Privacy charter Buurtteams Utrecht

Gemeente Utrecht biedt haar burgers sociale basiszorg via buurtteams. Hiertoe heeft zij twee buurtteamorganisaties gemandateerd; Buurtteamorganisatie Sociaal Utrecht (voor volwassenen) en Lokalis (voor jeugd & gezin). De buurtteams zijn samengesteld uit generalisten die in staat zijn om enerzijds de meervoudige problematiek van de betrokkene in kaart te brengen en de benodigde hulpverlening daarvoor te genereren. Anderzijds biedt de generalist zelf ook ondersteuning en jeugdhulp.

Voor elke Utrechter is er vanaf 1 januari 2015 een buurtteam. Achter de schermen werken hier twee teams, een team Jeugd & Gezin (vanuit Lokalis) en een team Sociaal (vanuit Buurtteamorganisatie Sociaal Utrecht). Er is een gezamenlijk doel om hoogwaardige sociale basiszorg te bieden, die herkenbaar en toegankelijk is voor alle inwoners met een ondersteuningsvraag. Beide teams hebben hun eigen expertise, maar werken samen vanuit dezelfde visie, zoals vastgelegd in de kader- en uitvoeringsnota's Meedoen naar Vermogen en Jeugd van de gemeente Utrecht.

De buurtteamorganisaties bieden vooral ondersteuning bij mensen thuis. Daarnaast zijn zij toegankelijk via een gezamenlijke (fysieke en digitale) voordeur. Ze gebruiken hetzelfde registratiesysteem. Inwoners van de gemeente Utrecht bellen voor beide organisaties naar hetzelfde telefoonnummer en komen via dezelfde voordeur binnen. Klanten met kinderen worden in de meeste gevallen doorgeleid naar team jeugd & gezin, de andere klanten naar team sociaal.

Buurtteamorganisatie Sociaal Utrecht en Lokalis zijn verantwoordelijk voor passende dienstverlening, waaronder een goede waarborg van privacy van de klant. Met deze privacy charter geven de buurtteamorganisaties handen en voeten aan de privacy waarborging in de praktijk. Het privacy charter is opgesteld in co-creatie met de gemeente Utrecht.

De (sectorale) wettelijke kaders vormen een elementaire randvoorwaarde. Bij toepassing van deze charter en voor specifieke situaties waarin de sectorale wetgeving niet voorziet is de Wet Bescherming Persoonsgegevens (Wbp) leidend. De Wbp biedt daarbij met algemeen geformuleerde normen ruimte voor maatwerk, waar de discussie en interpretatieverschillen ontstaan. Op die punten dwingt de Wbp tot een zorgvuldige afweging met betrekking tot noodzaak, subsidiariteit en proportionaliteit van de gegevensverwerking. De Privacy Impact Assesment 3D – die door de minister van BZK in november 2014 is aangeboden aan de Tweede Kamer - is een instrument dat hiertoe handvatten biedt in de vorm van concrete aanbevelingen. Deze privacy charter is mede ontwikkeld op basis van deze aanbevelingen. Dit heeft geleid tot een privacy charter dat sterk gericht is op het verankeren van privacybeleid binnen de cultuur en het kwaliteitsbeleid van de buurtteamorganisaties.

De scope van deze charter is de borging van privacy van klanten van de buurtteams. Voor de gemandateerde activiteiten zoals het afgeven van een verwijzing/ beschikking blijft de gemeente verantwoordelijk voor gegevensuitwisseling in de keten. De bevoegdheidsverdeling tussen gemeente en de buurtteamorganisatie met betrekking tot het verlenen van toegang tot een individuele- of maatwerkvoorziening is conform de verordeningen WMO 2015 en Jeugdhulp 2015 uitgewerkt in een mandaatsbesluit.

AFSPRAKEN

1. VERANTWOORDELIJKHEDEN

Alle betrokken personen en partijen dragen een verantwoordelijkheid als het gaat om naleven van deze privacy charter. Buurtteammedewerkers zijn aanspreekbaar op de privacy borging van de betreffende klant.

De buurtteamorganisaties faciliteren de buurtteammedewerkers om in hun dagelijks werk de juiste privacy afwegingen te maken. Ook monitoren de buurtteamorganisaties of buurtteammedewerkers handelen conform de privacy charter en sturen zij tussentijds bij.

De bestuurders van de buurtteamorganisaties zijn verantwoordelijk voor een adequate toepassing en werking van deze privacy charter en leggen hierover verantwoording af aan gemeente Utrecht, die hierop toeziet.

