PRIVACYBELEID 2016

Voor de gemeenten Tubbergen, Dinkelland en het
Openbaar lichaam Noaberkracht Dinkelland Tubbergen

INHOUDSOPGAVE

1. Uitgangspunten van beleid

Algemeen

De gemeenten Dinkelland en Tubbergen hebben gekozen voor één ambtelijke organisatie. Daartoe hebben de colleges van burgemeester en wethouders van beide gemeenten het openbaar lichaam - nu: de bedrijfsvoeringsorganisatie – Noaberkracht Dinkelland opgericht. Het bestuur van de bedrijfsvoeringsorganisatie bestaat uit de voltallige colleges van beide gemeenten. De medewerkers zijn formeel in dienst van Noaberkracht maar zijn materieel nog steeds ondergeschikt aan de beide colleges. De bedrijfsvoeringsorganisatie voert namens de beide colleges het beleid uit, zoals dat door de beide colleges is vastgesteld en waarvoor elk van beide colleges zich dient te verantwoorden jegens zijn eigen raad en zijn eigen burgers.

Hieruit volgt dat elk van beide colleges bevoegd is om het privacybeleid voor zijn eigen gemeente vast te stellen en dat het gehouden is daarvoor verantwoording af te leggen aan zijn gemeenteraad. Noaberkracht dient dit beleid uit te voeren. Noaberkracht heeft formeel rechtspersoonlijkheid en is dus bevoegd om extern op eigen naam op te treden. Maar de organisatie is ook een verlengstuk van elk van beide gemeenten, bestuurd door en ondergeschikt aan de beide colleges. Ook voor de uitvoering door Noaberkracht van het gemeentelijk vastgestelde beleid is het college van elk van beide gemeenten verantwoording verschuldigd aan zijn gemeenteraad.

Voor het Sociaal Domein hebben de colleges van Dinkelland en Tubbergen onlangs de uitgangspunten inzake privacy vastgesteld. Deze uitgangspunten sluiten direct aan op de in dit document genoemde algemene uitgangspunten. Het is goed om voor een zo belangrijk domein waar veel persoonlijke en ook gevoelige gegevens worden verwerkt specifiek aandacht te besteden aan de privacykaders.

De toepassing en uitvoering van de wettelijke privacykaders is in het algemeen gesproken complex van aard. De Wet bescherming persoonsgegevens (Wbp) biedt het algemeen kader en bevat open normen die in de praktijk invulling behoeven. Het onderwerp privacy is nogal eens voorwerp van discussie en wordt vaak als sta in de weg ervaren voor de verbetering van de dienstverlening en bedrijfsvoering.

De vraag die zich hier aandient is op welke manier geeft de organisatie uitvoering aan de privacywetgeving en wie is waarvoor verantwoordelijk? Anders gezegd, wie beslist binnen de organisatie over de invulling van de normen en weegt af of het belang van de privacy en daarvoor te treffen maatregelen opweegt tegen ‘het organisatiebelang’. In feite gaat het dan over privacybeleid.

Voor dat beleid gelden de volgende kaders en uitgangspunten:

1. Burgers hoeven de over hen bij de overheid bekende en beschikbare gegevens niet steeds opnieuw verstrekken.

2. Tenzij de wet anders bepaalt, bepalen burgers zelf in hoeverre zij hen de betreffende informatie willen vrijgeven. Burgers beschikken immers over het grondwettelijk recht op privacy, waaronder het recht op informationele privacy, wat inhoudt dat zij bepalen in hoeverre zij hen de betreffende informatie willen vrijgeven.

3. De persoonsinformatiehuishouding is deugdelijk. Dit geldt bij de dienstverlening en bedrijfsvoering als randvoorwaarde.

4. De naleving van wet- en regelgeving op het gebied van de privacybescherming is uitgangspunt van handelen bij de uitvoering van primaire processen en bedrijfsvoering. Privacybescherming wordt opgevat als een kenmerk van goede dienstverlening / kwaliteit.

5. Het privacybeleid moet bestuur, directie, management en medewerkers handvatten bieden om die ruimte zoveel als mogelijk concreet in te vullen. De Wbp gaat immers uit van zelfregulering en laat ruimte tot interpretatie.

6. Privacyafspraken binnen Noaberkracht dienen zoveel als mogelijk uniform in de organisatie te worden toegepast, waardoor cliënten niet tegen verschillen in de uitvoering kunnen aanlopen.

2. Beleid gebruik van persoonsgegevens algemeen

2.1 Organisatorische beleidsaspecten

1. Elke medewerker die persoonsgegevens nodig heeft voor de uitvoering van diens taak of taken, moet daarover op zo efficiënt mogelijke wijze kunnen beschikken.

2. Voor zover een algemeen gegeven (basisgegeven) over een persoon beschikbaar is in één van de basisregistraties, gebruikt de medewerker dat gegeven tenzij dat gegeven onjuist is.

3. Het takenpakket van een medewerker is bepalend voor de set aan gegevens waarover een medewerker mag beschikken evenals de wijze waarop deze gegevens ter beschikking worden gesteld.

4. Een afdelingshoofd dan wel een programmamanager is uit oogpunt van privacybescherming verantwoordelijk voor en beslist over de vaststelling van de inhoud van de gegevensset behorende bij het takenpakket van een medewerker. Een afdelingshoofd/programmamanager neemt daarbij de wettelijke uitgangspunten in acht met betrekking tot:

    a. doelbinding: gegevens worden uitsluitend voor een vooraf bepaald gerechtvaardigd doel gebruikt;

    b. proportionaliteit: er worden niet meer gegevens gebruikt dan noodzakelijk is;

    c. subsidiariteit: kan het doel zonder persoonsgegevens worden bereikt, dan heeft dat de voorkeur.

5. De afdelingshoofd dan wel de programmamanager beslist over privacyvraagstukken binnen zijn afdeling. De medewerkers hebben taken, die ze moeten uitvoeren met inachtneming van de privacyregels. Privacy is onderdeel van het werk. Bij problemen beslist het afdelingshoofd dan wel de programmamanager

6. De directie beslist over privacyvraagstukken die afdeling overstijgend zijn.

7. Bij nieuw uit te voeren processen waarbij de verwerking van persoonsgegevens, waaronder bijzondere persoonsgegevens, qua inhoud en omvang complex is en van substantieel belang is voor de uitvoering van het proces, maakt een privacy impact assessment deel uit van implementatieproces. Een privacy impact assessment[1] heeft als doel bij nieuwe werkzaamheden na te gaan wat dit betekent voor de bescherming van de persoonsgegevens. Dit is een wettelijke verplichting vanaf 1 juli 2018.

[1] Een **Privacy Impact Assessment** (**PIA**) is een onderzoek dat zich richt op de mogelijke **impact** op de **privacy** in gevallen waarin verwerkingen van persoonsgegevens betrokken zijn.

8. Bij het ontwerpen en beschrijven van werkprocessen wordt aandacht besteed aan zogenaamde ‘triage-momenten’. Dit zijn momenten in het proces waarbij persoonsgegevens uitgewisseld kunnen worden met derden. In beeld wordt gebracht op welke momenten er aandacht moet zijn voor privacyissues en wie hierover beslist. Binnen het sociaal domein geldt als uitgangspunt dat een uitwisseling van gegevens met derden altijd pas na zo’n triagemoment mag plaatsvinden.

Er is een informatiebeveiligingscoördinator/ CISO (chief information security officer). De informatiebeveiligingscoördinator/ CISO draagt, op basis van de Baseline Informatiebeveiliging Gemeenten (BIG), zorg voor een samenhangend pakket van maatregelen ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie.

De CISO

- is verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid van de organisatie;
- treedt op als informatiebeveiligingsadviseur (voor het management) bij nieuwe ICT-voorzieningen en bij ingrijpende veranderingen in de ICT-infrastructuur. Bijvoorbeeld binnen ontwikkelingen als het sociaal domein, flexibel werken, iBurgerlijke Stand, referentiearchitectuur;
- adviseert het (lijn)management bij de uitwerking van het informatiebeveiligingsbeleid in informatiebeveiligingsplannen en bij de implementatie hiervan;
- initieert periodieke beveiligingsaudits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses en/of voert deze uit;
- zet (periodieke) informatiebeveiligingsbewustzijnsprogramma’’s op en adviseert hierover.
- coördineert en adviseert bij beveiligingsincidenten en treedt zo nodig op bij calamiteiten;
- blijft op de hoogte van ontwikkelingen op het gebied van informatiebeveiliging. Je komt waar nodig met voorstellen voor aanvullingen of verbeteringen van producten, methodieken of werkwijzen;
- geeft voorlichting en training over het correct omgaan met informatie(systemen);
- is het aanspreekpunt voor iedereen binnen de organisatie als het gaat om informatiebeveiliging;
- leidt projecten die als doel hebben (organisatorische en technische) beveiligingsmaatregelen te implementeren of de kwaliteit van de beveiliging op langere termijn te handhaven en waar nodig te verbeteren;
- controleert de werking en naleving van het informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen;
- rapporteert periodiek aan het bestuur over beveiligingsincidenten en de afhandeling daarvan;
- vertegenwoordigt Noaberkracht in externe overleggen.

