



Gemeente Nieuwegein; burgemeester en wethouders; Privacy Beleid en Privacy Protocol Nieuwegein;

Privacy Beleid en Privacy Protocol gemeente Nieuwegein

Inhoudsopgave

1.	Inleiding/aanleiding	
2.	Reikwijdte	
3.	Juridisch kader	
4.	Uitgangspunten Beleid	
5.	Verwerking van persoonsgegevens	
6.	Gemeentelijk Privacy Beleid	
6.1	Algemeen	
6.2	Welke persoonsgegevens verwerkt de gemeente Nieuwegein?	
6.3	Hoe weet iemand dat de gemeente Nieuwegein persoonsgegevens verwerkt?	
6.4	Hoe lang bewaart de gemeente gegevens?	
6.5	Hoe gaat de gemeente om met privacygevoelige informatie binnen de organisatie?	
6.6	Hoe gaat de gemeente om met privacygevoelige informatie bij handhaving?	
6.7	Wanneer verstrekt de gemeente persoonsgegevens aan een andere afdeling of samenwerkende instantie?	
6.8	Hoe gaat de gemeente om met privacygevoelige informatie in verslagen (ambtelijke overleggen)?	
6.9	Hoe gaat de gemeente om met medische informatie?	
6.10	Hoe gaat de gemeente om met passieve openbaarmaking inzake de Wbp?	
6.11	Hoe gaat de gemeente om met passieve openbaarmaking inzake de WoB?	
6.12	Hoe gaat de gemeente om met actieve openbaarmaking?	
6.13	Hoe gaat de gemeente om met het ter inzage leggen van informatie?	
6.14	Hoe gaat de gemeente om met gedragsregels voor het verwerken van privacygevoelige informatie?	
6.15	Wie houdt toezicht op het naleven van de regels?	
7.	Bronnen	

Privacy Beleid

1. Inleiding/aanleiding

De gemeente Nieuwegein verzamelt en bewerkt persoonsgegevens in verband met de dienstverlening aan burgers en bedrijven. Hierbij kan gedacht worden aan de gegevens in de gemeentelijke basisregistratie, de registratie van bijstandsgerechtigden, het bijhouden van gegevens uit bouwaanvragen en het bijhouden van gegevens van mensen die een Wmo-voorziening hebben toegekend gekregen. De gemeente heeft als uitgangspunt dat zij zorgvuldig omgaat met deze gegevens in verband met de privacy van betrokkenen. Privacy is de bescherming van het privéleven, het recht om met rust gelaten te worden. Privacy regels vragen van gemeenten (en andere overheidsorganen), instellingen en bedrijven om zich niet onnodig te mengen in het persoonlijk leven van burgers.

In de maatschappij is privacy een onderwerp dat veel in de belangstelling staat. Privacy en het delen en openbaar maken van privacygevoelige informatie is dan ook een relevant onderwerp voor de gemeente Nieuwegein. Daarnaast speelt de trend van decentralisatie, waarbij de rijksoverheid steeds meer taken overdraagt aan de gemeentes. De gemeente Nieuwegein werkt in die overdracht samen met een breed scala aan partners in het maatschappelijke veld en deelt daarin, waar dit nodig is voor de uitoefening van de taak, ook persoonsgegevens.

De gemeente weet dus steeds meer over haar burgers en deelt dat functioneel met verschillende partijen. Hiermee wordt het bewaken van de privacy van burgers nog prangerder dan het van nature al was.

2. Reikwijdte

In dit beleid aandacht besteed aan de volgende onderwerpen:
welke gegevens door de gemeente worden verzameld;



o Door de gemeente Nieuwegein worden persoonsgegevens verzameld en bewerkt. Voor de uitvoering van diverse wetten geeft de betreffende wet veelal aan welke persoonsgegevens nodig zijn en dus verwerkt mogen worden.

waarom deze gegevens worden verzameld;

o Gegevens worden verzameld omdat zij nodig zijn ten behoeve van de uitvoering van bepaalde wetten en regelingen. Ook bij handhaving (zowel bestuursrechtelijk als strafrechtelijk) kan het nodig zijn om informatie te vergaren en uit te wisselen.

hoe de gemeente aan deze gegevens komt;

o In het merendeel van de gevallen worden deze gegevens door de betrokkene verstrekt. Soms zijn de gegevens afkomstig van derden, bijvoorbeeld van uitkeringsinstanties.

wat er precies mee gebeurt;

o Wat er precies met de verzamelde gegevens gebeurt, is vooraf afhankelijk van het doel waarvoor ze vergaard worden. Meestal worden ze in een geautomatiseerd systeem opgenomen en zijn ze alleen toegankelijk voor de medewerkers die belast zijn met de uitvoering. Er zijn daarvoor procesbeschrijvingen nodig en er zijn concern brede richtlijnen voor informatiebeveiliging. Voor bij hun werk belangrijke, veel voorkomende processen, kunnen afdelingen een specifieke procedure beschrijven, waarin voor dat proces wordt aangegeven hoe wordt omgegaan met privacygevoelige informatie.

de termijn voor het bewaren van gegevens;

o De bewaartermijnen van de gegevens lopen uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Daar waar er geen wettelijke regeling is die voorziet in een verplichte bewaartermijn, kan het college een besluit over de bewaartermijn nemen.

op welke manier de gegevens worden beveiligd;

o Voor de beveiliging van gegevens is in 2013 onder meer het Strategisch Informatiebeveiligingsbeleid vastgesteld, waarin de kaders en de maatregelen zijn opgenomen. Uitvoering daarvan is belegd in een Informatiebeveiligingsplan.

De beveiliging van de gegevens wordt, zoals ook volgt uit het Strategisch Informatiebeveiligingsbeleid, op verschillende manieren vorm gegeven. Zo zijn er natuurlijk de in de geautomatiseerde systemen ingebouwde beveiligingen (gebruikersnamen, wachtwoorden, doorzoekbaarheidsbeperkingen, autorisatieniveaus en dergelijke), de gedragscodes en protocollen voor de ambtelijke organisatie waarin staat aangegeven hoe om te gaan met privacygevoelige informatie en de fysieke maatregelen die getroffen zijn (toegang tot kantoorruimtes, afsluiten van kasten en dergelijke).

hoe de inwoners hierover worden geïnformeerd.

o Indien inwoners gegevens aan de gemeente Nieuwegein verstrekken worden op de hoogte gesteld van de gegevens die de gemeente nodig heeft.

Dikwijls staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene hoeft niet geïnformeerd te worden als deze al weet dat de gemeente persoonsgegevens van hem verzamelt en verwerkt en weet voor welk doel dat gebeurt. Als de gegevens bij de betrokkene zelf worden verkregen, moet de betrokkene vóór de verkrijging geïnformeerd worden. Meestal zal de informatie op het aanvraagformulier zijn opgenomen, waardoor de betrokkene de informatie dan heeft voordat hij de gegevens verstrekt. Als de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt hij geïnformeerd op het moment dat de gegevens vastgelegd worden of (als de gegevens alleen verzameld worden om deze aan een derde te verstrekken) uiterlijk op het moment van eerste verstrekking aan die derde.

3. Juridisch kader

De Wet bescherming persoonsgegevens (Wbp) regelt het algemene kader voor de omgang met privacy in ons land. Persoonsgegevens, verwerken en betrokkene zijn kernbegrippen uit de Wbp.

Persoonsgegevens:

Ieder gegeven dat is te herleiden tot een individuele persoon, valt onder het begrip persoonsgegeven. Het gaat niet alleen om vertrouwelijke gegevens over bijvoorbeeld iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaalde persoon.

Verwerken:

Dit is in de Wbp het kernbegrip voor alle handelingen die met persoonsgegevens kunnen worden verricht, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander en vernietigen.

Betrokkene:

De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is de degene van wie gegevens worden verwerkt. 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.

Wat is een bijzonder persoonsgegeven?



Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die zo gevoelig zijn dat de verwerking ervan iemands privacy ernstig kan aantasten. Zulke gegevens mogen dan ook alleen onder zeer strenge voorwaarden worden verwerkt. Onder bijzondere of gevoelige persoonsgegevens vallen, bijvoorbeeld, gegevens die iets zeggen over iemands ras, godsdienst, gezondheid, strafrechtelijk verleden of seksuele leven. Ook het burgerservicenummer (BSN) is een bijzonder persoonsgegeven.

