

Sector	: Bedrijfsvoering	Openbaar: <input checked="" type="checkbox"/>
Afdeling	: Personeel, Informatie en Facilitair	Niet openbaar: <input type="checkbox"/>
Zaaknummer(s) ingekomen stuk(ken)	:	Kabinet: <input type="checkbox"/>
Behandelend medewerk(st)er	: Marco van Dijk Tel.: (0495) 57 55 82 en: Marie-Lou Rosbergen	
Portefeuillehouder(s)	: A.A.M.M. Heijmans	Nummer B&W-advies: BW-008497

ONDERWERP

Privacybeleid gemeente Weert 2015

ADVIES

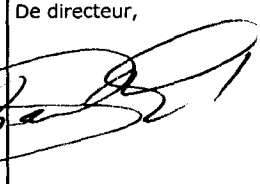





- Vaststellen van de beleidsnotitie "Privacybeleid gemeente Weert 2015
- Regionaal werven van de gezamenlijke functionaris gegevensbescherming (privacy officer) voor de Midden-Limburgse gemeenten

TOELICHTINGRelatie met vorig voorstel:

Privacybeleid en stappenplan sociaal domein, nr. B&W advies 007966 d.d. 27 januari 2015.

Algemeen:

Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. Binnen de gemeente is m.b.t. privacy thematisch gebied al veel geregeld. De uitbreiding met een aantal risicovolle toepassingen vraagt om een samenhangend integraal beleid, dat als kapstok dient voor de verdere uitwerking binnen de gemeentelijke processen en de samenhang met samenwerkende partijen. Voor u ligt het beleidsplan privacy voor onze gemeente. Op 27 januari 2015 heeft het college de uitgangspunten integraal privacybeleid en het stappenplan privacy vastgesteld waar dit beleidsdocument uit voortvloeit. Indien er binnen de gemeente een privacy incident plaatsvindt en blijkt dat geen of onvoldoende sprake is van een gestructureerde en beleidsmatige aanpak van privacy, dan zijn de bestuurlijke risico's erg groot. De wet wijst het college aan als probleemeigenaar van privacy beleidsvoering. Dit beleidsdocument voorziet in waarborgen van privacy rechten van de inwoner van de gemeente en in het beperken van de bestuurlijke risico's voor het college.

Weert, 4 juni 2015	De directeur,	S		B	W	W	W	W
					HL	FvE	PS	GG
<i>ph</i> 			akkoord					
			bespreken					
Behandeling uiterlijk in college van 9 juni 2015								

In te vullen door het B&W secretariaat:

- Akkoord
 Akkoord met tekstuele aanpassing door portefeuillehouder
 Anders, nl.:

- Niet akkoord
 Gewijzigde versie

- A-stuk
 B-stuk
 C-stuk

Beslissing d.d.:

Akkoord met advies
09 JUNI 2015

Nummer: **14**

De secretaris,


Totaal aantal pagina's: 3
Pagina 1

Het voorliggende beleidsdocument bevat in technische zin alle elementen die verder geïmplementeerd moeten worden binnen de gemeente. Hierbij wordt aangesloten bij het gemeentelijk informatiebeveiligingsbeleid en worden maatregelen zoveel mogelijk in overeenstemming met dit beleid getroffen. Er wordt een gemeentelijk team geformeerd dat belast wordt met de verdere implementatie. Dit team wordt het aanspreekpunt voor privacyvraagstukken binnen de organisatie (het privacyteam).

Activiteiten / tijdpad.

De implementatie vraagt om een strak besluitvormingsproces. In het tijdpad wordt uitgegaan van implementatie in 2015 en het aanstellen van een functionaris gegevensbescherming in september 2015.

Implementatie van dit beleidsplan.

Dit plan voorziet in de inrichting van de privacy structuur binnen de gemeente met als eerste stap het inrichten van een privacy team. Op basis van dit beleidsplan zal een plan aanpak worden opgemaakt om de implementatie ervan uit te kunnen voeren.

Aanstelling functionaris voor de gegevensbescherming (privacy officer).

Een goede uitvoering van het privacybeleid vraagt om de aanstelling van een Functionaris Gegevensbescherming. Om efficiency redenen wordt voorgesteld om over te gaan tot het werven en aanstellen van de functionaris gegevensbescherming (FG) voor de 7 Midden-Limburgse gemeenten gezamenlijk. De afzonderlijke gemeenten dienen de medewerker als functionaris gegevensbescherming aan te wijzen.

De gemeente Roermond heeft zich bereid verklaard het werkgeverschap voor de medewerker te vervullen. De salariskosten en bijkomende kosten zullen naar rato van het aantal inwoners worden verdeeld over de 7 gemeenten.

Argumenten:

Met het vaststellen van het privacybeleid gemeente Weert 2015 en het beleggen van de uitvoering hiervan binnen de gemeentelijke organisatie vindt een actualisatie plaats van het gevoerde privacybeleid. De gemeente Weert borgt hiermee verder het zorgvuldig omgaan met persoonsgegevens van de burger, ook voor de nieuwe taken binnen het sociale domein.

Kanttekeningen:

N.v.t.

JURIDISCHE GEVOLGEN (o.a. FATALE TERMIJNEN/HANDHAVING)

De functionaris gegevensbescherming zal naar verwachting medio 2016 verplicht worden als gevolg van Europese regelgeving. Met dit besluit wordt hierop geanticipeerd.

FINANCIËLE EN PERSONELE GEVOLGEN

De implementatiefase met daarbij het opbouwen van kennis zal inzet en tijd vragen van medewerkers die deel uit gaan maken van het privacy team en de medewerkers die een rol hebben binnen processen waarbij privacy aan de orde is.

Uiteindelijk zal het een regulier onderdeel van het werkproces moeten worden. Continue aandacht voor Privacy vereist structurele inzet van het privacyteam en betrokken medewerkers, maar zal leiden tot minder personele inzet voor het afhandelen van meldingen en klachten. Bovendien verkleint dit het financiële risico.

De consequenties zijn de volgende:

- 1 Aanstellen functionaris gegevensbescherming 1 FTE vanaf 1 september 2015. De kosten worden – als aangegeven - verdeeld over 7 gemeenten.

- 2 Het privacybeleid Weert 2015 voorziet in de instelling van een privacy team binnen de gemeente. Dit team vormt onder andere de vraagbaak binnen de gemeente voor privacy vraagstukken.
- 3 Training en workshops voor leden privacy team en medewerkers van de gemeente.

Begrotingspost:

Dekking wordt deels gevonden uit 4 beschikbare uren formatie juridisch medewerker concernstaf, voor het overige uit de concernbrede onderuitputting.

De kosten worden verantwoord op kostenplaats KB000 (Bedrijfsvoering/Directie).

Beschikbaar bedrag:

Uitgaande van schaal 12 en een verdeling over 7 gemeenten naar aantal inwoners dan bedragen de kosten voor de gemeente Weert circa € 38.000 voor 2 jaar.

COMMUNICATIE/PARTICIPATIE

Voor wie is dit advies van belang?:

- ❖ Inwoners van Weert
- ❖ Raadsleden
- ❖ Interne organisatie

Nadere specificatie:**Geadviseerd wordt de volgende communicatie-instrumenten te gebruiken:**

- ❖ TILS-lijst
- ❖ Persbericht
- ❖ Gemeentelijke website
- ❖ Intranet
- ❖ Overig: Algemene bekendmaking via de gebruikelijke kanalen.

Nadere specificatie: Het persbericht wordt door de samenwerkende gemeenten via de werkgroep communicatie decentralisaties verzorgd.

Interne organisatie door communicatie via het intranet.

Direct betrokkenen interne organisatie middels voorlichting sessies en training.

Geadviseerd wordt de volgende participatie-instrumenten te gebruiken:

- ❖ Niet van toepassing

OVERLEG GEVOERD MET

[Invulinstructie]

Intern:

DT (akkoord d.d. 3 juni 2015).

HRM, Financiën, MT-Bedrijfsvoering, MT-Inwoners.

Extern:

De notitie is mede tot stand gekomen in de regionale werkgroep privacy decentralisaties.

BIJLAGEN

Openbaar:

Privacybeleid gemeente Weert 2015

Niet-openbaar:

Niet van toepassing

Privacybeleid

Gemeente Weert 2015

Datum 29 april 2015

Status Definitief 1.0

Van Bedrijfsvoering

Tot stand gekomen in de Werkgroep privacy samenwerkende gemeenten Midden Limburg

Bewerkt door M. Rosbergen en M. van Dijk



Inhoud

Privacybeleid.....	1
1. Inleiding.....	3
2. Ambitie.....	4
3. Reikwijdte.....	4
4. Governance.....	5
5. Juridisch kader.....	8
6. Bewustwording, communicatie en evaluatie.....	9
7. Good governance: Privacybeleid toegepast in het sociaal domein.....	9
8. Convenanten en overeenkomsten.....	10
Bijlage A: Functionaris voor de gegevensbescherming.....	12
Toelichting functionaris voor de gegevensbescherming.....	12
Functieomschrijving FG Midden Limburg.....	13
Bijlage B: Bijlage toelichting wettelijke kaders.....	15
a) Jeugdwet.....	15
b) Wet maatschappelijke ondersteuning 2015.....	16
c) Participatiewet.....	17
d) Boek 1 Burgerlijk Wetboek.....	19
e) Algemene wet bestuursrecht.....	19
f) Wet publieke gezondheid.....	19
g) Wet op de beroepen in de individuele gezondheidszorg (Wet BIG).....	19
h) Wet bescherming persoonsgegevens (Wbp).....	20
i) Wet geneeskundige behandelingsovereenkomst (Wgbo).....	20
j) Wet politiegegevens.....	20
k) Wet justitiële en strafvorderlijke gegevens.....	21
l) Wetboek van strafvordering.....	21
m) Wet gemeentelijke schuldhulpverlening.....	21
n) Wet basisregistratie personen (Wet BRP).....	21
o) Wet algemene bepalingen Burgerservicenummer / Wet gebruik Burgerservicenummer in de zorg.....	22
Bijlage C: Privacymatrix.....	23

1. Inleiding

De gemeente heeft als gevolg van de decentralisatie van de Jeugdwet, WMO-2015 en de Participatiewet per 1 januari 2015 een belangrijke verantwoordelijkheid waar het gaat om de verwerking van persoonsgegevens van burgers. De complexiteit in het kader van de bescherming persoonsgegevens is toegenomen. Nog meer dan voorheen zullen burgers een beroep doen op ondersteuning en/of hulp door de gemeente. De gemeente zal door deze taakuitbreiding vaker dan vroeger het geval was, persoonsgegevens uitwisselen met instanties buiten de gemeentelijke organisatie.