9. Er is de functie van privacyfunctionaris. De functie van privacyfunctionaris is ondergebracht bij de concernjuristen van Noaberkracht. die teammanagers, afdelingshoofden, programmamanagers en directie gevraagd en ongevraagd van advies dient met betrekking tot de Wbp en de bescherming van de persoonlijke levenssfeer van degenen van wie in de organisatie van Noaberkracht persoonsgegevens worden verwerkt (zie bijlage 1 voor inhoud, taken en verantwoordelijkheden).

10. De privacyfunctionaris wordt betrokken bij de aanschaf en of ontwikkeling van informatiesystemen.

11. De privacyfunctionaris toetst wijzigingen in de wijze waarop uitvoering wordt gegeven aan primaire en bedrijfs-voeringprocessen met al dan niet volledige organisatiebrede consequenties aan de privacywetgeving. Wijzigingen kunnen immers van invloed zijn op de manier waarop met persoonsgegevens wordt omgegaan, bijvoorbeeld thuis werken, BYOD (bring your own device) en uitbesteding van werk aan een derde partij, gegevensdeling in het sociaal domein.

12. Bij uitbesteding van werkzaamheden aan derden, waarvan verwerking van persoonsgegevens deel uitmaakt, zorgt Noaberkracht er voor dat de beveiliging van persoonsgegevens wordt geregeld in een tussen partijen overeen te komen bewerkersovereenkomst. Noaberkracht hanteert daarbij zo veel mogelijk het model, opgenomen in bijlage 2 (artikel 14 Wbp).

2.2 Inhoudelijke beleidsaspecten

1. *Rechtmatige verwerking (artikel 6 Wbp)*

   Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

2. *Doelbinding (artikel 7 Wbp)*

   GR Noaberkracht verzamelt persoonsgegevens alleen voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel en verstrekt deze gegevens alleen voor zover dat binnen het doel is toegestaan. Afwijkend gebruik is slechts mogelijk na afweging van de wettelijke criteria.

3. *Rechtmatige grondslag (artikel 8 Wbp)*

   De verwerking van persoonsgegevens dient gebaseerd te zijn op een van de grondslagen als bedoeld in artikel 8 Wbp.

4. *Proportionaliteit*

   Noaberkracht verwerkt alleen die gegevens die noodzakelijk om het doel waarvoor ze nodig zijn te bereiken. De gegevensverwerking moet toereikend, ter zake

dienend en niet bovenmatig zijn. Noaberkracht hanteert daarbij de regel ‘need to know’ in plaats van ‘nice to know’.

5. *Bewaartermijnen*

   Noaberkracht bewaart gegevens volgens de wettelijk geldende termijnen of anders altijd zo kort mogelijk en ‘vernietigt’ deze daarna. De bewaartermijnen van de gegevens lopen uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Daar waar er geen wettelijke regeling is die voorziet in een verplichte bewaartermijn, kunnen de colleges een besluit over de bewaartermijn nemen. Deze zal zo kort mogelijk zijn.

6. *De verwerking van bijzondere gegevens binnen de organisatie*

   Bijzondere gegevens zijn onder andere gegevens betreffende de gezondheid, ras, etniciteit, seksuele leven en strafrecht. Noaberkracht verwerkt bijzondere gegevens alleen in de gevallen waarin die verwerking in een wet is voorzien of met ondubbelzinnige toestemming van degene wiens gegevens het betreft (betrokkene). Medewerkers gaan terughoudend om met deze in privacytechnisch opzicht gevoelige gegevens van burgers en worden daarover geïnstrueerd door de privacyfunctionarissen.

7. *Verstrekken van persoonsgegevens*

   Noaberkracht gaat terughoudend om met het verstrekken van persoonsgegevens binnen haar eigen organisatie en daarbuiten (aan samenwerkende instanties of derden). Persoonsgegevens worden zowel intern als extern alleen verstrekt (gedeeld) voor zover dat noodzakelijk is voor de taakuitvoering.

8. *Verstrekken van bijzondere gegevens omtrent de gezondheid*

   Voor het verstrekken van bijzondere gegevens omtrent de gezondheid gelden de volgende uitgangspunten.

   a. Het verstrekken van bijzondere gegevens omtrent de gezondheid binnen de organisatie is slechts mogelijk voor zover de wet daarin voorziet of met de ondubbelzinnige toestemming van de betrokkene.

   b. Indien de wet niet in de verstrekkingsmogelijkheid voorziet en betrokkene geeft geen toestemming, mag medische informatie alleen gedeeld worden in het uitzonderlijke geval van een evident belang van de betrokkene of een ander. Van een evident belang is bijvoorbeeld sprake als er ernstig gevaar voor de gezondheid van betrokkene of een ander is of de vrees daarvoor. De hulpverlener moet die afweging maken tussen de verschillende belangen: het belang van de cliënt dat het geheim bewaard blijft tegen het evidente belang. Van een evident belang zal in het geval van gegevensuitwisseling met een niet-hulpverlenende instantie niet snel sprake zijn.

9. *Meldingen van gegevensverwerkingen*

   Verwerkingen van persoonsgegevens meldt de privacyfunctionaris namens Noaberkracht bij de Autoriteit Persoonsgegevens, tenzij de verwerking is vrijgesteld van de melding op grond van het Vrijstellingsbesluit. Bij twijfel over de toepassing van het vrijstellingsbesluit wordt gemeld.

10. *Transparantie*

    De Wbp heeft als mede als doel om het verwerken van persoonsgegevens transparant te maken voor betrokkenen. Noaberkracht geeft de transparantie vorm door een openbaar register van alle verwerkingen van persoonsgegevens bij te houden dat voor een ieder raadpleegbaar is.

11. *Informatieplicht (artikelen 33 en 34 Wbp)*

    Noaberkracht informeert een betrokkene over het feit dat diens persoonsgegevens worden verwerkt, tenzij betrokkene daarvan op de hoogte is bijvoorbeeld omdat betrokken ze zelf heeft verstrekt in de hoedanigheid van aanvrager van een dienst (vergunning of uitkering). In uitzonderingsgevallen blijft de informatieplicht (tijdelijk) achterwege, bijvoorbeeld in verband met fraudeonderzoeken of in het kader van openbare orde en veiligheidsbeleid.

12. *Inzage en correctie (artikel 35 tot en met 39 Wbp)*

    Betrokkenen hebben het wettelijk recht op inzage en correctie met betrekking tot de over hen verwerkte persoonsgegevens.

13. *Wet Meldplicht Datalekken (artikel 34a Wbp)*

    Beveiligingsincidenten worden conform de Procedure Incidentmeldingen gemeld aan de CISO die in overleg met de privacyfunctionarissen een afweging maakt inzake de meldplicht aan de Autoriteit Persoonsgegevens.

14. *Specifieke beleidsterreinen*

    Het kan zijn dat het voor specifieke beleidsterreinen nodig is nadere beleidsafspraken te maken omtrent de wijze waarop wordt omgegaan met de verwerking van persoonsgegevens. We zien dit bijvoorbeeld terugkomen binnen het Sociaal Domein, waarvoor een eigen beleidskader is opgesteld inzake privacy dat is opgenomen als bijlage 3 van dit document. De privacyfunctionarissen dragen er zorg voor dat binnen dit beleid en de uitvoering er afstemming is met het algemene beleid. Afwijkingen van het algemene beleid dienen goed gemotiveerd te zijn.

3. Beleid gebruik persoonsgegevens uit de Basisregistratie personen

1. De verstrekking van persoonsgegevens uit de Basisregistratie personen en de wijze van verstrekking is gebaseerd op Wet Basisregistratie personen, Verordening gegevensverstrekking basisregistratie personen Noaberkracht 2014 en Autorisatiebesluit van de Minister van Binnenlandse Zaken d.d. 19 februari 2015, kenmerk 2015-0000030535 en opvolgende versies van dat besluit.

2. De gegevensuitwisseling tussen de Basisregistratie personen en de gebruikers van de Basisregistratie personen wordt vastgelegd in het register van gegevensverwerkingen. In het register zijn de volgende onderwerpen opgenomen:

    a. de inhoud van de taak of van de taken.

    b. de set aan gegevens die verstrekt wordt.

    c. de wijze van verstrekking: raadplegen (op persoonsniveau en/of op adresniveau) en/of mutatieberichten en/of selecties en/of koppelingen.

    d. additionele voorwaarden in het geval de gebruiker werkzaamheden laat uitvoeren door een derde waarbij persoonsgegevens uit de Basisregistratie personen nodig zijn.

    e. de aard en omvang van de verplichting tot terugmelding bij gerede twijfel over de juistheid van de gegevens uit de Basisregistratie personen.