Het exporteren van persoonsgegevens: doorgifte Het exporteren van persoonsgegevens, ook wel doorgifte genoemd, is een vorm van verwerking van persoonsgegevens. De gebruikelijke verwerkingsvoorwaarden zijn hierop onverkort van toepassing (voor deze voorwaarden zie: privacywet en persoonsgegevens). Daarnaast zijn er in veel gevallen bijzondere voorwaarden van toepassing op de doorgifte van persoonsgegevens. Hierbij wordt onderscheid gemaakt tussen doorgifte naar een EU-lidstaat en doorgifte naar een land buiten de Europese Unie. Op de export van persoonsgegevens naar een EU-lidstaat zijn geen extra regels van toepassing. Daarentegen is doorgifte naar een land buiten de Europese Unie aan strenge regels onderworpen.

Wat zijn de rechten van betrokkenen?

De Wbp richt zich niet alleen tot degenen die persoonsgegevens verwerken, maar kent ook rechten toe aan personen van wie de gegevens worden verwerkt.

Inzagerecht

Dit recht biedt iedereen de mogelijkheid om te controleren of, en op welke manier, zijn gegevens worden verwerkt.

Correctierecht

Wanneer iemand zijn inzagerecht heeft gebruikt en tot de conclusie komt dat zijn gegevens gecorrigeerd moeten worden, kan hij daartoe een verzoek indienen bij degene die verantwoordelijk is voor de gegevensverwerking.

Recht van verzet

Tegen bepaalde vormen van gegevensverwerking kan de betrokkene zich verzetten, als gevolg waarvan de verwerking van zijn persoonsgegevens mogelijk moet worden gestaakt.

Wie houdt toezicht?

Het College Bescherming Persoonsgegevens (CBP) houdt toezicht op de verwerking van persoonsgegevens. Daarnaast adviseert het CBP de regering met betrekking tot vraagstukken die te maken hebben met de verwerking van persoonsgegevens. Binnen de gemeentelijke organisatie is een Functionaris voor de Gegevensbescherming (FG) aangesteld om toezicht te houden op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp) binnen een organisatie (verwezen wordt naar hoofdstuk 6.15).

Er zijn meerdere wetten die zien op hoe we moeten omgaan met privacygevoelige gegevens. In de zorgsector, specifiek de gezondheidszorg en de jeugdzorg zijn naast de Wbp eigen wetten en regels over privacy van toepassing. Hierbij kan gedacht worden aan:

- de Wet op de Beroepen in de individuele gezondheidszorg (Wet BIG),
- de Wet inzake de geneeskundige behandelingsovereenkomst (Wgbo),
- de Jeugdwet.

Andere privacywetten zijn:

- de Wet basisregistratie personen (Wet BRP) is de nieuwe grondslag voor de basisregistratie van persoonsgegevens en vervangt de Wet gemeentelijke basisadministratie persoonsgegevens (Wet GBA),
- Wet politiegegevens,
- Wet justitiële en strafvorderlijke gegevens,
- Archiefwet (bewaartermijnen).

Uit onder meer de media en uit gegevens van het College Bescherming Persoonsgegevens blijkt dat het verwerken, en dan vooral het niet adequaat verwerken, van persoonsgegevens strijdig met de wet en een bron van ergernis is van burgers en zelfs kan leiden tot onacceptabele situaties, waarbij bijvoorbeeld iemands identiteit wordt 'gestolen' en misbruikt wordt. Juiste toepassing van de wettelijke regels achten wij van belang. Dit beleid en het protocol vormen een nadere uitwerking van de wettelijke regelgeving en een praktische handleiding voor de ambtelijke organisatie. Het college streeft er te allen tijden een zorgvuldige verwerking van persoonsgegevens na.

4. Uitgangspunten Beleid

Het wettelijk kader, zoals beschreven in de vorige paragraaf, is bepalend bij het formuleren van de uitgangspunten van beleid. Dit beleid komt niet in de plaats van al vastgestelde convenanten, privacyreglementen en privacy protocollen, maar moet gezien worden als een nadere formulering van het beleid van de gemeente Nieuwegein. Toekomstige convenanten, reglementen en protocollen



moeten voldoen aan dit privacy beleid. Gegevens worden veelal verzameld omdat zij nodig zijn ten behoeve van de uitvoering van bepaalde wetten of regelingen en worden in de meeste gevallen door de betrokkenen zelf aangeleverd. De zorgvuldigheidseisen die o.a. door de Wet bescherming persoonsgegevens worden bepaald worden daarbij in acht genomen.

Welke rechten burgers hebben als hun gegevens worden verwerkt wordt ook in acht genomen.

Regelmatig worden er ook vragen gesteld over het al of niet mogen verstrekken van persoonlijke gegevens aan derden. Vaak zijn het lastige vragen waarbij het antwoord niet gemakkelijk te geven is. Vragen gaan soms ook over de actieve openbaarmakingsplicht: welke gegevens moeten we uit eigen beweging op internet plaatsen of ter inzage leggen: namen en adressen van aanvragers? Dit nieuwe privacy beleid, waaraan voor de ambtelijke organisatie een protocol wordt gekoppeld, geeft handvatten voor de beantwoording van allerlei vragen op het gebied van privacy. Er wordt onder andere aandacht besteed aan het juridisch kader, aan passieve en actieve openbaarmaking van privacygevoelige informatie, aan persoonsgegevens in het algemeen, aan uitwisseling van gegevens met collega's en andere gemeentelijke diensten en aan medische persoonsgegevens. In het protocol worden ook praktische kwesties behandeld, zoals: mag ik dossiers waarin persoonsgegevens staan op mijn bureau achterlaten als ik ga lunchen?

Het privacy beleid is gestoeld op de volgende beleidsuitgangspunten:

- Binnen de geldende wet- en regelgeving de gegevens van burgers en bedrijven verwerken;
- Op een transparante manier duidelijk maken hoe de gemeente denkt over privacy en hoe de gemeente privacy te allen tijden probeert te borgen;
- Erop toezien dat daar waar sprake is van verwerking van persoonsgegevens werkwijzen worden vastgelegd en op professionele wijze uitgevoerd conform protocollen of procesbeschrijvingen;
- Afhandeling van klachten van burgers en bedrijven over privacy aspecten vindt plaats op een toegankelijke, laagdrempelige wijze;
- In geval van samenwerking met externe partners, specifiek binnen het sociale domein, waar sprake is van verwerking van persoonsgegevens worden afspraken gemaakt over:
 - eisen waar gegevensuitwisselingssystemen aan moeten voldoen;
 - scholing voor betrokkenen binnen de samenwerkingsrelatie over privacy regels.

Er zijn diverse beleidsonderwerpen waar verwerking van persoonsgegevens aan de orde zijn. Zonder uitputtend te willen zijn worden hier de meest in oog springende beleidsvelden genoemd:

- Dienstverlening aan burgers en bedrijven via de stadswinkel,
- Maatschappelijk ondersteuning (uitvoering Wet maatschappelijke ondersteuning 2015),
- Jeugdbeleid (uitvoering Jeugdwet),
- Onderwijsbeleid (inclusief leerlingenvervoer),
- Verzoeken van informatie van burgers en bedrijven (al dan gebaseerd op de Wet openbaarheid van bestuur),
- Omgevingsloket ,
- Inrichting en beheer van de openbare ruimte,
- Economische zaken,
- Openbare orde en veiligheid,
- Handhavingsbeleid,
- Gemeentelijke belastingen,
- Aansprakelijkstellingen,
- Archiefbeleid,
- Gemeentelijk personeelsbeleid.

Voor bij het werk belangrijke, veel voorkomende processen, worden specifieke procedures beschreven, waarin voor dat proces aangegeven hoe wordt omgegaan met privacygevoelige informatie. Die specifieke procedure dient te voldoen aan de uitgangspunten van dit concern brede beleid (en natuurlijk het wettelijk kader zoals beschreven in hoofdstuk 3) . Dergelijke specifieke procedures (werkprocessen) worden ter vaststelling te voorgelegd aan het college.

