RAADSINFORMATIEBRIEF
16R.00143

gemeente
WOERDEN

Van : college van burgemeester en wethouders
Datum : 29 maart 2016
Portefeuillehouder(s) : Burgemeester en wethouder Koster
Portefeuille(s) : Privacy en Sociaal Domein
Contactpersoon : E. van Eijk
Tel.nr. : 8662
E-mailadres : eijk.eric@woerden.nl

16R.00143

Onderwerp:

Informatieveiligheid en Privacy

Kennisnemen van:

De Raadsinformatiebrief en factsheet VNG privacy-toestemming-gegevensverwerking-vsept2016

Inleiding:

Naar aanleiding het rapport van de Rekenkamercommissie inzake Privacy heeft de burgemeester toegezegd een RIB op te stellen voor de aprilcyclus.
Wethouder Koster heeft in de beantwoording van de artikel 40 vragen van D66 (13 januari 2016) toegezegd met een uitgebreide RIB te komen over privacy in het sociaal domein.

Kernboodschap:

In de RIB wordt eerst ingegaan op Informatieveiligheid en Privacy in het algemeen. Vervolgens wordt ingegaan op privacy in het sociaal domein specifiek. In beide onderdelen wordt ingegaan op de aanbevelingen van de rekenkamercommissie.

Vervolg:

Er wordt een informatiebijeenkomst ingepland.

Bijlagen:

16i.00959 Raadsinformatiebrief
16.005849 factsheet VNG privacy-toestemming-gegevensverwerking-vsept2016

De secretaris

drs. M.H.J. van Kruijsbergen MBA

De burgemeester

V.J.H. Molkenboer

Informatieveiligheid en Privacy

Stef Nicolasen

Versie 0.3

Deze raadsinformatiebrief beoogt inzicht te geven in de inrichting van de gemeentelijke organisatie en de sturing op informatieveiligheid en privacy in het algemeen en vervolgens ten aanzien van het sociaal domein in het bijzonder. Tevens wordt ingegaan op de aanbeveling die de Rekenkamercommissie heeft gedaan en het raadsbesluit dienaangaande.

Informatieveiligheid

De gemeentelijke organisatie is afhankelijk van een ongestoorde werking van haar informatievoorziening. Uitval van bedrijfsprocessen, het verliezen van gegevensbestanden of het door onbevoegden manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de continuïteit van het primaire proces. Het kan zelfs leiden tot levensbedreigende situaties, bijvoorbeeld het bekend worden van opvangadressen van “Blijf-van-mijn-lijf”.

Inwoners en organisaties uit deze gemeente mogen bovendien van de gemeente verwachten, dat zij zorgvuldig omgaat met hun informatie en gegevens. De gemeente kan het zich vanuit haar wettelijke zorgplicht niet veroorloven dat gegevens “op straat komen te liggen”. Als de informatieveiligheid niet voldoende is geborgd, is het vertrouwen in de gemeente, en daarmee in de overheid, in het geding.

Om de informatieveiligheid te kunnen waarborgen is het noodzakelijk om gedegen processen in te richten op basis van erkende standaarden. Het is van belang om alle taken, rollen en verantwoordelijkheden goed te beleggen. Daarnaast moet er een informatiebeveiligingsbeleid zijn opgesteld en vastgesteld en vervolgens worden uitgedragen.

Binnen de VNG is middels een resolutie afgesproken om het gemeentelijk informatiebeveiligingsbeleid te baseren op de door de Infomatiebeveiligingsdienst voor gemeenten (IBD) van de VNG opgestelde Baseline Informatiebeveiliging Gemeenten (BIG). Dit resulteert in een vergelijkbaar niveau van informatieveiligheid tussen gemeenten onderling en maakt onderlinge samenwerking tussen gemeenten en met andere overheden eenvoudiger.

In de strategische baseline informatiebeveiliging gemeenten staat: *“Het college van burgemeester en Wethouders van een gemeente stelt het informatiebeveiligingsbeleid vast en draagt dit uit.”*

Het college van de gemeente Woerden heeft op 6 oktober 2015 het Beleidsplan Informatieveiligheid en Privacy vastgesteld evenals de bijbehorende Richtlijnen Informatieveiligheid en Privacy. Daarmee heeft het college de eerste aanzet gegeven tot uitvoering van de voornoemde VNG-resolutie.