De gemeente heeft in haar subsidiebeschikkingen als voorwaarde gesteld dat de privacy charter wordt nageleefd. Daarnaast blijft de gemeente verantwoordelijk voor de gegevensuitwisseling in de keten als het gaat om het verlenen van toegang tot een individuele/ maatwerkvoorziening.

2. LEIDENDE PRINCIPES

Privacy omhelst méér dan uitwisseling van persoonsgegevens. Ook is de vraag welke persoonsgegevens in welke situatie gedeeld mogen worden nooit eenduidig te beantwoorden. Dit vergt altijd een zorgvuldige afweging van het recht op privacy én het recht op passende dienstverlening. Vanuit het recht op privacy klinkt de roep om de mogelijkheid van gegevensdeling te beperken; vanuit het recht op passende dienstverlening klinkt de roep om gegevens te kunnen delen wanneer dit de dienstverlening ten goede komt.

Een vaste set regels voor alle voorkomende situaties in de dagelijkse praktijk volstaat niet. Daarom is in dit document – naast een aantal concrete maatregelen – een vijftal leidende principes benoemd. Alle professionals van de buurtteams onderschrijven deze principes en laten zich hierdoor in hun dagelijks werk leiden. De leidende principes zijn:

a) *De buurtteams gaan respectvol om met de persoonlijke levenssfeer van de klant. Het principe van eigen kracht is hier van toepassing.*
De klant krijgt naar vermogen maximaal de ruimte om zelf vorm te geven aan zijn dagelijks leven en de daarbij gewenste ondersteuning.

b) *Gegevens worden alleen vastgelegd en uitgewisseld voor zover noodzakelijk voor passende dienstverlening.*
De klant, diens mogelijkheden tot eigen regie, diens ondersteuningsvraag en de daarvoor benodigde dienstverlening staan telkens centraal bij de afweging of vastleggen en/ of delen van gegevens noodzakelijk is.

c) *De klant heeft zelf regie over zijn eigen dossier.*
De buurtteammedewerker draagt samen met de klant zorg voor het vullen en actualiseren van het dossier. De klant kan zijn dossier elk moment inzien. De klant

heeft zelf de regie welke persoonsgegevens verwerkt mogen worden in het dossier en welke gegevens hij of namens hem door het buurtteam uitgewisseld mogen worden.

d) *Veiligheid van de klant en/of zijn omgeving vormen altijd de ondergrens*
Wanneer de veiligheid van de klant en/ of zijn omgeving in het geding is, grijpt de buurtteammedewerker in en kan hij ook zonder toestemming van de klant gegevens vastleggen of delen met derden. De buurtteammedewerker doet dit altijd na collegiale consultatie en informeert altijd de klant waarom hij heeft besloten zonder toestemming van de klant te handelen.

e) *De buurtteams zijn open en transparant richting klanten* over de wijze waarop zij omgaan met het vastleggen van gegevens en het delen ervan met derden.

3. NOODZAAK EN TOESTEMMING BASIS VOOR GEGEVENSVASTLEGGING EN -UITWISSELING

Persoonsgegevens worden zo min mogelijk, maar zo veel als nodig geregistreerd en uitgewisseld. De buurtteammedewerkers starten met een leeg klantdossier. Er worden geen gegevens van de klant overgehaald vanuit andere (gemeentelijke) systemen. Uitzondering hierop is de BSN-verificatie, waardoor NAW-gegevens van de klant automatisch met hulp van het burger service nummer worden gegenereerd.

Het registratiesysteem is zo 'open mogelijk' ingericht, dat wil zeggen dat de buurtteammedewerker telkens met de klant de afweging maakt of en zo ja welke persoonsgegevens worden toegevoegd aan het dossier. Het systeem kent behoudens de NAW- gegevens van de klant geen verplichte invulvelden.

In lijn met leidend principe C (zie p. 1) vragen de buurtteammedewerkers altijd mondeling toestemming aan de klant of zijn/haar vertegenwoordiger voor het vastleggen en/of uitwisselen van diens gegevens. Relevante personen van de leefeenheid worden pas geregistreerd als deze personen hierover zijn geïnformeerd en daar toestemming voor hebben gegeven.

