PRIVACYBELEID BEST 2017

De route naar privacycontrol op 25 mei 2018

Versie 1.0

Datum: 31-03-2017

1. Noodzaak privacybeleid

1. Privacybeleid

In de afgelopen jaren heeft de gemeente Best gewerkt aan het op adequaat niveau brengen van de uitvoering van de privacywetgeving. Er is in kaart gebracht welke processen met persoonsgegevens de gemeente uitvoert en al deze processen zijn beoordeeld tegen de achtergrond van het omvangrijke wettelijk kader op privacygebied. Een aantal van die processen is gemeld bij de Autoriteit Persoonsgegevens (AP).

Het resultaat van die werkzaamheden heeft de gemeente Best voor de komende jaren geborgd door maatregelen te treffen in onderhoud, beheer en advisering. Dit betreft voornamelijk werkzaamheden op tactisch en operationeel gebied. De coördinatie en advisering op privacygebied is belegd bij juridische zaken. Het privacybeleid dient echter nog te worden ontwikkeld. Bestuur, management en medewerkers dienen te weten op welke wijze de gemeente Best uitvoering geeft aan de privacywet- en regelgeving en waarmee zij in hun werk rekening moeten houden als het om privacybescherming gaat. Onder privacywetgeving wordt in het algemeen verstaan de Wet bescherming persoonsgegevens (Wbp), privacyvoorschriften in sectorale wet- en regelgeving en de Algemene verordening gegevensbescherming (Avg).

2. Noodzaak van beleid

Gevoeligheid gegevens cliënten in het sociaal domein en veiligheid

Met de overdracht van taken in het sociaal domein heeft de gemeente meer en privacygevoeliger gegevens te verwerken gekregen. Door de integrale aanpak van meervoudige problemen worden gegevens uitgewisseld met maatschappelijke en zorgpartners. Daarbij is van belang dat de uitwisseling van die gegevens minimaal binnen de juridische kaders van de privacywetgeving plaatsvindt. VNG en KING adviseren om hiervoor beleid te ontwikkelen.

De rol van de gemeente op het gebied van openbare orde en met name veiligheid ondergaat verandering. Veiligheidsinstanties roepen de gemeente op om signalen uit de samenleving over vermoedelijke radicalisering door te geven en of gegevens te verzamelen in het kader van het creëren van een ondermijningsbeeld. De vraag is eigenlijk niet meer of de gemeente Best daaraan medewerking gaat verlenen, maar eerder onder welke privacybeschermende voorwaarden. Daar is beleid voor nodig en er dient bestuurlijke verantwoordelijkheid voor de privacy van de betrokkenen te worden genomen.

Nieuw wettelijk kader

Sinds 14 april 2016 is de Avg van kracht. De Avg heeft rechtstreekse werking in de lidstaten van de EU. De gemeente Best moet op 25 mei 2018 aan de Avg voldoen, dat wil zeggen aantoonbaar kunnen maken dat zij in control is op privacygebied. In de overgang

van Wbp naar Avg blijft de Wbp van kracht. Deze wet is sinds 1 januari 2016 uitgebreid met een meldplicht voor datalekken. Bij gelegenheid van deze wetswijziging is de naam van het College bescherming persoonsgegevens, verandert in Autoriteit Persoonsgegevens en de AP heeft de bevoegdheid gekregen om (hoge) boetes op te leggen als niet aan de Wbp wordt voldaan.

