

Ben W 23 september
Rend 30 oktober



Uitgangspunten Privacy Oudewater

Gemeente Oudewater
11 september 2014
Versie 0.3

Inleiding

Welzijn Oudewater vormt het sociaal stadsteam toegang Oudewater. De vragen van inwoners van Oudewater die betrekking hebben op het brede sociaal domein komen hier binnen. Vragen omtrent informatie en advies worden waar mogelijk door het sociaal stadsteam rechtstreeks afgehandeld dan wel verwezen naar organisaties die beter zijn toegerust om die vragen te beantwoorden. De leden zijn generalistische professionals getraind in vraagverhelderingstechnieken. Daarnaast onderhoudt het team nauwe samenwerkingsrelaties met informele organisaties en professionele organisaties uit de 1^e lijn. Het sociaal stadsteam kan doorverwijzen naar de 2^e lijn. Drie leden uit het stadsteam functioneren als sociaal coach. De sociaal coach is alleen betrokken bij inwoners met meervoudige, complexe ondersteuningsvraag. Zij organiseren op basis van de vraag, een multidisciplinair klantoverleg. Aan het klantoverleg nemen de inwoner en/of zijn of haar vertegenwoordigers, het eigen sociaal netwerk, de sociaal coach er op de vraag deskundige informele organisaties en professionals uit 1^e lijnorganisaties deel. Nav het klantoverleg wordt een passend ondersteuningsplan geformuleerd. De casusregie ligt vervolgens bij de inwoner. Het stadsteam ontwikkelt zelf een evaluatie cq. Feedbacksysteem om de effectiviteit van de ondersteuning te kunnen volgen en beoordelen. De gemeente Oudewater subsidieert Welzijn Oudewater. De medewerkers van het sociaal stadsteam zijn in dienst van Welzijn Oudewater (cao welzijn) en geen gemeentambtenaar.

Na het bovenstaande gelezen te hebben zijn er vragen die eerst beantwoord dienen te worden voordat de Privacy uitgangspunten vastgesteld kunnen gaan worden.

Wanneer is de gemeente Oudewater verantwoordelijk voor de uitvoering van het privacy beleid in het sociaal domein en wanneer gaat het hierbij om Welzijn Oudewater. Welzijn Oudewater heeft namelijk de medewerker rond de toegang en het sociaal stadsteam in dienst. Gemeente Oudewater is hierbij dus de opdrachtgever. Daarnaast worden de beschikkingen bijvoorbeeld het komende jaar nog steeds verstuurd op naam van de gemeente Oudewater. Hoe dit zal gaan verlopen zal in het transitie jaar duidelijk worden. Desondanks zijn er een aantal uitgangspunten geformuleerd waarover gediscussieerd kan gaan worden. Uitgangspunten waar een uitspraak (Gemeente verantwoordelijk of Stadsteam verantwoordelijk) over gedaan moet gaan worden, maar eventueel ook nog juridisch onderzocht moet gaan worden. In het kort gezegd kunnen dus een aantal uitgangspunten alleen voor de gemeente Oudewater gelden en een aantal alleen voor Welzijn Oudewater of misschien wel voor beiden.

Integrale aanpak mbv privacy raamwerk

Het privacy raamwerk geeft aan op welke onderdelen de gemeente zich gaat richten op het gebied van privacy. Het is namelijk meer dan alleen het opzetten van een juridisch kader of privacyprotocol. De op pagina 4 t/m 10 benoemde uitgangspunten kunnen ondergebracht worden in 1 of meerdere onderdelen van het raamwerk. De uitgangspunten zullen de komende tijd verder aangescherpt gaan worden met de opgedane ervaringen (lokaal, regionaal en landelijk).

Governance

Governance richt zich op de inrichting van de gemeente Oudewater of Welzijn Oudewater m.b.t. privacy. Hierbij moet gedacht worden aan rollen en verantwoordelijkheden, wie voert de regie, wie controleert, hoe wordt verantwoording afgelegd en op welke wijze. Dit wordt nader uitgewerkt in het informatiebeveiligingsbeleid.

Beleid

Dit onderdeel beschrijft het kader waarbinnen de verwerking van persoonsgegevens gegevensuitwisseling in het sociaal domein plaatsvindt. Het kader betreft zowel het beleidsmatige kader als het juridisch kader. Hierin wordt beschreven hoe de gemeente, zowel intern als extern, om gaan met persoonsgegevens.

