



Factsheet Privacy

Om als gemeente goede dienstverlening te kunnen bieden aan inwoners is het kunnen delen van (persoons)gegevens een randvoorwaarde. De wens van de gemeente om efficiënte en integrale dienstverlening te bieden, moet echter niet ten koste gaan van de privacy en keuzevrijheid van burgers. De decentralisaties van de zorg betekenen dat gemeenten meer gegevens zullen opvragen en gebruiken en hiervoor ook meer zullen samen werken met andere organisaties. Wanneer inwoners bepaalde zorg of dienstverlening ontvangen moeten ze erop kunnen vertrouwen dat er zorgvuldig wordt omgegaan met hun gegevens.

Regeling bescherming persoonsgegevens

Gemeente Zwolle onderneemt op een aantal manieren maatregelen om de privacy van inwoners te beschermen. In 2005 is de [Regeling Bescherming Persoonsgegevens](#) vastgesteld. Hierin worden regels beschreven waarbinnen de verwerking van persoonsgegevens en gegevensuitwisseling, ook in het sociaal domein, plaatsvindt. Omdat de regeling al een aantal jaren oud is en er in de tussentijd het nodige veranderd is, wordt de regeling binnenkort herzien.

Gemeente Zwolle heeft daarnaast besloten om (persoons)gegevens rondom zorg zo veel mogelijk op te slaan en uit te wisselen binnen 1 systeem: TOP. Dit borgt de privacy, omdat het systeem goed beveiligd is en alleen geautoriseerde medewerkers de informatie kunnen raadplegen. Daarnaast voorkomt het gebruik van 1 systeem onnodige gegevensoverdracht en dubbelingen in informatie.

Opvragen en gebruiken persoonsgegevens

In gesprek met de inwoner maakt de medewerker van het wijkteam een goede afweging of het verwerken van persoonsgegevens noodzakelijk is. De volgende stappen komen aan bod:

1. Behoefte aan gegevens

Samen met de inwoner wordt een ondersteuningsplan opgesteld. Om tot de beste ondersteuning te komen, wordt samen met de inwoner besproken welke persoonsgegevens daarvoor nodig zijn. Denk bijvoorbeeld aan gegevens vanuit de school, huisarts, Jeugdzorg IJsselland of de GGD. De noodzaak om deze gegevens op te vragen wordt met de inwoner besproken.

2. Afwegen gebruik gegevens

Het uitwisselen en gebruiken van gegevens moet afgewogen worden tegen de noodzaak van de ondersteuning voor de inwoner. Het wijkteam stelt zichzelf de volgende belangrijke vragen:

- Noodzaak: welke gegevens zijn noodzakelijk gegeven het gestelde doel van ondersteuning? (dat is iets anders dan mogelijk en wenselijk)
- Subsidiariteit: is het delen of opvragen van informatie de minst ingrijpende maatregel? Is er een methode (met hetzelfde effect) die minder ingrijpend is?
- Proportionaliteit: staan het delen of opvragen van de informatie en doel met elkaar in verhouding? Kan het ook met minder informatie?
- Kan en mag het: zijn er specifieke privacyregels die gelden voor de betrokken organisaties/personen?

Het is belangrijk om hierbij onderscheid te maken tussen gegevens die noodzakelijk zijn om een beslissing te kunnen nemen ten aanzien van bepaalde voorzieningen (toetsing aan criteria) en gegevens die noodzakelijk zijn om iemand beter te kunnen helpen of een beter beeld te krijgen van de situatie (verdieping van het onderzoek).

In de eerste situatie gaat het om voorwaarden die wettelijk gesteld mag worden aan een bepaalde voorziening. De inwoner heeft geen keuze, of hij of zij moet afzien van de aanvraag voor de betreffende voorziening. In het tweede geval kan de inwoner wel weigeren en aangeven dat hij of zij graag heeft dat het sociaal wijkteam zich beperkt tot de specifieke hulpvraag.