De Avg is in hoofdlijnen vergelijkbaar met de Wbp. De belangrijkste wijzigingen die het gevolg zijn van de Avg:

- Overheidsorganisaties moeten een functionaris voor de gegevensbescherming aanstellen, die toeziet op de naleving van de Avg.
- De Europese burger moet meer controle over en keuze in de verwerking van persoonsgegevens krijgen. De Europese wetgeving sluit beter aan op de nieuwe technologieën waarmee deze gegevens worden verzameld.
- De verordening brengt grote administratieve lasten met zich mee. Organisaties moeten investeren in het aanpassen van alle systemen die niet aan de Avg voldoen. Daarnaast moeten zij uitgebreide documentatie bijhouden over alle verwerkingen van persoonsgegevens die zij doen en alle verwerkingen die zij uitbesteden aan 'verwerkers' (nieuwe begrip voor bewerker, gebaseerd op artikel 4, lid 9 Avg).
- Bij processen waarvoor een hoog privacyrisico wordt voorzien dient de gemeente een gegevensbeschermingseffectbeoordeling (artikel 35 Avg) of wel een privacy impact assesments (PIA) uit te voeren, voordat de persoonsgegevens worden verwerkt.
- De Avg voorziet ook in een meldplicht datalekken zoals die nu al geldt onder de Wbp. Datalekken dienen te worden gemeld bij de nationale toezichthouder en bij degene wiens gegevens gelekt zijn.

3. Samenloop met beveiligingsbeleid

Artikel 30 Avg (13 van de Wbp) vormt het algemeen wettelijk kader voor de beveiliging van persoonsgegevens. Ingevolge dat artikel dient de verantwoordelijke de noodzakelijke beveiligingsmaatregelen te treffen ter voorkoming van misbruik en verlies van persoonsgegevens.

De ontwikkeling van gemeentebreed veiligheidsbeleid loopt parallel met de ontwikkeling van het privacybeleid. Waar privacybeleid met name gaat over hoe om te gaan met persoonsgegevens, gaat het beveiligingsbeleid over de strategische, tactische en operationele maatregelen die de gemeente treft om de persoonsgegevens te beveiligen. Best beschikt door de werkzaamheden van de afgelopen jaren over een actueel beeld van de persoonsinformatiehuishouding en heeft daarmee inzicht in wat er aan persoonsgegevens moet worden beveiligd. Door de onderhoud- en beheermaatregelen die reeds zijn getroffen zal dat beeld worden bijgehouden en

geactualiseerd. Het register van verwerkingen van persoonsgegevens vormt daarmee een substantieel deel van het instrumentarium dat nodig is om de beveiliging te kunnen regelen.

2. Governance en beleid

1. Directie en management zijn verantwoordelijk en hebben beleid nodig om hun verantwoordelijkheid te kunnen nemen op privacygebied

Alhoewel de Avg al van kracht is, blijft de Wbp tot 25 mei 2018 de overkoepelende wetgeving op het gebied van privacybescherming. De Wbp is een kaderwet waaraan publieke en private organisaties zich moeten houden.

De verantwoordelijkheid voor de uitvoering en handhaving ligt bij de verantwoordelijke, in casu de burgemeester, respectievelijk het college van burgemeester en wethouders. Voor gegevensverwerkingen bij de Griffier (bijvoorbeeld over de raadsleden zelf of gegevens over personen in aan de Raad gerichte post) is de gemeenteraad het verantwoordelijke bestuursorgaan.

Ambtelijke verantwoordelijkheid verloopt via de lijnen van het mandaatbesluit, waarbij de uitvoering in de lijn in (sub)mandaat bij de directie en afdelingsmanagers ligt. Net zoals een manager zich houdt aan de financiële kaders, moet deze ook de algemene privacykaders van de Wbp en de bijzondere regels in de wetgeving die hij/zij uitvoert in acht nemen.

Privacy speelt zich echter niet alleen in de lijn af. Een aantal privacy-issues is afdelingsoverstijgend. De verantwoordelijkheid voor dergelijke issues ligt bij de directie. Bijvoorbeeld voor de keteninformatisering die optreedt als gevolg van de invoering van de basisregistraties of het brede gebruik van de documentaire informatievoorziening, het thuiswerken of in de Cloud werken.