Vervolgens is een begin gemaakt met een nadere uitwerking van de richtlijnen. De BIG voorziet gemeenten van ca. 350 controlepunten voor een zogenaamde GAP-analyse, een analyse van de verschillen tussen de gewenste en huidige situatie. Deze analyse geeft op 11 onderdelen een beeld van de stand van zaken, zoals organisatorische aspecten, personele beveiligingsaspecten, het beheer van bedrijfsmiddelen en bedrijfscontinuïteit.

Uit deze analyse blijkt, dat aanvullende organisatorische of technische maatregelen noodzakelijk zijn om het gewenste niveau van informatieveiligheid en privacy te waarborgen. Deze maatregelen zijn opgenomen in het Implementatieplan Informatieveiligheid en Privacy. De aan die maatregelen verbonden incidentele en structurele kosten zijn berekend en opgenomen in het jaarplan van het domein Informatievoorziening, wat leidt tot knelpunten.

Daar waar mogelijk zijn maatregelen uit het implementatieplan uitgevoerd. Er is bijvoorbeeld een informatiebeveiligingsoverleg gestart onder voorzitterschap van de CISO (Chief Information Security Officer).

Zoals de portefeuillehouder bij de bespreking van de QuickScan “In eigen regie” van de Rekenkamercommissie heeft verwoord, worden de aanbevelingen van de Rekenkamercommissie door het college onderschreven. De mate waarin en de snelheid waarmee de door het college noodzakelijk geachte maatregelen kunnen worden uitgevoerd zijn echter afhankelijk van de inzet van mensen en middelen. Over het al dan niet nemen van de naar mening van het college vereiste maatregelen en de inspanning die daarvoor in geld en capaciteit is vereist wil het college graag in gesprek komen met een besloten commissie. De kwetsbaarheid van onze systemen verzet zich tegen openbare behandeling.

In dit kader kan worden gemeld, dat het aantal uiteenlopende bedreigingen en de ‘interesse’ voor gevoelige gegevens de afgelopen jaren enorm is gegroeid. Ter illustratie: voor 2013 werden er op ruim vijf miljoen .nl-domeinen 39 DDoS aanvallen gemeld in Nederland inclusief vermeende aanvallen die enkel een storing betroffen. De internetsite ‘norge digital attacks’ laat realtime de huidige situatie zien betreffende digitale aanvallen. Gelet op zowel de afhankelijkheid van onze digitale systemen voor onze bedrijfsvoering als de hierna nader benoemde eisen voor de bescherming van de persoonlijke levenssfeer van onze inwoners, dient het beschermingsniveau van onze organisatie gelijke tred te houden met de bedreigingen.

Privacy

De bescherming van de persoonlijke levenssfeer is (nu nog) op nationaal niveau geregeld in de Wet bescherming persoonsgegevens (Wbp) en in afzonderlijke wetten (zoals de Jeugdwet). De verwachting lijkt gerechtvaardigd, dat medio 2016 de Europese privacy verordening definitief zal worden. Deze verordening heeft na 2 jaar rechtstreekse werking voor alle lidstaten.

Informatieveiligheid en privacy zijn nauw met elkaar verbonden. Artikel 13 van de Wbp eist van de verantwoordelijke (College) dat er voldoende technische en organisatorische maatregelen zijn getroffen om de persoonlijke levenssfeer van ‘betrokkenen’ (de inwoners) te garanderen.

Sinds 1 januari 2016 is de Wbp uitgebreid met de Meldplicht Datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. In enige gevallen moet een datalek ook worden gemeld aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

Daarnaast is het College Bescherming Persoonsgegevens (CBP), inmiddels Autoriteit Persoonsgegevens (AP) geheten, middels de aanpassing van de Wbp voorzien van sanctiemiddelen die beduidend ingrijpender zijn dan voorheen. Voorheen kon het CBP een last onder dwangsom opleggen. De maximale boete die door de AP kan worden opgelegd is sinds 1 januari 2016 ruim €800.000. De Europese Verordening gaat daar in 2018 nog ver bovenuit, gelet op de tekst van de concept-verordening.