5. Verwerking van persoonsgegevens

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens. Het gaat er om of er enige feitelijke macht of invloed, al dan niet via een computersysteem, over de gegevens uitgeoefend kan worden. Kan er een handeling met de gegevens verricht worden? De Wbp noemt een aantal handelingen, die als verwerking worden aangeduid:

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



Dit zijn slechts voorbeelden; elke handeling met betrekking tot persoonsgegevens is een verwerking van persoonsgegevens. Ook voor deze verwerkingen geeft het Informatiebeveiligingsbeleid kaders en te nemen maatregelen. Op grond van de Wbp mogen persoonsgegevens alleen *verzameld* worden als daarvoor een **doel** bestaat. Dit doel moet welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn. Ook moet steeds nagaan worden of het verwerken van persoonsgegevens **noodzakelijk** is voor het doel. Dit heet doelbinding. Voor de uitvoering van diverse wetten (denk aan Wet op de ruimtelijke ordening (Wro) en de Wet werk en bijstand (Wwb)) zal in de betreffende wet dikwijls zijn aangegeven welke persoonsgegevens nodig zijn en dus verwerkt mogen worden. Daar waar over verwerking van persoonsgegevens in bijzondere wetgeving niets is geregeld, geldt dus het strikte regime van de Wbp. Verwerking is alleen toegestaan indien het verwerkingsdoel *niet op een andere* (minder belastende) *wijze* kan worden bereikt. Dit heet subsidiariteit. Wanneer is er sprake van verwerking van persoonsgegevens? Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. De wet noemt als voorbeelden van verwerking: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

Uit deze opsomming blijkt dat al gauw sprake is van het verwerken van persoonsgegevens. Je zou kunnen stellen dat alles wat men met een persoonsgegeven doet onder verwerken valt.

Voorwaarden voor verwerking: algemene regels

Hoofregel is dat persoonsgegevens alleen *in overeenstemming met de wet* en op *behoorlijke en zorgvuldige wijze* worden *verwerkt*. Dit noemen we rechtmatigheid.

Daarnaast mogen persoonsgegevens slechts worden verzameld als daarvoor een precieze doelomschrijving wordt gegeven. Bovendien bepaalt de wet dat persoonsgegevens slechts mogen worden verwerkt voor zover zij *toereikend, terzake dienend* en *niet bovenmatig* zijn. Dit noemen we proportionaliteit. De betrokkene heeft ook *recht op informatie* als er persoonsgegevens van hem worden verwerkt. Degene die persoonsgegevens vraagt moet hem onder andere laten weten wie hij is en wat voor gegevens hij waarvoor verwerkt. Dit noemen we transparantie. Een belangrijke verplichting die uit de wet voortvloeit is de *melding* die de verwerker moet doen bij het College Bescherming Persoonsgegevens (CBP), of bij de voor de organisatie benoemde Functionaris voor de Gegevensbescherming. Deze melding is bedoeld om de transparantie te bevorderen: alle bij het CBP gedane meldingen worden opgenomen in een openbaar register.

Sommige verwerkingen hoeven op grond van de wet niet aangemeld te worden, zoals het handelsregister van de Kamer van Koophandel. Daarnaast is in het Vrijstellingsbesluit Wbp een groot aantal verwerkingen opgenomen dat is vrijgesteld van melding. Voor dergelijke vrijgestelde verwerkingen blijven de overige vereisten van de Wbp gewoon van kracht.

Behalve bovengenoemde algemene regels geldt dat er voor elke verwerking van persoonsgegevens een rechtvaardigingsgrond aanwezig moet zijn. Dit wordt hieronder toegelicht.

Voorwaarden voor verwerking: rechtvaardigingsgronden

Naast bovengenoemde algemene regels stelt de wet als eis dat voor elke verwerking van persoonsgegevens ten minste één van de in de wet genoemde rechtvaardigingsgronden van toepassing moet zijn. De wet kent de volgende gronden:

Toestemming

De betrokkene (dit is degene wiens gegevens worden verwerkt) heeft voor de verwerking zijn ondubbelzinnige toestemming gegeven.

Uitvoering overeenkomst

De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is.

Wettelijke verplichting

De gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen.

Vitaal belang

De gegevensverwerking is noodzakelijk om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden.

Publiekrechtelijke taak

De gegevensverwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak.

Gerechtvaardigd belang

De gegevensverwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang van degene die de gegevens verwerkt (of van een derde aan wie de gegevens worden verstrekt). Dit betekent dat degene die de gegevens verwerkt zijn eigen belang moet afwegen tegen het belang en de rechten van de betrokken persoon. Ook moet de verwerker vooraf nagaan of hetzelfde resultaat niet kan worden bereikt met minder gegevens.

6. Gemeentelijk Privacy Beleid



6.1 Algemeen

Privacy is belangrijk. Dat vindt de Gemeente Nieuwegein ook. De gemeente verzamelt en verwerkt veel persoonsgegevens van burgers. Dat schept dus verplichtingen. De gemeente heeft daarom een Privacy Beleid opgesteld. Dit beleid past de gemeente intern toe en ook in samenwerkingsverbanden met andere organisaties. Daarmee weet iedereen waar deze zich aan te houden heeft bij het beschermen van de privacy van burgers. Ook voor de burger is het goed om te weten hoe de gemeente met diens privacy omgaat. Dit beleid is dan ook bedoeld als handvat voor de burger om de gemeente te kunnen volgen en aanspreken op het zorgvuldig omgaan met diens persoonsgegevens.

6.2 Welke persoonsgegevens verwerkt de gemeente Nieuwegein?

De gemeente verwerkt alleen gegevens van en over burgers die strikt noodzakelijk zijn voor het uitvoeren van gemeentelijke taken. De gemeente Nieuwegein verzamelt in het kader van de uitvoering van wet- en regelgeving gegevens die informatie kunnen verschaffen over een identificeerbare persoon. Dat kunnen gegevens zijn die naar hun aard feitelijke informatie over een persoon geven, zoals iemands naam, geboortedatum of geslacht. Ook gegevens over voorwerpen of objecten kunnen persoonsgegevens zijn. Of een dergelijk gegeven een persoonsgegeven is hangt af van de context waarin het gegeven wordt verwerkt. De waarde van een woning is bijvoorbeeld wel een persoonsgegeven wanneer dat gegeven wordt verwerkt in de administratie voor de WOZ-waarde. De persoon waar de gegevens betrekking op hebben moet vervolgens wel identificeerbaar zijn. Is de betrokkene niet identificeerbaar, dan is het gegeven geen persoonsgegeven. Een persoon is identificeerbaar als de identiteit van de persoon redelijkerwijs, zonder onevenredige inspanning vastgesteld kan worden. Als door versleuteling van de gegevens en/of afspraken over de toegang tot die gegevens daadwerkelijke identificatie redelijkerwijs is uitgesloten, is de persoon niet identificeerbaar. Steeds is de feitelijke situatie bepalend. Soms zijn de gegevens afkomstig van derden, bijvoorbeeld van uitkeringsinstanties. De persoonsgegevens betreffen naam, adres, woonplaats en dergelijke, maar soms ook inkomensgegevens, medische gegevens of gegevens over de gezinssamenstelling. De gegevensverwerking moet in overeenstemming zijn met de Wbp. Sommige wetten hebben voorrang op de Wbp en bevatten een aantal specifieke bepalingen over gegevensverwerking. In afdeling 7.5 van boek 7 van het Burgerlijk Wetboek (de overeenkomst betreffende geneeskundige behandeling) is bijvoorbeeld een speciale regeling opgenomen over (onder meer) inzage in medische dossiers.

6.3 Hoe weet iemand dat de gemeente Nieuwegein persoonsgegevens verwerkt?

De gemeente informeert burgers over het opslaan van persoonsgegevens. Indien inwoners gegevens aan de gemeente Nieuwegein verstrekken worden zij door middel van de invulformulieren of andere wijze (bijv. mondeling), dan wel de toelichting daarop op de hoogte gesteld van de gegevens die de gemeente nodig heeft. Dikwijls staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene hoeft niet geïnformeerd te worden als deze al weet dat de gemeente persoonsgegevens van hem verzamelt en verwerkt en weet voor welk doel dat gebeurt. Als de gegevens bij de betrokkene zelf worden verkregen, moet de betrokkene vóór de verkrijging geïnformeerd worden. Meestal zal de informatie op het aanvraagformulier zijn opgenomen, waardoor de betrokkene de informatie dan heeft voordat hij de gegevens verstrekt. Als de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt hij geïnformeerd op het moment dat de gegevens vastgelegd worden of (als de gegevens alleen verzameld worden om deze aan een derde te verstrekken) uiterlijk op het moment van eerste verstrekking aan die derde.