Bewustwording & Training

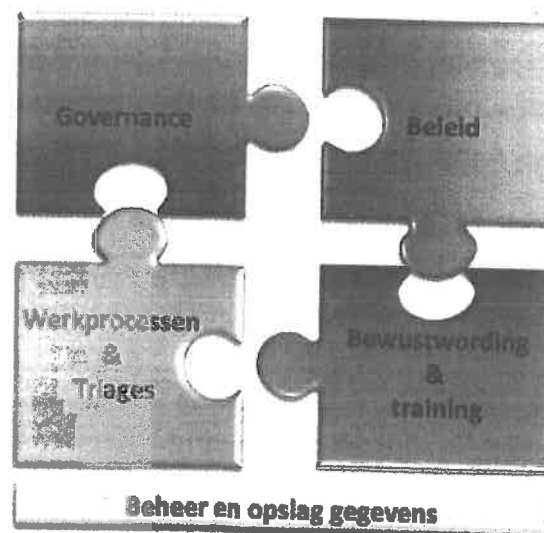
Betrokken professionals moeten over een zekere mate van privacy bewustzijn beschikken om privacy situaties te herkennen. Ze moeten getraind worden in hoe zij met specifieke situaties om moeten gaan. Communicatie intern en aan inwoners is essentieel.

Beheer en opslag gegevens

Persoonsgegevens worden in allerlei systemen geregistreerd, gedeeld en openbaar gemaakt. Denk bv. aan vragen als; is er nagedacht over wie welke informatie mag inzien? Wat voor type persoonsgegevens worden opgeslagen? En met welke termijn? Welke systemen intern en extern hier toegang tot hebben?

Werkprocessen & Triages

Het inrichten van werkprocessen rondom het omgaan met persoonsgegevens, het uitwerken van processen mbt vraagverheldering, selectie en toeleiding van vragen en het borgen van deze processen in werkafspraken en convenanten.



WBP is leidend

Het uitwisselen en het benutten van informatie over inwoners is een middel en geen doel. Het middel zal ten dienste staan van de dienstverlening aan die inwoner zelf. Daarom is het van groot belang dat het gebruik van die informatie zorgvuldig gebeurt en dat de privacybelangen van de inwoner continu gewaarborgd zijn.

Vanuit de Wet bescherming persoonsgegevens (Wbp) is vereist dat persoonsgegevens op een behoorlijke en zorgvuldige manier worden verwerkt (artikel 6) en alleen voor duidelijk omschreven doelen worden gebruikt (artikel 7). Voordat de informatievoorziening kan worden ingericht, is het noodzakelijk enkele vragen zorgvuldig af te wegen:

- Welke gegevens worden in welke situaties tussen welke professionals uitgewisseld?
- Wat is het doel van die uitwisseling?
- Waarom is de uitwisseling noodzakelijk? Zijn er geen minder ingrijpende alternatieven?
- Hoe worden de grondrechten van betrokkenen (inwoners en professionals) geborgd?
- Wat zijn de rechten (en eventueel plichten) van de betrokken inwoners hierin?

Andere wetten die de essentie raken van de uitwisseling van persoonsgegevens: de Wet op de Geneeskundige Behandeloovereenkomst (WGBO), de Wet Politiegegevens (Wpg) en de Wet Basisregistratie personen (BRP). Per 6 januari 2014 is de nieuwe wet in werking getreden. De wet BRP volgt de Wet GBA (Wet Gemeentelijke Basisadministratie persoonsgegevens) op en de Wet GBA is hierdoor komen te vervallen.

De uitwerking van de in deze wetten neergelegde algemene kaders en principes is vervolgens geregeld in verschillende **materiewetten**, waarin de uitwisseling van persoonsgegevens in de sectoren is geregeld. Voorbeelden zijn de sectoren werk en inkomen (WWB, Wet SUWI), jeugd (Wet op de Jeugdzorg, straks Jeugdwet), welzijn en zorg (Wmo, Wet Publieke Gezondheid, Awbz, Zorgverzekeringswet), de aanpak van huiselijk geweld en kindermishandeling (Wmo, Wet Meldcode), de omgang met schulden (Wet Gemeentelijke Schuldhulpverlening), of de aanpak van leerplicht en voortijdig schoolverlaten (Leerplichtwet).