Nu is de boetedreiging zeker niet de eerste drijfveer voor het college om zaken rondom privacy goed te regelen. Belangrijker is dat de gemeente betrouwbaar moet zijn en op professionele wijze moet omgaan met de belangen die inwoners hebben wat betreft hun persoonlijke levenssfeer.

Uiteraard heeft het onderwerp privacy sinds het ontstaan van de Wbp in 2000 in deze gemeente de vereiste aandacht gekregen. Zo zijn registraties van persoonsgegevens vanaf het begin gemeld bij het CBP, nu de AP, gemeld. Echter, de bedreigingen op het gebied van informatieveiligheid, de decentralisaties en de gewijzigde regelgeving stellen nieuwe en verdergaande eisen. Die eisen zijn in het Beleidsplan Informatieveiligheid en Privacy, de bijbehorende richtlijnen en het Implementatieplan verwerkt tot organisatorische en technische maatregelen.

Het is de ambitie van het college de inspanningen op het gebied van informatieveiligheid en privacy op het niveau te brengen waarmee minimaal kan worden voldaan aan de wettelijke eisen. Evenzeer is het college zich er van bewust dat absolute veiligheid een illusie is. Niet alleen zijn beveiligingsmaatregelen altijd een reactie op nieuwe bedreigingen, maar ook moet het niveau van beveiliging in balans worden gebracht met hetgeen beschermd dient te worden. Kosten en baten moeten immers in evenwicht zijn. Vanuit deze ambitie zijn de hiervoor genoemde plannen opgesteld.

Deze documenten wil het college graag delen met de door uw raad in te stellen besloten commissie, zoals die eerder in deze RIB is genoemd. Dat biedt uw raad de mogelijkheid te beoordelen of de ambitie van het college in overeenstemming is met hetgeen de raad voor ogen staat.

Eerder in deze RIB is al het RKC-rapport ‘In eigen regie’ aangehaald. Uw raad heeft over de uitkomsten van de QuickScan In uw besluit van 12 januari 2016 het college opdracht gegeven tot:

1. Het harmoniseren van de formele afspraken met zorgpartners omtrent privacy.

2. Het structureel aandacht geven aan de zorgvuldige omgang met privacy.
3. Het concreet invulling geven aan de verantwoording over privacy aan de raad en aan inwoners.
4. Het scherp in de gaten houden van de juridische) risico's met betrekking tot privacy. In het bijzonder ten aanzien van het leggen van de regie over gegevensverstrekking bij de inwoner zelf.

Ten aanzien van de opdrachten 1 en 4 wordt hierna ingegaan onder de kop ‘Privacy in het Sociaal Domein’.

Om de informatieveiligheid en privacy op adequate wijze vorm te geven, moeten er – zoals hiervoor al is aangegeven – organisatorische en technische maatregelen worden getroffen. Technische maatregelen betreffen bijvoorbeeld de aanschaf van software met betrekking tot DLP (Data Loss Prevention)[1], sandboxing[2], Deep Security Inspection[3] en Intrusion Detection and Prevention[4] en daaraan verbonden de visuele inspectie van de door de software gesignaleerde bedreigingen. De noodzaak van afdoende technische beveiliging blijkt bijvoorbeeld uit de cijfers van het emailverkeer van december 2015. In totaal kwamen 132.608 emails binnen, waarvan 56.949 als spam werden geblokkeerd. 271 emails bevatten een virus.

Daarnaast is het noodzakelijk tijd vrij te maken voor het opstellen en aanpassen van beleid, procedures, richtlijnen en handleidingen. De menselijke factor is op het gebied van informatieveiligheid en privacy minstens zo belangrijk als de technische component. Mensen moeten werken conform het beleid en de procedures en moeten bewust worden van de noodzaak daartoe (awareness).