6.4 Hoe lang bewaart de gemeente gegevens?

De gemeente bewaart gegevens volgens de wettelijk geldende termijnen of anders altijd zo kort mogelijk en vernietigt deze daarna. De bewaartermijnen van de gegevens lopen uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Ook de Archiefwet verplicht overheidsorganen, zoals de gemeente Nieuwegein, om gegevens te bewaren en zorg te dragen voor vernietiging van de daarvoor in aanmerking komende documenten als de bewaartermijn verstreken is. Daar waar er geen wettelijke regeling is die voorziet in een verplichte bewaartermijn, kan het college een besluit over de bewaartermijn nemen. Deze zal zo kort mogelijk zijn.

6.5 Hoe gaat de gemeente om met privacygevoelige informatie binnen de organisatie?

De gemeente gaat terughoudend om met informatie van en over burgers. Medewerkers worden daarover geïnstrueerd. De gemeente zal terughoudend omgaan met het verstrekken van persoonsgegevens aan andere organisatieonderdelen, Samenwerkende Instanties of derden. Daarvoor worden in het hierna volgende een aantal aspecten/normen gegeven die als uitgangspunt dienen bij de verwerking van persoonsgegevens:



Medewerkers gaan zorgvuldig om met privacygevoelige informatie. Dat geldt zowel voor informatie op het bureau, in kasten, dossiers, het mee naar huis nemen enz.

Medewerkers treffen waarborgen dat persoonlijke informatie niet ter beschikking komt van derden.

Waar mogelijk wordt gewerkt met geanonimiseerde gegevens; alleen namennoemen indien dat absoluut noodzakelijk is.

Deze uitgangspunten van het privacy beleid sluiten aan bij het Informatiebeveiligingsbeleid.

6.6 Hoe gaat de gemeente om met privacygevoelige informatie bij handhaving?

De gemeente gaat bij handhaving terughoudend om met informatie van en over burgers. Het uitgangspunt is dat terughoudend wordt omgegaan met het verzamelen, delen c.q. verstrekken van informatie. Dat geldt ook voor het geval er bestuursrechtelijke of strafrechtelijke handhaving plaatsvindt, waarbij het nodig is om informatie uit te wisselen en of te verstrekken. De informatie die dan verstrekt wordt moet uiteraard is wel duidelijk dat in dergelijke gevallen door de overheid informatie wordt gebruikt om de bewijsposities te krijgen enz.

Om een voorbeeld te noemen: in het kader van de Wet Werk en Bijstand (artikel 64) is het bijvoorbeeld voor organisaties verplicht om bepaalde informatie te verstrekken. En daarnaast geldt: juist bij ingrijpende maatregelen als handhavingstrajecten is het voor de zorgvuldigheid van belang dat het handhavende bestuursorgaan over alle relevante feiten beschikt.

6.7 Wanneer verstrekt de gemeente persoonsgegevens aan een andere afdeling of samenwerkende instantie?

De gemeente deelt persoonsgegevens intern en extern alleen voor zover dat strikt noodzakelijk is voor de taakuitvoering. Op grond van artikel 9, lid 1 Wbp mogen persoonsgegevens niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Vaak zullen gegevens aan een dienst worden verstrekt voor de uitvoering van een bepaalde wet (denk aan de Wet maatschappelijke ondersteuning (Wmo) of de Jeugdwet). Ze mogen dan alleen voor dat doel gebruikt worden. Bij de uitvoering van deze wetten en gemeentelijk beleid hieromtrent zijn de zorgprofessionals (en vrijwilligers) gehouden aan de wet- en regelgeving die gelden in zorgsector (verwezen wordt naar hoofdstuk 4). Als een andere afdeling of Samenwerkende Instantie vraagt om die gegevens ten behoeve van bijvoorbeeld de uitvoering van een andere wet, slaat die vraag op verwerking van de gegevens voor wellicht een ander - misschien onverenigbaar - doel. De gemeente kan bijvoorbeeld om informatie over mogelijkheden voor minima gericht te kunnen versturen, aan de RSD vragen om persoonsgegevens uit de registratie voor de Wmo. Hier doet zich dan de vraag voor of de Wmo-gerechtigden hun gegevens ook voor het doel 'informerende minima' verstrekt hebben. Als betrokkene ondubbelzinnig toestemming heeft verleend voor de verwerking door de andere dienst (en dat zou gevraagd kunnen worden) dan zouden de gegevens met de andere dienst gedeeld kunnen worden. Als meerdere afdelingen of Samenwerkende Instanties betrokken zijn bij een bepaalde kwestie kan het zijn dat verstrekte persoonsgegevens door die organisaties gedeeld worden. Dat kan ook, omdat in een dergelijk geval sprake is van verenigbare doeleinden.

6.8 Hoe gaat de gemeente om met privacygevoelige informatie in verslagen (ambtelijke) overleggen?

De gemeente zorgt ervoor dat persoonsgegevens niet voorkomen in verslagen. In verslagen van ambtelijke overleggen mogen geen privacygevoelige gegevens opgenomen worden die herleidbaar kunnen zijn tot een persoon. Evenmin is dit toegestaan in verslagen van overleggen waarbij (vertegenwoordigers van) andere instanties betrokken zijn.

6.9 Hoe gaat de gemeente om met medische informatie?

De gemeente deelt medische informatie van burgers alleen met toestemming van de burger. Voor het delen van medische informatie binnen de gemeentelijke organisatie geldt dat dat slechts kan met toestemming van de betrokkene. Is er geen toestemming van de betrokkene of is die toestemming redelijkerwijs niet te verkrijgen, dan kan de medische informatie NIET gedeeld worden met medewerkers van andere gemeentelijke diensten of Samenwerkende Instanties. Een uitzondering bestaat in slechts heel bijzondere gevallen. Zonder toestemming kan medische informatie gedeeld worden in het uitzonderlijke geval van een EVIDENT belang. Van een evident belang is bijvoorbeeld sprake als er ernstig gevaar voor de gezondheid van betrokkene of een ander is of de vrees daarvoor. De hulpverlener moet die afweging maken tussen de verschillende belangen: het belang van de cliënt dat het geheim bewaard blijft tegen het evidente belang. Van een evident belang zal in het geval van gegevensuitwisseling met een niet hulpverlenende instantie niet snel sprake zijn. Als het bij hoge uitzondering vanwege een evident belang onvermijdelijk is om medische informatie te delen, dan moet dat bij voorkeur MONDELING in een zo BEPERKT MOGELIJKE KRING. De informatie mag alleen gedeeld



worden met die persoon werkzaam voor de gemeente Nieuwegein, voor wie het kennisnemen met het oog op het in het geding zijnde evidente belang vereist is.

6.10 Hoe gaat de gemeente om met passieve openbaarmaking inzake Wbp?

De gemeente vertrekt op wettelijk verzoek van burgers de voor die burger geregistreerde gegevens. Iedereen mag vragen of, en zo ja welke persoonsgegevens de gemeente van hem verwerkt. Informatie die verstrekt wordt in het kader van de Wbp is openbaar voor degene aan wie de informatie verstrekt is. Bij Wbp-verzoeken is van belang dat wordt nagegaan dat degene die om informatie vraagt ook degene is over wie de informatie wordt gevraagd. Is de betrokkene jonger dan 16 jaar of onder curatele gesteld, dan moet het verzoek om inzage door de wettelijke vertegenwoordiger worden gedaan. Verwezen wordt naar paragraaf 3.

6.11 Hoe gaat de gemeente om met passieve openbaarmaking inzake WOB?

Als de gemeente gegevens openbaart als gevolg van een wettelijk verzoek, stelt de gemeente alles in het werk om gegevens van burgers te anonimiseren. Informatie die verstrekt kan worden in het kader van de Wob is voor altijd en voor iedereen openbaar. Daar kunnen ook gegevens van burgers bij zitten. De gemeente anonimiseert deze.

