Gemeente Helmond

GEMEENTEBLAD

Officiële uitgave van de gemeente Helmond

Nr. 168572

6 augustus 2018

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

Het college van burgemeester en wethouders
Collegevoorstel 33620496

B e s l u i t

Vast te stellen het Privacbeleid Gemeente Helmond

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 vanaf 25 mei 2018 aantoonbaar `in control` te zijn op privacy gebied. Dit is een vereiste van de Algemene Verordening Gegevensbescherming (AVG), die dan in werking treedt.

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.

Vanaf 25 mei 2018 kan het college verantwoording afleggen over de privacy bestendigheid van de gemeentelijke bedrijfsvoering.

2. Privacy beleidskader

2.1. Inleiding

De gemeente Helmond is zich bewust van onze de 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 heeft betrekking op de Wet bescherming persoonsgegevens (Wbp) en (vanaf 25 mei 2018) 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 uitvoeringsbeleid 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 convenanten 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, maar ook de Basisregistratie Personen (BRP). Het Privacybeleid loopt verder samen met het informatieveiligheidsbeleid. Waar privacybeleid vooral gaat over hoe om te gaan met persoonsgegevens, stelt het informatieveiligheidsbeleid het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen.

De BRP kent een eigen wettelijk en beleidskader dat een goede omgang met de gegevens in deze basisregistratie borgt. De Wbp (en AVG) zijn hier niet op van toepassing. Dit privacybeleid en het wettelijk en beleidskader BRP sluiten op elkaar aan.

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 o Afdelingsmanager of algemeen directeur op bedrijfsprocesniveau o Teammanager op deelprocesniveau o projectleider o Alle medewerkers (inclusief inhuur/externen)
A	Accountable/ Eindverantwoordelijk	o College
S	Supporting/Uitvoerend	o Afdelingsmanager of algemeen directeur op bedrijfsprocesniveau o Teammanager op deelprocesniveau o projectleider

		o Alle medewerkers (inclusief inhuur/externen)
C	Consulted/Adviserend, controlerend	o Privacy officer o IT auditor
I	Informed/Geïnformeerd	o Gemeenteraad 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 privacy officer als toezichthouder conform hoofdstuk IV van de AVG aangewezen.

Privacy 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

De directie is ambtelijk verantwoordelijk voor kaderstelling en sturing. Het kernteam is het directieteam met betrekking tot informatievraagstukken.

3.2.1. De directie:

a. stuurt op concernrisico's;
b. zorgt dat de privacy officer naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens:
c. beoordeelt periodiek het privacybeleid op basis van de evaluatie en aanpassingen van het privacybeleid.
d.

3.2. 2. Het kernteam:

a. stuurt op informatiseringsniveau;
b. controleert of de getroffen maatregelen voldoende bescherming bieden om de privacy van betrokkenen te beschermen (o.a. door audits), dit mede in relatie tot informatiseringsvraagstukken.

3.3 Management

De afdelingsmanagers/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. Zij zijn operationeel eindverantwoordelijke. Zij zijn ook verantwoordelijk voor het opstellen van specifiek uitvoeringsbeleid of specifieke privacy reglementen op hun werkterrein.

3.5. Samenwerkingsvormen

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

3.5.1. Verwerkers

Met organisaties die namens ons persoonsgegevens verwerken (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 dienstverleningsovereenkomst. 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 in Verseon vastgelegd.

3.5.2. Ketenpartners
Daarnaast maken we afspraken met ketenpartners via convenanten. 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

3.5.3. 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.

3.6 de privacy officer
De privacy officer is de onafhankelijk toezichthouder op de naleving van de privacywetgeving van de gemeente Helmond conform Hoofdstuk IV 4 van de AVG[1] en de Guidelines on Data Protection Officers[2] (Guidelines).
De privacy officer voldoet aan de wettelijke kwalificaties en oefent onafhankelijk zijn taken uit. Hij is verplicht tot geheimhouding en vertrouwelijkheid.

3.6.1. De taken
De privacy officer heeft zowel een toezichthoudende als adviserende taak. Door mee te denken over oplossingen houdt hij preventief toezicht. Op die manier hoeft de organisatie niet achteraf gecorrigeerd te worden, wat inefficiënt zou zijn.

De privacy officer:
- draagt bij aan het informatiebeveiligingsbeleid en is verantwoordelijk voor het ontwikkelen van normen en interne regelingen ten aanzien van privacy;
- adviseert het MT/college over de werking van het privacybeleid en nakoming van achterliggende wettelijke verplichtingen;
- adviseert het MT/college bij privacy incidenten over ernst en omvang;
- ziet toe op het documenteren, melden en meedelen van inbreuken in verband met persoonsgegevens aan betrokkenen en de toezichthoudende autoriteit;
- Verzamelt en registreert informatie ten aanzien van privacy incidenten;
- adviseert managers over het voor hun werkterreinen specifiek op te stellen uitvoeringsbeleid of specifieke privacy reglementen;
- adviseert projectleiders/ ontwerpers over te treffen maatregelen ter voorkoming van privacy schendingen (privacy by design);
- adviseert over Privacy Impact Analyses, dit advies heeft betrekking op:

1) *De wet spreekt van een dataprotection officer en in de Nederlandse vertaling wordt gesproken over een functionaris voor de gegevensbescherming. In Helmond is gekozen voor de term privacy officer.*
2) *van de Artikel 29-werkgroep van Europese privacytoezichthouders*