De structurele aandacht aan de zorgvuldige omgang met privacy (opdracht 2) zal vorm krijgen in een programma ter bevordering van de awareness, dat momenteel wordt voorbereid door het team Informatiebeleid. Daarmee wordt een eerste aanzet gegeven. Om deze aandacht voor privacy vast te houden zullen structurele maatregelen nodig zijn, waarvoor echter de middelen thans ontbreken. In dat kader verwijst het college u naar de RIB van maart, waarin knelpunten aan uw raad zijn gemeld.

Het college wil invulling aan de verantwoording over privacy aan de raad door jaarlijks op hoofdlijnen de raad te informeren en periodiek (bijvoorbeeld ieder half jaar) in een besloten commissie inzage te geven in de voortgang van de maatregelen zoals die in het genoemde implementatieplan zijn opgenomen.

De verantwoording aan de inwoners is feitelijk wettelijk geregeld. Maximale transparantie zal worden betracht, waarbij de rechten van de inwoner (inzagerecht, correctierecht en waar van toepassing toestemmingsrecht) op de websites (woerden.nl en woerdenwijzer.nl) worden opgenomen.

Privacy in het Sociaal Domein

Eric van Eijk

Inleiding

Binnen het sociale domein wordt gevoelige informatie van inwoners verwerkt. Hoewel de Baseline Informatiebeveiliging Gemeenten (BIG) het uitgangspunt is voor de informatiebeveiliging in het sociale domein, moeten er– omdat er bij het opstellen van de BIG geen rekening is gehouden met de drie decentralisaties voor jeugd, zorg en werk – extra maatregelen worden genomen binnen het sociale domein. Binnen het sociale domein is daarom formatieruimte vrijgemaakt voor een projectleider, die informatieveiligheid en privacy moet bevorderen. Er wordt in deze RIB beschreven welke organisatorische en technische maatregelen worden genomen om de privacy van inwoners op een juiste wijze te borgen. Er wordt ook ingegaan op de opdrachten 1 en 4 van de rekenkamercommissie.

In de huidige situatie speelt een belangrijke rol, dat de inrichting van het sociaal domein nog volop in ontwikkeling is. De posities van inwoners, de gemeente en professionele instellingen kunnen uiteen

[1] Software om datalekken op te sporen c.q. te voorkomen.
[2] Een sandbox (Engels voor "zandbak") is een afgeschermde ruimte waarin computerprogramma's kunnen werken zonder andere processen te verstoren. Doordat de uitvoerbare code als het ware opgesloten zit in een afgeschermde ruimte, komt het de beveiliging ten goede. Sandboxen worden voornamelijk gebruikt om code uit te voeren die niet vertrouwd wordt of onstabiel bevonden wordt.
[3] DSI bevat o.m. Virtual Patching, een oplossing waarbij wordt gecontroleerd welke kwetsbaarheden er op het systeem voorkomen. Dit betekent dat al het verkeer van en naar de server wordt onderzocht en indien men een software lek wil misbruiken waar het systeem kwetsbaar voor is dat wordt tegengehouden.
[4] Een Intrusion Detection System of IDS is een geautomatiseerd systeem dat hackpogingen en pogingen tot ongeautoriseerde toegang tot een informatiesysteem of netwerk detecteert.

lopen. Deze verschillende posities zijn van invloed op de belangen, de behoeften en (financiële) verantwoordelijkheden. Deze verschillende werkelijkheden komen soms overeen, maar soms schuren of botsen ze. Dat vertaalt zich ook naar hoe er wordt gekeken naar informatieveiligheid en privacy. We zijn nog maar aan het begin van een veranderend sociaal domein. Het is daarmee niet eenvoudig om overal een bevredigend antwoord op te hebben inzake informatieveiligheid en privacy die recht doet aan al deze posities. Daarvan is het college zich bewust.

Eigenaarschap en regie

Gemeente Woerden heeft als visie voor het sociaal domein dat inwoners (volledig) zelf de regie hebben bij het vormgeven van hun leven. Over privacy wordt in de visie gezegd dat inwoners:

> *eigenaar zijn van hun dossier en alle gegevens die daarvoor worden verzameld (privacy).*

Het eigenaar zijn over zijn/haar gegevens van de inwoner moet meer geduid worden. Een inwoner kan in juridische zin geen eigenaar zijn van de gegevens. Een inwoner is feitelijk geen eigenaar van bijvoorbeeld de gegevens in de basisregistratie personen. Dit laat onverlet dat de visie van de gemeente Woerden om regie (volledig) bij de inwoner te houden, blijft staan. Dit wordt o.a. vorm gegeven met de Inwonercloud, maar er is meer tijd nodig om deze regierol van de inwoner beter in te kleuren.