Het is enerzijds van belang dat directie en afdelingsmanagers zich bewust zijn van de rol en de verantwoordelijkheid die daarbij hoort en anderzijds dat ze daar ook naar kunnen en gaan handelen. Om dat te bewerkstelligen is een beleid en beheerinstrumentarium voor privacy noodzakelijk met bijbehorende besluitvormingsstructuur en –procedure. Burgemeester en wethouders stellen het beleid vast, directie en afdelingsmanagers voeren namens het college uit en besluiten over de beleidsissues die zij vanuit de organisatie ter besluitvorming krijgen voorgelegd.

2. Grip op privacy via de planning en controlcyclus

Om grip op privacy te krijgen en te houden is het nodig dit onderwerp (meer en integraal) mee te nemen als onderdeel van de bedrijfsvoering. De invulling daarvan ligt bij de managers. Elke manager zal uiteindelijk moeten aantonen in control te zijn op privacygebied.

3. Privacybeleid vergt kennis, kunde én capaciteit

3.1 FG/Avg

De uitvoering en handhaving van de privacywetgeving vergt tamelijk specialistische kennis en kunde, die logischerwijze niet bij directie en management voorhanden is. Een privacydeskundige kan directie en management hierin ondersteunen.

Vanaf 25 mei 2018 stelt de Avg de aanstelling van een functionaris voor de gegevensbescherming (kortweg FG) verplicht voor overheidsorganisaties. Dit is een privacydesdeskundige die naast coördinerende, toetsende, adviserende en beheertaken ook een toezichthoudende rol heeft. Bijlage 2 bevat een uitgebreide omschrijving van de taken, verantwoordelijkheden en bevoegdheden van de FG.

Belangrijkste taken FG in het kort

- Adviseren over de mogelijkheden van gebruik van persoonsgegevens en bij datalekken
- Begeleiden privacy impact assessments
- Aanleg en onderhoud openbaar register met verwerkingen persoonsgegevens
- Toezicht houden op het verwerken van persoonsgegevens in de organisatie
- Rapporteren over de omgang met persoonsgegevens door de organisatie
- Intermediair tussen burger en gemeente voor inzage en correctie

Het is uitdrukkelijk niet de bedoeling dat deze functionaris de taken op het gebied van de privacybescherming van de afdelingen overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het borgen van het omgaan met privacygevoelige gegevens.

3.2 Toetsing en advisering

De vrijwel permanente veranderingen in organisatie en processen als gevolg van nieuwe wetgeving, verbetering van de dienstverlening, samenwerkingen met andere gemeenten en met maatschappelijke partners, dienen getoetst te worden aan de kaders van de privacywetgeving. Dat geldt ook voor het koppelen van gegevensbestanden, zoals bijvoorbeeld is gebeurd tussen de basisregistratie personen enerzijds en de systemen die de bedrijfsprocessen ondersteunen anderzijds. Daarnaast hebben zich inmiddels nieuwe privacyvraagstukken aangediend op het gebied van het sociaal domein, moeten er besluiten genomen worden over bijvoorbeeld het thuiswerken met BRP-gegevens, het beschikbaar stellen van persoonsgegevens aan leveranciers voor testdoeleinden, big data, cloudcomputing en Bring Your Own Device (BYOD).

3.3 Administratieve en beheer taken

Onder de administratieve taken vallen onder meer het beheer van het register van gegevensverwerkingen en het doen van en intrekken van meldingen. De voornoemde veranderingen dienen verwerkt te worden in het openbaar register en bij de AP moeten (voorlopig nog) eventuele meldingen worden gedaan of juist worden ingetrokken.

3.4 Capaciteitsinzet

Voor een deugdelijke en adequate uitvoering van de rol van FG is formatieve capaciteit nodig. De omvang van die capaciteitsinzet voor Best is thans een kwestie van schatten. Onze ervaring met dit vraagstuk bij andere gemeenten leert ons dat de capaciteitsinzet zal uitkomen tussen een halve en een hele formatieplaats.