3. Informeren

De medewerker van het wijkteam stelt de inwoner op de hoogte van de afweging die gemaakt is. Als dit betekent dat er gegevens worden opgevraagd, is het van belang duidelijk te maken hoe de afweging tot stand is gekomen en welke gegevens worden opgevraagd en hoe dit bijdraagt aan de ondersteuning die geleverd kan worden. Wanneer de inwoner het hier niet mee eens is, kan de discussie aan gegaan worden. Voorbeeld: een ouder geeft geen toestemming voor het opvragen van gegevens van het kind. Er zijn echter sterke vermoedens van mishandeling. De wijkteammedewerker bepaalt in welke gevallen de gegevens toch worden opgevraagd.

4. Documenteren

In het gespreksformulier moet naast de mondelinge toestemming ook worden vastgelegd welke informatie wordt opgevraagd c.q. uitgewisseld. Voor het opvragen van informatie bij professionals met een beroepsgeheim (bijvoorbeeld huisartsen, psychologen, medische specialisten) dient wel een toestemmingsverklaring te worden ingevuld samen met de inwoner. Het gespreksformulier en eventueel de toestemmingsverklaring worden in TOP gedocumenteerd.

Aandachtspunten voor de sociale wijkteams

Burgerservicenummer (BSN)

Het BSN is persoonsgebonden. Het gebruik van het BSN binnen het wijkteam is bedoeld om duidelijkheid over identiteit te verkrijgen. Zo kan bijvoorbeeld voorkomen worden dat dossiers verwisseld worden. Ga dus zorgvuldig om met het vragen naar en het gebruik van het BSN.

Persoonsinformatie opslaan

Sla alle informatie over de inwoner, vanaf de registratie tot de facturatie, zoveel als mogelijk op in TOP. Andere systemen, zoals email en de Y-schijf, zijn toegankelijk voor anderen en/of niet voldoende beveiligd. Werk je bijvoorbeeld aan een conceptversie van het ondersteuningsplan, sla het bestand dan tijdelijk op je eigen schijf op. De relevante informatie uit de aantekeningen van het gesprek met inwoner neem je over in TOP. De originele aantekeningen verwijder je. De digitale aantekeningen gooi je in de prullenbak. De papieren aantekeningen maak je onleesbaar door ze door de shredder te halen.

Waarnemingsverzoek TOP

Bij het waarnemen op een dossier dient de medewerker van het wijkteam een waarnemingsverzoek in te dienen. De reden hiervoor is om de privacy van de inwoner te bewaken. Een medewerker mag er alleen in als noodzakelijk is en dat moet geregistreerd worden. De coördinator van het dossier in TOP heeft regie over het dossier en kan zien wie met welke reden in het dossier heeft gekeken.

Beveiliging TOP

Alleen de beheerder van TOP kent alle autorisaties van het systeem aan medewerkers toe. De medewerker van de wijkteams kan op een aantal manier bijdragen aan de beveiliging van TOP:

- Instellen van een uniek, persoonlijk wachtwoord om in te loggen.
- Aantal keer per jaar aanpassen van het wachtwoord. Hiervan verschijnt automatisch een melding. Als het wachtwoord niet op tijd gewijzigd wordt, neem dan contact op met de Servicedesk (038 498 4000).



- Niet uitwisselen van wachtwoorden met collega's. Als je voor lange tijd afwezig bent, zorg dan dat je dossier aan je collega's zijn overdragen. In TOP kun je de desbetreffende collega als 'betrokkene' toevoegen, waardoor het dossier overgenomen kan worden.
- Gebruik van mobiele telefoon (token/sms) bij het inloggen op de thuiscomputer.

Ambtseed, integriteitsverklaring en geheimhoudingsverklaring

Medewerkers worden in de toekomst verplicht om een ambtseed af te leggen, een integriteitsverklaring en/of een geheimhoudingsverklaring te tekenen. De medewerkers die dat nog niet hebben gedaan, zullen dit met terugwerkende kracht doen.

Overige informatie

- [Veel gestelde vragen over privacy \(website SWT\)](#)
- [Omgaan met privacygevoelige informatie \(intranetbericht Zwolle juni 2015\)](#)

Wet- en regelgeving

- [Regeling bescherming persoonsgegevens Gemeente Zwolle \(2005\)](#)
- [Wet bescherming persoonsgegevens Wbp \(2000\)](#)

Contactpersonen

[Nico Kuiper](#), functionaris gegevensbescherming (FG)

Tags

Bescherming persoonsgegevens, privacy, systeem, TOP, gegevensbescherming

Datum

Juli 2015