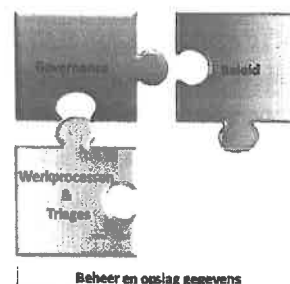
Uitgangspunten Privacy:

1. De inwoner is eigenaar van zijn eigen dossier.

In de visie van de gemeente Oudewater voeren inwoners zoveel mogelijk de eigen regie, al dan niet met ondersteuning, bij het vormgeven van hun leven. Deze visie maakt de inwoners dus ook eigenaar van hun eigen dossier.

Voor het transitie jaar 2015 (Korte Termijn) wordt er zoveel mogelijk naar dit uitgangspunt toegewerkt met het reeds aanwezige applicatielandschap van de gemeente Oudewater en/of het sociaal stadsteam. De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens (en dus het dossier). Het gaat er om of er enige feitelijke macht of invloed, al dan niet via een computersysteem, over de gegevens uitgeoefend kan worden (Kan er een handeling met de gegevens verricht worden?). De Wbp (Wet bescherming persoonsgegevens) noemt een aantal handelingen die als verwerking worden aangeduid:

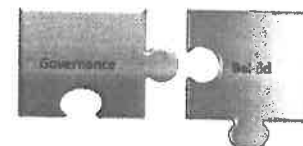
- verzamelen, vastleggen en ordenen;



- bewaren, bijwerken en wijzigen;
- opvragen, raadplegen, gebruiken;
- verstrekken door middel van doorzending;
- verspreiding of enige andere vorm van terbeschikkingstelling;
- samenbrengen, met elkaar in verband brengen; en
- afschermen, uitwissen of vernietigen van gegevens.

2. De inwoner bepaalt met wie en welke gegevens gedeeld worden.

De inwoner bepaalt welke informatie met wie gedeeld mag worden, wie toegang heeft tot het dossier en in welke hoedanigheid zoals bij uitgangspunt 1 geschetst. Dit kan offline gebeuren met toestemmingsformulieren waarin de inwoner gevraagd wordt toestemming te verlenen. Daarnaast kan de inwoner een verzoek indienen het dossier in te zien.



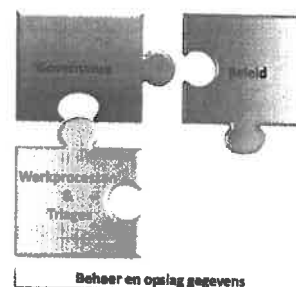
Beheer en opslag gegevens

Wanneer sprake is van een drang en dwang-kader, blijft de inwoner/het huishouden eigenaar van het dossier maar kan hij/zij dat specifieke deel van het dossier niet zelf beheren (minder inzage/correctierecht). Omgekeerd krijgen professionals vanuit het drang en dwang-kader slechts toegang tot dat specifieke deel van het dossier, tenzij de inwoner/het huishouden anders beslist. In uitzonderlijke gevallen is een gezinsvoogd eigenaar van het dossier. Dit laatste is het geval als dit als dwingende maatregel is opgelegd door de Raad van de Kinderbescherming/Kinderrechter en het gezin elke medewerking weigert.

3. De gegevens over de inwoner wordt verzameld met in achtname van het triage proces.

Triage is het proces van verhelderend, routeren en escaleren van vragen en casussen en is erop gericht om op een gestructureerde en gestandaardiseerde manier de mate van integraliteit vast te stellen. Is er sprake van een enkelvoudige, meervoudige vraag, of complexe (multiprobleem) - casuïstiek? Een enkelvoudige vraag kan bijvoorbeeld snel telefonisch worden afgehandeld of mbv een inloopsprekkuur.