Met alleen toestemming is er nog geen grond om klantgegevens te mogen vastleggen en/of uit te wisselen. Overeenkomstig het leidend principe B (zie p. 1) worden klantgegevens alleen indien noodzakelijk voor een goede dienstverlening vastgelegd en/of uitgewisseld. Elke keer bij het vastleggen en/of uitwisselen van gegevens dient de afweging gemaakt te worden of gegevensvastlegging/deling bijdraagt aan het doel dat bereikt dient te worden. Elke keer opnieuw dient de klant ook weer expliciet om toestemming gevraagd te worden. Een éénmalige toestemming bij aanvang volstaat niet. Dit alles geldt zowel voor schriftelijke uitwisseling van persoonsgegevens als voor mondelinge uitwisseling van persoonsgegevens van klanten.

Indien de veiligheid van de klant en/of zijn omgeving in het geding is, kan een buurtteammedewerker, zoals vermeld in leidend principe E (zie p. 1), kiezen om zonder toestemming of ondanks een bezwaar van de klant toch gegevens vast te leggen en/ of te delen met andere partijen**.** Op grond van de wet- en regelgeving rondom de Meldcode Kindermishandeling en Huiselijk Geweld zijn buurtteammedewerkers in een aantal gevallen hiertoe zelfs verplicht. Voordat een buurtteammedewerker hiertoe besluit legt hij de casus geanonimiseerd voor aan een ander teamlid en/of zijn leidinggevende ter raadpleging. Ook informeert hij de klant, waar mogelijk, over de stappen die hij gaat ondernemen, ook al heeft deze geen toestemming verleend. Ook legt de

buurtteammedewerker uniform, begrijpelijk en vindbaar vast waarom hij heeft besloten zonder toestemming van de klant te handelen, wie hij hierover heeft geraadpleegd en op welke wijze hij de klant heeft geïnformeerd.

In een aantal gevallen is het waardevol om klantgegevens uit te wisselen met derden terwijl er niet direct sprake is van doelbinding. Monitoring, intervisies of casuïstiekbesprekingen zijn voorbeelden waarbij dit het geval is. De buurtteamorganisaties passen deze werkwijze toe om hun lerende vermogen te vergroten en zo hun dienstverlening te verbeteren. Privacy van klanten komt in deze gevallen nooit in het geding, omdat persoonsgegevens altijd geanonimiseerd worden.

4. VEILIG EN VERANTWOORD REGISTRATIESYSTEEM

Klantgegevens mogen alleen worden geregistreerd en opgeslagen in een veilig en verantwoord registratiesysteem. KTSD is het registratiesysteem dat de buurtteams gebruiken. Gemeente Utrecht is eigenaar van de KTSD-applicatie. Zij draagt zorg voor de beveiligde gegevensopslag. De buurtteamorganisaties zien toe op zorgvuldig gebruik en inrichting van het systeem. KTSD wordt gehost binnen de gemeente Utrecht. Dit betekent dat de algemene beveiligingsmaatregelen op hetzelfde niveau zijn als die van de gemeente Utrecht. Er wordt gebruik gemaakt van kanaalversleuteling via de VDI-verbinding volgens de NEN 7512 en NEN 7510 normen. Het is niet mogelijk om vanuit het KTSD klantgegevens lokaal op laptops of tablets op te slaan.

Uitsluitend de buurtteamorganisaties, en dus niet de gemeente, hebben toegang tot persoonsgegevens van klanten. Uitzondering hierop is de functioneel beheerder van KTSD, die in dienst is van de gemeente Utrecht; deze heeft een geheimhoudingsplicht en deelt alleen gegevens met andere partijen in opdracht van de buurtteamorganisaties.

De klantgegevens zijn per buurtteamorganisatie (Sociaal en Jeugd & Gezin) afgeschermd en daarbinnen per buurtteam. Binnen één buurtteam is één buurtteam medewerker en maximaal één vervanger voor het dossier geautoriseerd.

Continuïteit van dienstverlening is belangrijk. Wanneer zowel de eerst aangewezen buurtteammedewerker (de vaste contactpersoon voor de klant en het gezin) als diens vervanger niet aanwezig zijn, bestaat de mogelijkheid voor niet geautoriseerde collega's tot inzage in de dossiers of zelfs bewerking van het dossier. Dit laatste wordt ook wel het "breaking glass" principe genoemd waarbij medewerkers die toegang zoeken tot het dossier van de klant van een collega een mededeling krijgen vanuit het systeem dat ze niet geautoriseerd zijn en slechts toegang krijgen na het invullen van de reden waarom ze toegang willen hebben. Dit wordt gelogd en er gaat een signaal of naar de teamleider/buurtondernemer of aangewezen teamlid. Deze situatie maakt het mogelijk om in specifieke situaties toch toegang aan andere medewerkers te verlenen en dit tegelijkertijd te monitoren en controleren. Deze werkwijze is gebaseerd op procedures die in de medische sector gebruikt worden als er bijvoorbeeld sprake is van vervanging, weekenddienst etc. Bij overdracht van dossier wordt autorisatie ook overgedragen. Eerdere hulpverleners kunnen dus niet (meer) bij het dossier, alleen de buurtteammedewerker die op dat moment contact persoon is voor de klant en het gezin.

