Gemeente Helmond

GEMEENTEBLAD

Officiële uitgave van de gemeente Helmond

Nr. 325299

9 december

2020

# Besluit van het college van burgemeester en wethouders van de gemeente Helmond houdende regels omtrent privacy

## 1 Inleiding

### 1.1 Belang

Binnen de gemeente Helmond werken we veel met persoonsgegevens van inwoners, medewerkers en zakelijke partners. Voor het uitvoeren van de gemeentelijke wettelijke taken, verzamelen we persoonsgegevens van inwoners. Bij onze medewerkers verzamelen we de gegevens die we nodig hebben als werkgever. Tot slot gebruiken we de persoonsgegevens van contactpersonen van onze zakelijke relaties. Alle betrokkenen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met zijn of haar persoonsgegevens omgaat.

Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy.
Deze beleidsnota stelt het kader en de algemene uitgangspunten voor de verwerking van persoonsgegevens bij gemeente Helmond. Daarnaast geeft de gemeente aan hoe zij concreet voorziet in passende organisatorische en technische maatregelen voor de bescherming van persoonsgegevens.

### 1.2 Doel

Het doel van de nota is om te waarborgen dat de gemeente de privacywetgeving naleeft zodat we persoonsgegevens in overeenstemming met de wet, behoorlijke en zorgvuldig verwerken. Bovendien is het doel om aantoonbaar `in control` te zijn op privacy gebied. Dit is een vereiste van de Algemene Verordening Gegevensbescherming (AVG).

### 1.3 De relatie met de gemeentelijke Missie

Mensen maken de stad en het is de taak van de gemeente om hen daarbij te faciliteren. De gemeente bedenkt niet langer van binnenuit wat goed is voor onze samenleving maar laat de samenleving aan zet en daarbij bieden we daar waar nodig ondersteuning. De klant is daarbij leidend en we benaderen vraagstukken integraal. Dit doen we door een betrouwbare partner te zijn en onze inwoners op een open en respectvolle wijze te benaderen.

Medewerkers werken in een organisatiecultuur die zich kenmerkt door samenwerking, verantwoordelijkheid, prestatiegerichtheid, innovatie en zorgvuldigheid. De werkgever geeft daarin het goede voorbeeld.

Goede bescherming van persoonsgegevens is cruciaal. Onze inwoners, medewerkers en zakelijke partners mogen er daarom op vertrouwen dat wij persoonsgegevens rechtmatig, behoorlijk en op een transparante wijze verwerken. Het college stuurt actief op privacy en beschermt de persoonsgegevens conform de AVG. Bij dilemma's gaan we het gesprek met de betrokkene(n) aan.

Jaarlijks legt het college verantwoording af over de privacy bestendigheid van de gemeentelijke bedrijfsvoering.

## 2. Privacy beleidskader

### 2.1. Inleiding

De gemeente Helmond is zich bewust van haar maatschappelijke verantwoordelijkheid die gepaard gaat met de verwerking van persoonsgegevens. Om deze reden voert gemeente Helmond actief privacy beleid en bewaakt de goede nakoming van wet- en regelgeving op het gebied van Privacybescherming. Het privacybeleid is opgesteld in lijn met de vigerende privacy wet- en regelgeving, op dit moment de Algemene Verordening Gegevensbescherming (AVG)

### 2.2 De uitgangspunten

Alle medewerkers van de gemeente Helmond zijn verantwoordelijk voor het correct omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen.

De algemene uitgangspunten worden door het college vastgesteld in het gemeentelijke privacy beleid. (zie bijlage1). Voor de inwoner is het privacy beleid te raadplegen op internet. Voor alle andere partijen bevat het bindende uitgangspunten voor samenwerking. Het gemeentelijke privacybeleid is uitgewerkt in een privacy reglement. Het reglement bevat een verdieping van het beleid en laat zien hoe de gemeente met privacy en wet, omgaat. Voor de diverse werkterreinen kan het college specifiek uitvoe-

ringsbeleid of specifieke privacy reglementen vaststellen. Denk bijvoorbeeld aan het Sociaal Domein en Veiligheid en Naleving.

De gemeente Helmond zet geheimhoudingsverklaringen en privacy protocollen in om met medewerkers afspraken te maken over hoe zij omgaan met de privacy en bewustwording te creëren.