3. Uitbreiding van de gegevensset van een medewerker, buiten de kaders van de regels als genoemd onder 1 is slechts mogelijk, indien door het ontbreken van een gegeven diens taak niet naar behoren is uit te voeren.

4. Tot het indienen van een gemotiveerd verzoek bij afdeligshoofd tot uitbreiding van de gegevensset als bedoeld onder 3 is bevoegd het hoofd van de afdeling waarbij de medewerker werkzaam is. Het afdelingshoofd vergewist zich of de uitbreiding van de gegevensset voor de uitvoering van de taak noodzakelijk is en niet in strijd is met de Wbp.

5. Bij onzekerheid over de uitleg van de privacywetgeving of vermoeden van strijd met deze wetgeving, legt het afdelingshoofd het verzoek, voorzien van een advies van de privacyfunctionaris ter besluitvorming voor aan de directie.

6. De directie neemt een beslissing over het verzoek. In het geval van bestuurlijke of politieke gevoeligheid, besluit het bestuursorgaan dat is aan te merken als de verantwoordelijke voor de verwerking van persoonsgegevens.

4. PRIVACYBELEID IN DE PRAKTIJK

Algemene paragraaf

Het opstellen van een privacybeleid en vaststellen van uitgangspunten is meestal een goed begin voor een goede uitvoering. Van groter belang is echter het toezien op die uitvoering en het ervoor zorgdragen dat de organisatie ‘in control’ is waar het gaat de uitvoering van dit beleid. Om dit te bereiken is het nodige om een goede governance-structuur te hebben als ook dat er (blijvend) aandacht is voor goede opleiding, trainingen dan wel werken aan de bewustzijn van de medewerkers op de werkvloer voor wat betreft de aandacht voor privacyvraagstukken.

In dit hoofdstuk willen we hier kort op ingaan. Kort, omdat het hier meer neerkomt op het doen dan het erover schrijven.

Governance

Voor de organisatie moet worden vastgelegd welke taken en bevoegdheden bepaalde functionarissen hebben bij de verwerking van persoonsgegevens en aan wie zij verantwoording afleggen.

Voor het opstellen van deze governance-structuur is aansluiting gezocht bij de inrichting van de Baseline Informatiebeveiliging Gemeenten zoals dit binnen de organisatie thans ook vorm wordt gegeven.

In bijlage 1 van dit document zijn de taken, verantwoordelijkheden en bevoegdheden alsook de verantwoordingsstructuur verder in beeld gebracht.

Opleidingen/training en bewustzijn

Voor wat betreft opleiding/training en bewustzijn van de privacyuitgangspunten binnen de organisatie stellen wij de volgende concrete acties voor:

Privacyfunctionarissen

Zoals gezegd worden de taken van de privacyfunctionarissen belegd bij de concernjuristen. Zij dragen er samen met hun afdelingshoofd zorg voor dat zij ten alle tijden voldoende geschoold zijn op het onderdeel privacy. Middels de jaarlijkse functioneringsgesprekken bespreken zij of dit nog aan de orde is en indien nodig worden extra cursussen, opleidingen en trainingen gevolgd.

Medewerkers

Alle medewerkers hebben vanuit hun eigen taakgebied en verantwoordelijkheid de taak om goed om te gaan met persoonsgegevens conform dit privacybeleid. Dit betekent nog niet dat zij altijd tot op detail op de hoogte kunnen zijn van de ins en outs rond privacyvraagstukken. Het is dan ook van belang dat zij zich bewust zijn van het

voorliggende privacybeleid en dat zij regelmatig met elkaar en de privacyfunctionarissen spreken over dit thema. De volgende acties worden dan ook ondernomen:

- Verspreiding ‘do’s en don’ts’ inzake privacybeleid. Zie bijlage 4. Dit document zal breed verspreid worden binnen de organisatie.
- Privacyfunctionarissen wonen minimaal 2 keer per jaar werkoverleggen bij om met de medewerkers te spreken over privacythema’s. Dit qua inhoud gaan over:
    - Bespreken van de ‘do’s en don’ts’
    - Actuele problematieken (casusbesprekingen)
    - Uitwisseling persoonsgegevens met derden
    - Wet meldplicht datalekken
    - Verantwoording richting gemeentebestuur over privacythema’s

Voor de goede orde: het management en niet de privacyfunctionarissen is aanspreekbaar zijn op de juiste uitvoering van deze acties.

Communicatie met de burger

Transparantie is een belangrijk uitgangspunt voor de uitvoering van de Wet bescherming persoonsgegevens. De burger zal via de website van de gemeenten worden geïnformeerd over:

- Het privacybeleid
- De verwerkingen van persoonsgegevens en hoe het register van verwerkingen van persoonsgegevens kan worden ingezien
- De wijze waarop de burger zijn rechten (inzage, correctie, verzet) kan uitoefenen

Bijlagen

BIJLAGE 1: PRIVACYBEHEER, TAKEN, VERANTWOORDELIJKHEDEN EN BEVOEGDHEDEN

1. De privacyfunctionaris (i.c. de concernjuristen) toetst de verwerking van persoonsgegevens aan de kaders van de privacywetgeving en adviseert gemeentesecretaris, afdelings- en teammanagers bij wijzigingen in procesuitvoering en bedrijfsvoering en de toepassing van een privacy impact assessment.

2. De privacyfunctionaris neemt als adviserend lid deel aan programma's (zoals bijvoorbeeld verbetering dienstverlening) en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens.

3. De privacyfunctionaris heeft verder als taak

   a. de uitleg van de privacyvoorschriften in de Wet bescherming persoonsgegevens en in de sectorale wetgeving, zoals bijvoorbeeld de Wet maatschappelijke ondersteuning en de Participatiewet;

   b. onderhouden van het privacybeleid;

   c. coördineren van de privacywerkzaamheden;

   d. beheren en openbaar maken van het overzicht van gegevensverwerkingen van de gemeenschappelijke regeling Noaberkracht. Dit overzicht bevat mede informatie over de bewaartermijnen de bewerkerscontracten/convenanten;

   e. verzorgen van meldingen en intrekkingen van meldingen van gegevensverwerkingen bij de Autoriteit Persoonsgegevens;

   f. te fungeren als aanspreekpunt voor de Autoriteit Persoonsgegevens;

   g. coördineren van verzoeken om inzage, correctie en verzet en adviseren over de afhandeling;

   h. jaarlijks te rapporteren aan het bestuur;

   i. richt in overleg met de beveiligingsfunctionaris/CISO procedures in voor het melden van datalekken waarbij persoonsgegevens betrokken zijn;

   j. ziet toe op een actieve voorlichting richting de organisatie door middel van "do's en don'ts" lijstjes en het bespreekbaar maken daarvan.

BIJLAGE 2: MODEL BEWERKERSOVEREENKOMST

Model Bewerkersovereenkomst gemeente *Gemeentenaam* – Bewerker <NAAM>

(*Gemeentenaam* 2015)

Ondergetekenden:

De gemeente *Gemeentenaam,* gevestigd aan <adres>, rechtsgeldig vertegenwoordigd door haar burgemeester,

hierna verder aangeduid als: "**de verantwoordelijke**",

en

<naam organisatie> gevestigd aan <adres/woonplaats>, rechtsgeldig vertegenwoordigd door de heer/mevrouw <naam, functie>,

hierna verder aangeduid als: "**de bewerker**",

verklaren te zijn overeengekomen een bewerkersovereenkomst als bedoeld in artikel 14, tweede lid, van de Wbp, tussen de gemeente *Gemeentenaam,* nader te noemen de verantwoordelijke en <naam organisatie>, nader te benoemen de bewerker.

Definities

Artikel 1.

1.1 bijlagen: aanhangsels bij deze overeenkomst die, na door beide partijen te zijn geparafeerd, deel uitmaken van deze overeenkomst.

1.2 verwerking van gegevens of het verwerken van gegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bewerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens.

1.3 bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

1.4 verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

1.5 bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

1.6 betrokkene: degene op wie een persoonsgegeven betrekking heeft.

1.7 derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken.

1.8 verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van persoonsgegevens.

1.9 datalek: een inbreuk op de beveiliging, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

1.10 de Autoriteit Persoonsgegevens: de toezichthouder als bedoeld in artikel 51 van de Wbp.

Ingangsdatum en duur

Artikel 2.

2.1 Deze overeenkomst gaat in op het moment van ondertekening en duurt voort zolang de bewerker de verantwoordelijke ter beschikking gestelde persoonsgegevens verwerkt.