De gemeente verzamelt en bewerkt persoonsgegevens in verband met de dienstverlening aan burgers en bedrijven. Het gaat bijvoorbeeld om de gegevens in de gemeentelijke basisregistratie personen, de registratie van uitkeringsgerechtigden, het bijhouden van gegevens uit bouwaanvragen en het bijhouden van gegevens van mensen die een Wmo-voorziening hebben aangevraagd, uitvoering van de Jeugdwet en de gemeentelijke schulddienstverlening. De gemeente heeft als uitgangspunt en als wettelijke verplichting dat zij behoorlijk en zorgvuldig omgaat met deze gegevens in verband met de privacy van betrokkenen. Bescherming van persoonsgegevens is een grondrecht. Gegevensverwerking vindt plaats op een faire, veilige en betrouwbare manier waardoor burgers op maat worden geholpen. Het is aan de gemeente om ervoor te zorgen en om begrijpelijk uit te leggen welke maatregelen zijn genomen om onrechtmatig gebruik van gegevens te voorkomen. Een zorgvuldige omgang met de gegevens van burgers vormt een essentiële bouwsteen voor het vertrouwen van burgers in de overheid. Bij privacy beleid gaat het niet enkel om naleving van de wet. Privacy beleid maakt deel uit van het kwaliteitsbeleid. Het leidt tot efficiënter werken. Gemeentelijk privacy beleid is daarnaast nodig voor het tot stand brengen van een goed gedocumenteerd stelsel van interne afspraken om persoonlijke en gemeentelijke belangen te waarborgen.

Door de al geschetste complexiteit is er in deze beleidsnotitie verhoudingsgewijs veel aandacht besteed aan het sociale domein. Vaker dan voorheen worden persoonsgegevens van de burgers buiten de gemeentelijke organisatie verwerkt. Dit beleidsdocument stelt de algemene kaders vast waarbinnen de gemeente de privacy van de burger regelt. Het geeft richting en kaders voor nader vast te stellen thematisch beleid.

Uit onder meer berichtgeving in de media en uit gegevens van het College Bescherming Persoonsgegevens (CBP) blijkt dat het verwerken van persoonsgegevens strijdig met de wet een bron van ergernis is van burgers. Vooral het niet adequaat verwerken is een ergernis en het kan zelfs leiden tot onacceptabele situaties, waarbij bijvoorbeeld iemands identiteit wordt 'gestolen' en wordt misbruikt. Juiste toepassing van de wettelijke regels is van groot belang. Dit beleid vormt een nadere uitwerking van de wettelijke regelgeving en is daarnaast een praktische handleiding voor de ambtelijke organisatie. Het CBP streeft te allen tijde een behoorlijke en zorgvuldige verwerking van persoonsgegevens na. Natuurlijk zal de gemeente over een goed stelsel van processen, werkafspraken en contracten moeten beschikken om de privacy te kunnen waarborgen. Dat is in het belang van de burger maar ook van de gemeente. Maar, processen en protocollen worden uitgevoerd door mensen. Daarom wil de gemeente graag een actief privacy beleid dat vooral is gericht op bewustwording, een open en kritische cultuur en kennisoverdracht.

2. Ambitie

De gemeente levert diensten van velerlei aard en biedt ondersteuning aan haar inwoners. Het is onontkoombaar dat daarbij informatie wordt verwerkt over personen. De verwerking van persoonsgegevens is inherent aan de gemeentelijke taakuitoefening. Voor een goede en zorgvuldige dienstverlening zal de gemeente gegevens van burgers moeten bewerken en soms met andere instanties moeten delen. Informatieverwerking gaat gepaard met de verantwoordelijkheid om effectieve privacybescherming te bieden.

De gemeente vindt dat de burgers moeten kunnen vertrouwen op een veilige werkwijze van persoonsgegevens. Dit niet alleen vanwege de wettelijke verplichting en de beheersing van bestuurlijke risico's maar vooral ook omdat in deze informatiesamenleving de digitale leefbaarheid van burgers bij de gemeente hoog in het vaandel staat. Vertrouwen in de publieke dienstverlening is van groot belang.

Onze gemeente vindt privacy een maatschappelijk vraagstuk en zoekt daarom actief naar manieren om burgers te betrekken bij dit onderwerp en de dilemma's die daar bij horen. Goede privacy services, communicatie, transparantie en dialoog met de inwoners vormen het fundament van het privacy beleid.

3. Reikwijdte

Het gemeentelijk privacy beleid is van toepassing op alle taken en processen waar de gemeente voor verantwoordelijk is. In de volgende beleidsuitgangspunten wordt het kader geschetst waarbinnen privacy beleid wordt gevoerd.

Uitgangspunten beleid: Het privacy beleid is gebaseerd op de volgende uitgangspunten:

- Gegevens van burgers worden binnen de kaders van de geldende wet- en regelgeving verwerkt en vindt uitsluitend plaats voor zover dit nodig is voor goede gemeentelijke taakuitoefening.
- Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt de inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt (subsidiariteit).
- De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel (proportionaliteit).
- Gegevens worden gebruikt voor duidelijk omschreven doelen en kunnen alleen worden gebruikt voor andere doelen of worden gedeeld voor zover de wet dat toestaat.
- Er wordt op een transparante wijze gecommuniceerd hoe de gemeente denkt over privacy en hoe de gemeente privacy zal borgen. De burger wordt in algemene zin pro-actief geïnformeerd met betrekking tot privacy beleid. Over wat er met zijn of haar informatie gebeurt en waarom. In het thematisch beleid zal nader worden uitgewerkt of en in hoeverre in individuele gevallen nadere informatie wordt verstrekt aan de burger.
- De gemeente ziet er op toe, dat daar waar sprake is van verwerking van persoonsgegevens, de werkwijzen worden vastgelegd en op professionele wijze uitgevoerd conform functionele en praktische protocollen of procesbeschrijvingen.
- Gegevens zijn steeds voldoende actueel en zijn een nauwkeurige weergave van de feitelijke situatie.
- Afhandeling van klachten en verzoeken van burgers en bedrijven over privacy aspecten vindt plaats op een toegankelijke, laagdrempelige wijze.

- In geval van samenwerking met externe partners, onder andere ook specifiek binnen het sociale domein, waarbij sprake is van verwerking van persoonsgegevens, worden afspraken gemaakt over de eisen waar gegevensuitwisselingssystemen aan moeten voldoen. Door middel van in control-statements wordt jaarlijks verantwoording afgelegd aan het college. Voor bij het werk belangrijke, veel voorkomende processen, worden specifieke procedures beschreven. Daarin wordt voor dat proces aangegeven hoe wordt omgegaan met privacygevoelige informatie. Die specifieke procedures dienen te voldoen aan de uitgangspunten van dit gemeentebrede beleid (en natuurlijk het wettelijk kader zoals beschreven). Dergelijke specifieke procedures (werkprocessen) worden ter vaststelling voorgelegd aan het college.
- De gemeente is altijd (eind)verantwoordelijk voor de gegevensverwerking en de privacy daarvan. Dit geldt ook als gegevens ter beschikking worden gesteld aan derden of worden gedeeld in samenwerkingsverbanden.

4. Governance

De wijze van verankering van het privacy beleid binnen de gemeente vormt als het ware het fundament van de borging van dit belangrijke thema. Volgens de Wet bescherming persoonsgegevens is het college van burgemeester en wethouders verantwoordelijk voor de juiste uitvoering ervan. Deze paragraaf geeft aan op welke wijze de taken, verantwoordelijkheden en de borging van het privacy beleid wordt georganiseerd binnen de gemeente.

1. Relatie met de raad

Zoals beschreven is het college verantwoordelijk voor de juiste naleving van de Wet bescherming persoonsgegevens. Deze wet reikt daarvoor de basisset van privacy management controls aan. Het college zal binnen de jaarlijkse planning en control cyclus de raad informeren over de risico's en over de getroffen beheersmaatregelen van de privacy binnen de processen waarvoor de gemeente verantwoordelijk is.

Op transparante wijze informatie verstrekken/verantwoording afleggen over het privacy beleid en daarmee over belangrijke rechten van onze inwoners, acht de gemeente van groot belang voor het vertrouwen van de burger in de overheid.

2. Vastleggen van verantwoordelijkheden binnen de gemeente

a. Vaststellen privacy beleid

Het college stelt het gemeentelijk privacy beleid vast met inachtneming van de aanbevelingen van de functionaris voor de gegevensbescherming (zie onder c) en bevordert de beschikbaarheid van voldoende middelen om privacybescherming passend te waarborgen. De naam functionaris gegevensbescherming (FG) wekt de indruk, dat het om een functionaris gaat die zich bezig moet houden met de volledige gegevensverwerking binnen een bedrijf ofwel met complete domein van de informatiebeveiliging. Wij gebruiken daarom in de praktijk de naam privacy officer.

b. Uitvoering van privacy beleid

Het college wijst uit haar midden een portefeuillehouder privacy aan die bestuurlijk verantwoordelijk is voor de uitvoering van het gemeentelijk privacy beleid en voor controle op de naleving van afspraken. De directeur bedrijfsvoering is ambtelijk verantwoordelijk voor algemeen privacy beleid en richt hiertoe een passende organisatie in waarin de privacy rollen worden belegd (privacy team).

c. Toezicht

Voor onafhankelijk toezicht op de uitvoering van het privacy beleid wijst het college een functionaris voor de gegevensbescherming (privacy officer) aan conform artikel 62-

64 Wet bescherming persoonsgegevens. De privacyfunctionaris fungeert tevens als privacy-ombudsman en is in voorkomende gevallen de liaison met de landelijke. Zijn positie en taakuitoefening worden nader geregeld in een door het college vastgesteld statuut.

d. Beheer van het beleid

De privacy officer is de beheerder van het gemeentelijk privacy beleid, in samenspraak met het privacy organisatie. De privacy officer doet het college verslag over de voortgang en kwaliteit van de uitvoering van het gemeentelijke privacy beleid en doet aanbevelingen die strekken tot verdere optimalisering.