Wij besteden aandacht aan privacy in afspraken die we maken met partijen. Gemaakte afspraken leggen we vast in samenwerkingsconvenanten en verwerkersovereenkomsten.

Zie de documentenmatrix in bijlage 2 voor een nadere toelichting op de diverse documenten.

### 2.3 Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid heeft raakvlakken met andere beleidsthema's zoals architectuur, integriteit, Inkoop en aanbesteding, arbeid, organisatie en gezondheid en communicatie. Het privacybeleid loopt verder samen met het informatieveiligheidsbeleid. Waar privacybeleid vooral gaat over hoe veilig om te gaan met persoonsgegevens, stelt het informatieveiligheidsbeleid het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen.

## 3. Inbedding in de organisatie

De manier waarop we het privacybeleid binnen de gemeente verankeren, vormt het fundament van de privacy borging. Elke medewerker die omgaat met persoonsgegevens draagt namens gemeente Helmond de verantwoordelijkheid over de verwerking van die gegevens conform de beginselen vanuit de AVG. Onderstaande tabel brengt de verantwoordelijkheden in beeld aan de hand van het RASCI-model (zie onderstaande tabel). Dit beschrijft de rollen en taken van de genoemde functies. Deze paragraaf geeft aan hoe we de taken, verantwoordelijkheden en borging van het privacybeleid binnen de gemeente organiseren.

| Verantwoordelijkheid | Rol | Wie |
|---|---|---|
| R | Responsible/Ambtelijk verantwoordelijk | o De directie<br>o Afdelingsmanager of gemeentesecretaris/algemeen directeur op bedrijfsprocesniveau<br>o Teammanager op deelprocesniveau<br>o projectleider<br>o Alle medewerkers (inclusief inhuur/externen) |
| A | Accountable/ Eindverantwoordelijk | o College van B&W |
| S | Supporting/Uitvoerend | o Afdelingsmanager of algemeen directeur op bedrijfsprocesniveau<br>o Teammanager op deelprocesniveau<br>o Projectleider<br>o Alle medewerkers (inclusief inhuur/ externen) |
| C | Consulted/Adviserend, controlerend | o Functionaris Gegevensbescherming<br>o Decentrale Security en Privacy Officers<br>o IT auditor |
| I | Informed/Geïnformeerd | o Gemeenteraad<br>o Betrokkene(n) |

### 3.1 Het college van B&W en de gemeenteraad

Het college van B&W

- is eindverantwoordelijk voor de naleving van privacywetgeving en voert proactief privacybeleid op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens. In evenwicht dus: behoorlijk, zorgvuldig en in overeenstemming met de wet.

- legt over de privacybeleidsvoering verantwoording af aan de raad en betracht beleidstransparantie met behulp van publieksvoorlichting.
- stelt beleid vast voor de bescherming van de privacy op basis van wet- en regelgeving;
- draagt zorg voor de documentatie van beleid en maatregelen zodat het op ieder moment maatschappelijk en juridisch uitleg kan geven over de deugdelijkheid van de aanpak.
- houdt een register van de gegevensverwerkingen bij die onder hun verantwoordelijkheid plaatsvinden zoals bedoeld in artikel 30 AVG.
- heeft de Functionaris Gegevensbescherming (FG) als toezichthouder conform hoofdstuk IV van de AVG aangewezen.

Privacy (en informatiebeveiliging) valt onder de bestuurlijke verantwoordelijkheid van de portefeuillehouder Informatiebeleid.

De Gemeenteraad
- heeft een toezichthoudende rol op basis van de controlerende taak die de Gemeentewet aan hen toekent.

### 3.2. De directie

a. De directie is ambtelijk verantwoordelijk voor kaderstelling en sturing.

b. zorgt dat de privacy officer naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens;
c. controleert of de getroffen maatregelen voldoende bescherming bieden om de privacy van betrokkenen te beschermen (o.a. door audits).

### 3.3 Management

De afdelingsmanagers en de gemeentesecretaris/algemeen directeur zijn verantwoordelijk voor de bedrijfsprocessen. De teammanagers zijn verantwoordelijk op deelprocesniveau. Tot hun verantwoordelijkheid behoort dat zij het proces zodanig inrichten dat de gemeentelijke taken uitgevoerd worden binnen de grenzen van de privacywetgeving en het beleidskader. De proceseigenaar is operationeel eindverantwoordelijke. Hij is ook verantwoordelijk voor het opstellen van specifiek uitvoeringsbeleid of specifieke privacy reglementen op hun werkterrein. Aan elk proces is één of meerdere Decentrale Security en Privacy Officers (DSPO) toegewezen. De DSPO's ondersteunen de proceseigenaren bij het uitvoeren van de gemeentelijke taken binnen de grenzen van de privacywetgeving en het beleidskader.