Hieronder volgen nog enkele voorbeelden van privacyvraagstukken ter onderbouwing van deze veronderstelling. Advisering bij

- datalekken;
- invoering nieuwe wet- en regelgeving;
- gegevensverzameling in het kader van criminaliteitsbestrijding (ondermijningsbeeld);
- periodieke aanpassingen in werkprocessen met persoonsgegevens;
- het gebruik van persoonsgegevens in Big data-projecten;
- toenemend aantal inzage en correctieverzoeken als gevolg van het toegenomen privacybewustzijn bij burgers.
- invoering van zaakgericht werken.

Bovendien zal de gemeente opvolging moeten geven aan adviezen van de AP, zoals bijvoorbeeld recent het verbod op het gebruik van camera's door de sociale recherche of naar aanleiding van de publicatie van de AP over toestemmingen in het sociaal domein (21 april 2016) en de publicatie van een adres van een wietkwekerij (6 juni 2016, Renkum).

De ervaring over de komende jaren zal uitmaken hoeveel tijd er uiteindelijk aan privacy besteed zal worden. Gelet op de betrokkenheid bij organisatie, procesinrichting en dagelijkse uitvoeringspraktijk, ligt een regionale invulling van de rol niet voor de hand. De ervaring bij andere gemeenten met een regionale FG leert dat de 'grotere afstand' ten opzichte van de organisatie en de verdeling van de aandacht over meerdere gemeenten aan een adequate invulling van de rol in de weg staan.

In de periode die loopt tot aan 25 mei 2018 zal de gemeente Best de privacyrol die juridische zaken vervult in meer adviserende zin moeten inzetten om zo tot een deugdelijke implementatie van de privacyvoorschriften te komen. Uiteindelijk zullen privacy en beveiliging als randvoorwaarden deel moeten gaan uitmaken van de kwaliteitscriteria waarmee beleids- en kwaliteitsmedewerkers rekening moeten houden bij de inrichting van (nieuwe) processen. De privacyrol van juridische zaken kan daardoor verschuiven van adviserend naar toezichthoudend. Het is aan de controller om te (laten) beoordelen of de gemeente in control is op privacy. Het is in dit kader dan ook

van belang dat de uiteindelijke FG niet meerdere functies uitoefent die zodanig invloed op elkaar kunnen uitoefenen, dat de integriteit in het geding komt.

3. Privacybeleid is vooral een belangenafweging

De toepassing en uitvoering van de wettelijke privacykaders is in het algemeen gesproken complex van aard. Bovendien is het onderwerp privacy nogal eens onderwerp van discussie en wordt vaak als sta in de weg ervaren voor de verbetering van de dienstverlening en bedrijfsvoering. De vraag die zich dan aandient is op welke manier geeft de organisatie uitvoering aan de privacywetgeving en wie is waarvoor verantwoordelijk. Anders gezegd, wie beslist binnen de organisatie of het belang van de privacy en de daarvoor te treffen maatregelen opwegen tegen 'het organisatiebelang'. In feite gaat het dan over privacybeleid. Voor dat beleid gelden de volgende uitgangspunten.

1. Uitgangspunten van beleid

1. Burgers hebben het recht om de over hen bij de overheid bekende en beschikbare gegevens niet opnieuw te hoeven verstrekken.
2. Burgers beschikken over het grondwettelijk recht op privacy, waaronder het recht op informationele privacy.
3. Best is voortdurend bezig de dienstverlening en bedrijfsvoering te verbeteren en een deugdelijke persoonsinformatiehuishouding geldt daarvoor 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 en wordt opgevat als kenmerk van goede dienstverlening / kwaliteit. Dat impliceert dat de wettelijke uitgangspunten in acht moeten worden genomen.
5. Het privacyrecht zal op een efficiënte en effectieve wijze worden toegepast.
6. De Wet bescherming persoonsgegevens (en ook de Avg) gaat uit van zelfregulering en laat ruimte tot interpretatie.
7. Directie, management en medewerkers hebben behoefte aan beleid op het gebied van de toepassing en uitvoering van de privacyregels.