e. Verantwoordelijkheid voor het ontwikkelen van thematisch beleid

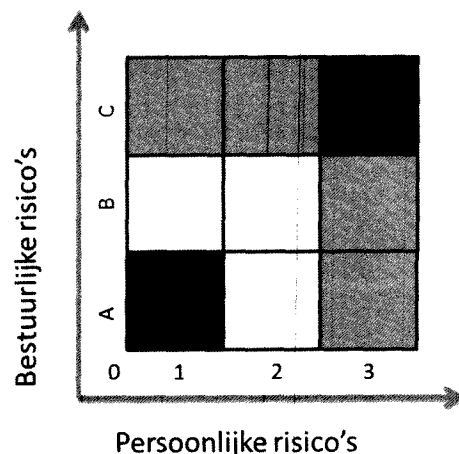
De directeur bedrijfsvoering ziet toe op de ontwikkeling en uitvoering van themagericht privacy beleid (themabeleid), zoals bijvoorbeeld Basisregistratie Personen, Participatie en Jeugd. De sectordirecteur, verantwoordelijk voor het thema, is hiervan proceseigenaar en zorgt voor adequate borging binnen de uitvoering. De proceseigenaar krijgt hiervoor ondersteuning van het privacy team.

f. Ontwikkeling van themabeleid en praktische privacy waarborgen

De proceseigenaar is verantwoordelijk voor de ontwikkeling en uitvoering van themabeleid binnen en conform de door het college gestelde kaders. Onder ontwikkeling en uitvoering van themagericht privacy beleid wordt met name ook verstaan: aantoonbare concretisering van beleid in praktische privacy waarborgen (documenteren), zodat ook op operationeel niveau structureel sprake is van behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet. Hierbij wordt bij voorkeur gebruik gemaakt van bestaande oplossingen, voor zover uit toetsing blijkt dat deze inpasbaar zijn.

g. Risico gedreven aanpak

De gemeentelijke uitvoering van het privacy beleid is evenwichtig. Oplossingen zijn gebaseerd op privacy impact assessments (PIA's). De effecten, zowel profijt als risico's voor personen en de gemeente, zijn in kaart gebracht en zijn afgewogen op basis van de inhoud. De risico's worden door praktische, organisatorische en technische maatregelen beheerst. Met een risicoanalyse (zie afbeelding) wordt de mate van persoonlijk- en bestuurlijk risico in kaart gebracht. Deze vormt het vertrekpunt voor het maken van beleidskeuzes.



h. Interne verantwoording

Proceseigenaren rapporteren minimaal een keer per jaar aan de portefeuillehouder over de resultaten die zij hebben bereikt bij realisatie en beheer van passende privacy waarborgen. Zij melden hem onverwijld privacy incidenten conform een vast te stellen privacy-incidentenprocedure.

Voor zover proceseigenaren op hun beurt verantwoordelijkheden hebben overgedragen of uitbesteed, dragen zij zorg voor een gelijkwaardige vorm van verantwoording. Afspraken hierover worden schriftelijk vastgelegd.

i. Verantwoordelijkheid van audit

De directeur bedrijfsvoering ziet in samenspraak met de privacy officer [en de concerncontroller] toe op totstandkoming van een privacy auditplan op basis van de uitgevoerde PIA's en de ijkpunten (key controls) van de gekozen beheersmaatregelen volgens het themabeleid en de nadere concretisering.

3. Privacy Control Systeem

Er is door de gemeente een stelsel van maatregelen getroffen om te waarborgen dat er continu wordt gewerkt aan het optimaliseren en borgen van de kwaliteit van de werkprocessen waarbij privacy een rol speelt. Juist omdat privacy voor een belangrijk deel mensenwerk is, moet er ruime aandacht zijn voor het cyclisch denken op alle niveaus binnen de gemeente. Door privacy vast op de verschillende agenda's te plaatsen ontstaat er een continu proces van veranderen en verbeteren. Door vanuit verschillende niveaus en rollen binnen de gemeente te kijken naar de kwaliteit van de uitvoering van privacy ontstaat er een evenwichtig systeem van checks and balances. Hieronder worden de belangrijkste elementen van deze borging van de gemeente beschreven.

a. Planning en control van de gemeente

Privacy vormt een aparte paragraaf binnen het planning en control proces van de gemeente. Jaarlijks zal het college verantwoording afleggen aan de raad waar het gaat over de risico's en beheersmaatregelen met betrekking tot het privacy beleid.

b. Onderdeel jaarplannen

Binnen de gemeente zal privacy een vaste paragraaf worden binnen alle (deel)plannen van de gemeente. Hierdoor zal er ruimte zijn voor beleidsmatige verbeteringen binnen de gemeente.

c. In control statement

De gemeente gaat werken met "in control statement" met betrekking tot privacy. In deze verklaring leggen de directeuren jaarlijks verantwoording af of de uitvoering van processen ter zake privacy verlopen volgens het beleid en geven tevens aan waar afwijkingen zijn en welke beheersmaatregelen worden getroffen.

d. Auditplan

Op basis van risicoanalyse en op verzoek van proceseigenaren en na advies van het privacy team zal de concerncontroller in samenspraak met de directeur bedrijfsvoering, een privacy auditplan opstellen.

e. Werkoverleg

Leidinggevenden en medewerkers maken privacy tot een onderdeel van het werkoverleg. Op deze wijze werkt de gemeente actief aan een open cultuur, optimaliseren van kennis en transparante procesuitvoering. Bevindingen of vragen kunnen worden voorgelegd aan het privacy team van de gemeente.

f. Privacy team

De gemeente heeft een privacy team waarin een aantal kernfuncties vertegenwoordigd zijn. De privacy officer zal als adviseur/lid deel uitmaken van dit team. Dit privacy team treedt op als adviseur voor het DT, vraagbaak voor de medewerkers en leidinggevenden en vormt de kern van het auditteam privacy binnen de gemeente.

g. Toezicht door de privacy officer

De privacy officer heeft een eigen agenda om te toetsen of de aanwezigheid en de werking van het privacy beleid afdoende binnen de gemeente is ingericht. Hij heeft vrij toegang tot systemen en processen van de gemeente. Hij rapporteert rechtstreeks aan het college van burgemeester en wethouders. Deze functionaris treedt eveneens op als

ombudsman voor burgers bij klachten over serviceverlening van de gemeente bij de uitoefening van de privacy rechten en de uitvoering van het privacy beleid.

4. Bemensing

a. Privacy Officer

Het aanstellen van de een privacy officer is een belangrijke stap in de het waarmaken van de maatschappelijke privacy ambities. Op termijn zal de aanstelling van een dergelijke functionaris verplicht worden gesteld. De gemeente stelt een privacy officer aan om daarmee eigen toezicht te organiseren. Hij heeft een belangrijke coördinerende rol, adviseert over oplossingen m.b.t. privacy. Belangrijk is ook dat hij aan de voorkant meekijkt met betrekking tot de inrichting van processen. De privacy officer maakt als lid/adviseur deel uit van het gemeentelijke privacy team.

b. Gemeentelijk privacy team

Binnen de gemeente wordt een privacy team opgericht. Dit team vormt de vraagbaak binnen de gemeente voor privacy vraagstukken, adviseert over beleid en uitvoering, draagt bij aan kennisverspreiding en cultuur en heeft een rol binnen het interne audit programma van de gemeente. Minimaal bestaat het team uit een privacy coördinator van de gemeente, een juridisch adviseur, een informatiedeskundige en een informatiebeveiligingsdeskundige, . Het team kan onder andere worden uitgebreid (eventueel op afroep) met een ICT specialist, kwaliteitsmedewerker, communicatiemedewerker en specifieke beheerders (suwinet, BRP etc).

5. Services richting burger

- a. Rechten van de burger zijn binnen de gemeente op transparante wijze ingericht. Het recht op inzage, informatie, correctie en verwijdering van gegevens is vertaald in heldere, laagdrempelige procedures en wordt helder gecommuniceerd richting de burger.
- b. Meldingen en klachten met betrekking tot privacy aspecten komen binnen bij de gemeente via de bestaande kanalen. Deze melding wordt bij binnenkomst geregistreerd in het zaakstelsel. De desbetreffende proceseigenaar is verantwoordelijk voor de afwikkeling en het treffen van eventuele verbetermaatregelen. Indien de burger niet tevreden is met de afwikkeling kan hij zich beklagen bij de gemeentelijke privacy functionaris.

5. Juridisch kader

De Wet bescherming persoonsgegevens (Wbp) regelt het algemene kader voor de omgang met privacy in ons land. De Wbp is te beschouwen als parapluwetgeving die van toepassing is op bijna alle sectoren, instellingen en bedrijven in Nederland. Voor het verwerken van persoonsgegevens voor privégebruik geldt de Wbp niet. De Wbp vereist dat voor elke verwerking van persoonsgegevens een beroep kan worden gedaan op één van de in artikel 8 Wbp genoemde grondslagen. Na vaststelling van die grondslag is het vervolgens mogelijk om op gestructureerde wijze te bepalen welke verwerking, van welke persoonsgegevens, voor welke doeleinden rechtmatig en noodzakelijk is.

Daarnaast zijn in tal van bijzondere wetten regels met betrekking tot privacy opgenomen. In de bijlage wordt een opsomming gegeven van relevante regelgeving.

6. Bewustwording, communicatie en evaluatie

Privacy is voor een belangrijk deel een zaak van bewustwording, cultuur en communicatie. Bestuur, ambtenaren en hulpverleners moeten zich bij de uitoefening van hun werk voortdurend bewust zijn van het belang van het waarborgen van de rechten van de burgers.

Naast het inrichten van het privacy beleid en werkprocessen is het van belang dat de personen die daadwerkelijk werken met deze gegevens weten wat hun verantwoordelijkheid is en hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Daarom is het belangrijk dat de professionals in het veld en binnen de gemeente zich bewust zijn van de regels en gedragsnormen rondom privacy. De gemeente ondersteunt dit proces door het ontwikkelen van privacy protocollen en afwegingskaders en organiseert trainingen over hoe zij met privacyvraagstukken om moeten gaan in hun functie en/of rol. De gemeente streeft een cultuur na waarbij professionals elkaar in alle openheid aanspreken op het eigen gedrag rondom privacy en daarmee van elkaar leren. Communicatie, openheid en toetsing zijn belangrijke randvoorwaarden voor het realiseren van een optimaal privacy beleid.

Daarnaast is communicatie met de burger over privacy van belang. De burger heeft het recht te weten wat er met zijn of haar gegevens gebeurt.

Het vorenstaande is binnen dit beleid verankerd en wordt jaarlijks door middel van een Privacy Impact Assessment geëvalueerd.