### 3.4. Samenwerkingsvormen

In alle afspraken die we maken met andere organisaties maken we afspraken over privacy. De manager is hiervoor verantwoordelijk.

*3.4.1. Verwerkers*

Met organisaties die ten behoeve van ons persoonsgegevens verwerken, waarbij de gemeente Helmond het doel en de middelen van de verwerking vaststelt (zoals een software leverancier), leggen we afspraken vast in een verwerkingsovereenkomst. De gemeente Helmond maakt afspraken door al in de uitvraag bij opdrachten en aanbestedingen aan te geven aan welke randvoorwaarden de verwerking van persoonsgegevens moet voldoen. Dit doet de gemeente door afspraken te maken conform de meest recente versie van de standaardverwerkersovereenkomst van de IBD. De Service manager stuurt hier op.

Ook met partijen, die in mandaat taken namens ons uitvoeren (uitvoeringspartners), leggen wij afspraken vast in een dienstverlenings- c.q. samenwerkingsovereenkomst. Daarnaast worden afspraken over de verwerking van gegevens voor de uitvoering van onze taken vastgelegd in een verwerkersovereenkomst conform de standaardverwerkersovereenkomst van de IBD. De Service manager stuurt hier op.

Verwerkersovereenkomsten worden vastgelegd.

*3.4.2. Ketenpartners*

Daarnaast maken we afspraken met ketenpartners via convenanten/privacyprotocollen. Of en hoe we dat doen is afhankelijk van de positie in de informatieketen en de aard van de samenwerking. In ieder geval wordt aangegeven:
- de betrokken organisaties, verantwoordelijken en relevante doelstellingen;
- of er bijzondere persoonsgegevens worden verwerkt;
- de wijze waarop betrokken inwoners worden geïnformeerd over het gebruik van hun persoonsgegevens;
- de belangrijkste verwerkingen die binnen de samenwerking plaatsvinden;

- de wijze waarop betrokkenen gebruik kunnen maken van hun rechten .

*3.4.3. Openbare ruimte*
In toenemende mate worden er data ingewonnen in de openbare ruimte. Dit heeft mogelijk veel invloed op de maatschappij en data-eigendom wordt steeds belangrijker. Hoewel de exacte rol van de overheid zich nog moet uitkristalliseren, mogen burgers en ondernemers verwachten dat wij duidelijkheid verschaffen over de normen en waarden die hierbij worden gehanteerd en dat daarbij de privacy wordt geborgd. Onze inwoners mogen er op vertrouwen dat we bij de ontwikkeling van onze stad naar een slimme, digitaal-dynamische samenleving steeds rekening houden met vastgestelde principes die ook recht doen aan de privacy van onze burgers.

### 3.5 De Functionaris Gegevensbescherming (FG)
De FG is de onafhankelijk toezichthouder op de naleving van de privacywetgeving van de gemeente Helmond conform de AVG en de Guidelines on Data Protection Officers[1] (Guidelines).
De FG voldoet aan de wettelijke kwalificaties en oefent onafhankelijk zijn taken uit. Hij is verplicht tot geheimhouding en vertrouwelijkheid.

*3.5.1. De taken*
De FG heeft zowel een toezichthoudende als adviserende taak. Door te adviseren en mee te denken over oplossingen bevordert de FG dat de organisatie haar verantwoordelijkheid neemt om rechtmatig persoonsgegevens te verwerken en deze gegevens te beschermen. De FG geeft zelf geen invulling aan de maatregelen in het kader van de privacywetgeving, aangezien dit haar onafhankelijkheid in gevaar zou brengen. Daarnaast bewaakt de FG de naleving van de privacyregels door onafhankelijk onderzoek te doen.

*3.5.2. Ondersteuning*
De organisatie ondersteunt de FG, hij krijgt voldoende middelen voor het vervullen van de taken en heeft toegang tot persoonsgegevens en verwerkingen. Management en college betrekken de FG dan ook tijdig bij verwerkingen van persoonsgegevens. Bovendien heeft de FG de bevoegdheid om ruimten te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen, conform artikel 5.2. van de Algemene Wet Bestuursrecht (AWB).