2. Beleid ten aanzien van gebruik van persoonsgegevens algemeen

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 een van de basisregistraties, gebruikt de medewerker dat gegeven tenzij dat gegeven onjuist is.
3. Het delen van gegevens is gebaseerd op de mogelijkheden die de wet biedt en in die gevallen waarin de wet niet voorziet wordt een noodzakelijkheidstoets uitgevoerd gebaseerd op het triagemodel (opgenomen in bijlage 3).

4. 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.

5. De afdelingsmanager 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. De afdelingsmanager neemt daarbij de wettelijke uitgangspunten in acht met betrekking tot:

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

    b. proportionaliteit: niet meer gegevens gebruiken, dan toereikend en strikt noodzakelijk is;

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

6. Het managementteam is verantwoordelijk voor de gemeentebrede naleving van de Wbp en de directie beslist over privacyissues die afdelingsoverschrijdend zijn.

7. Er is een FG die directie, afdelingsmanagers en managementteam gevraagd en ongevraagd van advies dient met betrekking tot de bescherming van de persoonlijke levenssfeer van degenen over wie in de organisatie van de gemeente Best persoonsgegevens worden verwerkt.

    Wijzigingen in de wijze waarop uitvoering wordt gegeven aan primaire en bedrijfsvoeringprocessen met al dan niet volledige organisatiebrede consequenties die ook van invloed zijn voor de manier waarop met persoonsgegevens wordt omgegaan, dienen te worden getoetst aan de privacywetgeving door de FG (bijvoorbeeld thuis werken, BYOD en uitbesteding van werk aan een derde partij, gegevensdeling in het sociaal domein). Het informatiebeleid zal in lijn moeten zijn met het privacybeleid.

8. 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 (gegevensbeschermingseffectbeoordeling) deel uit van het implementatieproces.

3. Beleid ten aanzien van gebruik van persoonsgegevens uit de BRP

1. De verstrekking van persoonsgegevens uit de BRP en de wijze van verstrekking is gebaseerd op de Wet BRP, de Verordening gegevensverstrekking basisregistratie personen Best 2014 en het Autorisatiebesluit van de Minister van Binnenlandse Zaken d.d. 19 februari 2015, kenmerk 2015-0000015068 en opvolgende versies van dat besluit.

2. De gegevensuitwisseling tussen de BRP en de gebruikers van de BRP wordt vastgelegd in het register van gegevensverwerkingen. Het register regelt de volgende onderwerpen.

    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 BRP nodig zijn;

    e. De verplichting tot terugmelding bij gerede twijfel over de juistheid van de gegevens uit de BRP.

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 tot uitbreiding van de gegevensset als bedoeld onder 3 is bevoegd de manager van de afdeling waarbij de medewerker werkzaam is. De afdelingsmanager vergewist zich of de uitbreiding van de gegevensset voor de uitvoering van de taak noodzakelijk is en niet in strijd is met de Wet bescherming persoonsgegevens.

5. Bij onzekerheid over de uitleg van de privacywetgeving of vermoeden van strijd met deze wetgeving, legt de afdelingsmanager het verzoek, voorzien van een advies van de FG, ter besluitvorming voor aan de directie. Directie of in voorkomend geval het bestuursorgaan, dat is aan te merken als de verantwoordelijke voor de verwerking van persoonsgegevens, besluiten.

4. Privacybeleid in de praktijk

1. Best heeft zicht op alle processen waarin persoonsgegevens een rol spelen

1.1 Primaire processen

De gemeente Best verwerkt persoonsgegevens op tal van beleidsterreinen. Dat gebeurt zowel binnen het sociaal domein, als op het gebied van openbare orde en veiligheid, fraude-opsporing en handhaving van illegale activiteiten, als voor het uitnodigen van burgers om een zienswijze te geven over een bestemmingsplan.