7. Good governance: Privacybeleid toegepast in het sociaal domein

De vorige paragrafen vormen een generiek beleidskader voor het gemeentelijk privacy beleid. Vanwege de toename van verwerkingen van (bijzondere) persoonsgegevens als gevolg van de decentralisatie per 1 januari 2015 wordt hieronder kort ingezoomd op de gegevensverwerking in het sociale domein. Uitvoering van de gedecentraliseerde taken brengt met zich dat gegevens dienen te worden uitgewisseld tussen gemeente en diverse instellingen en instanties. In de wetten en daarop gebaseerde besluiten is soms vrij nauwkeurig, soms meer in algemene termen, beschreven welke gegevens nodig zijn voor de taakuitoefening en welke instanties/instellingen op basis hiervan de bevoegdheid hebben om die te verstrekken (zie samenvatting bijlage). Bij het uitoefenen van die bevoegdheid dienen echter wel bepaalde principes in acht te worden genomen: behalve doelbinding (die in de meeste gevallen dus rechtstreeks uit de wet voortvloeit), gaat het daarbij om de principes van subsidiariteit en proportionaliteit. Dit zijn ook de leidende principes van de Wet bescherming persoonsgegevens. Bovendien gelden er strengere eisen in die gevallen waarbij sprake is van bijzondere gegevens (met name gezondheidsgegevens en strafrechtelijke gegevens). Bij het verwerken van gegevens betreffende de gezondheid van personen is in veel gevallen de Wet geneeskundige behandelingsovereenkomst leidend. Vooral met het oog op de uitwisseling van bijzondere gegevens is het gewenst om meer helderheid te scheppen over het beleid dat de gemeente voorstaat voor de uitvoering in de praktijk. Hiervoor zijn de volgende uitgangspunten geformuleerd:

- Hulpverleningsperspectief in veel gevallen leidend
- Gegevensverwerking op basis van 'need to know'
- Gegevensverwerking op basis van 'toestemming, tenzij'
- Zorg voor betrokkenheid burger

Hieronder volgt een nadere uitwerking van en toelichting op deze uitgangspunten. Deze dient als richtlijn voor de aanpak van themagericht privacy beleid.

7.1 Hulpverleningsperspectief in veel gevallen leidend

De gemeentelijke overheid is verantwoordelijk voor het toekennen van voorzieningen die voor een belangrijk deel betrekking hebben op hulpverlening als (zorg en ondersteuning). Soms met een gedwongen karakter, maar ook dan is nog sprake van hulpverlening. Een belangrijk aspect hiervan is dat er een vertrouwensrelatie ontstaat. Daarbij is het in de hulpverlener gestelde vertrouwen essentieel om taken goed te vervullen.

7.2 Gegevensverwerking op basis van 'need to know'

Dit uitgangspunt heeft enerzijds te maken met het vereiste van 'doelbinding': alleen die gegevens die noodzakelijk zijn vanuit een bepaald doel worden verwerkt. 'Need to know' is dus geen 'Nice to know'. Bij dit uitgangspunt speelt ook de vraag in hoeverre bij verwerking voldaan wordt aan de uitgangspunten van proportionaliteit (niet meer privacy inbreuk dan nodig) en subsidiariteit (ander middel dat minder inbreuk op privacy maakt om het gestelde doel te realiseren, heeft de voorkeur). Dit speelt vooral bij verwerking van gegevens in het kader van signalering en bij de vraag hoe lang gegevens moeten worden bewaard. In het kader van dit uitgangspunt is het belangrijk dat al vanaf het begin (toegang) geprioriteerd wordt en de privacy inbreuk zo beperkt blijft. Dat gebeurt door een goede vraaganalyse of vraagverheldering.

7.3 Gegevensverwerking op basis van 'toestemming, tenzij'

Gegevensverwerking vindt eerst en vooral plaats met toestemming van betrokkene. In geval van hulpverlening betekent toestemming voor de behandeling ook toestemming voor de gegevensverwerking. Is er eenmaal sprake van toestemming voor de behandeling (daaronder ook begrepen: begeleiding en verzorging), dan hoeft niet ook nog eens afzonderlijke toestemming te worden gevraagd voor het delen van gegevens tussen zorgverleners die rechtstreeks bij de behandeling zijn betrokken. In de bijlage over het wettelijk kader is dit verder uitgewerkt in de daar genoemde bepalingen van de Jeugdwet. Soortgelijke bepalingen zijn ook opgenomen in de Wet op de geneeskundige behandelingsovereenkomst (Wgbo). Wie rechtstreeks betrokken zijn bij de behandeling is op te maken uit het ondersteuningsplan, dat door betrokkene wordt ondertekend. Nadrukkelijk wordt aangetekend dat het verlenen van toestemming niet de enige grond is voor de verwerking van persoonsgegevens. In artikel 8 van de Wbp wordt een limitatieve opsomming gegeven van de gronden die een gegevensverwerking rechtvaardigen. Van belang is dat altijd sprake is van transparantie. Een burger moet immers gebruik kunnen maken van zijn recht op verzet.

7.4 Zorg voor betrokkenheid burger

Hoe meer de cliënt het gevoel heeft dat hij echt betrokken wordt, hoe minder noodzakelijk het wordt om hem voor diverse handelingen vooraf toestemming te vragen. Dit heeft veel te maken met het begrip transparantie, een begrip waarop vooral de in de Wgb uitgewerkte informatieplicht is gebaseerd. Uitgangspunt bij overleg moet zijn dat niet over de burger, maar met de burger wordt gepraat.

8. Convenanten en overeenkomsten.

Met het oog op de omgang met privacy van alle partijen waarmee de gemeente samenwerkt en waarbij verwerking van persoonsgegevens plaatsvindt worden convenanten,

bewerkersovereenkomsten en protocollen afgesloten. De gemeente moet de eisen omtrent gegevensverwerking borgen in contracten. Hier dient ook de grondslag te worden gelegd voor het uit laten voeren van een privacy-audit. Verwezen wordt ook naar de bij deze notitie behorende privacymatrix. Hoe er afspraken worden gemaakt met ketenpartners, is sterk afhankelijk van de positie in de informatieketen en de aard van de samenwerking Hierin wordt in ieder geval aangegeven:

- a) De betrokken organisaties, verantwoordelijken en relevante doelstellingen.
- b) De verwerking van bijzondere persoonsgegevens.
- c) De wijze waarop betrokken burgers worden geïnformeerd over het gebruik van hun persoonsgegevens.
- d) De belangrijkste verwerkingen van persoonsgegevens die binnen de samenwerking plaatsvinden, de melding daarvan bij het College bescherming persoonsgegevens en de eenduidige protocollering van de privacy-regels die bij de verwerking in acht genomen moeten worden.
- e) De wijze waarop bij betrokken burgers toestemming voor gegevensverwerking wordt verkregen.
- f) Een beschrijving van de gevallen waarin zonder toestemming van betrokkene gegevens worden verwerkt.
- g) Een beschrijving van een procedure in verband met escalatie bij spoed- en/of noodgevallen.
- h) De wijze waarop betrokkenen gebruik kunnen maken van hun rechten op grond van de Wet bescherming persoonsgegevens.
- i) De wijze waarop organisaties invulling geven aan informatiebeveiliging en geheimhoudingsverplichting.

Bijlage A: Functionaris voor de gegevensbescherming

Toelichting functionaris voor de gegevensbescherming

De 7 gemeenten in Midden Limburg werken samen op het gebied van privacy beleidsvoering. Binnen deze samenwerking wordt gestreefd naar de aanwijzing van een gezamenlijke privacy officer. In deze bijlage wordt uitgelegd wat dat inhoudt en hoe zo'n gezamenlijke privacy officer kan worden gerealiseerd. Voor 'privacy officer' wordt hierna de wettelijke term gehanteerd: 'functionaris voor de gegevensbescherming' – kortweg: FG.

A. Privacytoezicht algemeen

Om de FG goed te begrijpen, moet hier eerst het toezichtstelsel van de Wet Bescherming Persoonsgegevens (WBP) worden uitgelegd, want de WBP regelt toezicht op verschillende manieren.

Waar meestal als eerste aan wordt gedacht, is het toezicht door de landelijke toezichthouder, het College Bescherming Persoonsgegevens. Maar de WBP kent ook aan het college van B&W een toezichthoudende rol toe, als regievoerder en de controleur op nakoming van afspraken. Daarnaast zijn ook burgers in zekere zin toezichthouder, omdat de WBP hen het recht toekent om bij de gemeente de verwerking van hun eigen gegevens te controleren, waarbij ze recht hebben op schadevergoeding wanneer het gemeentelijk privacy beleid te kort schiet, en bij het CBP een handhavingsverzoek mogen indienen.

Daarmee moet de WBP worden gezien als een systeem van *checks and balances*. Dit systeem werkt alleen niet goed zolang er geen FG is aangewezen. Dit heeft er onder meer mee te maken dat privacy een complex vraagstuk is, dat ook met misverstanden omgeven is. Het CBP staat op een te grote afstand om op reguliere wijze privacy beleidsvoering van een gemeente te kunnen controleren.

De aanwijzing van een FG – eveneens een toezichthouder die in de WBP wordt genoemd – is daarom een logische zaak, zeker vanwege de extra privacyrisico's die gekoppeld zijn aan de nieuwe gemeentelijke taken in het sociaal domein.

B. Wat is een FG?

De FG laat zich het beste vergelijken met een accountant – met het grote verschil dat de FG, anders dan in de wereld van accountancy, advies en toezicht juist niet mag scheiden maar moet combineren.

Een FG denkt mee over privacy bestendige oplossingen (preventief toezicht) maar toetst ook achteraf of oplossingen daadwerkelijk binnen de kaders van de wet zijn vormgegeven ('privacyaudits'). Zijn aanbevelingen zijn bestemd voor het college. Dat neemt niet weg dat de FG in de praktijk vooral ook samenwerkt met afdelingen en, vooral, 'tweede lijn-professionals' zoals informatiemanagers, informatiebeveiligers, juristen en ICT-ers.

C. Functieprofiel FG

De FG is een multidisciplinaire senior. De wet vereist dat hij voldoende betrouwbaar is en stevig genoeg in zijn schoenen staat om in onafhankelijkheid te kunnen adviseren. Hij moet praktijkdeskundig zijn (kennis van organisaties, processen, ICT en informatiebeveiliging) en, vooral, een expert zijn op het gebied van privacywetgeving. Nog afgezien van zijn interne betrokkenheid, speelt hij ook extern een belangrijke rol. Hij geeft het gemeentelijk privacy beleid gezicht en heeft een bufferfunctie in de relaties met het College Bescherming Persoonsgegevens. Een FG zal daarom een goed gevoel moeten hebben voor interne en externe verhoudingen en zal

moeten beschikken over vaardigheden op het gebied van communicatie, public relations en regulatory affairs.