Tot slot maakt de inrichting van het KTSD het mogelijk om persoonsgegevens binnen een gezinsdossier af te schermen voor andere leden van het gezin. Voor meer informatie over het systeem is de handleiding KTSD ter inzage beschikbaar.

5. VERVOEREN EN BEWAREN VAN KLANTGEGEVENS

Klantgegevens worden alleen bewaard op de beveiligde Host-omgeving van de Gemeente Utrecht. Alleen indien noodzakelijk worden klantgegevens verstuurd per post. Dit altijd in een gesloten envelop met de vermelding 'vertrouwelijk'. Dit betreft persoonsgegevens die vallen onder de Wet op Persoonsbescherming zoals medische gegevens, inkomensgegevens en andere geldzaken.

Gegevens die in het kader van de toeleiding of toegang worden gedeeld met partijen binnen de aanvullende zorg (individuele voorzieningen cf. de Jeugdwet; maatwerkvoorzieningen cf. de WMO 2015) zijn tot een minimum beperkt en worden via het iWMO en iJeugd berichtenverkeer uitgewisseld. Aanvullend wordt in overleg met de klant bepaald of en zo ja (welke delen van) het ondersteuningsplan (Sociaal) of gezinsplan (Jeugd) worden uitgewisseld met partijen uit de aanvullende zorg (zie ook 6.3 van dit document).

Met inachtneming van eventuele wettelijke voorschriften worden de gegevens bewaard, zolang als noodzakelijk is, in het kader van de hulpverlening aan de betrokkene. Indien de bewaartermijn is verstreken worden de betreffende persoonsgegevens uit het registratiesysteem verwijderd en vernietigd, zulks binnen een termijn van één jaar, tenzij de Archiefwet en/ of -besluit zich daartegen verzet.

6. CRUCIALE AFWEGINGSMOMENTEN PRIVACY

Er is een aantal afwegingsmomenten dat cruciaal is in de privacywaarborging. Dit zijn de triagemomenten. Op deze momenten dient bepaald te worden welke mate van gegevensverwerking noodzakelijk is. De meest voorkomende triagemomenten van de buurtteams zijn:

1. Bij de ontvangst van de melding van de hulpvraag door de voordeurmedewerker. Hier wordt alleen informatie geregistreerd indien de hulpvrager in aanmerking komt voor dienstverlening van de buurtteams. Indien dit het geval is vindt er vraagverheldering plaats op basis waarvan beoordeeld kan worden door wie de hulpvraag het best behandeld kan worden. De overwegingen zijn:
    - vanuit welk team - team Sociaal of team Jeugd en gezin - wordt een buurtteammedewerker ingezet en vervolgens daarbinnen: welk buurtteam biedt de dienstverlening op basis van de postcode van de aanvrager,
    - en/of, is er sprake van een crisis en is directe opschaling vereist.
2. Bij het eerste gesprek met de buurtteammedewerker. Hier vindt verdere vraagverheldering plaats en wordt naast de zogenaamde 'dat' informatie[1] die vooral is geregistreerd bij triagemoment 1 ook de zogenaamde 'wat' informatie geregistreerd, maar alleen die 'wat' informatie die nodig is om te komen tot een ondersteuningsplan dat aansluit bij de behoefte van de klant, zijn eigen vermogen en de mogelijkheden van zijn/haar omgeving.
3. Bij toegang en/of toeleiding naar aanvullende zorg & ondersteuning. Hier worden alleen die onderdelen die relevant zijn uit het ondersteuningsplan gedeeld.

[1] 'dat-gegevens' zijn gegevens die aangeven dàt er sprake is van een bepaalde voorziening en/of hulpvraag, 'wat-gegevens' zijn gegevens die meer gaan over de inhoudelijke informatie over de problematiek / hulpvraag.