6.12 Hoe gaat de gemeente om met actieve openbaarmaking?

Als de gemeente zelf wettelijk gegevens openbaar moet maken, dan wordt aan betrokken burgers eerst om toestemming voor publicatie gevraagd en wordt gegevensverstrekking tot een minimum beperkt. De Wob kent als hoofdregel dat overheidsinformatie openbaar is. In artikel 8, lid 1 Wob is het beginsel van actieve openbaarmaking neergelegd. Dat wil zeggen: het uit eigen beweging verstrekken van informatie door een bestuursorgaan, zoals de gemeente. De plicht tot het verstrekken van informatie ontstaat voor de gemeente zodra dit in het belang is van een goed en democratisch bestuur. Soms geeft ook een bijzondere wet aan, dat informatie openbaar gemaakt moet worden. Er moet altijd een belangenafweging plaats vinden. Op de gemeente rust de plicht om ook bij actieve openbaarmaking een inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer te vermijden, dan wel zo beperkt mogelijk te houden. De Wob geeft immers als weigeringsgrond voor openbaarmaking de bescherming van de persoonlijke levenssfeer. Het is geen absolute weigeringsgrond, maar er moet een belangenafweging plaatsvinden (belang openbaarheid versus belang bescherming persoonlijke levenssfeer).

Indien we privacygevoelige gegevens actief openbaar moeten/willen maken, geldt dat we toestemming van de betrokkenen nodig hebben, of dat er een aantoonbare noodzaak moet zijn voor de openbaarmaking, zoals nakoming van een wettelijke verplichting. Denk bijvoorbeeld aan de plicht die voortvloeit uit de Woningwet, om een register bij te houden van verleendebouwvergunningen.

6.13 Hoe gaat de gemeente om met het ter inzage leggen van informatie?

Als de gemeente gegevens ter inzage legt, dan wordt van betrokken burgers de gegevensverstrekking tot een minimum beperkt. Een manier van openbaar maken van informatie is door het ter inzage te leggen. Bij het ter inzage leggen van stukken dient ook rekening gehouden te worden met de Wbp. Privacygevoelige gegevens die niet openbaar gemaakt moeten worden, dienen ook niet ter inzage gelegd te worden. Dit betekent dat documenten/dossiers die ter inzage liggen geschoond moeten worden op privacygevoelige gegevens. Dit betekent niet dat altijd alle persoonsgegevens onleesbaar moeten worden gemaakt (anonimiseren); soms heeft bijvoorbeeld de vermelding van naam en adres een duidelijke functie, denk aan de aanvraag voor een kapvergunning. Is de aanvraag gedaan door de rechthebbende en om welke boom gaat het precies? Om daar antwoord op te kunnen geven zijn naam van de aanvrager en het adres van het perceel waar de boom staat noodzakelijke gegevens. Ter inzage leggen (openbaar maken) is iets anders dan het recht op inzage op grond van de Wbp. Iedereen mag met redelijke tussenpozen vragen of, en zo ja welke persoonsgegevens ten aanzien van hem verwerkt worden. De informatie is dan alleen openbaar voor de betrokkene zelf (dan wel zijn wettelijke vertegenwoordiger).

6.14 Hoe gaat de gemeente om met gedragsregels voor het verwerken van privacygevoelige informatie?

De gemeente draagt via een intern protocol zorg voor het goed uitvoeren van bovenstaand beleid door medewerkers en Samenwerkende Instanties.

In het hiervoor gestelde is uitleg gegeven over wat privacywetgeving inhoudt en betekent voor de gemeente Nieuwegein. Daarbij is het van belang om te constateren dat privacy lastig is, er moeten diverse afwegingen worden gemaakt. Daarnaast zijn we van mening dat het van belang is om hiervoor



(nieuwe) normen te stellen, en die ook heel duidelijk met de ambtelijke organisatie af te stemmen. Daarvoor is het bijgevoegde protocol opgesteld dat als bindende norm voor de organisatie zal gelden.

6.15 Wie houdt toezicht op het naleven van de regels?

De gemeente voert toezicht uit op het privacy beleid en de uitvoering ervan. Het is van belang om ten aanzien van privacy ook te zorgen dat de normen in het beleid en protocol geëvalueerd worden. Daarom wordt het privacy beleid en de uitvoering ervan jaarlijks geëvalueerd. Dat kan dan leiden tot aanpassing van werkwijzen en/of het protocol. De Gemeente Nieuwegein heeft een Functionaris voor de Gegevensbescherming (FG) benoemd. Deze functionaris heeft tot taak om gemeentelijke zaken die betrekking hebben op privacy te coördineren. Het is uitdrukkelijk niet de bedoeling dat deze functionaris de taken op het gebied van bescherming van de privacy van de afdelingen overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het borgen van het omgaan met privacygevoelige gegevens.

7. Bronnen

Dit privacy beleid is tot gekomen met raadpleging/citering van de volgende bronnen:

Privacy Impact Assessment gemeentelijke 3D informatiehuishouding, Ministerie van Binnenlandse Zaken en Koninkrijksrelatie

De Kleine Gids omgaan met privacy en beroepsgeheim in de jeugdzorg 2011, Kluwer Editie 2011

Justitia.nl Privacy en bescherming persoonsgegevens

Privacy Protocol

Inhoudsopgave

1.	Algemeen	
2.	Regels persoonsgegevens	
3.	Regels medische informatie	
4.	Vastleggen van gegevens	
4.	1 Informeren	
4.	2 Toestemming	
4.	3 Correctie	
4.	4 Verslaglegging	
5.	Wat mag er buiten de organisatie gebracht worden?	
.	5.1 Informatieverstrekking aan de betrokkene op grond van de Wbp	
.	5.2 Passieve openbaarmaking Wbp	
.	5.3 Openbaarmakingsplicht Wob	
.	5.4 Actieve openbaarmaking	
.	5.5 Beroepshalve functioneren	
.	Bijlage 1: Praktijkvoorbeelden	
.	Bijlage 2: Interne gedragsregels	

Privacy Protocol

1. Algemeen

Beleidsuitgangspunt is dat terughoudend wordt omgegaan met het verstrekken van persoonsgegevens aan collega's en aan derden.

Dit protocol geeft geen antwoord op alle voorkomende vragen, maar geeft richtlijnen voor de uitvoeringspraktijk. Daar waar vragen niet op afdelingsniveau beantwoord kunnen worden, neem dan contact op met CJP.

2. Regels persoonsgegevens

1. Privacygevoelige informatie verdient bescherming.
2. Voor bijzondere persoonsgegevens, als ras, godsdienst en over de gezondheid, geldt een weigeringsgrond om ze openbaar te maken.
3. Voor openbaarmaking van overige persoonsgegevens (ook die van medewerkers van de gemeente) moet je een afweging maken tussen het recht op openbaarheid en het recht op bescherming van de persoonlijke levenssfeer.
4. Wees kritisch bij openbaarmaking - zeker bij openbaarmaking via Internet - en anonimiseer indien nodig (geen burgerservicenummer of handtekening openbaar maken).
5. Verstrekken van privacygevoelige informatie aan andere gemeentelijke afdelingen of Samenwerkende Instanties mag alleen als er sprake is van een verenigbaar doel of als betrokkene uitdrukkelijk toestemming heeft gegeven.
6. Neem in verslagen van ambtelijke overleggen en dergelijke geen privacygevoelige gegevens op die herleidbaar kunnen zijn tot een persoon.
7. Zorg ervoor dat de privacygevoelige informatie NIET IN TOT EEN PERSOON HERLEIDBARE VORM in openbare stukken of (afdwingbaar) openbaar te maken stukken terecht komt. In verslagen van (ambtelijke) overleggen vermeld je dus geen privacygevoelige gegevens die terug te leiden zijn



tot een herkenbare persoon. Van de informatieverstrekking zonder toestemming van de betrokkene aan een andere gemeentelijke dienst, maak je aantekening in het dossier van betrokkene.

3. Regels medische informatie
1. Delen medische informatie met andere gemeentelijke afdelingen of Samenwerkende Instanties alleen met toestemming van betrokkene.
2. Geen toestemming, dan geen informatie delen met anderen.
3. Uitzondering voor heel bijzondere gevallen (evident belang).
4. Delen van informatie in geval van evident belang bij voorkeur mondeling, in een zo beperkt mogelijke kring.
5. Vermelding in verslagen en dergelijke in niet tot een persoon herleidbare vorm.
6. Gegevensverstrekking melden in dossier.