D. Positie FG

De positie van de FG wordt beschreven in paragraaf 2 van hoofdstuk 9 WBP over derde lijn-toezicht. Paragraaf 1 van dit hoofdstuk regelt de positie van het CBP. De wet bevat geen bepalingen over een hiërarchische relatie. De FG is dus geen verlengstuk van CBP. Wél is het zo dat de FG bij twijfel het recht heeft om het CBP te consulteren, wat – mits goed aangepakt – kan helpen om bij het CBP begrip te kweken voor de gemeentelijke aanpak. Het CBP hecht veel waarde aan de aanwijzing van FG's. Organisaties die een FG aanwijzen, genieten bij de landelijke toezichthouder extra vertrouwen.

Vanwege zijn wettelijke rol en deskundigheid, is het oordeel van de FG juridisch zwaarwegend. In de praktijk wordt dat echter niet altijd begrepen. Ook komt het voor dat op een FG druk wordt uitgeoefend om zijn zienswijze te herzien. Het is belangrijk om dit soort dingen van te voren door te spreken. Een FG moet veilig kunnen adviseren en dient daarvoor goed de ruimte te krijgen. De wet geeft ook aan dat hij niet uit zijn functie kan worden gezet. Om over dit soort zaken duidelijk te zijn, verdient het sterk de aanbeveling om zijn positie te regelen in een statuut.

Door de aanwijzing van een FG functioneert het CBP meer op de achtergrond. Het CBP treedt weer op de voorgrond wanneer het gemeentelijk toezicht niet goed blijkt te functioneren.

E. Aanwijzing FG

De aanwijzing van een FG wordt onder de WBP aanbevolen en wordt onder de nieuwe EU-privacyverordening waarschijnlijk verplicht. Hij kan in dienst worden genomen, worden ingehuurd of worden betrokken via een organisatie waarbij een gemeente is aangesloten.

Het is het college die tot de aanwijzing moet besluiten en hem vervolgens moet melden bij het CBP,¹ die zijn gegevens overneemt in het openbare FG-register.² Het CBP beoordeelt niet de geschiktheid van de FG. De aanwijzing van een gekwalificeerde privacyfunctionaris (zie profiel) blijft dus de eigen verantwoordelijkheid van het college. De geschiktheid van een FG moet blijken uit zijn cv (studie, werkervaring, publicaties en bij voorkeur ook een certificaat van de IAPP, de internationale associatie van privacy professionals).

Het salarisniveau van een FG ligt in Nederland gemiddeld op 65.000 euro, wat lager is dan in andere EU-landen (85.000 euro).³ Het salaris hangt ook samen met de mate waarin de FG een coördinerende / leidinggevende rol speelt. Een FG heeft kantoorfaciliteiten, tooling en overige middelen nodig voor professionele invulling van taken, maar hiervoor zijn ook *lean & mean*-oplossingen denkbaar. Zo scheelt het wanneer de FG kan rekenen op een team van tweede lijn-professionals (zie hiervoor).

Functieomschrijving FG Midden Limburg

Functietitel: Privacy Officer Midden Limburg M/V

De zeven gemeenten Midden-Limburg streven naar een onderling gecoördineerde privacy management-aanpak en voorzien in dat kader in een gezamenlijke regeling voor regionaal privacy toezicht waarbij de gemeenten zich zullen aansluiten. Met deze aansluitingsregeling voorzien de gemeenten in een collectieve Functionaris voor de Gegevensbescherming conform artikel 62-64 Wet Bescherming Persoonsgegevens.

¹ https://cbpweb.nl/sites/default/files/atoms/files/fg_aanmeldingsformulier.pdf

² <https://cbpweb.nl/nl/zelf-doen/functionaris-gegevensbescherming/register-functionaris-gegevensbescherming-e-tm-h>

³ Onderzoek NGFG, gepubliceerd in *Privacy & Compliance* 04-05/2013.

De FG, die in de praktijk de functietitel Privacy Officer Midden Limburg hanteert, gaat samenwerken met colleges van B&W en gemeentelijke privacyteams. Met name door de nieuwe gemeentetaken in het sociaal domein die voortvloeien uit de Jeugdwet, de Wet Maatschappelijke Ondersteuning en de Participatiewet, is de behoefte aan professionele ondersteuning vergroot. De FGfunctie is nieuw voor de Midden-Limburgse gemeenten. Het is aan de FG om op basis deskundigheid en een constructief-kritische werkwijze, geloofwaardigheid op te bouwen en het maatschappelijk vertrouwen te versterken. In het begin zal vooral ook aandacht nodig zijn voor de opzet van het intergemeentelijk privacybureau.

De FG is de onafhankelijke privacyaccountant van de gemeenten Midden Limburg. Met name bewaakt hij dat de gemeenten persoonsgegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze verwerken en geeft hij desgevraagd advies bij meer complexe privacy-vraagstukken. Aan de hand van privacy impact assessments en analyse van wetgeving doet hij aanbevelingen voor verdere optimalisering van de privacybescherming en naleving van wettelijke voorschriften, op een zodanige manier dat er goede balans is tussen legitieme gemeentebelangen en privacybescherming. Hij ziet erop toe dat de nodige kennis m.b.t. privacy in de gemeenten aanwezig is en draagt zo nodig bij aan kennisoverdracht. Ook organiseert de FG in samenwerking met gemeenten controles op de goede werking van beleid en maatregelen en rapporteert daarover aan de colleges van B&W.

Het toezicht van de FG strekt zich tot alle informatieketens die onder de wettelijke verantwoordelijkheid van de gemeenten vallen, met inbegrip van de gegevensverwerking door uitvoeringsorganisaties ('bewerkers'). Ook fungeert de FG als bijzondere ombudsman in de gevallen dat gemeenten privacy-gerelateerde verzoeken of klachten niet naar tevredenheid afhandelen. De FG is tenslotte degene die voor de gemeenten Midden Limburg de relaties onderhoudt met landelijke privacytoezichthouders, met name het College Bescherming Persoonsgegevens.

Voor de invulling van de positie van FG, zoeken de gemeenten Midden Limburg een multidisciplinaire senior die onafhankelijk en oplossingsgericht de FG-functie kan helpen opbouwen, maar toch een teamspeler is. Kandidaten dienen affiniteit te hebben met gemeentelijke bedrijfsvoering, analytisch en praktijkdeskundig te zijn (kennis van organisaties, processen, ICT, risicomangement, toetsing), en te beschikken over minimaal 4 jaar ervaring in een vergelijkbare positie. Vooral dienen kandidaten te beschikken over aantoonbare expertise op het gebied van privacywetgeving. Houderschap van het CIPM-certificaat dat wordt uitgegeven door de internationale organisatie van privacy professionals IAPP is een voordeel. Naast vakinhoudelijke kwaliteiten dient de FG te beschikken over gevoel voor interne en externe verhoudingen, en vaardigheden op het gebied van public relations en regulatory affairs.

Bijlage B: Bijlage toelichting wettelijke kaders

a) Jeugdwet

Grondslag: taken waarvoor verwerking van persoonsgegevens is toegestaan. Voor de volgende taken is in de Jeugdwet een grondslag opgenomen voor verwerking van persoonsgegevens:

- De toeleidingstaak
- Jeugdhulpplicht
- Het doen van een verzoek tot onderzoek aan de raad voor de kindbescherming
- Het (laten) uitvoeren van kindbeschermingsmaatregelen en jeugdreclassering
- De financiering van jeugdhulp, kindbeschermingsmaatregelen en jeugdreclassering

Toestemming voor jeugdhulpverlening en dossiervoering Jeugdhulp wordt, met inachtneming van een in de wet vastgelegde informatieplicht, verleend met toestemming van betrokkene, tenzij het hulp betreft in het gedwongen kader (vooral hulp in het kader van kindbeschermingsmaatregelen of jeugdreclassering die door de rechter zijn opgelegd). Er zijn twee uitzonderingen hierop:

- a. Voor kinderen met een leeftijd tussen twaalf en zestien jaar: toestemming van ouders met gezag of voogd is dan ook vereist, tenzij betrokkene bij weigering van de toestemming de hulp weloverwogen blijft wensen of indien die hulp kennelijk nodig is om ernstig nadeel voor betrokkene te voorkomen;
- b. Voor personen van zestien jaar en ouder die niet in staat kunnen worden geacht tot een redelijke waardering van hun belangen ter zake: dan dienen de jeugdhulpverlener en de curator of mentor uit te gaan van een weigering als dit blijkt uit de kennelijke opvatting van betrokkene op basis van eerdere uitingen toen betrokkene nog wel in staat was tot een redelijke waardering van belangen. De jeugdhulpverlener kan hiervan echter afwijken als hij daartoe gegronde redenen aanwezig acht.

Plicht van jeugdhulpverlener om voor de hulp aan betrokkene een dossier in te richten en bij te houden. Hieraan dient hij desgevraagd een door betrokkene afgegeven verklaring toe te voegen. Er geldt een bewaartermijn van ten minste vijftien jaar. Verder dient het dossier (of delen daarvan) op verzoek van betrokkene binnen drie maanden vernietigd te worden, tenzij aannemelijk is dat bewaring van aanmerkelijk belang is voor een ander of een wettelijke regeling zich hier tegen verzet.

De jeugdhulpverlener dient ervoor zorg te dragen dat hij geen informatie over betrokkene (of inzage in of afschrift van het dossier) aan anderen dan de patiënt verstrekt dan met zijn toestemming; onder deze anderen zijn niet begrepen:

- rechtstreeks bij de hulpverlening betrokkenen en degenen die de jeugdhulpverlener vervangen, voor zover dit noodzakelijk is voor de taakuitoefening;
- de curator of mentor van betrokkene; verstrekking geschiedt slechts voor zover daardoor de persoonlijke levenssfeer van de ander niet wordt geschaad.

De verstrekking kan ook opgelegd zijn bij of krachtens de wet, in welk geval er geen beperkingen gelden. Verder kan de jeugdhulpverlener altijd besluiten niet te verstrekken in de gevallen dat hij dit in strijd acht met goed hulpverlenerschap.

Alle hierboven genoemde verplichtingen gelden jegens ouders die het gezag over betrokkene uitoefenen of diens voogd indien betrokkene nog geen twaalf jaar oud is. Datzelfde geldt in de gevallen dat betrokkene ouder is dan twaalf jaar maar niet in staat kan worden geacht tot een redelijke waardering van zijn belangen ter zake, tenzij betrokkene meerderjarig is en er een mentor of curator is benoemd jegens wie de verplichtingen gelden. Is er geen mentor of curator, dan is de volgorde: schriftelijk gemachtigde, echtgenoot/geregistreerde partner/levensgezel (tenzij deze dat niet wenst), ouder, kind, broer of zus (tenzij deze dat niet wenst).