4. Bij tussentijdse evaluatiemomenten. Hier stemt de buurtteammedewerker met de klant af of het ondersteuningsplan effectief is en nog steeds aansluit bij diens behoefte. Indien dit niet het geval is wordt het ondersteuningsplan samen met de klant herzien en/of uitgebreid.
5. Als één van de leden van het gezin bezwaar heeft tegen inzage van de zijn persoonsgegevens door andere gezinsleden, moet de afweging gemaakt worden om de leefeenheid te knippen en een persoonlijk dossier aan te maken.
6. Bij escalatie in gevallen waarin de buurtteammedewerker zonder toestemming of ondanks bezwaar van de klant toch meent gegevens te moeten delen met andere partijen. Dit is onder punt 3 beschreven.

Gezien het belang van deze momenten, besteden de buurteamorganisaties in opleidingen en casuïstiekbesprekingen extra aandacht aan hoe bij deze momenten de leidende principes te volgen. Om de inschatting goed te kunnen maken zetten de buurteamorganisaties privacyambassadeurs in die zich specialiseren in het onderwerp en gebruikt kunnen worden als vraagbaak in geval buurtteammedewerkers twijfelen over de afweging die zij moeten maken. De privacy ambassadeurs gaan in 2015 tevens aan de slag met het doorontwikkelen van richtlijnen om de triagemomenten en de daarbij behorende afweging te expliciteren in welke gevallen welke gegevens (niet) te verwerken.

7. LEREND ONTWIKKELEN

De buurteamorganisaties zetten aankomende jaren stevig in op privacy waarborging. Er wordt geleerd van zaken die goed en minder goed gaan bij de implementatie van deze privacy charter. Door een gedegen kwaliteitscyclus zorgen de buurteamorganisaties dat zij in staat zijn om zich al lerende te ontwikkelen op dit gebied.

De volgende middelen zetten de buurteamorganisaties hierbij in:

- Privacy ambassadeurs; dit zijn personen die werken in de buurtteams (als medewerker en/of als leidinggevende) en privacy waarborging als aandachtsgebied hebben, ze blijven op de hoogte van de meest actuele ontwikkelingen op dit gebied, zijn vraagbaak en zetten het onderwerp doorlopend in de spotlight door erover te communiceren en door collega's te prikkelen.
- Privacy-monitor; In 2015 wordt een monitor ontwikkeld waarin KPI's als afgeleide van de leidende principes worden geformuleerd. Halverwege 2015 start de monitoring. Periodiek worden de uitkomsten geëvalueerd en op basis hiervan verbeteracties geformuleerd en geïmplementeerd.
- Opleiding, instructie & intervisie; Medewerkers krijgen bij aanvang van hun dienstverband een specifieke instructie waarin uitgelegd wordt wat er van hen verwacht wordt in het kader van privacy en informatieveiligheid en waarom dit van hen verwacht wordt. Jaarlijks krijgen de medewerkers een opfrissingsinstructie waarin ook de uitkomsten uit de privacy evaluatie wordt toegelicht. Daarnaast wordt in alle trainingen, intervisies, leercirkels, casuïstiekbesprekingen aandacht gevraagd voor het thema privacy.

Bovenstaande middelen faciliteren de buurtteammedewerkers in het maken van een zorgvuldige afweging van de noodzaak tot gegevensvastlegging en gegevensdeling. De leidende principes geven daarbij houvast alsook de principes van subsidiariteit, proportionaliteit, doelmatigheid zoals verwoord in de Wet bescherming

persoonsgegevens. Op basis van praktijksituaties werken de buurtteamorganisaties het afwegingskader hiervoor uit.

8. KENNISGEVING EN OPENBAAR REGISTER

De eindverantwoordelijke maakt door middel van melding bij het college bescherming persoonsgegevens het bestaan van de gegevensverwerkingen bekend. Een afschrift van de melding aan het College Bescherming Persoonsgegevens is vanaf 1 januari 2015 ter inzage beschikbaar. De buurtteamorganisaties zorgen verder ieder op de voor hen gangbare wijze voor bekendmaking van het bestaan van de gegevensverwerkingen.

9. LOOPTIJD, OVERDRACHT EN OVERGANG

Onverminderd eventuele wettelijke bepalingen is deze charter van kracht gedurende het bestaan van de buurtteams Utrecht. In het geval de opdracht voor de uitvoering van de buurtteams wordt gegeven aan een andere partij(en) is met de gemeente Utrecht overeengekomen dat zij de nieuwe partijen verplicht te handelen conform dit privacy kader. De buurtteamorganisaties stellen alle personen waarvan gegevens zijn geregistreerd in kennis van de overheveling van de opdracht, zodat zij tegen overdracht of overgang van op hun persoon betrekking hebbende gegevens bezwaar kunnen maken.