Alle processen met persoonsgegevens van alle beleidsterreinen zijn in kaart gebracht en getoetst aan de privacyvoorschriften. Een register met deze processen is beschikbaar en biedt, ook aan burgers, inzicht in:

- Het doel van de verwerking van persoonsgegevens;
- De categorieën van personen over wie gegevens worden verwerkt;
- De gegevens per categorie van personen die worden verwerkt;
- Met wie (delen van de set aan) persoonsgegevens worden gedeeld;
- De rechtmatige grondslag waarop de verwerking is gebaseerd;
- De bewaartermijn die geldt voor de persoonsgegevens;
- Of de gemeente werkzaamheden heeft uitbesteed, waarvoor een bewerkersovereenkomst moet zijn vastgesteld;
- De herkomst van de gegevens, bijvoorbeeld afkomstig van de burger zelf of uit een basisregistratie.

Processen die daarvoor in aanmerking komen, zijn gemeld bij de AP en terug te vinden op https://www.cbpweb.nl.

Wijzigingen in wet- en regelgeving, processen, dienstverlening, en andere zaken worden getoetst aan de privacyvoorschriften. De administratieve werkzaamheden van de Wbp leiden vervolgens tot een aanpassing of intrekking van een melding, dan wel een nieuwe melding. Daarnaast leiden die werkzaamheden tot aanpassing van het register.

1.2 Bedrijfsvoering

Naast gegevens van burgers in primaire processen, verwerkt de gemeente Best persoonsgegevens van haar medewerkers. Persoonsgegevens van medewerkers zijn te vinden in de personeels- en salarisadministratie, ICT-administratie (ten behoeve van autorisaties en beveiligingsbeheer), maar ook als behandelaar van een aanvraag van een burger. De verwerking van persoonsgegevens van personeelsleden is vastgelegd in een privacyreglement, dat jaarlijks dient te worden geactualiseerd. Voor de monitoring van

het gebruik van informatiesystemen, telefonie en internet zijn door de OR goedgekeurde protocollen beschikbaar.

1.3 Communicatie en training medewerkers gemeente en partners

Het bestuurlijk/juridisch instrumentarium dat de gemeente Best inzet om privacyproof uitvoering te geven aan haar taken, zal ook in de praktijk van de medewerkers moeten landen.

Medewerkers van de gemeente en van partners moeten kennisnemen van deze regels en geïnstrueerd worden over de manier waarop ze met persoonsgegevens kunnen en moeten omgaan. Een en ander zal worden geborgd door middel van een communicatie-plan.

1.4 Communicatie met de burger

Burgers worden op allerlei manieren op de hoogte gehouden van de bestuurlijke en maatschappelijke veranderingen. Voor wat betreft de verwerking van persoonsgegevens is het van belang dat de burger geïnformeerd wordt over het doel van de verwerking van diens gegevens, welke gegevens op welk moment in het proces nodig zijn (ook wel triage genoemd) en met wie welke gegevens noodzakelijkerwijze gedeeld gaan worden. Het moment van informeren is in de meeste gevallen het moment waarop een burger om hulp vraagt. In sommige situaties, bijvoorbeeld in het geval de burger niet zelf om hulp vraagt, kan de burger op een later moment worden geïnformeerd. De informatie-plicht jegens de burger is in de procesinrichting van gemeente en partners voorzien.

Het moment van informeren wordt tevens benut om, indien nodig toestemming te vragen om gegevens te mogen verwerken of uit reeds bestaande dossiers bij de gemeente gegevens te hergebruiken en om eventuele bijzondere gegevens omtrent de gezondheid te mogen opvragen bij een medicus.

Buiten de informatieplicht heeft een burger te allen tijde recht op inzage en kan deze de gemeente verzoeken foutieve gegevens te corrigeren.