*3.5.3. Onafhankelijkheid*
De FG kan vrij en onafhankelijk zijn advies uitbrengen. De FG heeft een autonome rol en ontvangt geen instructies over de behandeling van een zaak, of wordt op andere wijze beïnvloed. De FG geeft geen bindend advies, maar zijn advies is wel zwaarwegend. Hem wordt de gelegenheid geboden om een (eventuele) afwijkende mening duidelijk te maken aan het college en er wordt vastgelegd waarom een advies niet wordt opgevolgd. De FG kan rechtstreeks aan het college rapporteren. Bovendien krijgt de FG geen andere taken of plichten opgelegd die kunnen leiden tot een belangenconflict.

De FG doet jaarlijks verslag van zijn werkzaamheden. De raad wordt via de planning en control cyclus geïnformeerd.

*3.5.4. Toegang*
We zorgen er voor dat betrokkenen (zowel binnen als buiten de organisatie) en de AP gemakkelijk, direct en vertrouwelijk contact op kunnen nemen met de FG. Daarom worden de contactgegevens van de FG bekend gemaakt.

### 3.6 Decentrale Security & Privacy Officer (DSPO)
De DSPO ondersteunt de afdelingsmanager bij het beheer, de coördinatie en het advies ten aanzien van de informatieveiligheid en privacy voor zijn/ haar bedrijfsproces. De DSPO is het eerste aanspreekpunt voor de afdelingsmanager, de CISO en de FG en ambassadeur voor informatieveiligheid en privacy binnen dit bedrijfsproces.

De DSPO's zijn binnen de gemeente degenen die kaders stellen op het gebied van domein specifieke informatiebeveiliging en beveiligingsbewustzijn. De DSPO bevordert draagvlak bij het management en medewerkers. Tevens monitort de DSPO of de informatiebeveiliging conform de kaders uitgevoerd wordt. Hij is direct betrokken bij de implementatie hiervan in de lijn en kent de processen en relevante wetgeving. Hij zorgt daarmee dat de organisatie specifieke informatiebeveiliging doorvoert in haar processen, conform wet- en regelgeving.

1 ) *van de European Data Protection Board (EDPB), het onafhankelijke Europese orgaan voor gegevensbescherming*

Verder richt de DSPO zich op de uitvoer en naleving van de (domein specifieke) privacywetgeving. De DSPO stelt - wanneer nodig - een data protection impact assessment (DPIA) op en adviseert bij het gebruik van persoonsgegevens. De DSPO toetst bij gegevensaanvragen op doelbinding, rechtmatigheid, proportionaliteit en andere aspecten vanuit de AVG en aanvullende privacywetgeving. De DSPO rapporteert periodiek over de informatieveiligheid/privacy aan de afdelingsmanager, CISO en FG.

## 4. Maatregelen

### 4.1 Doelstelling

Met de maatregelen beschreven in dit hoofdstuk kunnen de doelstellingen van het privacybeleid worden gehaald en de risico's worden beperkt.

### 4.2 Maatregelen

Onderstaande maatregelen zijn getroffen om persoonsgegevens rechtmatig, behoorlijk en transparant te kunnen verwerken, volgens geldende wet- en regelgeving.

*4.2.1 Transparantie*

Betrokkene(n) krijgen vooraf duidelijke informatie via de dienstverlening (telefonisch, schriftelijk, email) over de verwerking van hun persoonsgegevens en het doel van de verwerking.
In de privacyverklaring op de website van de gemeente Helmond wordt aangegeven hoe de gemeente Helmond omgaat met de verwerking van persoonsgegevens.

*4.2.2 Naleving van het informatiebeveiligingsbeleid*

Naast een FG beschikt de gemeente Helmond over een gekwalificeerde coördinerende informatiebeveiliger (CISO). Zij hebben samen een strategisch informatieveiligheidsbeleid 2020-2024, een tactisch informatiebeveiligingsbeleid en een privacy- en informatiebeveiligingsplan opgesteld. Op beleidsstukken en plannen zijn maatregelen getroffen om de bescherming en veilige verwerking van persoonsgegevens te waarborgen.