In het huidige werkproces van WoerdenWijzer.nl waarin inwoners een aanvraag doen voor ondersteuning, wordt op dit moment gewerkt met een toestemmingsverklaring om gegevens te verwerken en te delen. Het delen van informatie is nodig om integrale dienstverlening aan inwoners meer mogelijk te maken. Dit is niet alleen een handtekening op papier. De toestemming wordt ook besproken in het gesprek tussen de medewerker en inwoner. In dit gesprek kunnen inwoners ook aangeven of en aan wie of niet informatie gedeeld mag worden. Het is tevens aan de inschatting van de medewerker dat wanneer hij/zij dit nodig acht, extra toestemming wordt gevraagd. De richtlijn is: bij twijfel niet oversteken. Inwoners moeten erop kunnen vertrouwen dat er zorgvuldig wordt omgegaan met persoonsgegevens wanneer zij bepaalde zorg of dienstverlening ontvangen.

Toestemmingsverklaringen

Het werken met een algemene toestemmingsverklaring vooraf is naar het inzicht van VNG niet afdoende. In de bijlage van deze brief zit de factsheet van de VNG *'Factsheet omgaan met toestemming bij gegevensverwerking in het sociaal domein'*. Hier wordt bij deze naar verwezen. De kern het inzicht is dat een algemene toestemmingsverklaring vooraf, niet als grondslag kan dienen voor gegevensverwerking. De inwoner bevindt zich namelijk in een afhankelijkheidspositie ten opzichte van de gemeente. Er is dus geen sprake van ondubbelzinnige vrijwillige toestemming. De grondslag voor verwerking van gegevens in het kader van de WMO, Jeugdwet en de Participatiewet moet gezocht worden in de wettelijke verplichting of de goede vervulling van een publiekrechtelijke taak.

Toestemming is dus niet altijd noodzakelijk voor het verwerken van gegevens. Transparantie is dat wel. Dat betekent dat de betrokkene altijd moet worden geïnformeerd over het doel en de noodzaak van de te verwerken gegevens, tenzij de situatie dat niet toelaat. De inwoner heeft ook altijd het recht om bezwaar te maken tegen verwerking van bepaalde gegevens.

Er is dus sprake van een bijzondere en soms ingewikkelde balans tussen het belang van de professionele afweging om te komen tot de noodzakelijke gegevensverwerking vanuit de wettelijke taak en maatschappelijke opgave en de borging van de privacy van de inwoner. Een bijzondere situatie ontstaat wanneer de veiligheid van de inwoner, zijn/haar omgeving of medewerker in het geding is. Ook in deze situatie dienen wij gericht te zijn op toestemming en transparantie van de inwoner, maar ook hier zijn weer uitzonderingen op. En dit is niet altijd in regels te vatten. Medewerkers moeten hier kunnen handelen, en vooral zelf beargumenteren en documenteren waarom men informatie heeft gedeeld en/of bepaalde handelingen heeft gedaan.

Werkproces

De lijn van transparantie naar inwoners willen we nu al inzetten, maar het huidige werkproces is nog niet volledig ingericht vanuit het inzicht dat de VNG heeft neergezet. Dit betekent dat het werkproces opnieuw stap voor stap wordt bekeken. Er wordt gekeken naar de gegevens die worden geregistreerd, de grondslag die daarvoor is en waar mogelijk expliciete toestemming van inwoners alsnog nodig is. Hier zijn wij begin maart mee begonnen en we willen dit eind april afgerond hebben in de vorm van een bijgewerkt werkproces en een vernieuwde werkinstructie aangaande privacy daarbij.