2. Privacybeleid in specifieke beleidsterreinen

2.1 Sociaal domein

De nieuwe taken die de gemeente in het sociaal domein sinds 1 januari 2015 in uitvoering heeft genomen gaan gepaard met de verwerking van, veelal bijzondere, persoonsgegevens van nieuwe klantgroepen. Bestaande processen zijn of worden opnieuw ingericht en de regie op de integrale behandeling van meervoudige problemen is bij een ondersteuningsteam belegd. De verwerking van persoonsgegevens in de nieuwe processen moet voldoen aan de privacywetgeving, waardoor burgers erop kunnen vertrouwen dat de gemeente en haar partners zorgvuldig omgaan met hun persoonsgegevens.

2.1.a Overleg over cliënten

Efficiency, effectiviteit en kwaliteit van de dienstverlening zijn er mee gebaat dat daar waar nodig en mogelijk, zowel intern als extern afstemming over een cliënt plaatsvindt

tussen de verschillende onderdelen van het sociaal domein. Ondanks dat dit ook een van doelstellingen is van de wetgever, heeft deze het nagelaten om dat te regelen.

Participatiewet, Jeugdwet en WMO 2015 kennen daarvoor ieder hun eigen regels. In die gevallen dat het gewenst is om gegevens uit te wisselen, geldt de wet waarop een verzoek is gebaseerd als uitgangspunt van handelen. Dat betekent in het geval van de WMO 2015 dat de WMO-consulent toestemming van de betrokkene nodig heeft om de reeds bij de gemeente beschikbare gegevens over een uitkering of schuld op te vragen bij de bijstandsconsulent respectievelijk de medewerker schuldhulpverlening (artikel 5.1.1. lid 4 WMO 2015). Bij de inrichting van het overleg dient dit als uitgangspunt te gelden.

2.2 Openbare orde en veiligheid

De afgelopen jaren is de gemeente Best steeds meer persoonsgegevens gaan verwerken van personen die een bedreiging (kunnen) vormen voor de openbare orde en veiligheid. Het oplossen van problemen met (potentiële) overlastgevers is steeds vaker een bestuurlijke in plaats van een politionele aangelegenheid en gegevens van politie en justitie worden meegenomen in casusoverleg in het sociaal domein. De uitwisseling van dergelijke gegevens levert in de praktijk de nodige vraagstukken op privacygebied op die moeten worden opgelost.

3. Openbaarheid van bestuur

Publicatie van persoonsgegevens op internet wordt tot het uiterste beperkt. In de eerste plaats dient te worden afgewogen of aan publicatie van persoonsgegevens (spontaan zowel als op verzoek) niet valt te ontkomen. Als publicatie onontkoombaar is, dan wordt afgewogen of het publicatiemiddel internet het kanaal is waarlangs gepubliceerd wordt. De gemeente Best hanteert daarbij als uitgangspunt de Richtsnoeren voor actieve openbaarmaking en de Richtsnoeren inzake de publicatie van persoonsgegevens op internet. Mocht publicatie van persoonsgegevens op internet noodzakelijk zijn, dan zullen die gegevens worden afgeschermd voor zoekmachines.

Bijlage 1: Register verwerkingen persoonsgegevens

(apart bestand)

Bijlage 2:
Functionaris voor de gegevensbescherming (FG)
Taken, verantwoordelijkheden en bevoegdheden

1. De FG beoordeelt de verwerking van persoonsgegevens tegen de achtergrond van de kaders van de privacywetgeving en adviseert directie en afdelingsmanagers bij wijzigingen in procesuitvoering en bedrijfsvoering en de toepassing van een privacy impact assessment.