Als bijv. een bijstandsgerechtigde bijzondere bijstand aanvraagt voor sociaal-medische zaken, zal de cliënt daartoe medische gegevens overleggen, die vallen onder het begrip bijzondere persoonsgegevens. Het is van het allergrootste belang dat daar zorgvuldig mee wordt omgegaan. In de uitvoering mag je geen informatie over de cliënt dan wel inzage in of afschrift van gegevens uit het dossier aan anderen dan de cliënt verstrekken, zonder dat je daarvoor toestemming hebt verkregen van de cliënt. Ook voor verstrekking van sociaal-medische informatie aan andere afdelingen of Samenwerkende Instanties moet je toestemming hebben van de cliënt.

4. Vastleggen van gegevens
4. 1 Informeren

Je hoeft de betrokkene niet te informeren als deze al weet dat je persoonsgegevens van hem verzamelt en verwerkt en weet voor welk doel je dat doet. Als je de gegevens bij de betrokkene zelf verkrijgt, moet je de betrokkene vóór de verkrijging informeren. Over het algemeen zal uit de informatie die de gemeente verstrekt (brochures, aanvraagformulieren en dergelijke) voor betrokkene duidelijk zijn, dat de gemeente de verstrekte persoonsgegevens verzamelt en bewerkt en voor welk doel. Meestal zal de informatie op het aanvraagformulier zijn opgenomen, waardoor de betrokkene de informatie dan heeft voordat hij de gegevens verstrekt.

Als je de gegevens via een andere weg verkrijgt, dus buiten de betrokkene om, moet je hem informeren op het moment dat je de gegevens vastlegt of (als je de gegevens alleen verzamelt om deze aan een derde te verstrekken) uiterlijk op het moment van eerste verstrekking aan die derde.

Niet in alle gevallen waarin je de gegevens via een andere weg verkrijgt, hoeft je de betrokkene te informeren: dat hoeft bijvoorbeeld niet als informatieverstrekking onmogelijk is, of alleen met een evenredige inspanning kan plaatsvinden. Je hoeft de betrokkene ook niet te informeren als je de gegevens vastlegt of verstrekt op grond van een wettelijke plicht. Voorbeeld van dit laatste: op grond van artikel 64 Wwb is de gemeente gerechtigd informatie te vragen van bijvoorbeeld een uitkeringsinstantie, en die instantie heeft dan de plicht de gevraagde informatie te verstrekken. Die uitkeringsinstantie hoeft daarover de betrokkene dan niet te informeren. Een ander voorbeeld daarvan is het verstrekken van informatie, indien daar in het kader van een strafrechtelijk onderzoek naar wordt gevraagd door een bijzonder opsporingsambtenaar (bijvoorbeeld bij vermeende uitkeringsfraude kan een sociaal rechercheur gegevens opvragen over afvalgegevens).

4.2 Toestemming

Een betrokkene kan toestemming geven om zijn of haar gegevens te verwerken. Zo'n toestemming moet ondubbelzinnig zijn en er moet uit blijken voor welke specifieke verwerkingen deze toestemming geldt. Uit bewijstechnische overwegingen is het verstandig om zo nodig te vragen om schriftelijke (of per e-mail) toestemming te vragen. Ook voor openbaarmaking van persoonlijke gegevens kan een betrokkene toestemming geven. Op het aanvraagformulier voor een omgevingsvergunning wordt hier bijvoorbeeld expliciet naar gevraagd. Hiervoor geldt natuurlijk ook, dat de toestemming ondubbelzinnig moet zijn. Het is dus niet zo, dat 'wie zwijgt stemt toe', maar de toestemming moet boven alle twijfel verheven zijn. Dit geldt zowel voor passieve openbaarmaking als voor actieve openbaarmaking. Een eenmaal gegeven toestemming kan altijd weer worden ingetrokken. Het is daarom goed, zeker bij openbaarmaking via het internet, om een adequate technische procedure in te richten om de informatie weer van internet te kunnen verwijderen.

4.3 Correctie

De betrokkene mag je verzoeken om zijn gegevens te corrigeren. Daarbij moet hij of zij de gewenste wijzigingen aangeven.

Correctie houdt in:

- verbeteren;
- aanvullen;
- verwijderen;
- afschermen; of
- er op een andere manier voor zorgen dat je de onjuiste gegevens niet langer gebruikt.

Je bent alleen verplicht de gegevens te corrigeren als de gegevens:

- feitelijk onjuist zijn;
- onvolledig of niet ter zake dienend zijn voor het doel waarvoor je ze verwerkt; of



- op andere wijze in strijd zijn met een voorschrift van de Wbp of een andere wet zijn verwerkt. Je moet binnen 4 weken schriftelijk aangeven of je aan het correctieverzoek zult voldoen. Als je weigert moet je dat gemotiveerd doen. Het is niet relevant of je een verwijt kan worden gemaakt van de onjuiste verwerking. Als je de gegevens gaat corrigeren moet je dat zo snel mogelijk doen. Als je de gegevens corrigeert moet je derden aan wie je de (onjuiste) gegevens hebt verstrekt, van de correctie op de hoogte stellen. Je moet zelf onderzoeken aan welke anderen je de (onjuiste) gegevens eerder hebt verstrekt. Als het niet mogelijk is om dat na te gaan of als je daarvoor een onevenredige inspanning moet leveren hoeft je die mededeling niet te doen. De onderzoeksplicht gaat natuurlijk verder naarmate de correctie ingrijpender is of de aard van de gegevens daar aanleiding toe geeft.

4.4 Verslaglegging

Ga in overleggen met collega's of andere instanties terughoudend en zorgvuldig om met privacygevoelige gegevens. Indien verslagen worden gemaakt van dergelijke overleggen, zorg er dan voor dat privacygevoelige gegevens niet herleidbaar zijn tot een persoon.

Besluitnota's worden veelal in grote kring verspreid. Het heeft daarom de voorkeur om daar geen volledige namen in op te nemen. Doe dat bijvoorbeeld niet in een voorstel om aan iemand een financiële toelage te verstrekken op humanitaire gronden, gebruik dan initialen. In een nota waarin wordt voorgesteld iemand te benoemen tot lid van een bezwaarschriftcommissie speelt de bescherming van de persoonlijke levenssfeer een minder belangrijke rol dan de openbaarheid. In een dergelijke nota kan de persoon dan bij de volledige naam worden genoemd.

5. Wat mag er buiten de organisatie gebracht worden?

5. 1 Informatieverstrekking aan de betrokkene op grond van de Wbp

Een persoon wiens gegevens worden verwerkt, moet kunnen nagaan wat er met die gegevens gebeurt. De Wbp bevat daarom een regeling over informatieverstrekking aan de betrokkene. Deze regeling maakt op een aantal punten onderscheid tussen de situatie dat je de gegevens bij de betrokkene zelf verkrijgt en de situatie dat je de gegevens op een andere manier verkrijgt.

5.2 Passieve openbaarmaking Wbp

Als de informatie alleen openbaar gemaakt wordt op verzoek van iemand, dan spreken we over passieve openbaarmaking. We maken onderscheid tussen passieve openbaarmaking op grond van de Wob en passieve openbaarmaking op grond van de Wbp.

Over passieve openbaarmaking op grond van de Wbp geeft dit protocol je informatie. Iedereen mag vragen of, en zo ja welke persoonsgegevens de gemeente van hem verwerkt. Alleen als iemand je buitensporig vaak met een dergelijk verzoek benadert, hoeft je daaraan geen gehoor te geven. De term 'buitensporig vaak' is natuurlijk een soort open norm; je moet per geval bekijken of het een onredelijke vraag betreft.

Op een verzoek om inzage moet je binnen 4 weken antwoorden. Het antwoord moet schriftelijk zijn; per mail wordt ook als schriftelijk gezien. Alleen als er een belangrijke reden is om op een andere manier de informatie te geven kan het in een andere vorm, bijvoorbeeld mondeling. Het antwoord moet in een begrijpelijke manier bevatten:

- een volledig overzicht van de door je dienst verwerkte gegevens van de betrokkene;
- een omschrijving van het doel of de doeleinden van de gegevensverwerking;
- een omschrijving van de categorieën van gegevens waarop de verwerking betrekking heeft;
- de ontvanger of categorieën van ontvangers;
- alle beschikbare informatie over de herkomst van de gegevens.