  - of er al of niet een PIA uitgevoerd moet worden;
  - welke methodiek voor de PIA gebruikt moet worden;
  - of de PIA intern uitgevoerd of uitbesteed moet worden;
  - welke waarborgen (zoals technische en organisatorische maatregelen) ingebouwd moeten worden om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
  - of de PIA correct uitgevoerd is en de conclusies daaruit (de vraag of de verwerking door moet gaan en welke waarborgen er ingebouwd moeten worden om aan de wet te voldoen);
- fungeert als contactpersoon met de toezichthoudende autoriteit en ziet toe op de opvolging van verzoeken van de toezichthoudende autoriteit;
- fungeert als contactpersoon voor personen die gebruik willen maken van hun privacyrechten;
- helpt privacy klachten tot een goed einde te brengen (privacy-ombudsman);
- onderhoudt een inventarisatie van gegevensverwerkingen van persoonsgegevens (het verwerkingenregister conform artikel 30 AVG);
- verzorgt voorlichting en opleidingen aan gegevensverwerkers van persoonsgegevens;
- houdt toezicht op de nakoming van privacybeleid en relevante privacywetgeving;
- plant en bewaakt onderzoeken naar de bescherming van persoonsgegevens, in samenwerking met concern-control en eventuele externe auditors.

3.6.2. Ondersteuning
De organisatie ondersteunt de privacy officer. Hij krijgt voldoende middelen voor het vervullen van de taken en heeft toegang tot persoonsgegevens en verwerkingen. Management en college betrekken de privacy officer dan ook tijdig bij verwerkingen van persoonsgegevens. Bovendien heeft de privacy officer de bevoegdheid om ruimten te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen, conform artikel 5.2. van de Algemene wet bestuursrecht.

3.6.3. Onafhankelijkheid
De privacy officer kan vrij en onafhankelijk advies uitbrengen. Hij heeft een autonome rol en ontvangt geen instructies over de behandeling van een zaak, of wordt op andere wijze beïnvloed. De privacy officer kan geen bindend advies geven, 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 privacy officer kan rechtstreeks aan het college rapporteren. Bovendien krijgt de privacy officer geen andere taken of plichten opgelegd die kunnen leiden tot een belangenconflict.

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

3.6.4. Toegang
We zorgen er voor dat betrokkenen (zowel binnen als buiten de organisatie) en de Autoriteit Persoonsgegevensgemakkelijk, direct en vertrouwelijk contact met de Privacy officer op kunnen nemen. We zorgen er daarom voor dat de contactgegevens van de privacy officer bekend worden gemaakt.

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 website en de dienstverlening (telefonisch, schriftelijk, email) over de verwerking van hun persoonsgegevens en het doel van de verwerking.

4.2.2 Naleving van het informatiebeveiligingsbeleid
Gemeente Helmond beschikt over een gekwalificeerde coördinerende informatiebeveiliger (CISO) en een informatieveiligheidsbeleid. Op basis van dit beleid zijn maatregelen getroffen om de bescherming van persoonsgegevens te waarborgen.

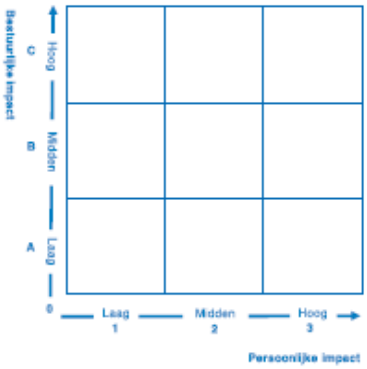
4.2.3 Bewustwording en communicatie

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.

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 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. We oefenen op privacy-incidenten, incident management en crisiscommunicatie.

4.2.6 Privacy Impact Analyses (PIA's) en Privacy by design en default
Voor (nieuwe en veranderende) processen, diensten en producten en informatiesystemen, waar persoonsgegevens worden verwerkt, worden PIA's uitgevoerd. Binnen het procesmanagement en de methodiek van procesoptimalisatie in Helmond wordt daarom expliciet aandacht besteedt aan het rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens en de maatregelen die hiervoor noodzakelijk zijn (privacy by design). Hierbij wordt gebruik gemaakt van Privacy impact assessments (PIA's)[3]. PIA-scores worden bepaald aan de hand van de hiernaast afgebeelde matrix. Hoe hoger de PIA-score, hoe robuuster de beheersmaatregelen teneinde de privacy te waarborgen.



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 privacy officer bepaalt concern control periodiek of een privacy audit wordt uitgevoerd in aanvulling op het toezicht door de privacy-officer. Dit laat onverlet dat concern control hier ook een eigen bevoegdheid heeft.

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

3) De term die in artikel 35 van de AVG wordt gebruikt

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 Wet Bescherming Persoonsgegevens (Wbp) als wettelijk kader. Vanaf 25 mei 2018 is er een nieuw wettelijk kader: de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming

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.
- Wij persoonsgegevens alleen met een rechtvaardige 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

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 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 namens de gemeente taken uitoefent en daarbij gegevens verwerkt of op een andere manier gegevens 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:

Documenten Matrix privacy						
		INTERN		EXTERN		
	DOCUMENTEN	A Externe	B Medewerker	C Inwoner	D Ketenpartner	F Verwerker
Collectief	① Privacybeleid	①	①	①	①	①
	② Convenant				②	
	③ Privacyreglement			③	③	
	④ Verwerkersovereenkomst					④
Indiv.	⑤ Geheimhoudingsverklaring	⑤			⑤	
	⑥ Privacyprotocol	⑥	⑥		⑥	

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.

Aldus vastgesteld door burgemeester en wethouders van gemeente Helmond op: 19 december 2017

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

mr. drs. A.P.M. ter Voert
de secretaris