Bewustzijn

Een goed werkproces is één stap om de privacy te waarborgen. Een tweede belangrijke stap is de kennis, houding en gedrag van de medewerkers die het werkproces uitvoeren. We willen dat onze medewerkers over privacy bewustzijn beschikken en privacy vraagstukken op tijd herkennen in hun werkzaamheden. De volgende zaken worden hier op ingezet:

- het kennen van de werkinstructie;
- training in communicatie met inwoners over privacy vraagstukken;
- een aantal praktische gedragsregels zijn reeds ingevoerd:
  - clean screen;
  - clean desk;
  - richtlijnen opslag/bewaren gegevens.

Technische aspecten

Naast de organisatorische kant is de technische ICT-kant minstens zo belangrijk. Op dit moment is het zo dat wij nog werken met ‘onbeveiligde’ email, waardoor de kans dat informatie wordt onderschept theoretisch bestaat. Om dit risico te managen zijn de volgende maatregelen genomen:

- korte termijn:
  ondersteuningsplan kan vooralsnog gewoon via info@woerdenwijzer.nl of via de post verstuurd worden; de mogelijkheden om op andere wijze veilig berichtenverkeer te hebben willen we in april helder hebben; Indien mogelijk wordt dit voor de zomer geïmplementeerd;
- korte termijn:
  emailverkeer tussen professionals en medewerkers wordt geminimaliseerd. Waar mogelijk worden documenten gecodeerd verstuurd. Aangezien dit een onhandige werkwijze is voor onze medewerkers en professionele partners wordt de mogelijkheid van een eigen platform onderzocht. Vanuit dit platform kunnen documenten veilig worden gedeeld.
- Langere termijn:
  met de bouw van ‘cumulus’ en de Inwonercloud willen we deze risico’s oplossen.

Rekenkamercommissie

In het onderdeel ‘Informatieveiligheid en Privacy’ van de RIB is al ingegaan hoe er omgegaan wordt met de opdrachten 2 en 3 die door de rekenkamercommissie zijn opgesteld.
Voor wat betreft de harmonisatie van de formele afspraken met zorgpartners (opdracht 1) omtrent privacy worden bewerkersovereenkomsten opgesteld, zoveel mogelijk in samenwerking met de regio Utrecht West. Over de voortgang zullen wij de raad berichten.
Opdracht 4 houdt in dat wij de (juridische) risico's met betrekking tot privacy scherp in de gaten houden. In het bijzonder ten aanzien van het leggen van de regie over gegevensverstrekking bij de inwoner zelf. Dit is geen gemakkelijke opgave. Privacy is een juridisch complex vraagstuk. Te meer omdat we aan het begin staan van een veranderend sociaal domein. De juridische kennis t.a.v. privacy moet verder toenemen in onze organisatie. Concreet wordt op dit moment in beeld gebracht wat de juridische grondslagen zijn voor het verwerken van gegevens in het werkproces van WoerdenWijzer.nl.

Risico overzicht

Om de risico’s inzichtelijk te maken en welke maatregelen hier voor worden ingezet, hierbij onderstaande tabel:

Risico	**Kleine kans/ Grote kans**	**Korte termijn oplossing**	**Lange termijn oplossing**
Omdat inwoners ondersteuningsplan via onbeveiligde mail opsturen kan deze worden onderschept	Kleine kans	Inwoners kunnen per post versturen. Mogelijkheden als MijnOverheid worden onderzocht.	Inwonercloud
Ondersteuningsplannen zouden kunnen gaan zwerven in organisatie	Kleine kans	Documenten worden direct bij binnenkomst gescand en opgenomen in beschermde ICT	Documenten worden direct bij binnenkomst gescand en opgenomen in beschermde ICT

		omgeving. Clean Screen. Clean Desk.	omgeving. Clean Screen. Clean Desk.
Bestanden kunnen worden onderschept die door een medewerker via onbeveiligde mail zijn verstuurd	Kleine kans	Mailverkeer verminderen. Versturen van gecodeerde bestanden naar organisaties. Ontwikkeling eigen platform.	Inwonercloud
Medewerker deelt onterecht of te veel informatie met collega of externen	Kleine kans	Duidelijke werkinstructie. Training/casuïstiek die privacy bewustzijn bevordert. Anoniem bespreken.	Duidelijke werkinstructie. Training/casuïstiek die privacy bewustzijn bevordert. Anoniem bespreken.

