zich bewust zijn van uw privacybeleid en bijbehorende reglementen en dit kunnen vertalen naar de dagelijkse praktijk. Evalueer ook regelmatig bijvoorbeeld door middel van intervisie en tijdens werkoverleg. Zorg ook dat professionals zich bewust zijn van de taken die bij een bepaalde rol horen en zich bewust zijn van het eventueel ophebben van 'verschillende petten'. | Zorgen voor structurele inbedding<br>Verder uitwerken opleidingsplan |
| 3 | Wordt de burger actief geïnformeerd over het privacybeleid: inzage, bezwaar- en beroepprocedures en manier waarop met persoonsgegevens wordt omgegaan via website en andere kanalen? | Ja | Beleid en protocol staan op internet en er is een folder die in de WIJteams wordt uitgereikt | Zorg ervoor dat er actief en op een transparante manier richting de burger gecommuniceerd wordt over het privacybeleid van de gemeente. Burgers dienen op de hoogte te zijn van hun rechten omtrent de verwerking van hun persoonsgegevens, zoals o.a. inzagerecht, recht op correctie en recht op verzet. Communiceer hoe zij aanspraak kunnen maken op dit recht door middel van uw inzage-, bezwaar- en beroepprocedures. | |

| | Vraag | Ja/ nee | Toelichting bij antwoord | Aanbevolen acties | Eigen acties |
|---|---|---|---|---|---|
| 4 | Werkt u in het sociaal domein vanuit het transparantiebeginsel? | Ja | Transparantie is een uitgangspunt; dat is ook genoemd in het Beleidsplan VSD 2014/2015 en in het Samenwerkingsconvenant voor de WIJteams | Transparantie naar de burger is een belangrijk uitgangspunt bij het verwerken van persoonsgegevens. Dit betekent dat de gemeente de burger altijd informeert (mondeling tijdens een gesprek, via een folder en via de website) over welke gegevens worden verwerkt en waarom, tenzij de situatie dat om zwaarwegende redenen (tijdelijk) niet toelaat (onder gegevensverwerking wordt ook het delen van gegevens verstaan dus communiceer ook naar de burger met wie er eventueel gegevens worden gedeeld en waarom) | |
| 5 | Is er sprake van toetsing/ evaluatie door leidinggevenden of de Functionaris Gegevensbescherming? | Deels | Kan worden geïntensiveerd, sommige managers doen het anderen niet. Wij hebben geen FG ingesteld. | Het is van belang dat leidinggevenden zich bewust zijn van hun verantwoordelijkheid m.b.t. de zorgvuldige omgang met persoonsgegevens. Het is aan te bevelen dat zij hierover regelmatig het gesprek voeren met professionals. | Leidinggevenden hierover informeren. Onderzoek naar instelling FG verder prioriteren. |

# Werkprocessen en triage

| | Vraag | Ja/ nee | Toelichting bij antwoord | Aanbevolen acties | Eigen acties |
|---|---|---|---|---|---|
| 1 | Heeft u in het werkproces momenten ingebouwd waarop professionals zich nadrukkelijk afvragen of de verwerking van persoonsgegevens noodzakelijk en proportioneel is en aan de eisen van subsidiariteit voldoet? Op de momenten dat er een afweging gemaakt wordt over de routering of aanpak van de vraag is vaak impilciet ook de vraag welke gegevens daar voor nodig zijn bijvoorbeeld bij de routering van een casus waardoor gegevensverwerking plaatsvindt? En legt de professional deze afweging ook vast? | Ja | Systeemtechnisch is dat in geen enkel systeem ingebouwd. Betreft een procesafspraak, wel is het mogelijk dit in de workflow (mits aanwezig, bijv. in de suites) in te bouwen. | Benoem met medewerkers in het sociaal domein die de werkprocessen opstellen of in de praktijk uitvoeren deze specifieke privacymomenten, breng in kaart welke functies op deze momenten de afweging maken en zorg er voor dat medewerkers periodiek getraind worden als het gaat om privacy en gegevensverwerking in sociaal domein. Professionals moeten deze afweging namelijk steeds bewust maken en vastleggen.<br><br>(zie handreiking VNG: Triagekader en instrument) | Onderdeel laten uitmaken van opleiding/training medewerkers. |
| 2 | Heeft u na het benoemen van bovengenoemde momenten in het werkproces een informatieanalyse uitgevoerd om inzichtelijk te maken wie op welke momenten gegevens delen en inzien: Om wat voor gegevens gaat het? Waar komen ze vandaan? Waarom is het nodig de informatie te delen? | Ja | In het verlengde van doelbinding zijn autorisatiematrices gemaakt. Een matrix is afgestemd met de uitvoering en vertaald naar de inrichting van systemen. Logging maakt het mogelijk om controles uit te voeren. Dat laatste gebeurt te weinig. | Het is aan te bevelen een informatieanalyse uit te voeren op het werkproces. Betrek medewerkers uit de praktijk en laat een juridisch adviseur per processtap beoordelen of de gewenste deling van gegevens binnen de wettelijke kaders mogelijk is en op basis van welke grondslag de gegevensverwerking plaatsvindt. Zie handreiking VNG: opstellen informatieanalyse | Plan maken over controles op loggegevens. |