2. De FG neemt als adviserend lid deel aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens.

3. De FG heeft verder als taak

    a. de uitleg van de privacyvoorschriften in de Wbp, Avg, en in de sectorale wetgeving;

    b. onderhouden van het privacybeleid;

    c. coördineren van de privacywerkzaamheden;

    d. beheren en openbaar maken van het overzicht van gegevensverwerkingen van de gemeente Best;

    e. (tot 25 mei 2018) verzorgen van meldingen en intrekkingen van meldingen bij de AP;

    f. te fungeren als aanspreekpunt voor de AP;

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

    h. procedures in te richten voor het melden van datalekken waarbij persoonsgegevens betrokken zijn.

4. De FG is bevoegd

    a. jaarlijks te rapporteren aan de directie over de uitvoering van de privacyregelgeving door de organisatie;

    b. meldingen en intrekkingen van meldingen te ondertekenen.

5. De FG is verantwoordelijk voor het in stand houden van de kennis die voor het vakgebied noodzakelijk is.

6. Vanaf 25 mei 2018 vervult de FG ook de rol van toezichthouder.

Bijlage 3: Triagemodel gegevensdeling

Dit model geldt voor de professionals van de gemeente Best als uitgangspunt voor het maken van de afweging of en wanneer persoonsgegevens mogen worden gedeeld met personen of organisaties in het sociaal domein. Het model volgt het afwegingsproces geredeneerd vanuit de professional / hulpverlener.

Er wordt uitgegaan van de wettelijke mogelijkheden tot uitwisseling van gegevens. Dat betekent dat geen toestemming hoeft te worden gevraagd in die situaties waarin de van toepassing zijnde wetgeving mij als professional de bevoegdheid geeft gegevens van een cliënt te verwerken1. Is er geen wettelijke bevoegdheid, dan is toestemming vereist. In die gevallen waarbij de toestemming voor het verwerken of delen van gegevens niet kan worden verkregen, weeg ik de gewenste gegevensverwerking/-uitwisseling af tegen de noodzaak van de hulp, zorg of bijsturing die ik wil verlenen. Met wie wil ik welke informatie delen en op welk moment? Is mijn aanpak zuiver gericht op de beoogde doelstellingen?

- <u>Komen tot een aanpak</u>

In samenspraak met de cliënt en personen in zijn omgeving kom ik tot een passende aanpak voor de geconstateerde problemen. Ik neem in deze aanpak mee met wie ik wil samenwerken en welke gegevens ik daarvoor wens te verwerken en uit te wisselen. Dit bespreek ik met de cliënt. Mochten de cliënt niet instemmen met mijn aanpak, dan stel ik hem in de gelegenheid zijn bezwaren te uiten.

- <u>Afwegen gegevensverwerking/-uitwisseling</u>

Ik stel mijzelf de volgende algemene vragen:

  - Noodzaak: welke gegevens zijn noodzakelijk gegeven het gestelde doel?
  - Subsidiariteit: is het delen of opvragen van informatie de minst ingrijpende maatregel? (need-to-know)
  - Proportionaliteit: staan het delen of opvragen van informatie en het doel met elkaar in verhouding? Kan het ook met minder informatie?
  - Kan en mag het: zijn er specifieke privacyregels die gelden voor betrokken partijen?

- <u>Informeren</u>

Is het in het belang van de cliënt om hem op de hoogte te stellen van mijn afweging vóórdat ik overga tot het uitwisselen van gegevens of is in het belang van de cliënt om

[1] Bijvoorbeeld artikel 5.1.1 WMO: Het college is bevoegd tot het verwerken van persoonsgegevens van de cliënt, waaronder persoonsgegevens betreffende de gezondheid die noodzakelijk zijn voor de beoordeling van diens behoefte aan ondersteuning van zijn participatie of zelfredzaamheid dan wel opvang of beschermd wonen ….etc.

dat op een later tijdstip te doen? In beide gevallen stel ik (uiteindelijk) de cliënt op de hoogte van de gemaakte afweging(en).

- Documenteren

Ik motiveer en documenteer kort en krachtig mijn besluit en afwegingen in het informatie- en registratiesysteem.