De verplichtingen zijn echter niet van toepassing als deze niet verenigbaar zijn met zorg van een goed hulpverlener. Ook geldt dat de vertegenwoordiger zijn taak goed dient te vervullen en betrokkene zoveel mogelijk hierbij betreft. Mocht die zich verzetten, dan kan een verrichting van ingrijpende aard waarvoor geen toestemming is verleend slechts worden uitgevoerd indien zij kennelijk nodig is om ernstig nadeel voor betrokkene te voorkomen.

Gebruik Burgerservicenummer.

De gecertificeerde instelling, de jeugdhulpaanbieder, de raad voor de kindbescherming en het college (lees: de gemeente) dienen bij hun taakuitoefening gebruik te maken van het Burgerservicenummer van betrokkene, uitgezonderd uitwisseling van gegevens in het kader van de jeugdreclassering ten behoeve van het strafrecht en uitgezonderd situaties waar afwijking van deze regel noodzakelijk is in verband met spoedeisende gevallen. Om als gemeente conform de wettelijke eisen te zorgen voor de uitvoering van reclassering en jeugdhulp in dat kader, is geregeld dat de Minister van Justitie en Veiligheid aan een door het college aangewezen ambtenaar of aan een door het college aangewezen en onder zijn verantwoordelijkheid werkzame functionaris het Burgerservicenummer kan verstrekken van een jeugdige ten aanzien van wie dat bepaald is in een strafrechtelijke beslissing.

b) Wet maatschappelijke ondersteuning 2015

Bevoegdheid toezichthouders

Toezichthoudende ambtenaren mogen voor zover dat noodzakelijk is in het kader van hun taak inzage in dossiers vragen, met dien verstande dat zij gebonden zijn aan dezelfde geheimhoudingsplicht als die op de aanbieder van toepassing is. Uitzonderingen: bij wilsonbekwaamheid van betrokkene of indien noodzakelijk ter bescherming van cliënten.

Grondslag: taken waarvoor verwerking van persoonsgegevens is toegestaan

Om te beoordelen of iemand in aanmerking komt voor een Wmo-voorziening, een Pgb of om het verhaalsrecht uit te oefenen, mogen de uit onderzoek verkregen persoonsgegevens, waaronder gezondheidsgegevens, worden verwerkt. Persoonsgegevens van de mantelzorger van cliënt mogen worden verwerkt voor zover deze noodzakelijk zijn om te bepalen welke hulp deze aan de cliënt kan bieden en voor zover deze zijn verkregen van de cliënt of de mantelzorger en deze noodzakelijk zijn voor de uitvoering van de wet. Een soortgelijke bepaling is opgenomen met betrekking tot persoonsgegevens van andere personen in het sociaal netwerk van de cliënt. Indien uit een melding een redelijk vermoeden van huiselijk geweld kan worden afgeleid, mag Veilig Thuis (AMHK) in het kader van haar taakuitvoering persoonsgegevens registreren van personen die bij het huiselijk geweld betrokken zijn. Gemeente mag bepaalde persoonsgegevens verstrekken aan aanbieders van Wmo voorzieningen, het CAK, de instantie die de eigen bijdrage int, de Sociale Verzekeringsbank en toezichthoudende ambtenaren.

Toestemmingsvereiste bij afstemming van hulp in kader van uitvoering van andere wetten en bij opvragen persoonsgegevens bij zorgverzekeraar

Ondubbelzinnige toestemming van betrokkene is vereist voor verwerking van persoonsgegevens van betrokkene zelf dan wel van personen in zijn directe omgeving, met het oog op een goede afstemming van de hulp in het kader van aan de gemeente opgedragen taken in andere wetten (Jeugdwet, Participatiewet, Wet gemeentelijke schuldhulpverlening), ervan uitgaande dat dit noodzakelijk is voor uitvoering van wet. Dat geldt ook voor persoonsgegevens van betrokkene die worden opgevraagd bij een zorgverzekeraar.

Uitzondering op toestemmingsvereiste bij verstrekken gegevens aan Veilig Thuis / AMHK

Derden die beroepshalve beschikken over inlichtingen die kindermishandeling kunnen beëindigen of nodig zijn om een redelijk vermoeden van kindermishandeling te onderzoeken, kunnen deze gevraagd en ongevraagd aan Veilig Thuis (Advies- en Meldpunt Kindermishandeling / AMHK) verstrekken zonder toestemming van degene die het betreft, indien nodig met doorbreking van de plicht tot geheimhouding op grond van de wet hun ambt of beroep.

Identificatieplicht

Clïent is verplicht om zich te identificeren bij de aanbieder van een maatwerkvoorziening.

Gebruik Burgerservicenummer

Gemeente, Veilig Thuis (AMHK), aanbieders, toezichhouders en andere uitvoerende instanties zijn verplicht bij verstrekkingen gebruik te maken van het Burgerservicenummer van betrokkene.

Informatieplicht bij meldingen Veilig Thuis (AMHK)

Bij meldingen bij Veilig Thuis (AMHK) door een ander dan betrokkene, wordt betrokkene zo spoedig mogelijk, maar in ieder geval binnen vier weken, hiervan op de hoogte gesteld. Uitstel is alleen mogelijk als dit noodzakelijk is om een situatie van huiselijk geweld te beëindigen of een redelijke vermoeden daarvan te onderzoeken.

Uitoefening privacy-rechten bij Veilig Thuis (AMHK)

Geclausuleerd recht op inzage, afschrift en vernietiging van persoonsgegevens op verzoek van betrokkene.

Gebruik persoonsgegevens voor onderzoek

Het recht om zonder voorafgaande toestemming van betrokkene persoonsgegevens te verstrekken ten behoeve van statistiek of wetenschappelijk onderzoek. Hierbij gelden strenge voorwaarden als uitwerking van de principes van subsidiariteit en proportionaliteit. Ook geldt de restrictie dat betrokkene niet uitdrukkelijk bezwaar heeft gemaakt.

c) Participatiewet

De Wet werk en bijstand gaat per 1 januari 2015 over in de Participatiewet. Vanaf dat moment is deze wet toegankelijk voor een bredere doelgroep, die voorheen een beroep deed op de Wet Wajong (Wet werk en arbeidsondersteuning jonggehandicapten) of de Wsw (Wet sociale werkvoorziening).

Gegevensverwerking en Suwinet (Inkijk)

Gegevensverwerking in de Participatiewet is geregeld conform een gesloten verstrektingsregime om zo de privacy van burgers binnen de sociale zekerheid zo goed mogelijk te waarborgen. Dat regime houdt in dat Werk en Inkomen gegevens uitsluitend worden hergebruikt als daar een wettelijke grondslag voor is of als de burger daar toestemming voor heeft gegeven. Bij het uitvoeren van de Participatiewet maakt Werk en Inkomen gebruik van de landelijk beschikbare applicatie Suwinet-Inkijk. Suwinet-Inkijk mag niet voor andere doeleinden dan voor de uitvoering van de Participatiewet gebruikt worden. Via deze Inkijk mogen gegevens in het kader van de Wet structuur en uitvoeringorganisatie werk en inkomen (Wet SUWI) en de Wbp tussen organisaties binnen het SUWI-stelsel worden uitgewisseld. Maar gegevens van werkzoekenden mogen in beginsel alleen aan organisaties buiten SUWI worden verstrekt als daar een uitdrukkelijke wettelijke grondslag of verplichting voor bestaat of als de cliënt daar toestemming voor heeft gegeven.

Grondslag voor verwerking gegevens werkzoekende, inlichtingenplicht

De uitvoering van de wettelijke taken op het gebied van werk en inkomen brengt mee dat er veel privacygevoelige gegevens worden verwerkt. Zo wordt aan werkzoekenden in verband met hun arbeidsinschakeling gevraagd naar hun tijdsbesteding en dagritme, maar ook naar het gebruik van alcohol en verdovende middelen. Verder worden vragen gesteld over medische aangelegenheden, zoals over het gebruik van geneesmiddelen, over lichamelijke beperkingen en over de aanwezigheid van sociale of psychische problemen. Een werkzoekende heeft de verplichting om mee te werken en de gevraagde gegevens te verstrekken. Een werkzoekende heeft echter ook recht op privacy. De gemeente moet daarom altijd aan de cliënt duidelijk kunnen maken waarom het noodzakelijk is dat hij bepaalde gegevens aan de gemeente verstrekt. Een inbreuk op de persoonlijke levenssfeer mag alleen plaatsvinden als daar een wet aan ten grondslag ligt en de inbreuk noodzakelijk is in het kader van de uitvoering van die wet.

Grondslag voor verwerking gegevens van verwanten/huisgenoten

Bijzondere aandacht dient te worden besteed aan gegevens van verwanten van de werkzoekende. De gemeente heeft soms gegevens nodig van kinderen of inwonende ouders van de werkzoekende. Het gaat dan bijvoorbeeld om inkomensgegevens van meerderjarige kinderen in verband met de afdracht van kostgeld en de berekening van het gezinsinkomen of om inkomensgegevens van de ex-partner in verband met de afdracht van alimentatie. Het verstrekken van deze gegevens wordt door de betrokkenen doorgaans ervaren als een grote inbreuk op hun privacy. Daarom dient het vragen van gegevens van derden tot een minimum beperkt te blijven. Gegevens van verwanten kunnen nodig zijn om bijvoorbeeld het gezinsinkomen te bepalen of om vast te stellen of de aanvrager wel recht heeft op een uitkering. Ook hierbij geldt dat als de gemeente deze gegevens vraagt van verwanten/huisgenoten, voor deze mensen de noodzaak tot verstrekking van hun gegevens, in relatie tot de uitkering van de werkzoekende, duidelijk dient te zijn.

Inlichtingenverplichting instanties

In de Participatiewet zijn de instanties vermeld die verplicht zijn om kosteloos opgaven en inlichtingen aan de gemeente te verstrekken die noodzakelijk zijn voor de uitvoering van de wet. Voor de niet vermelde instanties geldt dat zij zelf dienen af te wegen of verstrekking van de gegevens aan de gemeente verenigbaar is met het doel waarvoor zij de gegevens verkregen hebben en gebruiken. In een aantal gevallen is het instanties (of personen) verboden om inlichtingen aan de gemeente te verstrekken. Het gaat dan om personen die uit hoofde van hun beroep of functie een geheimhoudingsplicht hebben, waaronder met name medici en paramedici op grond van de Wet geneeskundige behandelingsovereenkomst (WGBO), de Wet Beroepsbeoefenaren individuele gezondheidszorg (BIG) of hun beroepscode. Denk bijvoorbeeld aan huisartsen, keuringsartsen en psychologen. Gegevensverstrekking aan de gemeente door personen of instanties met een geheimhoudingsplicht kan alleen na (vrijwillig gegeven) schriftelijke toestemming van de werkzoekende (machtiging). Verder is in de Participatiewet vastgelegd dat bij verstrekkingen door het college, het Inlichtingenbureau en de in de wet genoemde instanties geldt dat zij, indien daartoe bevoegd, gebruik dienen te maken van het Burgerservicenummer.