Wanneer er sprake is van een meervoudige vraag van de inwoner wordt er het Stadsteam ingezet voor integrale afhandeling van de hulpvragen van de betreffende inwoner onder regie van een sociaal coach. Wanneer er sprake is van een zware multi probleem casus (Drang en Dwang) is het wellicht nodig om te zorgen voor escalatie naar bijvoorbeeld het Veiligheidshuis. Door middel van triage wordt er bepaald waar de vraag thuis hoort en welke mate van gegevensverwerking, gegevensverstrekking en gegevensuitwisseling noodzakelijk is. Bij een eenvoudige en enkelvoudige vraag is de gegevensverwerking beperkt terwijl er bij een complexere vraag wellicht meer partijen betrokken zijn en er dus meer gegevens uitgewisseld worden.



Beheer en opslag gegevens

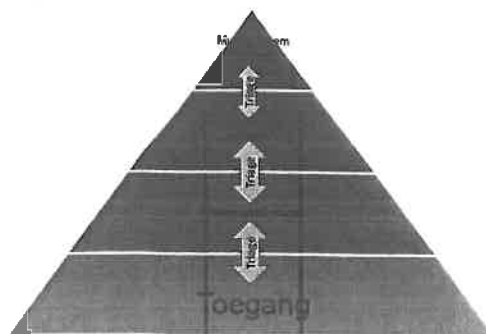
Triage draagt bij aan het zorgvuldig uitwisselen van informatie. Het is niet per definitie onwenselijk dat gegevens binnen en over verschillende domeinen en samenwerkingsverbanden worden gedeeld. Sterker nog, soms is dit juist noodzakelijk voor een adequate hulpverlening richting de inwoner en dus in het belang van de inwoner.

- **Noodzaak:** In het triageproces wordt er een besluit genomen over de route van de casus en wordt het doel bepaald waarvoor informatiedelen noodzakelijk is.
- **Proportionaliteit:** De inbreuk op de belangen van de bij de verwerking van persoonsgegevens van de betrokkene mogen niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel.
- **Subsidiariteit:** Het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid is. Dat het niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene mindere nadelige wijze kan worden verwezenlijkt.

Het is van belang om de afweging vast te leggen. Zo is het voor de inwoner ook inzichtelijk te maken wat er met zijn/haar gegevens is gebeurd en waarom. Er zijn drie triagemomenten binnen de gemeente Oudewater te onderscheiden:

1. Intake en vraagverheldering

Als een inwoner zich bij Welzijn Oudewater (zie notitie 'Integrale Toegang sociaal domein Oudewater voor uitgebreide informatie) meldt met een verzoek tot ondersteuning zal de gemeente zich in eerste instantie een beeld willen vormen van de situatie van de inwoner.



Een dilemma hierbij is om in het kader van de intake 'breed' genoeg te kijken, maar hoe breed is breed genoeg? De beoogde oplossing is om de intake vragen (middels een boomstructuur) zo te formuleren dat alleen datgene boven tafel komt wat strikt nodig is om een goed beeld te krijgen van de zorgvraag (en dus de benodigde persoonsgegevens). Daarnaast wordt ook de professionaliteit van de consultant meegewogen bij het doorvragen.

2. Selecteren en routeren van meervoudige en/of complexe vragen

Wanneer er het vermoeden bestaat dat er sprake is van een meervoudige of complexe vraag vindt er een tweede triagemoment plaats. Dit wil zeggen dat er meerdere partijen betrokken zijn bij de casus en dat de hulpvragen zich afspelen op meerdere leefgebieden. Uitgaande van de hulpvraag van de inwoner (en/of de signalen over de inwoner) kan het noodzakelijk zijn om breder te kijken en meer gegevens te verzamelen/in te zien/te verstrekken.

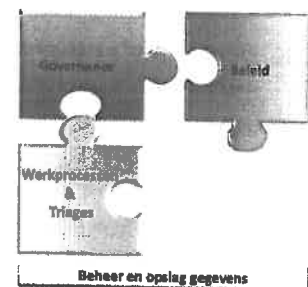
In het geval van een complexe casus kan er specifieke expertise geraadpleegd worden door het sociaal stadsteam. In dit triage moment wordt een duidelijke afweging gemaakt over de noodzaak, proportionaliteit en subsidiariteit ten aanzien van het verwerken van de gegevens van de inwoner. Naar de inwoner dient transparant gecommuniceerd te worden wat er met zijn/haar gegevens gebeurt en waarom. Het triagebesluit dient vastgelegd te worden. Het besluit is inclusief de route van de vraag, afweging en juridische grondslag om persoonsgegevens te verwerken/delen. Hierdoor wordt de professionele afweging expliciet gemaakt en wordt er een dossier gemaakt als onderbouwing van de gemaakte afweging.