Onderwerp van deze overeenkomst

Artikel 3.

3.1 De bewerker verwerkt persoonsgegevens in opdracht van de verantwoordelijke in het kader van de registratie van gegevens voor de uitvoering van werkzaamheden, zoals omschreven in de samenwerkingsovereenkomst tussen partijen d.d....., meer in het bijzonder: <omschrijving werkzaamheden>,

3.2 De bewerker verbindt zich om in het kader van die werkzaamheden de door de verantwoordelijke ter beschikking gestelde persoonsgegevens gegevens behoorlijk en zorgvuldig en in overeenstemming met de Wet bescherming persoonsgegevens (Wbp) te verwerken.

Naleving wet- en regelgeving

Artikel 4.

4.1 Het college van burgemeester en wethouders van de gemeente *Gemeentenaam* is verantwoordelijke in de zin van de Wbp.

4.2 De concernjuristen, werkzaam bij Noaberkracht Dinkelland Tubbergen, zijn in hun hoedanigheid als privacyfunctionaris aanspreekpunt voor de bewerker voor zover het betreft de uitvoering van deze overeenkomst.

4.3 De bewerker verwerkt gegevens ten behoeve van de verantwoordelijke, in overeenstemming met diens instructies.

4.4 De bewerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt onder deze overeenkomst komt nimmer bij de bewerker te berusten.

4.5 De bewerker handelt bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden in overeenstemming met de toepasselijke wet- en regelgeving betreffende de bescherming van persoonsgegevens. De bewerker verwerkt persoonsgegevens slechts voor zover dit volgt uit de samenwerkingsovereenkomst en zal alle redelijke instructies van de verantwoordelijke opvolgen, behoudens afwijkende wettelijke verplichtingen.

4.7 De bewerker zal, onverminderd het bepaalde in artikel 6.6., te allen tijde op eerste verzoek van de verantwoordelijke onmiddellijk kopie te verstrekken van – dan wel inzage te verlenen in - alle persoonsgegevens waarop deze overeenkomst betrekking heeft. 4.8 De bewerker zal, als deze overeenkomst overeenkomstig artikel 2.1 eindigt, alle van de verantwoordelijke afkomstige persoonsgegevens waarop deze bewerkersovereenkomst betrekking heeft terug overdragen aan de verantwoordelijke, zonder daarvan een kopie, afschrift of backup, in welke vorm dan ook, achter te houden. Dit geldt onverminderd het bepaalde in artikel 8.2.

4.9 De bewerker stelt de verantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Wbp, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet, alsmede de verplichtingen op grond van de Wet meldplicht datalekken.

Geheimhoudingsplicht

Artikel 5.

5.1 Personen in dienst van, dan wel werkzaam ten behoeve van de bewerker, evenals de bewerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt. De medewerkers van de bewerker tekenen hiertoe een geheimhoudingsverklaring.

5.2 Indien de bewerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de bewerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de bewerker de verantwoordelijke, voorafgaand aan de verstrekking, ter zake informeren, tenzij wettelijke bepalingen dit verbieden.

Beveiligingsverplichtingen door bewerker

Artikel 6.

6.1 De bewerker neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens die worden verwerkt ten dienste van de verantwoordelijke te beveiligen en beveiligd te houdentegen enige vorm van onrechtmatige verwerking.

6.2 Maatregelen als bedoeld in lid 1 houden ten minste voorzieningen in tegen:

a. beschadiging of verlies van persoonsgegevens;

b. onbevoegde wijziging van persoonsgegevens;

c. ontvreemding van persoonsgegevens;

d. kennisneming van persoonsgegevens door onbevoegden;

e. onnodige verdere verwerking en verzameling van persoonsgegevens.

6.3 De bewerker informeert de verantwoordelijke onverwijld over **alle** inbreuken op de beveiliging, waarvan hij kennis krijgt en verstrekt in dat verband alle informatie die hij heeft aan de verantwoordelijke. Ook in geval van twijfel over een dergelijke inbreuk, informeert de bewerker de verantwoordelijke. De bewerker doet zelf geen melding van een datalek bij de Autoriteit Persoonsgegevens.

6.4 De bewerker houdt de verantwoordelijke op de hoogte van nieuwe ontwikkelingen rond de inbreuk op de beveiliging en van de maatregelen die de bewerker treft om aan zijn kant de gevolgen van de inbreuk op de beveiliging te beperken en om herhaling te voorkomen.

6.5 Behoudens uitdrukkelijke schriftelijke toestemming van de verantwoordelijke is bewerker niet bevoegd tot verwerking en in het bijzonder opslag van de persoonsgegevens buiten Nederlands grondgebied noch bij een bedrijf waarvan de verwerking van persoonsgegevens mede onderhevig is aan de wettelijke regels van een land of gebiedsdeel buiten de Europese Unie.

6.6 De verantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te (doen) controleren. De bewerker is verplicht de verantwoordelijke of controlerende instantie in opdracht van verantwoordelijke toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden.

6.7 De verantwoordelijke zal de audit (laten) uitvoeren na een voorafgaande schriftelijke melding aan de bewerker.

6.8 De bewerker verbindt zich om binnen een door de verantwoordelijke te bepalen termijn de verantwoordelijke of de door de verantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie. Hierdoor kan de verantwoordelijke, of de door de verantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door de bewerker van deze overeenkomst. De verantwoordelijke, of de door de verantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.

6.9 Bewerker staat er voor in, de door de verantwoordelijke of ingeschakelde derde, aangegeven aanbevelingen ter verbetering binnen de daartoe door de verantwoordelijke te bepalen termijn uit te voeren.

6.10 De bewerker rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze overeenkomst.

Inschakeling derden

Artikel 7.

7.1 De bewerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande schriftelijke toestemming van de verantwoordelijke.

7.2 De verantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze bewerkersovereenkomst.

7.3 De bewerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze bewerkersovereenkomst.

Wijziging overeenkomst

Artikel 8.

8.1 Wijziging of beëindiging van deze overeenkomst kan slechts schriftelijk plaatsvinden.

8.2 Zodra de samenwerking is beëindigd, vernietigt bewerker de persoonsgegevens die hij van de verantwoordelijke heeft ontvangen, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen. Deze vernietiging moet, binnen nader overeen te komen termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt. Dit geldt onverminderd het bepaalde in artikel 4.8.

8.3 Elk van de partijen is gerechtigd de aan de verwerking ten grondslag liggende samenwerkingsovereenkomst op te zeggen in geval van overmacht, waaronder mede begrepen een zodanige wijziging van wettelijke regels dat een verdere voortzetting van de overeenkomst niet kan worden verlangd.

8.4 Opzegging als bedoeld in het vorige lid geschiedt schriftelijk. Bij het opzeggen van de overeenkomst, wordt de reden van opzegging vermeld, en treden partijen met elkaar in overleg over de wijze van afhandeling van de opzegging.

Aansprakelijkheid

Artikel 9.

9.1 Indien de bewerker tekortschiet in de nakoming van de verplichting uit deze overeenkomst kan verantwoordelijke hem in gebreke stellen. Bewerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de bewerker een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is bewerker in verzuim.

9.2 Bewerker is aansprakelijk voor alle schade of nadeel voortvloeiende uit het niet-nakomen van, of in strijd handelen met de bij of krachtens de Wbp gegeven voorschriften en/of het niet-nakomen van, of in strijd handelen met het in deze overeenkomst bepaalde. Onverminderd de aanspraken op grond van wettelijke regels. Bewerker is aansprakelijk voor schade of nadeel voor zover ontstaan door zijn werkzaamheid. Bewerker is tevens aansprakelijk voor alle schade of nadeel voortvloeiende uit de door zijn werkzaamheid ontstane inbreuken op de persoonlijke levenssfeer van betrokkenen. De aansprakelijkheid is beperkt tot maximaal € 2.500.000,-- per gebeurtenis.

Toepasselijk recht

Artikel 10.

10.1 Op deze overeenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.

Citeertitel

Artikel 11.

11.1 Deze overeenkomst kan worden aangehaald als 'Bewerkersovereenkomst uitvoering naam werkzaamheden.

Aldus in tweevoud opgesteld en getekend de dato

De gemeente *Gemeentenaam*, naam organisatie,

Naam en functie bevoegd tot ondertekening

BIJLAGE 3: PRIVACY IN HET SOCIAAL DOMEIN

Inleiding

Gemeenten zijn sinds dit jaar verantwoordelijk voor jeugdhulp, werk en inkomen en zorg aan langdurig zieken en ouderen. Een deel van deze taken hadden de gemeenten al, een deel daarvan hebben zij overgenomen van de Rijksoverheid. Dit staat bekend als de decentralisaties. De decentralisaties brengen met zich mee dat de gemeente, meer dan voorheen, aandacht moet geven aan een zorgvuldige verwerking van persoonsgegevens van inwoners met één of meerdere hulpvragen. Zowel de raad als het college hechten veel waarde aan het waarborgen van de privacy van inwoners in relatie tot deze gegevensverwerking.

