Privacy-charter Buurtteams Utrecht

De buurtteams en de gemeente Utrecht hebben gezamenlijke privacy-afspraken gemaakt, opgenomen in deze privacy-charter:

1. VERANTWOORDELIJKHEDEN

Alle hieronder genoemde 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 meestal niet 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 viertal 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 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 op verzoek inzien. Voor zover wettelijk mogelijk is, heeft de klant zelf de regie welke persoonsgegevens verwerkt mogen worden in het dossier en welke gegevens hij of namens hem door het buurtteam uitgewisseld mogen worden.

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.
Het delen van gegevens vindt als regel uitsluitend plaats met toestemming van de klant.

c) *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 klantgegevens 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.

d) *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.

In hoofdstuk 3 zijn de leidende principes waar nodig nader uitgelegd en uitgewerkt.

3. NOODZAAK EN TOESTEMMING BASIS VOOR GEGEVENSVASTLEGGING EN -UITWISSELING

Klantdossier
De buurtteammedewerkers informeren de klant over de werkwijze van het buurtteams. Onderdeel hiervan is het vastleggen van noodzakelijke gegevens in het klantdossier.
Voor klanten die onder de Jeugdwet vallen is er een dossierplicht. Wanneer klanten van het buurtteam instemmen met de aangeboden ondersteuning en er sprake is van vrijwillige hulpverlening, worden er persoonsgegevens van de klant vastgelegd in een dossier. De buurtteammedewerkers betrekken de klant of zijn/haar vertegenwoordiger altijd bij het vullen van het klantdossier. Relevante personen van de leefeenheid worden pas geregistreerd als deze personen hierover zijn geïnformeerd en daar toestemming voor hebben gegeven.

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 verificatie van Burgerservicenummer (BSN). BSN-verificatie is verplicht bij een maatwerkaanvraag. Het BSN wordt opgevraagd bij de klant en vervolgens verifieert de buurtteammedewerker de gegevens met de gegevens uit de gemeentelijke basisadministratie (GBA).

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.

Toestemming
In lijn met leidend principe B (zie hoofdstuk 2) vragen de buurtteammedewerkers altijd toestemming aan de klant of zijn/haar vertegenwoordiger voor uitwisselen van diens gegevens met derden. Voor kinderen tot 12 jaar geeft de ouder met gezag/voogd toestemming. Voor kinderen van 12 tot 16 jaar geldt dat zowel de ouder met gezag/voogd als het kind toestemming moet geven. Kinderen vanaf 16 jaar geven zelf toestemming.

Met alleen toestemming is er nog geen grond om klantgegevens te mogen uit te wisselen. Klantgegevens worden alleen indien noodzakelijk voor een goede dienstverlening vastgelegd en/of uitgewisseld. Elke keer bij het uitwisselen van gegevens dient de afweging gemaakt te worden of gegevensdeling bijdraagt aan het doel dat bereikt dient te worden.

Indien het noodzakelijk is om gegevens uit te wisselen met derden, streven de buurtteammedewerkers naar een driegesprek, waarbij de buurtteammedewerker samen met de klant de gegevens uitwisselt met de derde partij. Hierdoor is de eigen regie van de klant optimaal.
Als een driegesprek niet lukt, dan wordt de klant expliciet om toestemming gevraagd. Dit dient de buurtteammedewerker elke keer opnieuw te doen. 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 C (zie hoofdstuk 2), 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. De buurtteammedewerker legt in het klantdossier 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 of omdat een klant toestemming geeft om zijn casus te bespreken voor dit doeleinde.

Rechten van de klant
Klanten hebben recht op inzage in hun persoonsgegevens. Een klant kan een schriftelijk verzoek indienen bij het buurtteam. De klant hoeft geen reden voor het verzoek aan te geven. Het buurtteam laat de klant op een duidelijke en begrijpelijke manier weten of de organisatie zijn persoonsgegevens gebruikt, en zo ja: om welke gegevens het gaat, wat het doel is van het gebruik, aan wie de organisatie de gegevens eventueel heeft verstrekt, en wat de herkomst is van de gegevens, als deze bekend is.
Het recht op inzage betreft alleen inzage in iemands eigen gegevens. Klanten hebben dus geen recht op informatie over anderen. Persoonlijke werkaantekeningen vallen ook niet onder het inzagerecht, tenzij deze aantekeningen zijn opgenomen in het klantdossier.