| | Vraag | Ja/ nee | Toelichting bij antwoord | Aanbevolen acties | Eigen acties |
|---|---|---|---|---|---|
| 3 | Heeft u processen ingericht zodat de burger zijn rechten ten aanzien van de verwerking van zijn eigen persoonsgegevens kan uitoefenen, zoals bezwaar en beroep en inzage? | Deels | Staat op website en in informatiefolder Privacy, die in WIJteams wordt uitgedeeld. Er is echter geen proces aanwezig, waarmee we direct vragen van burgers kunnen beantwoorden. Er is geen zicht op de systemen waarin de persoonsgegevens van een burger allemaal zijn geregistreerd. | Gemeenten moeten een formeel en laagdrempelig proces inrichten waaruit duidelijk blijkt tot welke instantie de burger zich moet richten om zijn rechten uit te kunnen oefenen: de gemeente of een instantie aan wie bepaalde taken zijn uitbesteed. Het is bij een eenvoudig verzoek van de burger om informatie over welke gegevens van hem/ haar worden verwerkt niet altijd nodig om de formele weg te kiezen. De burger kan altijd informeel (bijv. tijdens een keukentafelgesprek) aan de betreffende hulpverlener vragen welke gegevens van hem/ haar worden verwerkt. | |
| 4 | Sluiten de autorisaties aan op de werkprocessen (zie ook beheer en opslag gegevens)? | Ja | Is geregeld, alleen de controles moeten ingebed worden. | Alleen medewerkers die een taak hebben in het werkproces moeten bij persoonsgegevens in de systemen kunnen. Bepaal welke autorisaties bij welke functie horen. Zorg dat het verstrekken (of accorderen) van nieuwe autorisaties belegd is bij een inhoudelijk leidinggevende in het sociaal domein | Plan maken om te controleren op loggegevens en op de autorisaties in de systemen door functioneel beheer. Plan maken voor audit op proces door de afdeling PI&A. Er loopt een traject SIEM (security incident and event monitoring). Hierbij worden logs automatisch geanalyseerd. |

# Beheer en opslag gegevens

| | Vraag | Ja/ nee | Toelichting bij antwoord | Aanbevolen acties | Eigen acties |
|---|---|---|---|---|---|
| 1 | Heeft u een overzicht van de systemen waarin persoonsgegevens worden verwerkt binnen het sociaal domein? | Ja | Is aanwezig, classificatie is gebeurd. | Zorg voor een overzicht van de systemen waarin persoonsgegevens worden verwerkt binnen het sociaal domein. Is dat er niet, zorg er voor dat een dergelijk overzicht wordt opgesteld. | |
| 2 | Bent u op de hoogte van de bewaartermijnen van de persoonsgegevens die u heeft opgeslagen? | Ja | Bij DIV en ICT | Inventariseer wat de bewaartermijnen zijn van de persoonsgegevens die u heeft opgeslagen en draag zorg voor de vernietiging, anonimisering of archivering van de gegevens als de bewaartermijn verstreken is, al naar gelang het wettelijke vereiste (dossierplicht). | |
| 3 | Zijn uw systemen zo ingericht dat de gebruiker alleen toegang krijgt tot de persoonsgegevens die noodzakelijk zijn voor zijn specifieke rol en verantwoordelijkheid (autorisatie)? | De els | Autorisaties via LTB (logische toegangsbeveiliging), maar de LTB is nog onvoldoende ingeregeld. | Zorg ervoor dat de gebruikers alleen toegang hebben tot de persoonsgegevens die voor hen noodzakelijk zijn om hun rol en activiteiten uit te kunnen voeren. De beschrijvingen van de werkprocessen waarin persoonsgegevens worden verwerkt gelden als uitgangspunt voor de toewijzing van deze autorisaties. Zorg dat deze altijd actueel en correct zijn. | Verder inrichten LTB. |
| 4 | Wordt aan de vereisten voldaan van de Baseline Informatiebeveiliging Gemeenten (BIG)? | De els | De BIG is wel als beleidskader vastgesteld, maar de eisen moeten nog verder worden geïmplementeerd. | In de Baseline Informatiebeveiliging Gemeenten (BIG) is een basisniveau beschreven waaraan de informatiebeveiliging bij gemeenten moet voldoen. Alle gemeenten in Nederland moeten in kaart brengen op welke onderwerpen de informatiebeveiliging in het sociaal domein nog niet aan de BIG voldoet en hier acties op ondernemen. | Verdere implementatie BIG-eisen. |