3. Escalatie

Wanneer er meerdere partijen uit het zorgdomein, alsmede partners uit de justitieketen betrokken zijn bij een casus en/of als er sprake is van casuïstiek van meerdere personen uit één gezin, dan is er sprake van een complexe multiprobleemcasus. In dit geval kan er geëscaleerd worden naar de tot daartoe bevoegde instanties. Naar de inwoner dient transparant gecommuniceerd te worden wat er met zijn/haar gegevens gebeurt en waarom. Het triagebesluit dient vastgelegd te worden. Het besluit is inclusief de routing van de vraag, de afweging en juridische grondslag om persoonsgegevens te verwerken/delen. Hierdoor wordt de professionele afweging expliciet gemaakt en wordt er een dossier gemaakt als onderbouwing van de gemaakte afweging.

4. Voor het uitvoeren van wettelijke taken is de gemeente gerechtigd gegevens te verzamelen voor de noodzakelijke uitvoer.

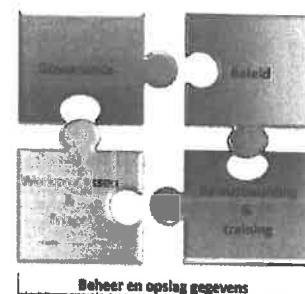
Op grond van de Wbp mogen persoonsgegevens alleen verzameld worden als daarvoor een doel bestaat. Dit doel moet welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn. Ook moet steeds nagegaan worden of het verwerken van persoonsgegevens noodzakelijk is voor het doel. Voor de uitvoering van diverse wetten (denk aan Wet op de ruimtelijke ordening (Wro) en de Wet werk en bijstand (Wwb)) zal in de betreffende wet dikwijls zijn aangegeven welke persoonsgegevens nodig zijn en dus verwerkt mogen worden. Daar waar over verwerking van persoonsgegevens in bijzondere wetgeving niets is geregeld, geldt dus het strikte regime van de Wbp.



De gemeente Oudewater en Welzijn Oudewater verzamelt en verwerkt heel veel soorten persoonsgegevens in het kader van de uitvoering van allerlei wet- en regelgeving. In het merendeel van de gevallen worden deze gegevens door de betrokkene verstrekt. Soms zijn de gegevens afkomstig van derden, bijvoorbeeld van uitkeringsinstanties. De persoonsgegevens betreffen naam, adres, woonplaats en dergelijke, maar soms ook inkomensgegevens, medische gegevens of gegevens over de gezinssamenstelling. De gegevensverwerking moet in overeenstemming zijn met de Wbp. Sommige wetten hebben voorrang op de Wbp en bevatten een aantal specifieke bepalingen over gegevensverwerking. In afdeling 7.5 van boek 7 van het Burgerlijk Wetboek (de overeenkomst inzake geneeskundige behandeling) is bijvoorbeeld een speciale regeling opgenomen over (onder meer) inzage in medische dossiers.

5. De informatiebeveiliging is georganiseerd binnen de gemeente.

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van de organisatie processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Het begrip 'informatiebeveiliging' heeft betrekking op: *beschikbaarheid / continuïteit*: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers; *exclusiviteit / vertrouwelijkheid*: het beschermen van informatie tegen



kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn; *integriteit / betrouwbaarheid*: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Informatie is één van de belangrijkste bedrijfsmiddelen van een organisatie. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een organisatie, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan inwoners en raadsleden en die met minimale middelen maximale resultaten behaalt. De bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekort schietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn: clean desk policy, hoe om te gaan met mobiele devices en aanwijzingen voor telewerken.

Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: GBA, SUWI, BAG en PUN, maar ook de archiefwet. Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

→ De gemeente Oudewater stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

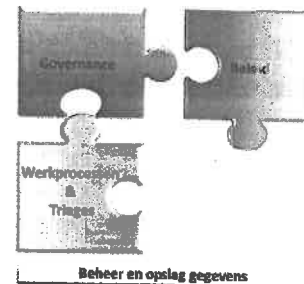
De volgende uitgangspunten op het gebied van informatiebeveiliging zijn ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). *Hierbij moet juridisch onderzocht worden wat van toepassing is op de relatie gemeente Oudewater en Welzijn Oudewater.*

1. Alle informatie en informatiesystemen zijn van kritiek en vitaal belang voor de organisatie. De verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management, met het **College van B&W als eindverantwoordelijke**. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. Door **periodieke controle, organisatie brede planning én coördinatie** wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
3. Informatiebeveiliging is een **continu verbeterproces**. 'Plan, do, check en act' vormen samen het **management systeem** van informatiebeveiliging.
4. De **informatiebeveiligingsfunctionaris/Chief Information Security Officer (CISO)** ondersteunt vanuit een **onafhankelijke positie** de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.
5. De organisatie stelt de benodigde **mensen en middelen beschikbaar** om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze gesteld in dit beleid.

6. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en **vastgesteld**. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht waar nodig gegevens en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

6. Er gaat stuurinformatie ingewonnen worden met in achtname van de privacy

Stuurinformatie kan vanuit verschillende perspectieven (inwoner, aanbieders organisaties en gemeenten) bekeken en ingericht worden. Het is bijvoorbeeld belangrijk om de effectiviteit van beleid in beeld te krijgen en waar nodig doelen bij te stellen en beleid te herijken. De informatie wordt gegenereerd uit de operationele bestanden, waarin de gegevens van de klanten in het sociaal domein zijn opgeslagen



De toepassing van stuurinformatie mag niet ten koste gaan van de privacy van de inwoners. Dat betekent dat deze informatie niet te herleiden mag zijn tot individueel natuurlijke personen. Om dat te bewerkstelligen is het nodig dit uitgangspunt vanaf het begin van de ontwikkelingen in het oog te houden, en niet achteraf toe te passen. "Privacy bij design" is daarbij een belangrijk hulpmiddel. Privacy by Design gaat uit van het principe dat er in een vroeg stadium nagedacht wordt over het gebruik van persoonsgegevens, de noodzaak van het gebruik van deze gegevens en de bescherming ervan. Privacy by design wordt toegepast zowel bij de inrichting van de uitvoeringsprocessen als bij de ontwikkeling van stuurinformatie.

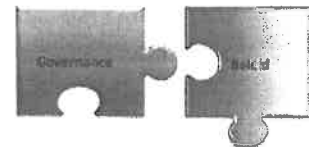
Voor wat betreft de inrichting van de uitvoeringsprocessen geldt de Wbp als uitgangspunt. In het kader van de uitvoering van de Wbp beschikt de gemeente Woerden over een register van alle processen waarin persoonsgegevens worden verwerkt. Van elk proces is daarin opgenomen voor welk doel, over welke personen, welke gegevens worden verwerkt en met wie gegevens wordt gedeeld. Elk proces is getoetst aan de Wbp en de privacyvoorschriften in de sectorale wetten die de gemeente uitvoert en indien noodzakelijk, gemeld bij het College bescherming persoonsgegevens (Cbp). In dat register zijn ook de processen van het sociaal domein opgenomen, zoals die tot eind 2014 worden uitgevoerd. De nieuwe taken in het sociaal domein betekenen eerst en vooral een uitbreiding van de bestaande processen met de nieuwe klanten voor WMO, Jeugdzorg en Werk en inkomen. Daarnaast zal integrale gevalsbehandeling als nieuw proces aan het register toegevoegd worden en gemeld worden bij het Cbp. Voor een deugdelijke toetsing aan de privacywetgeving is het nodig nadere invulling te krijgen op de inhoud van zowel de individuele processen als de integrale gevalsbehandeling.

De informatie die nodig is om een privacytoets uit te voeren betreft:

- Procesinrichting, deelnemers aan c.q. uitvoerders van het proces;
- Nieuwe categorieën van personen waarover gegevens worden verwerkt;
- Gegevensset te gebruiken per proces en integraal en herkomst van de gegevens (inwoner zelf of langs andere weg);

- Uitwisseling / deling van welke gegevens met wie;
- Gegevensopslag en bewaartermijnen;
- De verhouding gemeente / wijkteams: wie doet wat, wat is de reikwijdte van de dienstverlening door de wijkteams etc. in verband met de verantwoordelijkheidstoedeling;
- Convenanten / reglementen (met name bij integrale gevalbehandeling en deling gegevens met instanties/organisaties).