De gemeenten zijn op dit moment volop bezig nieuwe werkwijzen te ontwikkelen om de dienstverlening in het sociaal domein zo effectief en efficiënt mogelijk te organiseren. Daarin maken zij keuzes. De gemeente wordt expliciet gevraagd om in te zetten op ontwikkeling en vernieuwing van werkwijzen om invulling te geven aan de maatschappelijke opgave die de gemeente heeft meegekregen, namelijk integrale dienstverlening én kostenbesparing. De gemeente heeft hierbij bewust beleidsvrijheid gekregen om de werkwijzen optimaal af te stemmen op de situatie van haar inwoners in de gemeente. Daarbij is het belangrijk om oog te hebben voor de borging van de privacy en ervoor te zorgen dat het borgen van de privacy deel uitmaakt van dit ontwikkelproces.

De gemeenten Dinkelland en Tubbergen hebben gekozen voor één ambtelijke organisatie. Daartoe hebben de colleges van burgemeester en wethouders van beide gemeenten het openbaar lichaam - nu: de bedrijfsvoeringsorganisatie – Noaberkracht Dinkelland opgericht. Aan de bedrijfsvoeringsorganisatie zijn geen bevoegdheden of beleidsbepalende taken toegekend. Het bestuur van de bedrijfsvoeringsorganisatie bestaat uit de voltallige colleges van beide gemeenten. De medewerkers zijn formeel in dienst van Noaberkracht maar zijn materieel nog steeds ondergeschikt aan de beide colleges. De bedrijfsvoeringsorganisatie voert namens de beide colleges het beleid uit, zoals dat door de beide colleges is vastgesteld en waarvoor elk van beide colleges zich dient te verantwoorden jegens zijn eigen raad en zijn eigen burgers.

Hieruit volgt dat elk van beide college bevoegd is om het privacybeleid voor zijn eigen gemeente vast te stellen en dat het gehouden is daarvoor verantwoording af te leggen aan zijn gemeenteraad. Noaberkracht dient dit beleid uit te voeren. Noaberkracht heeft formeel rechtspersoonlijkheid en is dus bevoegd om extern op eigen naam op te treden. Maar de organisatie is ook een verlengstuk van elk van beide gemeenten, bestuurd door en ondergeschikt aan de beide colleges. Niet slechts voor de vaststelling maar ook voor de uitvoering door Noaberkracht van het gemeentelijk vastgestelde beleid is het college van elk van beide gemeenten verantwoording verschuldigd aan zijn gemeenteraad.

Deze beleidsnota “Privacy in het sociaal domein” wordt door beide colleges, de colleges van Dinkelland en Tubbergen, gelijkluidend vastgesteld. Vanuit hun positie als medebestuurder van Noaberkracht, dragen beide colleges de verantwoording voor

de uitvoering van deze nota. De nota beoogt de kaders voor de omgang met persoonsgegevens in het sociaal domein inzichtelijk te maken en daar praktische invulling aan te geven. Onder sociaal domein verstaan we in dit verband het geheel van de gedecentraliseerde domeinen jeugdhulp, werk en inkomen en zorg aan langdurig zieken en ouderen.

Kader

a. Gegevensverwerking in het sociale domein

Voor het overgrote deel van de situaties waarin inwoners een beroep doen op de gemeente voor ondersteuning, geldt dat de dienstverlening zich afspeelt binnen één domein. Het gaat om dan om enkelvoudige problematiek. De wijze van gegevensverwerking binnen een domein is neergelegd in de algemene regelgeving over het verwerken van persoonsgegevens, voornamelijk de Wbp, en in de relevante sectorwetgeving.

Uitgangspunt van de decentralisaties is de betrokkenheid van de inwoner en zijn omgeving bij het tot stand komen van ondersteuning. Dit betekent dat ook de ondersteuning en de daarvoor noodzakelijke gegevensverwerking en gegevensuitwisseling in samenspraak met de betrokkene(n) dient plaats te vinden. Echter ook dan heeft de gemeente de plicht om terughoudend om te gaan met de uitvraag en registratie van persoonsgegevens. Zij is dan gehouden aan de in de Wbp vastgelegde criteria van doelbinding, noodzaak, subsidiariteit, proportionaliteit en doelmatigheid. Slechts in een zeer beperkt aantal gevallen zal de gemeente gegevens uitwisselen buiten de betrokkenheid en zonder samenspraak met de inwoner. In dergelijke situaties is er sprake van een noodzaak tot handelen omdat de veiligheid en /of gezondheid van betrokkenen of omgeving in het geding is.

Gegevensverwerking in het sociale domein kan niet los gezien worden van de maatregelen die genomen worden ten aanzien van informatiebeveiliging. De beide gemeenten sluiten aan bij de Baseline Informatiebeveiliging Gemeenten zoals die vanuit de VNG voorgeschreven wordt. Vanuit de activiteiten rondom Informatiebeveiliging en het in lijn brengen van de organisatie met de nieuwe Europese privacywetgeving die in 2016 van kracht wordt en de net ingegane wet Meldplicht Datalekken wordt vanuit de activiteiten vanuit privacy hierop zoveel mogelijk aansluiting gezocht.

b. Wettelijk

De Wet bescherming persoonsgegevens (Wbp) is leidend als kader voor het goed en zorgvuldig
omgaan met persoonsgegevens. Voor het sociaal domein zijn verder de verschillende materiële wetten en dan met name de Jeugdwet, Wet maatschappelijke ondersteuning 2015 (Wmo 2015) en Participatiewet van belang. Bij medische zorg speelt bovendien de Wet geneeskundige behandelingsovereenkomst, met daarin het medisch beroepsgeheim, een rol.

<u>Wet bescherming persoonsgegevens (Wbp)</u>
De Wbp vereist dat persoonsgegevens op een behoorlijke en zorgvuldige manier worden verwerkt en
alleen gebruikt kunnen worden voor duidelijk omschreven doelen. ‘Transparantie’ en ‘doelbinding’ zijn

twee zeer wezenlijke aspecten van deze wet. Persoonsgegevens mogen slechts worden verwerkt als daar een wettelijke grondslag voor is. De Wbp somt limitatief de gronden op voor gegevensverwerking. Voor zover van belang worden hier genoemd:

- de betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend, of
- de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke is onderworpen, of
- de gegevensverwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt.

Medische gegevens zijn (evenals bijvoorbeeld strafrechtelijke gegevens) bijzondere persoonsgegevens volgens de Wbp. Daarvoor geldt een verzwaarde toets: in principe mogen deze gegevens niet verwerkt worden. Voor de verwerking van deze gegevens is in beginsels een wettelijke grondslag nodig. De Wmo 2015 en de Jeugdwet biedt gemeenten hiervoor een wettelijke grondslag en geven goed aan welke medische gegevens in welke situaties mogen worden verwerkt. Daarbuiten mogen alleen met uitdrukkelijke toestemming of als gegevens uitdrukkelijk openbaar zijn gemaakt worden gebruikt. Hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening mogen gegevens betreffende de gezondheid verwerken voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene noodzakelijk is.

Bij elke verwerking moet voldaan zijn aan de beginselen van proportionaliteit en subsidiariteit. Het proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Ingevolge het subsidiariteitsbeginsel mogen persoonsgegevens alleen worden verwerkt als dat doel in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze kan worden verwerkelijkt. De Wbp bepaalt voorts dat er niet méér gegevens mogen worden verwerkt dan noodzakelijk zijn voor het doel. De verantwoordelijke moet de nodige maatregelen treffen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn.
Verdere verwerking van persoonsgegevens is alleen toegestaan op een wijze die verenigbaar is met de doeleinden waarvoor ze zijn verkregen. Bij de afweging of verdere verwerking verenigbaar is wordt rekening gehouden met:

- de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
- de aard van de betreffende gegevens;
- de gevolgen van de beoogde verwerking voor de betrokkene;
- de wijze waarop de gegevens zijn verkregen en
- de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Met dit kader voor ogen zal steeds de afweging gemaakt moeten worden of verwerking van persoonsgegevens in het specifieke geval rechtmatig is. In het algemeen geldt dat terughoudend omgegaan moet worden met het verwerken van persoonsgegevens. Voorts bepaalt de Wbp dat betrokkene geïnformeerd dient te worden over

de verwerking van zijn persoonsgegevens. Als de gegevens van betrokkene zelf verkregen worden dient hij voorafgaand aan de vraag naar persoonsgegevens geïnformeerd te worden over het doel van de verwerking en wie de verantwoordelijke is. Als de gegevens op een andere wijze verkregen worden, dient betrokkene geïnformeerd te worden op het moment van vastlegging of verstrekking aan een ander van de persoonsgegevens. Het informeren kan achterwege blijven als het onmogelijk is, een onevenredige inspanning kost of indien vastlegging of verstrekking van de gegevens bij wet is voorgeschreven. Ten slotte worden het rechten van betrokkene (inzage en correctie) beschreven en wordt de verantwoordelijke verplicht passende technische en organisatorische maatregelen te nemen om de persoonsgegevens te beveiligen. Dit juridisch kader van de Wbp geldt in principe voor alle gegevensverwerkingen, tenzij in de betreffende bijzondere wet daarvan wordt afgeweken. Zoals bijvoorbeeld bij het medisch beroepsgeheim opgenomen in de Wet op de geneeskundige behandelingsovereenkomst.