| | Vraag | Ja/ nee | Toelichting bij antwoord | Aanbevolen acties | Eigen acties |
|---|---|---|---|---|---|
| 5 | Is er een Incident Management en Responsbeleid? | Ja | Er is een incidentmeldingen-proces. De medewerker kan de ICT-help-desk bellen en daar worden incidenten vastgelegd. Bij ernstige incidenten kan het proces 'ernstige verstoringen' worden opgestart. Maandelijks worden de gemelde incidenten aan de CFIB gerapporteerd. De CFIB analyseert of er een trend te herkennen is en doet evt. aanvullende verbetervoorstellen. | Incident Management en Responsebeleid op het gebied van informatiebeveiliging omvatten de monitoring en detectie van beveiligingsincidenten (security events) op een computer of computernetwerk, maar ook het waarnemen van verdachte activiteiten (niet integer handelen) door het personeel, en de uitvoering van de juiste antwoorden op deze gebeurtenissen. De belangrijkste te verwachten incidenten kunnen van te voren bedacht worden en de bijpassende reactie en escalatie procedure kan dus ook van te voren uitgewerkt en geoefend worden. | |
| 6 | Is er sprake van logging en worden de loggegevens regelmatig gereviewd? | Deels | Niet elk systeem logt de transacties of de juiste gegevens. | Om beveiligingsincidenten te kunnen detecteren en analyseren is het toepassen van logging en monitoring aan te bevelen. De logging is van belang bij het analyseren van incidenten; als de detectie pas in een laat stadium plaatsvindt kan met behulp van de logging worden achterhaald welke gebeurtenissen eraan vooraf gingen. | |
| 7 | Is de fysieke beveiliging (kasten op slot etc) gewaarborgd? | Deels | Kan beter, maakt wel onderdeel uit van bewustwordingscampagne. Voorts hebben we toegangspoortjes op een deel van de locaties,zonering, bemande recepties, clean-deskbeleid etc. Het gedrag van medewerkers kan strakker op dit punt. | Besteed aandacht aan de fysieke beveiliging. Doel van de fysieke beveiliging is het voorkomen van ongeautoriseerde toegang om schade aan ICT-voorzieningen in gebouwen en schade aan of verstoring van informatie te voorkomen. Onder fysieke toegang tot informatie wordt ook gerekend het meelezen van beeldschermen en het kunnen kennisnemen van niet voor de lezer bedoelde informatie op papier. Medewerkers moeten gestimuleerd worden om er een "clean desk" en "clean screen" op na te houden als elementaire maatregelen ter bescherming van informatie. | Medewerkers informeren Controleplan opstellen en uitvoeren. |
| 8 | Heeft u een proces ingericht voor het melden van datalekken? | Ja | Via ICT-servicedesk. | Richt een proces in voor het melden van datalekken aan het College bescherming persoonsgegevens CBP). Op 1 januari 2016 gaat de Meldplicht Datalekken in. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij het CBP zodra zij een ernstig datalek hebben. | |

# Checklist documenten

Onderstaande lijst geeft een overzicht van aanbevolen documenten die op basis van de aanbevelingen opgesteld kunnen worden:

- Beleidsuitgangspunten privacy sociaal domein
- Privacybeleid gemeente (gemeentebreed)
- Bewerkersovereenkomsten
- Contracten met samenwerkingspartners/ organisaties aan wie gemeentelijke taken worden uitbesteed en met wie wordt samengewerkt op casusniveau
- Gedragscode professional
- Toestemmingsverklaring (alleen nodig voor het vragen van specifieke toestemming)
- Informatiemateriaal inwoners
- Informatieanalyse op werkprocessen
- Werkprocessen met daarin triagemomenten benoemd
- Geheimhoudingsverklaringen
- Privacyconvenant
- Informatiebeveiligingsplan

# Handreikingen VNG

## Governance

- **Inrichting van de governance rondom privacy in het sociaal domein**
  Dit document geeft gemeenten informatie en handvatten voor het inrichten van de governance als het gaat om het borgen van privacy in het sociale domein. Het helpt gemeenten om rollen, verantwoordelijkheden en taken vast te leggen en borgt een goede en zorgvuldige verwerking van persoonsgegevens.
- **Aandachtspunten privacy voor bestekteksten over uitbesteding van taken in het sociaal domein**
  Wanneer gemeenten taken in het sociaal domein uitbesteden aan een andere organisatie, moeten bestekteksten en/of programma's van eisen daar op de juiste manier invulling aan geven. Een gemeente blijft altijd verantwoordelijk voor het correct borgen van de privacy van haar burgers. Dit document noemt een aantal aandachtspunten dat hierbij van belang is.