Geheimhoudingsplicht, wettelijke grondslag of toestemming voor verstrekking

Voor een ieder die betrokken is bij de uitvoering van de Participatiewet geldt een geheimhoudingsplicht: wat hem wordt medegedeeld mag niet verder worden bekend gemaakt dan voor de uitvoering van de wet noodzakelijk is dan wel op grond van de wet is voorgeschreven of toestaan. Verstrekking aan niet bij wet of regeling benoemde instanties is alleen met schriftelijke toestemming van de werkzoekende mogelijk. Wel kunnen desgevraagd gegevens aan derden worden verstrekt ten behoeve van wetenschappelijke onderzoek of statistiek voor zover de persoonlijke levenssfeer van de betrokkenen daardoor niet onevenredig wordt geschaad. Indien er een wettelijke grondslag is voor verstrekking aan de gemeente, dient de verstrekker na te gaan of degene aan wie hij de gegevens verstrekt redelijkerwijs bevoegd is te achten om die gegevens te verkrijgen.

Geen algemene machtiging en geen dwang

Algemeen geformuleerde machtigingen waarmee de werkzoekende toestemming geeft aan derden om inlichtingen te verschaffen aan de gemeente zijn niet toegestaan. In een machtiging moet staan bij wie de gegevens opgevraagd worden en om welke gegevens het gaat. De machtiging kan slechts betrekking hebben op een specifiek geval en mag dus niet algemeen geformuleerd worden. Een machtiging dient vrijwillig door een werkzoekende getekend te worden. Een machtiging mag niet gekoppeld zijn aan een formulier dat de werkzoekende verplicht is in te vullen. Dit wekt namelijk de indruk dat de werkzoekende ook verplicht is om de machtiging te tekenen.

Bestandsvergelijking

Er zijn verschillende vormen van bestandsvergelijking, de wettelijk verplichte en de niet wettelijk verplichte (themacontroles). Bij wet is geregeld dat het Inlichtingenbureau (IB) de bestanden van een aantal organisaties binnen de keten van werk en inkomen met elkaar vergelijkt. Is er ergens sprake van overlap, dan stuurt het IB een samenloopsignaal naar de organisatie die hier belang bij

heeft. Deze organisatie zoekt het signaal uit en onderneemt indien nodig actie in de richting van de werkzoekende. Bij bestandsvergelijkingen in het kader van themacontroles zijn er twee varianten: geanonimiseerde bestandsvergelijking en de vergelijking waaruit tot het individu herleidbare gegevens voortkomen. Geanonimiseerde bestandsvergelijkingen kunnen statistisch materiaal opleveren over bepaalde risicofactoren. Deze gegevens kunnen gebruikt worden voor het opstellen van een risicoprofiel. Over geanonimiseerde bestandsvergelijkingen hoeft de werkzoekende niet te worden geïnformeerd. Voorwaarde hiervoor is wel dat de gegevens op geen enkele manier te herleiden zijn (of zullen worden) tot individuele personen. De Participatiewet staat het vergelijken van bestanden met de daar genoemde organisaties toe mits voldaan is aan een aantal criteria. Zo moet de bestandsvergelijking ten eerste noodzakelijk zijn voor een goede uitvoering van de Participatiewet. Verder moet bestandsvergelijking niet een te zwaar middel zijn in verhouding tot het doel dat men wil bereiken (het proportionaliteitsbeginsel). Ook moet het doel niet op een andere wijze, die minder belastend is voor de persoonlijke levenssfeer, kunnen worden bereikt. Dit is het zogenoemde subsidiariteitsbeginsel.

Het ontvangen van tips

Nadat een tip is binnengekomen beoordeelt de gemeente of deze verwerkt mag worden. Alleen rechtmatig verkregen tips mogen verwerkt worden. Een ander aandachtspunt is de plicht van de gemeente de werkzoekende op de hoogte te stellen van het feit dat zij informatie over hem verkregen heeft. Op grond van de Wbp is het mogelijk om de informatieplicht op te schorten in het belang van het onderzoek. De werkzoekende moet na afloop van het onderzoek alsnog geïnformeerd worden over de met de tip verkregen gegevens en de wijze waarop het onderzoek heeft plaatsgevonden. Deze verplichting geldt ongeacht het resultaat van het onderzoek. De werkzoekende wordt dus ook geïnformeerd over een onderzoek dat geen fraude aan het licht heeft gebracht.

d) Boek 1 Burgerlijk Wetboek

Hierin zijn diverse bepalingen opgenomen met betrekking tot het door de rechter opleggen en het door gecertificeerde instellingen uitvoeren van kindbeschermingsmaatregelen. Verschaffen van inlichtingen aan Raad voor de Kinderbescherming. Degene die op grond van de wet, ambt of beroep tot geheimhouding verplicht is, kan zonder toestemming van degene die het betreft, aan de raad voor de kindbescherming inlichtingen verschaffen, indien dit noodzakelijk is voor de uitoefening van de taken van de raad.

e) Algemene wet bestuursrecht Ambtsgeheim.

Hierin is een bepaling opgenomen die geheimhouding oplegt aan een ieder die betrokken is bij de uitvoering van de taak van een bestuursorgaan ten aanzien van 'gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden'. Dat geldt ook voor de instellingen en de daarvoor werkzame personen die door een bestuursorgaan worden ingeschakeld of de die een bij of krachtens de wet toegekende taak uitoefenen. Naar dit ambtsgeheim wordt vervolgens ook weer in andere wetten verwezen, zoals de Wet bescherming persoonsgegevens en het Wetboek van strafvordering.

f) Wet publieke gezondheid

Meldingsplicht infectieziekten, dossierplicht jeugdgezondheidszorg

Hierin is een meldingsplicht geregeld voor bepaalde besmettelijke ziekten (artsen mogen de hierop betrekking hebbende persoonsgegevens zonder toestemming van betrokkene verstrekken), alsmede de plicht om voor de uitvoering van de jeugdgezondheidszorg eendigitaal bestand bij te houden.

g) Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)

Titelbescherming, tuchtrechtspraak, medisch beroepsgeheim

Deze wet gaat over de kwaliteit van de beroepsuitoefening, met onder meer bepalingen over titelbescherming en tuchtrechtspraak. Tevens is in deze wet de plicht opgenomen om 'geheimhouding in acht te nemen ten opzichte van al datgene wat hem bij het uitoefenen van zijn

beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd, of wat daarbij als geheim ter kennis van hem is gekomen of wat daarbij ter kennis is gekomen en waarvan hij het vertrouwelijke karakter had moeten begrijpen'.

h) Wet bescherming persoonsgegevens (Wbp)

Doelbinding, informatieplicht, privacy-rechten

Geeft, ter uitvoering van art. 10 van de Grondwet, aanvullende regels voor gebruik van persoonsgegevens teneinde het recht op bescherming van de persoonlijke levenssfeer te waarborgen. Doelbinding, transparantie (uitgewerkt in informatieplicht en privacy-rechten), proportionaliteit en subsidiariteit zijn hierbij kernbegrippen.

i) Wet geneeskundige behandelingsovereenkomst (Wgbo)

Geheimhoudingsplicht, dossierplicht, positie wilsonbekwamen

Deze wet is van toepassing op handelingen met betrekking tot de geneeskunst. Geeft bepalingen met betrekking tot geheimhoudingsplicht, dossierplicht, positie meerderjarige wilsonbekwame patiënten en minderjarigen. Wat betreft verwerking van persoonsgegevens zijn er kleine verschillen tussen Wgbo en de Wbp, waarbij de Wgbo, als *lex specialis*, voorgaat voor zover toepassing van beide wettensrijdigheid zou opleveren. De Wgbo geeft de patiënt het recht om een aanvulling in het dossier op te nemen (in Wgb is alleen het recht opgenomen om onjuiste gegevens te corrigeren), kent een ongeclausuleerd vernietigingsrecht (in Wbp is verwijderingsrecht wel aan voorwaarden gebonden) en kent een bewaartermijn van vijftien jaar (Wbp kent geen vaste bewaartermijn, maar zegt wel dat persoonsgegevens niet langer bewaard worden dan noodzakelijk is).

j) Wet politiegegevens

Incidentele en structurele verstrekkingen door politie

De Wet politiegegevens kent een gesloten verstrekkingensysteem. Dat wil zeggen dat limitatief is benoemd aan wie de politie in het kader van de taakuitoefening gegevens mag verstrekken (dit is uitgewerkt in het Besluit politiegegevens). Op degenen die deze gegevens vervolgens ontvangen, rust een eveneens in deze wet geregelde geheimhoudingsplicht die een verbijzondering is ten opzichte van de algemene geheimhoudingsplicht in de Awb en de Wbp. Uitzondering op deze geheimhoudingsplicht is er als de wet dat voorschrijft of de gegevens noodzakelijk zijn om een taak uit te voeren. Bijvoorbeeld kan in het kader van de Jeugdwet de gemeente gegevens van de politie ontvangen over gedragingen van een jeugdige en deze delen met de Raad voor de Kinderbescherming en gecertificeerde instellingen met het oog op de voorbereiding van kindbeschermingsmaatregelen of jeugdreclassering.

Is de verstrekking niet expliciet benoemd, dan kunnen in bijzondere gevallen, voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang en in overeenstemming met het bevoegd gezag politiegegevens incidenteel worden verstrekt aan personen of instanties voor de volgende doeleinden:

- a. het voorkomen en opsporen van strafbare feiten;
- b. het handhaven van de openbare orde;
- c. het verlenen van hulp aan hen die deze behoeven;
- d. het uitoefenen van toezicht op het naleven van regelgeving.