Je moet altijd zeker weten dat degene die om informatie vraagt, ook degene is over wie informatie wordt gevraagd. Als de betrokkene jonger is dan 16 jaar of onder curatele is gesteld, dan moet het verzoek om inzage door de wettelijke vertegenwoordiger (bijvoorbeeld een ouder) worden gedaan. Het antwoord moet je dan ook geven aan die vertegenwoordiger. Om je ervan te vergewissen dat je de juiste persoon voor je hebt, kun je om legitimatie vragen.

Als iemand op grond van de Wob vraagt om gegevens over hemzelf, is het verstandig om de persoon te vragen het verzoek om te zetten in een verzoek op grond van de Wbp, omdat anders de gegevens altijd en voor iedereen openbaar zijn.

5.3 Openbaarmakingsplicht Wob

De Wet openbaarheid van bestuur (Wob) kent als hoofdregel dat overheidsinformatie openbaar is. In artikel 8, lid 1 Wob is het beginsel van actieve openbaarmaking neergelegd. Dat wil zeggen het uit eigen beweging verstrekken van informatie door een bestuursorgaan, zoals de gemeente. De plicht tot het verstrekken van informatie ontstaat voor de gemeente zodra dit in het belang is van een goed en democratisch bestuur.

Soms geeft ook een bijzondere wet aan, dat informatie openbaar gemaakt moet worden, denk aan de publicatie van een bouwvraag op grond van artikel 41 Woningwet. In de Wob zijn uitzonderingen genoemd op de openbaarheid; er zijn weigeringsgronden om informatie openbaar te maken. Dit is bijvoorbeeld het geval als sprake is van bijzondere persoonsgegevens in de zin van paragraaf 2 van hoofdstuk 2 van de Wet bescherming persoonsgegevens (Wbp; bijzondere persoonsgegevens zijn iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging). Het verstrekken van informatie



ingevolge de Wob blijft bijvoorbeeld ook achterwege voor zover het belang daarvan niet opweegt tegen het belang van eerbiediging van de persoonlijke levenssfeer.

Overheidsinformatie kan verschillende persoonsgegevens bevatten. Het verstrekken van die gegevens valt onder de definitie van 'verwerking van persoonsgegevens' uit de Wbp. Op grond van de Wbp mogen persoonsgegevens slechts verwerkt worden als daarvoor een grondslag bestaat. Daarvan is bijvoorbeeld sprake als de verwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke (gemeente) onderworpen is. Actieve openbaarmaking op grond van artikel 41 Woningwet is een dergelijke verplichting. Er kan dus spanning ontstaan tussen het recht op toegang tot overheidsinformatie aan de ene kant en het recht op eerbiediging van de persoonsgegevens aan de andere kant. Hieronder staat hoe je daar als medewerker van deze gemeente mee om kunt gaan, zonder dat daarbij al te veel afbreuk wordt gedaan aan beide rechten.

5.4 Actieve openbaarmaking

Bij het verstrekken van overheidsinformatie in het kader van actieve openbaarmaking vindt er, zoals hierboven ook al vermeld, samenloop plaats tussen de Wob of bijzondere wet en de Wbp, indien die informatie persoonsgegevens bevat. Door die samenloop kan er een spanningsveld ontstaan tussen het recht op toegang tot overheidsinformatie en het recht op bescherming van persoonsgegevens. Bijvoorbeeld in het geval dat de gemeente op grond van artikel 8, lid 1 Wob de plicht tot actieve openbaarmaking heeft, maar het verstrekken van de informatie misschien wel achterwege moet blijven vanwege de eerbiediging van de persoonlijke levenssfeer (artikel 10, lid 1, aanhef en onder e Wob). Vraag is hoe je daar een afweging in maakt.

Bij openbaarmaking op grond van de Wob moet je het volgende in de gaten houden:

- openbaarheid is de hoofdregel;
- als informatie openbaar wordt gemaakt is het voor iedereen openbaar;
- eens openbaar is altijd openbaar.

Voor de betekenis van het recht op eerbiediging van de persoonlijke levenssfeer is van belang of er sprake is van een inmenging in het privéleven van de betrokkene die noodzakelijk is in een democratische samenleving. Het begrip 'privéleven' heeft dezelfde betekenis als 'persoonlijke levenssfeer' en is ruimer dan het begrip 'persoonsgegeven'. Het bevat bijvoorbeeld ook het recht op persoonlijke ontwikkeling en het recht om relaties aan te gaan en te ontwikkelen met andere mensen. Er moet dus altijd een belangenafweging plaats vinden. Op de gemeente rust de plicht om ook bij actieve openbaarmaking een inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer te vermijden, dan wel zo beperkt mogelijk te houden.

Actieve openbaarmaking kan op meerdere manieren plaatsvinden. Je kunt documenten ter inzage leggen, je kunt de informatie bekendmaken door het te publiceren in dagbladen of huis aan huisbladen of je kunt openbaar maken door plaatsing op internet. De Wob schrijft niet voor welk medium je moet gebruiken, alleen dat op een begrijpelijke en toegankelijke wijze openbaar gemaakt wordt.

Internet biedt natuurlijk enorme mogelijkheden om informatie sneller, klantvriendelijker, goedkoper, in grotere hoeveelheden, beter gesorteerd en 24 uur per dag te verstrekken. Aan de andere kant gaat het openbaar maken op internet met grote risico's gepaard. Je moet je dus altijd afvragen of plaatsing van informatie op internet wel de juiste manier is om actief openbaar te maken. Wees vooral zorgvuldig met persoonsgegevens: benut alle bestaande mogelijkheden om inbreuk op de persoonlijke levenssfeer van betrokkene te beperken, bijvoorbeeld door anonimisering van zijn persoonsgegevens: zorg er voor dat je die goed weglakt en daarmee onleesbaar maakt. Denk dan aan naam- en adresgegevens, het burgerservicenummer, en de 'natte' handtekening. Het doel van actieve openbaarmaking, namelijk het belang van openbaarheid, kan in redelijkheid ook bereikt worden door die gegevens weg te lakken. Als je bijvoorbeeld een brief van een burger op internet wilt plaatsen vereist het belang van openbaarheid niet, dat bekend wordt wie die brief heeft geschreven, waar die persoon woont en hoe zijn/haar handtekening er uit ziet. Het burgerservicenummer en de handtekening van een burger of zijn gemachtigde moet je nooit publiceren; overige persoonsgegevens alleen als daarvoor uitdrukkelijk toestemming is verleend.

Let op: ook bij het ter inzage leggen van stukken moet de afweging gemaakt worden of er privacygevoelige gegevens in het document staan, die niet openbaar gemaakt horen te worden. Zo nodig moeten de privacygevoelige gegevens uit het document verwijderd worden.

5.5 Beroepshalve functioneren

Het belang van de eerbiediging van de persoonlijke levenssfeer ziet op alle in de overheidsinformatie genoemde personen, zowel burgers als ambtenaren.

Strikt persoonlijke gegevens van ambtenaren (zoals naam, adresgegevens, privé-bankrekeningnummer en handtekening) verdienen een zelfde mate van bescherming als de persoonsgegevens van niet publieke personen. Functionele gegevens van ambtenaren (zoals doorkiesnummer of e-mailadres) genieten ook een zekere mate van bescherming, maar daarvan zal bij de afweging om deze al dan niet openbaar te maken eerder de conclusie worden getrokken dat het belang van openbaarheid zwaarder weegt dan het belang van eerbiediging van de persoonlijke levenssfeer van de betrokken ambtenaar.

6. Bijlage 1: Praktijkvoorbeelden

Uit de richtsnoeren van het College bescherming persoonsgegevens (CBP) komen de volgende voorbeelden:

1. NAW-gegevens zittingslijsten huurcommissie



In dit geval speelde de vraag of zittingslijsten van een huurcommissie openbaar konden worden gemaakt. De Afdeling rechtspraak van de raad van state (hierna de Afdeling) concludeert dat verstrekking van de naw-gegevens een inbreuk zou maken op de persoonlijke levenssfeer van de betrokken personen. Het recht op bescherming van het privéleven moet daarom voorgaan op het belang van openbaarmaking van die zittingslijsten.