Klanten hebben recht op correctie en verwijdering van hun persoonsgegevens. Zij mogen het buurtteam vragen hun persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Dat kan wanneer hun persoonsgegevens feitelijk onjuist zijn, onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld of op een andere manier in strijd met een wet worden gebruikt.
Het correctierecht is niet bedoeld voor het corrigeren van professionele indrukken, meningen en conclusies waarmee iemand het niet eens is, voor zover deze ter zake doen. Een verzoek om correctie of verwijdering van gegevens kan worden geweigerd, op het moment dat:

- De gegevens wettelijk moeten worden bewaard;
- Het bewaren van de gegevens noodzakelijk is om de klant een goede kwaliteit van dienstverlening te bieden of de klant te beschermen, bijvoorbeeld tegen geweld;
- Het bewaren van de gegevens noodzakelijk is in verband met een gerechtvaardigd belang van de buurtteams. Bijvoorbeeld bij een lopende klachtenprocedure.

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.

Een klantdossier is niet inzichtelijk voor iedereen. Er is een autorisatiemodel, dat zo is opgesteld dat zo min mogelijk en alleen relevante personen toegang hebben tot dossiers van klanten. De buurtteammedewerkers die toegang hebben tot uw dossier hebben een geheimhoudingsplicht. Zij delen alleen gegevens met andere partijen in opdracht van de buurtteamorganisaties en na toestemming van de klant.
Medewerkers van de gemeente Utrecht hebben geen toegang tot dossiers van klanten van de buurtteams. Een uitzondering hierop is de functioneel beheerder van het KTSD. Zij is gehouden aan een geheimhoudingsplicht.

Het autorisatiemodel is op te vragen bij de buurtteams.
De buurtteammedewerker die de klant en het gezin begeleidt, is degene die het klantdossier bijhoudt en coördineert. Deze coördinator is samen met zijn vervanger geautoriseerd om het klantdossier in te zien en te bewerken.

Continuïteit van dienstverlening is belangrijk. Wanneer zowel de coördinator 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 gelogd worden. De naam van de betreffende persoon en de ingevulde reden van de toegang tot het systeem, wordt in het klantdossier weergegeven. De coördinator en zijn vervanger zijn verantwoordelijk om kritisch te kijken of de gezochte toegang door de betreffende personen terecht was.
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.

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 gebeurt altijd in een gesloten envelop met de vermelding 'vertrouwelijk'. Dit geldt voor 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) zijn tot een minimum beperkt en worden via het iWMO en iJeugd berichtenverkeer uitgewisseld.

Met inachtneming van eventuele wettelijke voorschriften worden de gegevens bewaard, zolang als noodzakelijk is, in het kader van de hulpverlening aan de betrokkene. Bij Jeugdwet-dossiers, bij plannen van aanpak t.b.v. de aanvraag voorzieningen Jeugdhulp en WMO en de her-controle hierop, bij sancties Jeugdhulp en WMO klanten geldt een bewaartermijn van vijftien jaar.
Als 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[2] geregistreerd. Alleen de 'wat' informatie, die wettelijk noodzakelijk en 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, wordt geregistreerd.
3. Bij toegang en/of toeleiding naar aanvullende zorg & ondersteuning. Hier worden alleen die onderdelen die relevant zijn uit het ondersteuningsplan gedeeld.
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 zijn persoonsgegevens door andere gezinsleden, moet de afweging gemaakt worden om de leefeenheid op 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 leidend principe C (hoofdstuk 2) beschreven en hoofdstuk 3 verder toegelicht.

7. KENNISGEVING EN OPENBAAR REGISTER

De eindverantwoordelijke maakt door middel van melding bij het Autoriteit Persoonsgegevens het bestaan van de gegevensverwerkingen bekend. Een afschrift van de melding aan de Autoriteit Persoonsgegevens is ter inzage beschikbaar.

8. DATALEK

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat de Buurtteamorganisaties direct een melding doen bij de Autoriteit Persoonsgegevens, zodra zij een ernstig datalek hebben. Wanneer dit nodig is, wordt het datalek ook gemeld aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). De buurtteams houden van alle datalekken een registratie bij.

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 aan een andere partij(en) wordt gegeven, is met de gemeente Utrecht overeengekomen dat zij de nieuwe partijen verplichten 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.

[1] 'dat-informatie' zijn gegevens die aangeven *dat* er sprake is van een bepaalde voorziening en/of hulpvraag.

[2] 'wat-informatie' zijn gegevens die meer gaan over de inhoudelijke informatie over de problematiek / hulpvraag.