Factsheet omgaan met toestemming bij gegevensverwerking in het sociaal domein

Versie september 2015

Doel factsheet

Deze factsheet is bedoeld als een praktische handreiking voor professionals in het sociaal domein voor het omgaan met toestemming in hun werk. In deze factsheet spreken we steeds over 'de gemeente' of 'het College', omdat het gaat over gegevensverwerking in het kader van de gemeentelijke taken in het sociaal domein, die plaats vinden onder verantwoordelijkheid van het College van B&W. De feitelijke verwerking kan ook plaatsvinden door medewerkers van andere organisaties die door de gemeente zijn gemandateerd om deze taken uit te voeren. De gemeente blijft in die gevallen verantwoordelijk.

Geen algemene toestemmingsverklaring vooraf

Veel gemeenten vragen burgers bij de start van een traject voor hulp of ondersteuning vooraf om een algemene toestemmingsverklaring te ondertekenen om persoonsgegevens te verwerken. Dit gebeurt vanuit de veronderstelling dat daarmee voldaan wordt aan een eis van de Wet bescherming persoonsgegevens. Ondubbelzinnige toestemming is één van de mogelijke grondslagen die in de Wbp genoemd worden. Toestemming kan hier echter niet als grondslag dienen. De burger bevindt zich namelijk altijd in een afhankelijkheidspositie ten opzichte van de overheid, in dit geval de gemeente. Er is dus geen sprake van ondubbelzinnige vrijwillige toestemming. De Wet bescherming persoonsgegevens (Wbp) noemt dit een ongelijke machtsverhouding. De grondslag voor verwerking van gegevens in het kader van de Wmo, de Jeugdwet en de Participatiewet moet eerder gezocht worden in de wettelijke verplichting of de goede vervulling van een publiekrechtelijke taak. Er is nog een aantal redenen waarom het geen goed idee is om toestemming als grondslag te kiezen voor het verwerken van persoonsgegevens voor de uitvoering van gemeentelijke taken in het sociaal domein:

- Het is natuurlijk mogelijk dat iemand geen toestemming geeft. Dat zou betekenen dat er geen grondslag is en er dus geen gegevens verwerkt kunnen worden en bij gevolg ook geen hulp of ondersteuning geboden kan worden. Dat is niet zo (zie hieronder).
- Daarnaast is het ook mogelijk dat iemand zijn toestemming intrekt. Wanneer die toestemming als grondslag bedoeld is voor de verwerking van de gegevens, is er na intrekking van de toestemming dus ook geen grondslag meer voor de verwerking die al

plaatsgevonden heeft. Verzamelde gegevens zouden dan weer verwijderd/vernietigd moeten worden.
- Tot slot is het zo dat toestemming, ook wanneer die ondubbelzinnig verleend zou zijn, nooit de andere voorwaarden die de Wbp stelt, zoals noodzaak en proportionaliteit, kan vervangen of compenseren. Dus ook met toestemming mogen geen gegevens verwerkt worden die niet noodzakelijk zijn voor de taak die op dat moment verricht wordt.

Het is dus onnodig en onwenselijk om burgers vooraf een algemene toestemmingsverklaring te laten tekenen. Dit betekent echter niet dat er nooit toestemming nodig is.

Wanneer is toestemming wel vereist?

In specifieke gevallen is toestemming nodig om geheimhoudingsverplichtingen (zoals het medisch beroepsgeheim) te doorbreken. Ook in die gevallen dient de gegevensverwerking noodzakelijk te zijn voor de goede gemeentelijke taakuitvoering. De professional moet aan de burger duidelijk maken met welk doel hij of zij gegevens wil verwerken (opvragen, delen enz.) en hiervoor expliciet om toestemming vragen. Deze toestemming moet specifiek zijn en gemotiveerd en daarin kan dus niet worden voorzien met een algemene toestemmingsverklaring