Wet maatschappelijke ondersteuning 2015 (Wmo 2015)
De Wmo 2015 voorziet in een wettelijke basis voor het overdragen van individuele cliëntgegevens aan gemeenten voor zover noodzakelijk voor het uitvoeren van de wettelijke taken. De Wmo 2015 regelt welke gegevens het college, de aanbieder van een voorziening (in natura of middels pgb), het Centraal Administratiekantoor (CAK), de Sociale Verzekeringsbank (SVB) of de instantie die belast is met de vaststelling en inning van een eigen bijdrage in de maatschappelijke opvang en/of beschermd wonen, de toezichthoudende ambtenaren en het Advies- en Meldpunt Huiselijk Geweld en Kindermishandeling (AMHK) mogen verwerken. Limitatief is opgesomd aan welke entiteiten en onder welke voorwaarden gemeenten gegevens kunnen verstrekken. Vervolgens is per entiteit bepaald aan welke entiteiten zij persoonsgegevens mogen verstrekken, indien noodzakelijk ter uitvoering van met name genoemde acties uit de Wmo 2015. Verder besteedt de Wmo 2015 aandacht aan de rechten van betrokkene op het gebied van informatie en inzage, aan de bewaartermijn en vernietiging van het dossier. Tot slot krijgt het college de opdracht de wijze van uitvoering van de Wmo af te stemmen met zorgverzekeraars en afspraken met hen te maken over beleid ten aanzien van maatschappelijke ondersteuning, publieke gezondheid, zorg, jeugdzorg, welzijn en preventie, teneinde te komen tot een integrale dienstverlening aan cliënten en verzekerden. Ter uitvoering van die afspraken verstrekken het college en de aanbieders de benodigde persoonsgegevens aan de zorgverzekeraars.

Jeugdwet
Binnen de taken die de Jeugdwet kent waarbij persoonsgegevens worden verwerkt, moet
onderscheid gemaakt worden tussen:
1. de toegang;
2. de uitvoering van jeugdhulp;
3. de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering;
4. de financiering.

Ad 1. Bij de toegang tot jeugdhulp (en het treffen van de voorziening op het gebied van jeugdhulp) mogen gegevens verwerkt worden die het mogelijk maken om te bepalen of het nodig is dat voor een jeugdige een voorziening wordt getroffen. Afhankelijk van de route die door de jeugdige en diens ouders wordt gevolgd (via de huisarts

of via de gemeentelijk te organiseren toegang) zijn hier verschillende regels op van toepassing.

Ad 2. Bij de uitvoering van de jeugdhulp zijn de instellingen die de jeugdhulp leveren gebonden aan de regels van het desbetreffende werkveld, ook wat betreft de gegevensverwerking (jeugdhulp, waaronder geneeskundige behandeling).

Ad 3. De uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering geschiedt feitelijk door de gecertificeerde instelling. In dit kader zal de gecertificeerde instelling persoonsgegevens delen met de jeugdhulpaanbieder in het kader van de uitvoering van jeugdhulp en met de gemeente in het kader van de financiering. De gecertificeerde instelling is gehouden aan het privacy kader dat voor hem geldt.

Ad 4. Inzake de financiering zal de gemeente gegevens verwerken in verband met de inkoop, bekostiging en betaling van jeugdhulp en de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering. Voor zover het daarbij om persoonsgegevens gaat, betreft het met name gegevens in het kader van de facturering. Ook waar sprake is van zeldzame, kostbare jeugdhulp, die niet door de gemeente is ingekocht, zal de gemeente om zijn jeugdhulpplicht uit te voeren, moeten weten voor welke persoon en welk probleem een voorziening moet worden getroffen.

<u>Participatiewet</u>
De Participatiewet harmoniseert de Wet werk en bijstand (WWB), Wet sociale werkvoorziening (WSW) en Wajong. Gegevensverwerking is in deze wetten geregeld conform het gesloten verstrekkingenregime SUWI. Dat regime houdt in dat in de sector werk en inkomen gegevens uitsluitend hergebruikt mogen worden als daar een wettelijke grondslag voor is.
De wet SUWI biedt in artikel 9 de grondslag voor de samenwerking tussen de ketenpartners W&I, UWV, SVB en gemeenten. In artikel 62 wet SUWI wordt de grondslag voor de gegevensverwerking via elektronische voorzieningen gelegd. Deze wordt verder uitgewerkt in artikel 5.24 Besluit SUWI en hoofdstuk 6 van de Regeling SUWI. De geheimhoudingsplicht is in artikel 74 van de wet SUWI vastgelegd.

In 2008 is de Wet eenmalige gegevensuitvraag van kracht geworden. Die houdt in dat aan een burger geen gegevens gevraagd mogen, waar de uitvoerder al over kan beschikken. Welke gegevens het betreft is in bijlage II van het Besluit Suwi opgenomen. In het SUWI gegevensregister zijn alle gegevens, die in de sector W&I worden verwerkt opgenomen, op grond van welke wettelijke titel, voor welk doel en door wie zij mogen worden verwerkt. Gegevens uit het domein W&I hebben een wettelijke titel nodig voor aanwending ervan voor taken in het kader van de WMO, AWBZ en Jeugdwet.

Beleidsuitgangspunten

c. Rijksbeleid

Vanwege de roep vanuit onder andere het Cbp om een overkoepelende visie, heeft het Rijk in het voorjaar van 2014 de beleidsvisie “Zorgvuldig en bewust, gegevensverwerking en privacy in een gedecentraliseerd sociaal domein” gepresenteerd. De conclusie is dat het bestaande en in de nieuwe wetten gegeven kader voor gege-

vensverwerking zou moeten kunnen volstaan voor de uitvoering in de praktijk van de verschillende taken en werkzaamheden van gemeenten.

De visie van het Rijk is gebouwd op drie pijlers:

1. Balans tussen noodzakelijke gegevensverwerking vanuit de maatschappelijke opgave in het sociale domein en borging van de privacy;
2. Versterking van de positie van de burger;
3. Versterking van de democratische verantwoording over gegevensverwerking en privacy op lokaal niveau.

Balans tussen noodzakelijke gegevensverwerking en borging van privacy
De burger moet erop kunnen vertrouwen dat niet onnodig of bovenmatig gegevens verwerkt worden en dat gegevens goed zijn beveiligd tegen ongeoorloofde inzage en gebruik. De nieuwe Wmo vraagt van gemeenten om breed te kijken als een burger zich meldt met een hulpvraag. Zij moeten onderzoeken of samenwerking met instanties uit andere domeinen noodzakelijk is (waaronder zorg, jeugdhulp, onderwijs, werk en inkomen). Dit roept een dilemma op: wanneer is 'breed kijken' breed genoeg en wanneer wordt het onnodig of bovenmatig? Hieruit volgt dat het van belang is om effectief het onderscheid te maken tussen 'eenvoudige' situaties en potentiële multiprobleemsituaties. Dat kan door het inrichten van een zorgvuldig proces van triage waarin stapsgewijze afwegingen ten aanzien van gegevensverwerking een plaats hebben. Privacy wordt zo een onderdeel van de kwaliteit van het dienstverleningsproces en de professionaliteit van de medewerker.

Versterking van de positie van de burger
Het is van belang dat de burger weet en het vertrouwen heeft dat hij tegen gegevensverwerking door de overheid in verweer kan komen. Hij moet een zichtbare, laagdrempelige en gezaghebbende plek hebben om klachten te uiten met betrekking tot de verwerking van zijn persoonsgegevens en privacy.
Gemeenten en samenwerkingspartners moeten een actief beleid hebben om burgers te wijzen op hun rechten, zoals bezwaar en beroep, inzage en correctie van gegevens. Het moet eenvoudiger worden voor burgers om te kunnen weten welke personen op welk moment zijn gegevens hebben ingezien, tenzij er zwaarwegende redenen zijn om dit niet te doen. Met betrekking tot gegevensbeveiliging is het uitgangspunt dat gegevensuitwisseling tenminste voldoet aan de Baseline Informatiebeveiliging Gemeenten en uiteraard aan de verplichtingen die voortvloeien uit de materiële wetten, waaronder de Jeugdwet en Wmo 2015. Toegang van persoonsgegevens is beveiligd op basis van autorisaties. Alle gegevensuitwisseling vindt plaats in beveiligde systemen en via beveiligde infrastructuren. De wijze waarop gemeenten omgaan met de verwerking van persoonsgegevens in het kader van de decentralisaties wordt onderdeel van de evaluatie van de decentralisaties van het Rijk.