## Beleid

- **Stappenplan: hoe stel ik mijn privacybeleid voor het sociaal domein op?**
  Aan de hand van zes stappen wordt gewerkt naar een door de gemeenteraad vastgesteld privacybeleid. Het vormt de basis voor de uitwerking van de overige aandachtsgebieden van het privacy raamwerk.
- **Handreiking verantwoording privacy aan gemeenteraad**
  Het College van B&W is verantwoordelijk voor de zorgvuldigheid van de gegevensverwerking die door of namens de gemeente plaatsvindt. Het College is daarmee verantwoording verschuldigd aan de gemeenteraad over de wijze waarop hieraan invulling wordt gegeven. Dit document biedt een handreiking voor het inrichten van dit verantwoordingsproces.

## Werkpocessen en triage

- **Factsheet Triage**
  Triage is het proces van verhelderen, routeren en escaleren van vragen en casussen. Triage is erop gericht om op een gestructureerde en gestandaardiseerde manier de mate van samenhang tussen deze zaken vast te stellen. De factsheet licht het belang van triage toe en de verschillende momenten van afweging in het sociaal domein.
- **Triagekader en instrument**
  Het triagekader geeft een toelichting op het begrip triage en beschrijft op welke wijze triage een rol speelt bij de borging van privacy. Het beschrijft drie triagemomenten en bijbehorende aandachtspunten voor de inrichting. Ook bevat het document een instrument dat professionals kunnen inzetten op de triagemomenten. Het triagekader sluit af met een praktijkvoorbeeld van de gemeente Leeuwarden.
- **Informatieanalyse op het werkproces sociaal domein**
  Gezien het maatwerk binnen de gemeenten zijn de processen die de gemeente inricht/vormgeeft in het sociaal domein het startpunt voor de informatieanalyse. Van daaruit kan in kaart worden gebracht welke gegevens verwerkt, verzameld en gedeeld mogen worden. Dit document is een handreiking om de gemeente te ondersteunen bij het analyseren van informatie (gegevensverwerking) in bepaalde werkprocessen en het hanteren van een eenduidige werkwijze tav gegevensverwerking.
- **Excel Format Informatieanalyse op het werkproces**
- **Werkprocessen bij de Gemeente: Inzage, wijzigen en verwijderen van gegevens**
  De Wet Bescherming Persoonsgegevens schrijft voor dat de burger recht heeft op inzage en correctie/ verwijdering van persoonsgegevens. Dit document is een uitwerking van de werkprocessen

waarbij de burger een verzoek doet voor inzage, wijzigen en verwijderen van persoonsgegevens

- **Factsheet Toestemming verwerking van persoonsgegevens**
  Deze factsheet is bedoeld als een praktische handreiking voor professionals in het sociaal domein over het omgaan met toestemming van de burger in hun werk.

## Bewustwording en communicatie

- **Handreiking Communiceren met burgers over privacy**
  Het is als gemeente belangrijk om transparant te zijn over het verwerken van persoonsgegevens. Stel daarom een beleid op om de burger actief te informeren over het verwerken van persoonsgegevens en zorg dat instanties waaraan taken zijn uitbesteed dit ook doen.
- **Handreiking Privacy voor de professional**
  Het doel van dit document is gemeenten te ondersteunen bij het opstellen van een handreiking voor het verwerken van persoonsgegevens voor professionals in het sociaal domein. Goed en zorgvuldig gegevens delen wordt, naast een borging in de processen, organisatie en systemen, ook in belangrijke mate bepaald door de manier waarop medewerkers omgaan met persoonsgegevens.
- **Factsheet De gegevens van uw kind vastgelegd: het dossier**
  Voor ieder kind dat jeugdhulp ontvangt, wordt een dossier aangemaakt dat alle relevante gegevens over de hulp bevat. In deze factsheet wordt kort aangegeven waar het dossier toe dient, welke gegevens erin staan, welke rechten ouders en kinderen zelf hebben en wat er met het dossier van het kind gebeurt nadat de behandeling beëindigd is.

## Beheer en opslag gegevens

- Randvoorwaarde voor het zorgvuldig omgaan met persoonsgegevens is een goede informatiebeveiliging. Hiervoor biedt de Informatiebeveiligingsdienst gemeenten (IBD) bij de producten en diensten aan). Zie voor meer informatie de volgende websites:
- VNG/KING programma ISD: https://www.visd.nl/visd/informatiebeveiliging-het-sociaal-domein
  De volgende documenten zijn hierop te vinden:
  - Baseline Informatieveiligheid Gemeenten (BIG)
  - Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Download de handreiking Informatieveiligheid Sociaal Domein
  - Handreiking Informatiebeveiligingsmaatregelen Sociaal Domein

Zie ook de website van de IBD: https://www.ibdgemeenten.nl/

## Meer informatie

https://vng.nl/isd-privacy-en-gegevensuitwisseling