*4.2.3 Bewustwording en communicatie*

Bewustwording is essentieel voor het borgen van privacy in de organisatie. Het is belangrijk dat iedereen die werkt met privacygevoelige informatie zich bewust is van het belang om hier zorgvuldig mee om te gaan. Doorlopend wordt er aandacht geschonken aan de bewustwording, via intranet, presentaties en opleidingsaanbod in de Helmond Academie. Daarbij is ook aandacht voor privacy-incidenten, incident management en crisiscommunicatie. Dit beleidsdocument licht in lijn met en sluit aan bij het (nog vast te stellen) communicatieplan bewustwording informatiebeveiliging en privacy Gemeente Helmond 2020-2021.

*4.2.4 Verwerkingenregister*

Een register houdt alle verwerkingsactiviteiten van persoonsgegevens per proces bij. Hierin worden onder andere de doeleinden van de verwerking, categorieën van betrokkene(n) en persoonsgegevens, derden ontvangers, bewaartermijn en technische en organisatorische (beveiligings)maatregelen opgenomen.

*4.2.5 Het melden van datalekken*

Er is een procedure voor het melden van incidenten informatieveiligheid. Deze procedure ziet ook toe op het melden van datalekken. Er wordt een register bijgehouden van gemelde incidenten.

*4.2.6 Risicomanagement*

Voor (nieuwe en veranderende) processen, diensten en producten en informatiesystemen wordt een risicoanalyse (RIA) uitgevoerd. Hiervoor is een handreiking risicomanagement opgesteld. Het vaststellen van risico's leidt tot processen waarbij de informatieveiligheid is geborgd. In het geval persoonsgegevens worden verwerkt bij processen, diensten, producten en informatiesystemen, wordt naast een RIA ook een DPIA uitgevoerd. Binnen een DPIA wordt expliciet aandacht besteed aan het veilig verwerken van persoonsgegevens en de te nemen maatregelen (privacy by design).

*4.2.7 Toezicht en rapportage*

Vragen, klachten en het incident management toetsen steekproefsgewijs het privacybeleid. Het is belangrijk om periodiek te controleren of beleid en de dagelijkse praktijk overeenkomen.
Samen met de FG bepaalt concern control periodiek of een privacy audit wordt uitgevoerd in aanvulling op het toezicht door de FG. Dit laat onverlet dat concern control hier ook een eigen bevoegdheid heeft.

Jaarlijks legt het college verantwoording af aan de raad waar het gaat over de risico's en beheersmaatregelen met betrekking tot het privacy-beleid.

## 5 Communicatie en evaluatie van dit beleid

Na vaststelling van dit beleid door het college wordt dit beleid gepubliceerd en via het lijnmanagement gecommuniceerd met medewerkers en relevante externe partijen. Verdere communicatie momenten zijn uitgewerkt in het informatiebeveiligings en privacyplan.

Het privacybeleid geldt voor een periode van 5 jaar en wordt met een frequentie van 5 jaar geëvalueerd of eerder bij belangrijke wijzigingen. De geldigheid van het privacybeleid loopt synchroon met het strategisch informatiebeveiligingsbeleid 2020 – 2024.

*Aldus besloten in de vergadering van het college van burgemeester en wethouders van gemeente Helmond van 10 november 2020*

*Burgemeester en wethouders van Helmond*

*mevrouw P.J.M.G. Blanksma-van den Heuvel*
*de burgemeester*

*de heer E. de Ruiter*
*de secretaris*

## Bijlage 1

Privacy beleid gemeente Helmond

Persoonsgegevens zijn privé, en ieders privacy is belangrijk. Dat onderschrijft gemeente Helmond. De gemeente verzamelt en verwerkt veel persoonsgegevens. Om inzicht te geven hoe we hiermee omgaan is een privacy beleid opgesteld. Dit biedt ook een kader voor onszelf en voor organisaties waarmee we samen werken. Zo is het bij iedereen duidelijk hoe we omgaan met de privacy van onze inwoners, medewerkers en zakelijke contacten. Dit beleid is dan ook bedoeld als handvat zodat iedere betrokkene de gemeente Helmond kan aanspreken op het zorgvuldig omgaan met zijn of haar persoonsgegevens.

Wettelijke kaders voor de omgang met gegevens
De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor geldt de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (uAVG) als wettelijk kader.