Versterking van de democratische verantwoording over privacy op lokaal niveau.
Het college is verantwoordelijk voor de zorgvuldigheid van de gegevensverwerking die door of namens de gemeente plaatsvindt. Zij stelt eisen aan beveiliging en borging van privacy en is verantwoording verschuldigd aan de raad voor de wijze waarop het hieraan invulling geeft. De afspraken die gemeenten maken over gegevensverwerking en privacy dienen transparant te zijn en onderdeel van het lokale democratische proces. Voor zover de gemeente haar taken in samenwerking uitvoert, is

het college ervoor verantwoordelijk dat gegevensverwerking is ingebed in een zorgvuldig proces van triage en maakt het hierover afspraken met samenwerkingspartners. Ook indien de gemeente een deel van haar taken uitbesteedt aan private partijen, blijft de gemeente verantwoordelijk voor de zorgvuldigheid van de gegevensverwerking. Zij moet dit borgen in de contracten met de uitvoerende partijen, waarin een beveiligingsniveau moet worden afgesproken dat minimaal op het niveau als neergelegd in de Baseline Informatiebeveiliging Gemeenten (BIG) moet zijn. Ook moet continuïteit van dienstverlening worden geborgd (bv. bij storingen of faillissement).

a. Gemeentelijk beleid

Het beschermen van de privacy begint bij de grondhouding van de betrokken bestuurders, ambtenaren en andere betrokkenen. Deze grondhouding moet niet zijn 'verzamelen' omdat dat handig is', maar 'nee, tenzij'. Privacy begint met het niét verzamelen van persoonsgegevens. Met deze grondhouding kan recht worden gedaan aan de basisprincipes van het privacyrecht. Persoonsgegevens worden uitsluitend voor een bepaald doel verzameld, indien dat voor dit doel noodzakelijk is, en niet verder dan nodig voor het bereiken van dat doel. Dit gebeurt – wettelijke uitzonderingen daargelaten – niet 'achter de rug van de burger om' (transparantie). Dát is het privacyrecht in een notendop. Vanuit deze achtergrond hanteren we de volgende primaire uitgangspunten voor wat betreft het omgaan met privacy in het sociale domein:

1. Uitgangspunt bij het verzamelen van persoonsgegevens is *'Nee, tenzij'*. Bij het inrichten van een werkproces is altijd de eerste vraag, of het wel noodzakelijk is om persoonsgegevens te verzamelen. Privacy begint bij het niét verzamelen van gegevens.
2. Alleen die persoonsgegevens worden verzameld, die noodzakelijk zijn voor een bepaald, concreet omschreven doel (subsidiariteit), en vervolgens niet meer dan strikt nodig voor dát doel (proportionaliteit). Er is een belangrijk verschil tussen 'dat informatie' (het gegeven dat iemand bekend is, ondersteuning krijgt) en 'wat informatie' (de inhoud en achtergronden van de ondersteuning).
3. Artikel 8 van de Wbp kent een zestal limitatieve situaties waarin persoonsgegevens mogen worden verwerkt. Persoonsgegevens worden door ons in principe alleen verwerkt indien hiertoe op grond van een publiekrechtelijke taak noodzaak toe is. Indien deze of één van de andere gronden uit artikel 8 niet van toepassing is, wordt aan betrokkene toestemming gevraagd voor de verwerking. Daarbij wordt aangegeven wat het doel is van de verwerking, wat ermee gebeurt, wie inzage heeft en wat de bewaartermijn is. Verzamelde persoonsgegevens worden zo min mogelijk gedeeld en gekopieerd. Alleen daar, waar dat noodzakelijk is voor een bepaald doel (subsidiariteit), en dan niet meer dan strikt nodig is voor dat doel (proportionaliteit).
4. Persoonsgegevens worden niet langer bewaard dan strikt noodzakelijk. Verwijdering vindt, daar waar dat mogelijk is, plaats op geautomatiseerde wijze (incl. backups).

Als persoonsgegevens verstrekt of ontvangen worden (bij de uitwisseling van persoonsgegevens), zijn twee aanvullende algemene uitgangspunten en normen van belang. Dit zijn:

5. Persoonsgegevens worden slechts verstrekt met inachtneming van het doel waarvoor de te verstrekken gegevens eerder verzameld zijn en die anderzijds betrekking heeft op het doel waarvoor de gegevens nu (in een later stadium) verstrekt en gebruikt worden, en
6. Geheimhoudingsverplichtingen worden gerespecteerd;

De twee extra vragen bij verstrekken/uitwisselen van gegevens gaan ook op als reeds aanwezige gegevens voor een ander doel (lees: een andere hulpvraag die losstaat van de eerdere al behandelde hulpvraag) hergebruikt worden.

Samenwerking

b. Gegevensuitwisseling

Werken volgens het principe 1 gezin, 1 plan, 1 regisseur betekent intensief samenwerken met zowel professionals als cliënten. Een belangrijke basis onder deze werkwijze richt zich dan ook allereerst op het uitwisselen van gegevens naar nut en noodzaak tussen professionals die betrokken zijn bij de dienstverlening, zorg en ondersteuning voor (sociaal kwetsbare) inwoners. Om een goede begeleiding op maat te kunnen bieden, is het in voorkomende gevallen noodzakelijk dat de verschillende bij de cliënt of het gezin betrokken professionals van elkaars betrokkenheid op de hoogte zijn en in staat zijn zo nodig gezamenlijk een plan opstellen. In het eerste hoofdstuk is aangegeven dat de bestaande wetgeving vooralsnog voldoende ruimte geeft om de noodzakelijke gegevensuitwisseling te realiseren.

Voor het uitwisselen van gegevens maken we onderscheid in “dat-“ en “wat-informatie”:

- Wat-informatie betreft de inhoudelijke informatie van een klant uit een sector van het sociaal domein;
- Dat-informatie betreft de informatie dat er inhoudelijke informatie van een klant is binnen een sector, zonder dat de inhoud wordt prijs gegeven;
- Gecumuleerde informatie betreft alle informatie die afgeleid is van de wat- en dat-informatie en die gedepersonaliseerd is.

De wat-informatie kan bij de professionele instellingen in de verschillende domeinen blijven. De dat-informatie kan door regisseurs- en managementfuncties geraadpleegd worden. Wij hanteren het uitgangspunt dat er zo min mogelijk wat-informatie over de domeinen binnen het sociale domein heen worden uitgewisseld (doelbinding).

De basisuitgangspunten kunnen met deze definities praktisch uitgewerkt worden:

1. Binnen een domein is voor de professionals van dat domein de volgende informatie toegankelijk:
   a. De wat-informatie uit het eigen domein;
   b. De dat-informatie uit alle domeinen, uitsluitend voor zover noodzakelijk;
   c. Alle gecumuleerde informatie;
2. Voor de regisseur is de volgende informatie toegankelijk:
   a. De wat-informatie, uitsluitend voor zover noodzakelijk:
   b. De dat-informatie van alle domeinen;
   c. Alle gecumuleerde informatie.

3. Voor andere partijen zoals management e.d. is alleen de gecumuleerde informatie toegankelijk.

Met de partijen met wie de gemeente in het nieuwe stelsel contractueel samenwerkt zullen convenanten worden aangegaan. In de convenanten zal naast de samenwerking in algemene zin ook de onderlinge gegevensuitwisseling geconcretiseerd worden. De hier geformuleerde noodzaak tot samenwerking en gegevensdeling zal in de komende jaren onderdeel gaan vormen van de inkoopbestekken dan wel subsidievoorwaarden in het sociale domein.

c. Uitbesteding

Een deel van onze taken in het sociale domein hebben wij uitbesteed aan derden. Wij zijn ook in die gevallen verantwoordelijk voor de zorgvuldigheid van de gegevensverwerking, borging van de privacy en beveiliging van gegevens conform de geldende wetgeving. Dit borgen wij door bewerkersovereenkomsten met de uitvoerende partijen te sluiten. De bewerkersovereenkomst is de overeenkomst tussen verantwoordelijke en bewerker, waarin wordt vastgelegd hoe de bewerker met de persoonsgegevens moet omgaan. De verantwoordelijke is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. De bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Borging

d. Governance

Voor de organisatie moet worden vastgelegd welke taken en bevoegdheden bepaalde functionarissen hebben bij de verwerking van persoonsgegevens in het sociale domein, en aan wie zij verantwoording afleggen. De inrichting kan plaatsvinden volgens het RASIC-model (Responsible – uitvoerder, Accountable – eindverantwoordelijk, Supportive – ondersteunt uitvoerder, Informed – achteraf informeren, Consulted – vooraf geraadpleegd, kan resultaat beïnvloeden). Een goede inrichting leidt tot heldere rollen en verantwoordelijkheden en tot helderheid bij een vraag wie aan zet is.