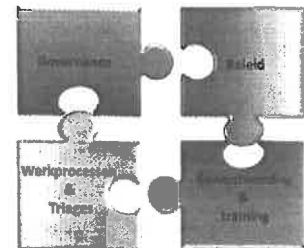
7. Bezwaar en de mogelijkheid voor het indienen van een klacht is georganiseerd binnen de gemeente.



De inwoner heeft het recht inzage te krijgen in de verwerking van zijn persoonsgegevens. Als deze gegevens onjuist zijn kan hij een verzoek indienen om de persoonsgegevens te wijzigen. Vindt de inwoner dat de gemeente Oudewater en/of Welzijn Oudewater de persoonsgegevens onjuist of ten onrechte registreert dan kan hij hierover een klacht indienen bij het College bescherming persoonsgegevens.

Voor bezwaar tegen een besluit van de gemeente en klachten over de behandelingen door (medewerkers van) de gemeente en/of Welzijn Oudewater bestaan de algemene bezwaar- en klachtenregelingen. *Hierbij moet juridisch onderzocht worden wat van toepassing is op de relatie gemeente Oudewater en Welzijn Oudewater.*

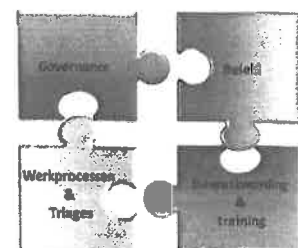
8. Er bestaat een gedragscode binnen de gemeente Oudewater en Welzijn Oudewater.



Een onderdeel van de gedragscode is om de medewerkers en de professionals in het sociaal domein te trainen over hoe zij met privacy vraagstukken om moeten gaan in hun functie en/of rol. De medewerkers en de professionals moeten zich bewust zijn van het belang van privacy en hoe zij persoonsgegevens op een zorgvuldige manier dienen te verwerken. Daarvoor worden er bijvoorbeeld een aantal aspecten/normen gegeven die als uitgangspunt dienen bij de verwerking van persoonsgegevens:

- Medewerkers gaan zorgvuldig om met privacygevoelige informatie. Dat geldt zowel voor informatie op het bureau, in kasten, dossiers, het mee naar huis nemen enz.
- Medewerkers waarborgen dat persoonlijke informatie niet ter beschikking komt aan derden.
- In email, collegenota's en andere beleidsstukken zo mogelijk werken met geanonimiseerde gegevens; alleen namen noemen indien dat absoluut noodzakelijk is.
- Medewerkers laten geen documenten met privacygevoelige informatie onbeheerd/onbeschermd achter (clean-deskpolicy).

9. Er wordt breed gecommuniceerd met de inwoner wat het privacybeleid is.



→ Er gaat op een transparante manier richting de inwoner gecommuniceerd worden over het privacybeleid van de gemeente. De inwoner dient op de

hoogte te zijn van zijn rechten omtrent de verwerking van zijn persoonsgegevens, zoals o.a. inzage, recht op correctie en recht op verzet. De gemeente Oudewater en/of Welzijn Oudewater gaat communiceren met de inwoner hoe zij aanspraak kunnen maken op dit recht door middel van inzage, bezwaar- en klacht procedures.

10. Er worden privacy convenanten met dienstverleners afgesloten waarmee de gemeente een contract heeft.

De gemeente Oudewater en/of Welzijn Oudewater gaat privacyconvenanten afsluiten met de dienstverleners met wie vanaf 1 januari 2015 persoonsgegevens gedeeld gaan worden. Dit convenant beschrijft het doel, de hoeveelheid en de soort informatie die gedeeld wordt. Het geeft daarnaast inzicht in de grondslagen (bijvoorbeeld, publiekrechtelijke taak van één van de convenantpartners, 'vitaal belang' van de betrokken inwoner, 'conflict van plichten') voor het verwerken van gegevens, maar ook in de verantwoordelijkheid voor gegevensverwerking en zaken als inzage en bewaartermijnen. *Hierbij moet juridisch onderzocht worden wat van toepassing is op de relatie gemeente Oudewater en Welzijn Oudewater.*