In het kader van de Wmo is expliciet de verplichting opgenomen toestemming te vragen voor:
- gebruik van persoonsgegevens die de gemeente verkregen heeft ten behoeve van de uitvoering van de participatiewet of de jeugdwet voor zover die noodzakelijk zijn voor de beoordeling van de behoefte van de cliënt aan ondersteuning in het kader van de Wmo.
- gebruik van persoonsgegevens die de gemeente verkregen heeft van zorgverzekeraars en zorgaanbieders voor zover die noodzakelijk zijn voor de beoordeling van de behoefte van de cliënt aan ondersteuning.
- verstrekken van persoonsgegevens aan een zorgverzekeraar en zorgaanbieder voor zover die noodzakelijk zijn voor het uitvoeren van taken krachtens de zorgverzekeringswet.
- inlichtingen verstrekken aan anderen dan de betrokkene, inzage in of afschrift van bescheiden.
- indien de betrokkene minderjarig is en jonger dan 12 jaar of tussen 18 en 12 jaar en niet in staat geacht kan worden tot een redelijke waardering van zijn belang, dan is in die gevallen dat toestemming vereist is de toestemming van zijn wettelijke vertegenwoordiger vereist.

Er zij ook enkele uitzonderingen op bovenstaande verplichting opgenomen in de Wmo waarin de gemeente geen toestemming nodig heeft van de betrokkene, namelijk voor:
- het gebruik van gegevens die verkregen zijn van het CIZ en die noodzakelijk zijn voor de beoordeling van de behoefte van de cliënt aan ondersteuning.
- Verstrekken van gegevens aan anderen waarvan beroepshalve de medewerking vereist is bij de uitvoering van de taken van het college, een aanbieder, een derde aan wie ten laste van een persoonsgebonden budget betalingen worden gedaan, het CAK, de Sociale verzekeringsbank, toezichthoudende ambtenaren en het AMHK.

Transparantie richting de burger: leg uit wat je doet en waarom

Toestemming is dus niet altijd noodzakelijk voor het verwerken van gegevens. Transparantie is dat wel. Dat betekent dat de betrokkene altijd wordt geïnformeerd over het doel en de noodzaak van de te verwerken, tenzij de situatie dat niet toelaat. De burger heeft ook altijd het recht om bezwaar te maken tegen verwerking van bepaalde gegevens.

Bezwaar tegen verwerking of geen specifieke toestemming. En dan?

Ook als toestemming niet noodzakelijk is, kan het zijn dat een betrokkene bezwaar maakt tegen de verwerking van zijn of haar persoonsgegevens. Tenslotte is nog mogelijk dat betrokkene geen toestemming verleent voor gegevensverwerking in de onder 3 genoemde situaties, ook nadat de professional hem of haar geïnformeerd heeft over belang en noodzaak De gemeente heeft dan nog altijd een publiekrechtelijke taak om zorg of ondersteuning te bieden. Dat plaatst de professional voor een nieuwe afweging. Grofweg zijn er drie mogelijkheden:

1. De dienstverlening stopt, omdat het niet mogelijk is verdere diensten te verlenen;
2. De dienstverlening blijft beperkt tot het deel dat op basis van de beschikbare gegevens verleend kan worden;
3. Naar het professionele oordeel van de professional is de situatie dusdanig, dat er toch stappen gezet moeten worden omdat de gezondheid of veiligheid van betrokkene of mensen in de omgeving in het geding zijn. Dan kom je in de onvrijwillige dienstverlening.

Het laatste betekent een zware inperking van de persoonlijke levenssfeer van mensen. Een stap die dan ook alleen na zeer zorgvuldige afweging gezet mag worden. Houd daarbij altijd de volgende drie vuistregels in het oog:

1. Vergewis jezelf ervan dat je de betrokkene voldoende duidelijk hebt proberen te maken van het belang van de dienstverlening die nu geen doorgang kan vinden.
2. Consulteer een collega of expert om je oordeel te toetsen en doe dat eventueel op basis van geanonimiseerde gegevens.
3. Leg de overwegingen om toch stappen te zetten en in dat kader de noodzakelijke gegevens te verwerken tegen de wil van betrokkene vast, informeer hem of haar over je afweging en beslissing, en informeer hem of haar over haar rechten.