Dat kan ook structureel zijn indien dit is ten behoeve van een samenwerkingsverband van politie met personen en instanties. In dat geval worden extra eisen gesteld aan de vastlegging van de daarop betrekking hebbende beslissing. Bij incidentele verstrekkingen moet men denken aan crisisachtige situaties, bijvoorbeeld wanneer er een KIZ-aanpak is (KIZ: Kleinschalige Incidenten of Zedenzaken). Bij structurele meldingen gaat het altijd om via een convenant/reglement vastgelegde verstrekkingen, zoals bijvoorbeeld bij de aanpak van veelplegers in het kader van het Veiligheidshuis of de aanpak van jeugdoverlast in het kader van een wijkgerichte, sluitende aanpak.

k) Wet justitiële en strafvorderlijke gegevens**Verstrekingen strafvorderlijke gegevens door OM**

Deze wet stelt regels met betrekking tot de verwerking van justitiële gegevens in persoonsdossiers en de verklaring omtrent het gedrag.

Regelt onder andere dat het College van procureurs-generaal (namens het Openbaar Ministerie) strafvorderlijke gegevens kan verstrekken aan personen of instanties (waaronder met name de burgemeester) voor de volgende doeleinden:

- a. het voorkomen en opsporen van strafbare feiten,
- b. het handhaven van de orde en veiligheid,
- c. het uitoefenen van toezicht op het naleven van regelgeving,
- d. het nemen van een bestuursrechtelijke beslissing,
- e. het beoordelen van de noodzaak tot het treffen van een rechtspositionele of
- f. tuchtrechtelijke maatregel,
- g. het verlenen van hulp aan slachtoffers en anderen die bij een strafbaar feit betrokken zijn, of
- h. het verrichten van een privaatrechtelijke rechtshandeling door een persoon of instantie die met een publieke taak is belast.

Die verstrekking moet noodzakelijk zijn met het oog op een zwaarwegend belang of de vaststelling, de uitoefening of de verdediging van een recht in rechte. Bovendien moet redelijkerwijs worden voorkomen dat de gegevens herleidbaar zijn tot een andere dan betrokkene. Veel verstrekkingen aan de burgemeester met het oog op orde en veiligheid vallen hieronder, bijvoorbeeld ook in verband met diens taakuitoefening in het kader van de Wet tijdelijk huisverbod.

l) Wetboek van strafvordering**Verschoningsrecht**

De wet biedt getuigen in een rechtszaak die gebonden zijn aan een geheimhoudingsplicht op grond van een ambts- of beroepsgeheim de mogelijkheid om zich te verschonen, te weigeren een antwoord te geven. Ook kan het zijn dat om die reden de in de wet geregelde aangifteplicht niet geldt. Het is aan de rechter om te bepalen of en in welke mate het verschoningsrecht van toepassing is, wat neer komt op een belangenafweging.

m) Wet gemeentelijke schuldhelpverlening**Identificatieplicht en uitwisseling gegevens**

Deze wet heeft tot doel het ondersteunen bij het vinden van een adequate oplossing gericht op de aflossing van schulden indien redelijkerwijs is te voorzien dat een natuurlijke persoon niet zal kunnen voortgaan met het betalen van zijn schulden of indien hij in de toestand verkeert dat hij heeft opgehouden te betalen, alsmede de nazorg. Voor een goede werking van de wet zal er sprake zijn van informatie-uitwisseling. Betrokkene moet zich bij aanmelding in het kader van deze wet legitimeren. Ten behoeve van een integraal overheidsoptreden ten aanzien van de voorkoming en bestrijding van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, de voorkoming en bestrijding van belasting- en premiefraude en het niet naleven van de arbeidswetten, wordt samengewerkt door de colleges van burgemeester en wethouders, het Uitvoeringsinstituut werknemersverzekeringen en de Sociale verzekeringsbank.

n) Wet basisregistratie personen (Wet BRP)**Verstrekingen aan andere overheidsorganen en derden**

Deze wet vormt het algemeen kader voor de uitvoering van de zogenaamde 'basisregistratie personen' door de overheid (BRP was voorheen GBA: gemeentelijke basisadministratie). Geregeld is onder meer in welke gevallen de gemeente gegevens uit deze registratie mag verstrekken aan andere overheidsorganen of derden. In het kader van deze wet kan onder bepaalde voorwaarden toegang worden verleend tot (delen) van de basisregistratie.

**o) Wet algemene bepalingen Burgerservicenummer / Wet gebruik
Burgerservicenummer in de zorg**

Gebruik Burgerservicenummer

Deze wetten verplichten de overheid en zorgaanbieders om bij hun taakuitoefening gebruik te maken van Burgerservicenummers. Ook is hierin een legitimatieplicht geregeld. Dat moet zorgen voor minder fouten bij gegevensuitwisseling, voorkomen van persoonsverwisseling, eenvoudiger declareren en betere bescherming tegen identiteitsfraude.

Bijlage C: Privacymatrix

		PRIVACY MATRIX									
		INTERN					EXTERN				
DOCUMENTEN	A - Externe Medewerker	B - Medewerker	C - Burger	D - Samenwerken de Instantie (SI)	E - Medewerker bij SI	F - Bewerker (BW)	G - Medewerker er bij BW	H - Externe (niet-bewerker)			
	① Privacy beleid	①	①	①	①		①		①		
② Conenant/overeenkomst				②							
③ Privacy Reglement			③	③				③			
④ Bewerkerovereenkomst						④					
⑤ Geheimhoudingsverklaring	⑤			⑤	⑤			⑤			
⑥ Privacy Protocol	⑥	⑥		⑥	⑥			⑥			
Collectief											
Indiv.											

SI : Samenwerkende Instantie

BW : Bewerker in de zin van de Wet bescherming persoonsgegevens

Documenten

1. In een *Privacy Beleid* staat wat de uitgangspunten inzake privacy zijn voor de gemeente. Dat moet kort, simpel en transparant verwoord zijn. Het is een publiek document (Internet/Intranet) dat voor een breed publiek toegankelijk moet zijn. Het beleid is intern en extern en van toepassing. Voor burgers is het een statement, voor alle andere partijen bevat het bindende uitgangspunten voor samenwerking.
2. In een *Conenant* wordt contractueel omschreven wat het doel van de overeenkomst is en wordt naar het Privacy Reglement verwezen naar welke regels er gelden m.b.t. de informatiebeveiliging en in het verlengde daarvan de privacy. Te denken valt ook aan de inkoopovereenkomst en uitvoeringsovereenkomst bij subsidiebesluiten. Ook het enkele subsidiebesluit met daaraan verbonden voorschriften is mogelijk.
3. In een *Privacy Reglement* staat verwoord wat de regels inzake privacy zijn waar partijen zich aan moeten houden. Dat is een nadere uitwerking van het Privacy Beleid, concreet dus. Dat wordt strikt verwoord en heeft de status van Openbaar Reglement. Het is een onderlegger van elke overeenkomst met een externe samenwerkende partij die geen Bewerker is.

4. In een *Bewerksvereenkomst* wordt contractueel omschreven hoe een externe partij met de bewerking van privacygevoelige informatie om moet gaan, wat het doel van de overeenkomst is en welke regels er gelden m.b.t. de informatiebeveiliging en in het verlengde daarvan de privacy. Het bevat o.a. sancties.
5. In een Geheimhoudingsverklaring wordt contractueel omschreven waar een persoon aan gehouden is m.b.t. geheimhouding en privacy. Het is de gepersonaliseerde versie van een reglement. Het bevat o.a. sancties.
6. In een Privacy Protocol staan de gedragsregels voor personen die omgaan met privacygevoelige informatie. Als het Privacy Reglement of Convenant het 'Wat' omschrijft, dan gaat een protocol over 'Hoe'.

Partijen (collectief) en Individuen

- A.** Een *Externe* die onder direct gezag van de gemeente intern werkzaamheden verricht, zal als onderdeel van het contract met hem/haar of diens werkgever een individuele Geheimhoudingsverklaring moeten ondertekenen. Daarbij wordt verwezen naar het Privacy Beleid (Internet/Intranet). Ter ondersteuning van de dagelijkse praktijk krijgt de externe ook het Privacy Protocol overhandigd.
- B.** Een *Medewerker* die onder direct gezag van de gemeente werkzaamheden verricht, legt de ambtse af. Binnen de gemeentelijke cao zijn de sancties vermeld die betrekking hebben op het schenden van de ambtse af. Dat dekt het formele aspect van geheimhouding. Daarnaast wordt verwezen naar het Privacy Beleid (Internet/Intranet). Ter ondersteuning van de dagelijkse praktijk krijgt de medewerker ook het Privacy Protocol overhandigd.
- C.** Een *Burger* zoekt naar houvast en transparantie over hoe de gemeente met informatiebeveiliging en diens privacy omgaat. Dat staat helder verwoord in het Privacy Beleid. Ook wil hij weten wat de regels zijn, met name die hem aangaan over inlichten, bezwaren en klachten. Hier voorziet het Privacy Reglement in.
- D.** Een *Samenwerkende Instantie* trekt samen met de gemeente op in uitvoering van taken namens de gemeente. Dat betekent dat deze zoveel mogelijk gefaciliteerd moeten worden en dat de gemeente een extra verantwoordelijkheid heeft in het afdwingen van regels en protocollen op grond van haar eigen expertise en verantwoordelijkheid.
- E.** Het bovenstaande uit punt **D** strekt zich dan per definitie uit naar een *Medewerker/Vrijwilliger* bij de Samenwerkende Instantie, die daar taken uitvoert waarbij het in geding komen van de informatieveiligheid of privacy van burgers altijd de gemeente aangerekend zal worden.
- F.** Een *Bewerker* is een professionele partij die namens de gemeente gegevens opslaat en mogelijk ook bewerkt. Hiertoe sluiten partijen een contract af, waarbij de informatieveiligheid en privacy voorzieningen die de Bewerker treft in de Bewerksvereenkomst benoemd worden. Hierin staat o.a. dat een Geheimhoudingsverklaring en Privacy Protocol expliciet tot de interne verantwoordelijkheid van de Bewerker horen.
- G.** Het bovenstaande uit punt **F** strekt zich dan per definitie uit naar een *Medewerker* bij de *Bewerker*, die daar taken uitvoert waarbij het in geding komen van de informatieveiligheid of privacy van burgers direct de Bewerker contractueel aangerekend zal worden. De bewerker organiseert zichzelf op dit punt en is daarop contractueel aanspreekbaar.
- H.** Een *Externe* die in opdracht van de gemeente (extern) werkzaamheden verricht, zal als onderdeel van het contract met hem/haar of diens werkgever een individuele Geheimhoudingsverklaring moeten ondertekenen. Daarbij wordt verwezen naar het Privacy Beleid (Internet/Intranet). Ter ondersteuning van de dagelijkse praktijk krijgt de externe ook het Privacy Protocol overhandigd.