Om met privacy in control te zijn, is het nodig de juiste maatregelen op technisch- (informatiebeveiliging), organisatorisch- (bv. beperkte autorisaties) en gedragsgebied (bewustwording) te nemen, en wel in goede onderlinge samenhang. Het waarborgen van de privacy van de burger is altijd het resultaat van het nemen van de juiste maatregelen op deze drie gebieden. Persoonsgegevens mogen niet voor een ieder toegankelijk zijn (autorisaties), dienen zorgvuldig te worden beheerd (bv. bewaartermijnen) en dienen goed beveiligd te zijn. Systemen zullen moeten voorzien zijn van adequate beveiliging om inbreuken door derden te voorkomen. Zij moeten voldoen aan de Baseline informatiebeveiliging Gemeenten (VNG).

e. Triage

Triage is het proces van het verhelderen, routeren en escaleren van vragen en casussen. Door middel van triage wordt bepaald waar de hulpvraag thuis hoort en daarmee welke mate van gegevensverwerking noodzakelijk is. Triage draagt bij aan het zorgvuldig uitwisselen van informatie. Triage voorkomt dat onnodig teveel persoonsgegevens worden verzameld of gedeeld. In het triageproces besluit men over de route van een casus en bepaalt men het doel waarvoor informatiedeling noodzakelijk is. Het bepalen van het doel van informatiedeling is noodzakelijk voor het delen

van informatie en het waarborgen van de privacy. De bedoeling is dat personen, instellingen en domeinen selectief informatie delen: zoveel als moet, zo weinig als mogelijk. Naast noodzaak is ook proportionaliteit van de gegevensverwerking van belang: Hoe verhouden het doel en de daarvoor noodzakelijke gegevensuitwisseling zich tot de schending van de persoonlijke levenssfeer van de betrokkene en zijn omgeving? De gegevensverwerking moet ook voldoen aan de eis van subsidiariteit. De vraag: is het doel ook te bereiken met een minder ingrijpende methode? Deze afweging kan expliciet gemaakt worden in een triagebesluit. Wanneer men besluit over de route van een vraag/casus maakt men meteen de afweging wat de noodzakelijke gegevensverwerking is die daarbij hoort. Het is van belang om deze afweging vast te leggen.

In het sociaal domein zijn drie triagemomenten te onderscheiden. Het eerste moment is wanneer er een vraag bij de gemeente binnenkomt. Dit triagemoment wordt ook wel vraagverheldering genoemd. Het tweede triagemoment is wanneer een hulpvraag niet meer eenvoudig kan worden afgehandeld maar er echt sprake is van een meervoudige of complexe vraag. Waarschijnlijk zijn er al meerdere partijen betrokken bij deze burger en is regie op de samenwerking wenselijk. Om te bepalen of er daadwerkelijk sprake is van meervoudige en/of complexe casuïstiek en vervolgens een besluit te nemen ten aanzien van de routering van deze casus is het van belang om ook dat tweede triagemoment in te richten. Een derde triagemoment is het moment van escalatie, er wordt bepaald of escalatie naar een andere overlegtafel (bijvoorbeeld het Veiligheidshuis of een interventieteam) noodzakelijk is.

f. Bewustwording

De privacyregelgeving is bijzonder gedetailleerd. Niet mag en kan worden verwacht, dat alle betrokken medewerkers op de hoogte zijn van alle regelgeving. Wel moeten zij beschikken over een goed ‘privacybewustzijn’. Vragen als ‘is het wel nodig om nu deze gegevens te delen?’, ‘hoe lang mag ik dit bewaren?’ moeten medewerkers die dat bewustzijn hebben ontwikkeld, stellen.
Schendingen van de privacy worden dan, aan de voorkant, voorkomen. Op het gebied van privacy is het van groot belang de burger juist en zorgvuldig te informeren. De persoon wiens gegevens worden verwerkt heeft recht op informatie over de geregistreerde gegevens. Daarnaast heeft hij het recht om die gegevens te laten corrigeren. In een aantal gevallen kan de betrokkene bezwaar maken tegen gegevensverwerking (‘verzet’).

g. Training

Het is van belang dat professionals, gemeentelijke beleidsambtenaren en juristen van organisaties (permanent) worden getraind in het formuleren van heldere doelstellingen op macro- én microniveau, om van daaruit te kunnen beoordelen welke gegevens in het kader van de geformuleerde doelstellingen dienen te worden uitgewisseld.

Niet alleen de overheid maar ook professionals en hun beroeps- en branche organisaties dienen dit onderwerp te agenderen, te ontwikkelen en te verwerken binnen de eigen beroepscodes. Randvoorwaarden creëren zoals scholing en training van professionals, binnen de gemeente én buiten de gemeente, bij het zorgvuldig toepassen van de principes doelbinding, noodzaak, subsidiariteit, proportionaliteit en doelmatigheid, is geen activiteit van de gemeente alleen, maar van alle professionals in het

sociaal domein. Bij die trainingen dienen naast permanente aandacht voor kennis van de formele kant van de mogelijkheden voor gegevensuitwisseling, ook de informele kant in de vorm van cultuur, gewoonten en gedrag van professionals in het sociaal domein, maar ook van juristen, ten aanzien van de privacy van cliënten, een vast onderwerp van bespreking te zijn.

BIJLAGE 4: DO'S EN DON'TS VOOR HET OMGAAN MET PERSOONSGEGEVENS

1. **Less is more**. Vraag en gebruik niet meer informatie dan je nodig hebt voor het doel van de verwerking. Privacy begint bij het niet vragen en vastleggen van persoonsgegevens.

2. **Alleen persoonsgegevens die noodzakelijk** zijn voor een bepaald concreet omschreven doel worden verzameld.

3. **Bij hulpvragen: maak de hulpvraag van de burger leidend**. Ga dus niet op zoek in de organisatie wat nog meer bekend is over de burger. Werk zoveel mogelijk in samenspraak met en op basis van informatie die de burger zelf geeft.

4. In de regel is **het verkrijgen van toestemming niet nodig** bij het uitoefenen van de publiekrechtelijke taak die jij uitvoert. In bijzondere situaties is dit (bijvoorbeeld bij het uitvragen van medische gegevens bij derden) wel nodig. Leg de burger dan uit waarom dit nodig is en geef aan wat er met de gegevens gebeurt (opslag, wie kan het inzien, bewaartermijn, etc). Let wel: deze instemming wordt in vrijheid gegeven. De enkele weigering om gegevens te verstrekken betekent niet dat er geen aanspraak kan worden gemaakt op een gevraagde voorziening.

5. Haal bij voorkeur pas gegevens op **uit registraties als je een specifiek gegeven echt nodig hebt,** bijvoorbeeld voor een formeel toekenningsproces.

6. Werk zoveel mogelijk **met 'dat' in plaats van 'wat'-gegevens. Maak onderscheid** tussen regie-informatie en inhoudelijke informatie en scheidt deze twee. Dit houdt in dat het vaak voldoende bijvoorbeeld is te weten of een persoon gebruik maakt van een wmo-voorziening zonder exact te hoeven weten wat dit is.

7. Behandelinformatie (wat-informatie) blijft bij de betreffende zorgverleners/medewerkers en komt niet in andere (gemeentelijke) bestanden.

8. Hou je aan **de informatiebeveiligingsvoorschriften** (autorisaties, wachtwoorden, toegangscontroles, etc.). De geheimhoudingsverplichting wordt gerespecteerd.

9. Pas op bij het **verstrekken van persoonsgegevens aan derden.** In beginsel is dit niet toegestaan. Indien dit wel moet (bijvoorbeeld opdrachtverstrekking aan een zorgaanbieder) verstrek alleen die informatie die strikt noodzakelijk. Ook hier geldt **"Less is more".** Bespreek deze verstrekkingen met je direct leidinggevende en/of de privacyfunctionarissen.

10. De burger heeft **rechten**: wijs hem of haar daarop, wees open en transparant en help hem of haar bij het activeren van die rechten.

11. Wees alert op **beveiligingsincidenten en datalekken**. Meld dit per ommegaande aan de concernjuristen. Datalekken (niet iedere beveiligingsincident is een datalek) moeten binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens en indien er sprake is van mogelijke ernstige gevolgen voor betrokkenen ook aan betrokkenen. De concernjuristen coördineren dit.