Uitgangspunten
De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente houdt zich aan de volgende uitgangspunten:

*Welke persoonsgegevens verwerkt de gemeente Helmond?*

- Wij gebruiken alleen gegevens van en over inwoners die noodzakelijk zijn voor de uitvoering van gemeentelijke taken. U kunt bijvoorbeeld denken aan een inwoner die ons om hulp vraagt bij het oplossen van zijn schulden. We hebben zijn financiële gegevens nodig om hem goed te kunnen helpen.
- Wij gebruiken alleen gegevens van en over onze medewerkers die noodzakelijk zijn voor de uitvoering van onze taken als werkgever. Voor de salarisadministratie hebben wij gegevens nodig van onze medewerkers, zodat het salaris op tijd wordt betaald en wij aan onze belasting- verplichtingen kunnen voldoen.
- Van onze zakelijke relaties gebruiken we alleen de persoonlijke gegevens die nodig zijn om contact te kunnen onderhouden. Van bijvoorbeeld een medewerker van een andere gemeente leggen we een telefoonnummer en e-mail adres vast, zodat wij contact met hem kunnen opnemen om te overleggen.

*Dit betekent dat:*

- Wij persoonsgegevens in overeenstemming met de wet op een behoorlijke en zorgvuldige wijze verwerken.
- Wij persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen gebruiken.
- Wij persoonsgegevens alleen met een rechtmatige grondslag verwerken.
- Wij terughoudend om gaan met persoonsgegevens en maatwerk leveren.
- Wij streven naar een minimale gegevensverwerking. Waar mogelijk gebruiken wij minder of geen persoonsgegevens.
- Wij geen gegevens verzamelen, gebruiken of bewaren met als (enkele) reden dat het nu of later “handig” kan zijn.
- Wij ons altijd afvragen wat zwaarder weegt: het belang dat wij hebben voor het gebruiken van de gegevens of het recht op privacy van betrokkene. Daarbij zorgen wij er voor dat de inbreuk op de privacy van de betrokkene zoveel mogelijk wordt beperkt.

Hoe weet ik dat de gemeente Helmond mijn persoonsgegevens verwerkt?

- Wij informeren betrokkenen over het gebruik van persoonsgegevens

*Dit betekent dat:*

- Wij betrokkene vooraf in eenvoudige en duidelijk taal informeren dat en waarom wij zijn of haar persoonsgegevens gebruiken.
- Wij, alleen wanneer het niet anders kan, een betrokkene niet vooraf maar achteraf informeren. Dat kan bijvoorbeeld het geval zijn bij handhaving.

Hoe lang bewaart de gemeente Helmond persoonsgegevens?

- Wij bewaren gegevens zo kort als mogelijk en vernietigen ze daarna. Het bewaren van gegevens kan nodig zijn om onze taken goed uit te kunnen oefenen. Wij houden ons aan onze wettelijke verplichtingen.

Hoe gaan de medewerkers van gemeente Helmond om met privacygevoelige informatie?

- Wij gaan terughoudend om met informatie. Wij zorgen er bovendien voor dat persoonsgegevens correct en actueel zijn.

Dit betekent dat:

- Wij zorgvuldig omgaan met persoonsgegevens en ze vertrouwelijk behandelen.
- Persoonsgegevens alleen worden verwerkt door medewerkers met een geheimhoudingsplicht.
- Wij voor passende beveiliging van persoonsgegevens zorgen. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

Verstrekt de gemeente mijn persoonsgegevens aan een ander?

- Wij delen persoonsgegevens intern en extern alleen voor zover dat strikt noodzakelijk is voor de uitvoering van wettelijke taken. U kunt bijvoorbeeld denken aan de situatie waar een inwoner een rolstoel nodig heeft. De leverancier van de rolstoel krijgt in dat geval de gegevens die nodig zijn om de juiste rolstoel te leveren.

Dit betekent dat:

- Wij vooraf afspraken maken over de eisen waar de gegevensuitwisseling aan moet voldoen.
- Deze afspraken voldoen aan de wet.
- De gemeente deze afspraken controleert.

Dit privacybeleid treedt in werking na vaststelling door het college van burgemeesters en wethouders. Het beleid wordt iedere vijf jaar geëvalueerd en indien nodig herzien.