2. Kenteken voertuig

In een geval waarin om openbaarmaking van het kenteken van een voertuig werd gevraagd stelde de Afdeling ook de vraag centraal of de betrokken persoon met het verstrekken van dat gegeven kon worden geïdentificeerd. De Afdeling concludeerde dat openbaarmaking van het kenteken van het voertuig het belang van eerbiediging van de persoonlijke levenssfeer kan schaden nu de identiteit van de bestuurder van dat voertuig achterhaald zou kunnen worden indien het kenteken openbaar zou worden gemaakt.

3. Anonieme briefschrijver

In dit geval ging het om het achterwege laten van openbaarmaking van een met de hand geschreven anonieme tip. Een letterlijke weergave van de inhoud van de anonieme tip werd wel verstrekt. Mede daarom overwoog de Afdeling: Openbaarmaking van de handgeschreven anonieme tip kan het belang van de eerbiediging van de persoonlijke levenssfeer schaden, nu de identiteit van de briefschrijver aan de hand van zijn handschrift achterhaald zou kunnen worden. Veelal kan echter worden volstaan met het weglakken van de persoonsgegevens. Als het belang van de persoonlijke levenssfeer in het geding is, moet je dan ook nagaan of openbaarmaking toch mogelijk is met weglating van gegevens die de persoonlijke levenssfeer kunnen bedreigen dan wel door de openbaarmaking te beperken tot gedeelten van documenten.

4. Schoolgegevens

In dit geval speelde de vraag of aan een vader de adresgegevens van de school waarop zijn dochter in een bepaalde periode had gezeten openbaar gemaakt konden worden. De Afdeling overwoog, dat de omstandigheid dat de verzoeker de vader is van degene over wie hij om informatie vraagt geen rol speelt, omdat ten aanzien van de openbaarheid geen onderscheid wordt gemaakt naar de persoon van de verzoeker. Omdat gevraagd was om openbaarmaking van naam en adres van de school van de dochter, en dus op een gegevens over een geïdentificeerde persoon, betreft dit een persoonsgegeven, waarvan openbaarmaking de persoonlijke levenssfeer aantast.

5. Integriteit van de overheid (belangenverstrengeling ambtenaar

De integriteit van een gemeente was in het spel bij het (volledig) openbaar maken van een rapport over mogelijke belangenverstrengeling van een ambtenaar. De Afdeling kende het belang van openbaarheid om die reden een doorslaggevend gewicht toe. De Afdeling vond dat de ambtenaar wel een belang had bij weglating van zijn naam uit het rapport, maar de Afdeling meent dat het uitgangspunt van de Wob (openbaarheid), en de omstandigheid dat in dit geval de integriteit van het openbaar bestuur in het geding is, waarover in openbaarheid commotie was ontstaan, waarbij ook namen zijn genoemd, van groter belang was. Het was belangrijker het publiek duidelijkheid te verschaffen.

7. Bijlage 2: Interne gedragsregels

Als medewerker van de gemeente ga je de hele dag om met informatie, ook met gevoelige informatie, waaronder persoonsgegevens. Om dat naar behoren te doen, gelden hiervoor de volgende regels. Met deze **tien gouden regels** vatten wij de belangrijkste hiervan samen. Wij verzoeken je deze goed door te lezen omdat zij deel uitmaken van je functie binnen de gemeente.

1. Ken het informatiebeveiligingsbeleid

Het binnen de gemeente geldende Strategische Informatiebeveiligingsbeleid is op iedereen in onze organisatie van toepassing. Raadpleeg hiervoor de Kennissite '**Informatieveiligheid**' op SharePoint.

2. Houd je aan de Gedragscode

In de gedragscode zijn regels neergelegd die aangeven hoe medewerkers van de gemeente behoren om te gaan met de zakelijke ter beschikking gestelde informatie en hulpmiddelen. Tevens bevat de code regels voor de manier waarop interne controle kan plaatsvinden. Deze gedragscode is op Huisnet te vinden (informatiebeveiliging).

3. Houd je wachtwoorden persoonlijk

Je wachtwoorden zijn strikt persoonlijk en dienen uitsluitend door jou gebruikt te worden om toegang te krijgen tot de betreffende systemen. Geef je wachtwoord dus niet aan derden, of aan een collega of je manager, en bewaar ze op een *veilige* plek, dus *niet* in je agenda of op een geel briefje.

4. Houd je aan de geheimhoudingsplicht

Binnen de gemeente wordt veel met persoonsgegevens gewerkt. Voor het werken en de omgang met persoonsgegevens zijn vanuit de overheid regels gesteld, verwoord in de Wet bescherming persoonsgegevens (Wbp), de Wet SUWI en de Wwb. In de CAO zijn daarom geheimhoudingsbepalingen opgenomen die inhouden dat je persoonsgegevens niet verder bekend mag maken dan voor de uitoefening van je functie noodzakelijk is. Dit betreft persoonsgegevens die jou uit hoofde van je functie bekend worden, en ook overige informatie waarvan je weet of redelijkerwijze kunt vermoeden dat deze een vertrouwelijk karakter hebben.

5. Geen gegevensverstrekking aan derden via de telefoon

Het uitgangspunt is dat niet aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen. Dat betekent dat ook geen telefonische informatie over klanten wordt verstrekt aan



personen of instanties die beweren namens de betrokkene te bellen. Vragen moeten schriftelijk bij de gemeente bij de betreffende afdeling worden ingediend. In uitzonderlijke gevallen kan informatie verstrekt worden aan derden, mits de identiteit van deze derde voldoende is vastgesteld (bijvoorbeeld door middel van terugbellen via een centraal telefoonnummer) en een schriftelijk verzoek tot informatie *niet* mogelijk is.

6. Zorg voor Clear desk / clear screen

De vertrouwelijke omgang met persoonsgegevens houdt o.a. in dat elke werkplek zodanig is ingericht, dat onbevoegden niet in jouw afwezigheid aan deze gegevens kunnen komen. Dat betekent dat jij je werkstation bewust dient te vergrendelen met behulp van de screensaver wanneer jij je werkplek verlaat en dat je vertrouwelijke gegevens, zoals dossiers of verslagen, niet onbeheerd op je bureau of in een niet afsluitbare kast achterlaat.

7. Geen vertrouwelijke gegevens in de prullenbak

De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen de gemeente. Ook het vernietigen van deze gegevens moet op een veilige manier plaats vinden. Daarom zijn er speciale gekenmerkte blauwe papiercontainers met brievenbusklep binnen de gemeente aanwezig. Maak gebruik van deze speciale papiercontainers en stop vertrouwelijke gegevens *nooit* in de prullenbak.

8. Spreek onbekende personen in het gebouw aan

Ben je al een keer in de situatie geweest, dat je iemand binnen het gebouw tegenkwam, waar officieel geen publiek zonder begeleiding mag komen en je niet wist wie deze persoon was en wat deze daar te doen had? Spreek deze persoon aan, stel jezelf voor en vraag wat hij of zij hier komt doen. Hiermee worden personen die niet bevoegd zijn om zich op deze plek te bevinden op deze overtreding gewezen, terwijl gasten en nieuw of ingehuurd personeel het doorgaans op prijs stellen om aangesproken te worden en op deze manier contacten te kunnen leggen. Wijs onbevoegden, beleefd maar duidelijk, de weg naar het publieke gedeelte van het gebouw en – belangrijk – begeleid ze daar naartoe.

9. Meld beveiligingsincidenten

Binnen de gemeente is een collega belast met het uitvoeren van activiteiten rond het thema informatiebeveiliging. Je leidinggevende kan je vertellen wie dat is. Het is belangrijk om dit te weten, omdat beveiligingsincidenten zo snel als mogelijk bij deze persoon gemeld dienen te worden. Voorbeelden van incidenten zijn een virusmelding op het systeem, waarmee je op dat moment werkt, een inbraak of een poging tot inbraak, of een deur die op slot had moeten zijn maar niet op slot is.

10. Vermijd haast, stress en werkdruk als het om informatieveiligheid gaat

Informatiebeveiliging krijg je niet gratis – het kost je energie en werkt vaak tegen je als je haast hebt en de werkdruk hoog is. Echter, informatiebeveiliging is uitermate belangrijk voor je werk binnen de gemeente en hoort bij een professionele en bekwame uitvoering van het werk. Neem informatiebeveiliging daarom serieus – je cliënten én je collega's vertrouwen erop.