## Bijlage 2. Documentenmatrix

### Documenten

1. In een *Privacy Beleid* staat wat de uitgangspunten inzake privacy zijn voor de gemeente. Dat moet kort, simpel en transparant verwoord zijn. Het is een publiek document (Internet/Intranet) dat voor een breed publiek toegankelijk moet zijn. Het beleid is intern en extern van toepassing. Voor inwoners is het een statement, voor alle andere partijen bevat het bindende uitgangspunten voor samenwerking.
2. In een *Convenant* wordt contractueel omschreven hoe wat het doel van de overeenkomst is en wordt naar het Privacy Reglement verwezen naar welke regels er gelden m.b.t. de informatiebeveiliging en in het verlengde daarvan de privacy.
3. In een *Privacy Reglement* staat verwoord wat de regels inzake privacy zijn waar partijen zich aan moeten houden. Dat is een nadere uitwerking van het Privacy Beleid, concreet dus. Het is een verdieping van het beleid en laat zien hoe de gemeente met privacy, en vooral de wet, omgaat. Dat wordt strikt verwoord en heeft de status van Openbaar Reglement.
4. In een *Verwerkersovereenkomst* wordt contractueel omschreven hoe een externe partij met de bewerking van privacygevoelige informatie om moet gaan, wat het doel van de overeenkomst is en welke regels er gelden m.b.t. de informatiebeveiliging en in het verlengde daarvan de privacy.
5. In een *Geheimhoudingsverklaring* wordt contractueel omschreven waar een persoon aan gehouden is m.b.t. geheimhouding en privacy. Het is de gepersonaliseerde versie van een reglement.
6. In een *Privacy Protocol* staan de gedragsregels voor personen die omgaan met privacygevoelige informatie. Als het Privacy Reglement of Convenant het 'Wat' omschrijft, dan gaat een protocol over 'Hoe'.

### Partijen (collectief) en Individuen

A. Een *Externe* die onder direct gezag van de gemeente intern werkzaamheden verricht, zal als onderdeel van het contract met hem/haar of diens werkgever een individuele Geheimhoudingsverklaring moeten ondertekenen. Daarbij wordt verwezen naar het Privacy Beleid (Internet/Intranet).
B. Een *Medewerker* die onder direct gezag van de gemeente werkzaamheden verricht, legt de ambtseed af. Binnen de gemeentelijke cao zijn de sancties vermeld die betrekking hebben op het schenden van de ambtseed. Dat dekt het formele aspect van geheimhouding. Daarnaast wordt verwezen naar het Privacy Beleid (Internet/Intranet).
C. Een *Inwoner* zoekt naar houvast en transparantie over hoe de gemeente met informatiebeveiliging en diens privacy omgaat. Dat staat helder verwoord in het Informatiebeveiliging en Privacy Beleid. Ook wil hij weten wat de regels zijn, vooral die hem aangaan over inlichten, bezwaren en klachten. Hier voorziet het Privacy Reglement in.
D. Een *Ketenpartner* trekt samen met de gemeente op in uitvoering van taken. Dat betekent dat deze zoveel mogelijk gefaciliteerd moeten worden en dat de gemeente een extra verantwoordelijkheid heeft in het afdwingen van regels en protocollen op grond van haar eigen expertise en verantwoordelijk.
E. Een Verwerker is een professionele partij die ten behoeve van de gemeente taken uitoefent en daarbij persoonsgegevens verwerkt. Hiertoe sluiten partijen een contract af, waarbij de informatieveiligheid en privacy voorzieningen die de Verwerker treft in de Verwerkersovereenkomst benoemd worden.

Wanneer dit wordt weergegeven in een matrix ziet dit er als volgt uit (zie volgende pagina):

| Documenten Matrix privacy | | | | | | |
|---|---|---|---|---|---|---|
| | | INTERN | | EXTERN | | |
| DOCUMENTEN | | A<br>Externe | B<br>Medewerker | C<br>Inwoner | D<br>Ketenpartner | F<br>Verwerker |
| Collectief | ① Privacybeleid | ① | ① | ① | ① | ① |
| | ② Convenant | | | | ② | |
| | ③ Privacyreglement | | | ③ | ③ | |
| | ④ Verwerkersovereenkomst | | | | | ④ |
| Individueel | ⑤ Geheimhoudingsverklaring | ⑤ | ⑤ | | ⑤ | |
| | ⑥ Privacyprotocol | ⑥ | ⑥ | | ⑥ | |